बैंक ऑफ़ बड़ौदा
Bank of Baroda
विजया VIJAYA | देना DENA

बैंकिंग में साइबर अपराध

बैंक ऑफ़ बड़ौदा द्वारा "बैंकिंग में साइबर अपराध" विषय पर आयोजित सेमिनार में प्रस्तुत आलेखों का संकलन

बैंकिंग में साइबर अपराध

Cyber Crime in Banking

बैंक ऑफ़ बड़ौदा
Bank of Baroda
विजया VIJAYA | देना DENA

राजभाषा विभाग
प्रधान कार्यालय, बड़ौदा

राजभाषा विभाग
प्रधान कार्यालय
"बड़ौदा भवन"
पांचवा तल
आर सी दत्त रोड,
अलकापुरी, बड़ौदा - 390007
फोन : 0265-2316580/81
ई-मेल: rajbhasha.ho@bankofbaroda.co.in

प्रथम संस्करण
सन् 2023

संपादन कार्य :

पुनीत कुमार मिश्र, सहायक महाप्रबंधक
अम्ब्रेश रंजन कुमार, मुख्य प्रबंधक
प्रमोद बर्मन, वरिष्ठ प्रबंधक

डिजाइनिंग एवं लेआउट :

हिमानी पटेल, व्यवसाय सहयोगी

प्रस्तावना

पिछले कुछ वर्षों में वैश्विक स्तर पर वर्चुअल दुनिया का हस्तक्षेप बहुत ही तेजी से बढ़ा है। इस नई दुनिया ने मानव समाज के जीवन से जुड़ी कई आवश्यक प्रक्रियाओं को आसान बनाया है। वर्चुअल वर्ल्ड एक तरह से हम सभी के लिए एक एक्स्टेंडेड वर्ल्ड है यह असीमित, आभासी और तकनीक-आधारित है। वर्चुअल वर्ल्ड को साइबर वर्ल्ड के नाम से भी जाना जाता है और इस असीमित दुनिया में घटित हो रही गतिविधियों को दुरूस्त रखने के लिए साइबर सुरक्षा और कानून का सहारा लिया जाता है। आज व्यवसाय जगत सहित अन्य क्षेत्रों की गतिविधियां तकनीक-आधारित हो गई हैं। जहां तक बैंकिंग और अन्य वित्तीय उद्योग का सवाल है तो इस क्षेत्र के भविष्य को डिजिटल रूप में ही देखा जा रहा है। आज भी बैंकिंग, बीमा और अन्य वित्तीय संस्थानों का स्वरूप पारंपरिक कम और डिजिटल रूप में अधिक हो गया है।

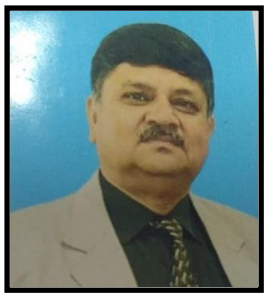
बैंक ऑफ़ बड़ौदा पिछले 8 वर्षों से लगातार विभिन्न समसामयिक बैंकिंग विषयों पर हिंदी भाषा में अखिल भारतीय सेमिनार का आयोजन करता रहा है। मौजूदा बैंकिंग के स्वरूप को देखते हुए ही हमने पिछले वर्ष बैंकिंग में साइबर अपराध विषय पर हिंदी में अखिल भारतीय सेमिनार का आयोजन किया था। सेमिनार के विषय के दो उप-विषय थे – (i) *डिजिटल ऋण: चुनौतियां एवं संभावनाएं* और (ii) *डिजिटल ऋण: जोखिम एवं विनियामक आवश्यकताएं*। दोनों ही उप-विषयों पर बैंक को 100 से भी अधिक गुणवत्तापूर्ण आलेख प्राप्त हुए। इन आलेखों में से श्रेष्ठतम आलेख प्रस्तुतकर्ताओं को सेमिनार में प्रस्तुति तथा चर्चा के लिए आमंत्रित किया गया। सेमिनार हेतु प्राप्त आलेखों को हमने एक अभिलेख के रूप इस संकलन को तैयार किया है।

हम जानते हैं कि तकनीक की उन्नत सुविधाओं की उपलब्धता ने इसके दुरूपयोग की संभावनाओं को भी बढ़ाया है। तकनीक के दुरूपयोग के कारण ही साइबर अपराध जैसी समस्याएं सामने आ रही हैं। हमारे लिए यह जरूरी है कि हम तकनीक के दुरूपयोग के अलग-अलग माध्यमों और इनसे बचाव के उपायों को भी समझें। इस प्रकार से हम दैनिक बैंकिंग गतिविधियों में भी साइबर अपराध जैसी घटनाओं से बच सकते हैं। इस डिजिटल पुस्तिका में बैंकिंग में साइबर अपराध के प्रत्येक पहलुओं पर विस्तार से चर्चा की गई है। मुझे विश्वास है कि यह पुस्तिका बैंकिंग, वित्तीय एवं बीमा संस्थानों में कार्यरत स्टाफ सदस्यों को साइबर अपराध के सभी पक्षों से अवगत कराने में सक्षम होगी। अंत में मैं सभी लेखकों का आभार प्रकट करता हूं जिन्होंने सेमिनार हेतु अपनी प्रविष्टियां भेजीं और उनके सहयोग से हम यह प्रकाशन तैयार करने में सक्षम हुए हैं।

शुभकामनाओं सहित,

(संजय सिंह)
प्रमुख - राजभाषा एवं संसदीय समिति

बैंकिंग में साइबर अपराध



अवनीश कुमार गुप्ता

पदनाम:- वरिष्ठ शाखा प्रबंधक
संस्था का नाम:- केनरा बैंक
मोबाइल नं. :- 6353026231
ई-मेल:- avkrgupta@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

बैंकों में धोखाधड़ी की समस्या आज के वित्तीय क्षेत्र में उभरते हुए तमाम जोखिमों में सबसे वृहद है। पिछले पांच वित्तीय वर्षों के दौरान वित्तीय धोखाधड़ी की मात्रा और इसमें शामिल राशि दोनों में काफी बढ़ोत्तरी हुई है। इस अवधि के दौरान धोखाधड़ी की मात्रा में 19.6 प्रतिशत की वृद्धि हुई है। साइबर अपराधों का आलम ये है कि यदि बैंकों की प्रणालियों और प्रक्रियाओं में कमियां पाई जाती हैं तो असामाजिक तत्व उनका दुरुपयोग बैंक व उनके ग्राहकों के अहित में करेंगे। (संदर्भ : राष्ट्रीय अपराध रिकॉर्ड ब्यूरो)

आरबीआई निर्देश :

भारतीय रिज़र्व बैंक के अनुसार, धोखाधड़ी के जोखिम प्रबंधन, निगरानी और जांच कार्य की अंतिम जिम्मेदारी बैंक के मुख्य कार्यकारी अधिकारी, बोर्ड की लेखा परीक्षा समिति और बोर्ड की विशेष समिति की है। जहां बोर्ड की लेखा परीक्षा समिति सामान्यत: धोखाधड़ियों के सभी मामलों की निगरानी करेगी, वहीं रुपए एक करोड़ वा अधिक के धोखाधड़ी मामलों की निगरानी वा अनुवर्ती कार्रवाई के लिए बैंकों को बोर्ड की विशेष समिति (SCBF) का गठन करना है।

रिज़र्व बैंक ऑफ इंडिया को धोखाधड़ी की रिपोर्टिंग :

बैंकों को किसी भी धनराशि के मामले में धोखाधड़ी पकड़े जाने के 3 सप्ताह के भीतर प्रत्येक धोखाधड़ी मामले की रिपोर्ट, फ्रॉड मॉनिटरिंग रिटर्न (एफ एम आर) के द्वारा आरबीआई को इलेक्ट्रॉनिक माध्यम से भेजनी होती है।

बैंकों में साइबर अपराधों हेतु जोखिम प्रबंधन के उपाय :

बैंकों का कार्यक्षेत्र अत्यंत व्यापक है। ऐसा कोई भी कार्यक्षेत्र नहीं है जिसमें धोखाधड़ी की संभावना न हो। अत: बैंकों को अपने हर कार्य क्षेत्र में धोखाधड़ी रोकने के व्यापक इंतजाम करने होंगे।

निवारक नियंत्रण/ निवारक सतर्कता :

निवारक सतर्कता से तात्पर्य प्रणालियों एवं प्रक्रियाओं के सहज संचालन और उनकी प्रभावोत्पादकता को बनाए रखने के लिए धोखाधड़ी होने से पहले किए गए प्रयत्नों से है। किसी दुर्घटना के घट जाने पर जो नुकसान होता है वह दुर्घटना की रोकथाम के लिए किए गए प्रयत्नों पर किए गए खर्च से कई गुना अधिक होता है।

बैंकों द्वारा निम्नलिखित क्षेत्रों में अपेक्षित प्राथमिक निवारण उपाय किए जाने चाहिए।

1. सही भर्ती
2. उचित प्रशिक्षण
3. मजबूत प्रणालियां और प्रक्रियाएं
4. सर्वव्यापी सतर्कता

यह सर्वविदित है कि विकास के साथ-साथ विध्वंसक प्रवृत्तियां भी जन्म लेने लगती हैं, वास्तव में बैंकिंग जगत में साइबर क्राइम इसी की देन है। साइबर क्राइम बहुत खतरनाक एवं नुकसानदायक है क्योंकि यह पैसे से जुड़ा है।

कोई भी ऐसा कार्य जो कंप्यूटर, इंटरनेट पर अवैधानिक तरीके से किया गया है एवं जिसमे बैंक, संस्था अथवा ग्राहक की राशि का कपटपूर्ण आहरण, दुरुपयोग अथवा हानि शामिल है, वह साइबर क्राइम कहलाता है, इसमें निम्नलिखित क्राइम शामिल हैं:

1 कंप्यूटर वायरस
2 इंटरनेट पायरेसी
3 हैकिंग
4 डिडलिंग डेटा तथा इंटरनेट टाइम चोरी
5 लॉजिक बम या ई-मेल बॉम्बिंग/डिनाइल ऑफ सर्विसेज अटैक

साइबर अपराध और जोखिम :

साइबर क्रांति ने बैंकों को सुविधाएं तो प्रदान की हैं लेकिन जोखिम को भी बढ़ाया है। इंटरनेट पर खतरे तेजी से बढ़ रहें हैं और इंटरनेट इस्तेमाल करने वालों को अरबों का नुकसान हो रहा है। पिछले साल के मुकाबले इस साल, कंप्यूटर में वायरस के हमले कई गुना बढ़ गए हैं। इंटरनेट पर लोगों को अक्सर ई-मेल के जरिए बेवकूफ बनाया जाता है। प्रौद्योगिकी के साथ कार्य करते हुए हम अक्सर निम्नलिखित जोखिमों को अपने सामने पाते हैं:

1. स्विफ्ट संदेश प्रणाली का दुरुपयोग
2. एटीएम /डेबिट कार्ड का गलत उपयोग
3. वैयक्तिक सूचनाओं का चोरी होना
4. रेनसमवेयर हमला
5. बैंक के सर्वर में अनधिकृत सेंधमारी
6. फर्जी ई-मेल /फिशिंग मामले
7. फर्जी और लालच देने वाली कॉल
8. वेंडर और सॉफ्टवेयर कंपनियों पर अधिक निर्भरता
9. तकनीकी क्षेत्र के लिए प्रशिक्षण की कमी
10. नई तकनीक के प्रति ग्राहकों की उदासीनता
11. छोटे व्यापारियों द्वारा डिजिटल सुविधाओं में रुचि न लेना
12. सूचना एवं तकनीक से संबंधित उपयोगी प्रचार वा सुरक्षा मैनुअल का अभाव
13. क्रेडिट कार्ड का समय पर भुगतान न होना

साइबर धोखाधड़ी करने के विविध तरीकों में फिशिंग, विशिंग, शोल्डर सर्फिंग, पासवर्ड चुराना, हैकिंग आदि आते हैं जिनसे प्रणाली की जटिल सुरक्षा व्यवस्थाओं तथा उनके एंक्रिप्शन, फायरवॉल आदि को भेदकर बैंक या उसके ग्राहकों के साथ छल किया जाता है।

साइबर अपराध के प्रकार:

1 हैकिंग:

इसके अंतर्गत साइबर अपराधी कंप्यूटर/मोबाइल नेटवर्क में प्रवेश कर निजी जानकारी जैसे नेट बैंकिंग पासवर्ड, क्रेडिट कार्ड या डेबिट कार्ड की जानकारी चुरा लेता है।

2 फिशिंग :

इसमें साइबर अपराधी फर्जी ई-मेल के द्वारा जानकारी चुराते हैं।

3 विशिंग:

इसमें फर्जी कॉल द्वारा ग्राहक से एटीएम कार्ड नंबर, पिन, पासवर्ड आदि चुराकर उनका दुरुपयोग किया जाता है।

4 वायरस अटैक:

साइबर अपराधी कुछ ऐसे सॉफ्टवेयर कंप्यूटर/नेटवर्क पर भेजते हैं जिससे उनकी कार्य क्षमता प्रभावित होती है।

साइबर सुरक्षा हेतु हम निम्नलिखित उपाय कर सकते हैं:

1. कर्मचारियों में यह विश्वास होना चाहिए कि यदि वे किसी धोखाधड़ी या होने वाली धोखाधड़ी का पर्दाफाश करेंगे तो उन्हें इसके कारण कोई नुकसान नहीं होगा बल्कि पुरस्कृत किया जाएगा, सम्मान दिया जाएगा।
2. अपने ग्राहक को जानिए (Know Your Customer) के अंतर्गत बैंक द्वारा अपने सभी ग्राहकों का केवाईसी कड़ाई से पूरा किया जाना चाहिए, इसके लिए उनसे प्राप्त आधिकारिक वैध दस्तावेज (OVD) की सघन जांच हो ताकि फर्जी केवाईसी दस्तावेज के माध्यम से कोई व्यक्ति बैंक के साथ धोखाधड़ी न कर पाए।
3. यह आवश्यक है कि ग्राहक की गोपनीय जानकारी और बैंकों के साथ उपलब्ध अन्य डेटा /जानकारी पर्याप्त रूप से सुरक्षित रखी जाए ताकि यह सुनिश्चित हो सके कि धोखेबाज इस डेटा या जानकारी को चुराकर दुरुपयोग न कर सकें।
4. नए धोखाधड़ी के प्रकारों पर कानून प्रवर्तन एजेंसियों के बीच बैंक द्वारा जागरूकता पैदा करनी चाहिए। बैंक, पुलिस और गृह मंत्रालयों के अधिकारियों को धोखाधड़ी से संबंधित चुनौतियों और सुझावों पर चर्चा करने करने के लिए नियमित रूप से बैठकों का आयोजन करना चाहिए।
5. बैंकों द्वारा दिए गए पीओएस टर्मिनलों पर स्किम्ड/चोरी किए गए कार्ड का इस्तेमाल करने वाले व्यापारियों के खिलाफ कार्रवाई करनी चाहिए।
6. सिर्फ बैंकों पर ही नही बल्कि संपूर्ण कॉर्पोरेट जगत पर **रैनसमवेयर** (Ransomware) के रूप में नया खतरा आया है। मई 2017 में आततायियों ने **वाना क्राई** (WannaCry) नाम का **रैनसमवेयर** बना लिया था जिसके बलबूते कई बड़ी कंपनियों के कंप्यूटरों को हैक कर लिया गया था तथा उन कंपनियों से क्रिप्टो करेंसी के रूप में पैसा मांगा गया था।
7. धोखाधड़ी जोखिम प्रबंधन हेतु वित्तीय फोरेंसिक जांच के क्षेत्र में कर्मचारियों का कौशल बढ़ाने के लिए आईबीए के तत्वावधान में बैंकों द्वारा एक प्रशिक्षण संस्थान स्थापित किया जा सकता है। संकाय और सामग्री बैंकों और अन्य विशेषज्ञों द्वारा उपलब्ध कराई जा सकती है।

बैंकिंग जगत में साइबर क्राइम से बचने के अन्य सुरक्षात्मक उपाय:

1. साइबर क्राइम से बचने के लिए उपभोक्ताओं को शिक्षित एवं जागरूक बनाना चाहिए, इसके लिए बैंक द्वारा समय-समय पर पैम्फलेट का वितरण, शाखाओं में वीडियो के माध्यम से ग्राहकों को जानकारी देना आदि शामिल हैं।
2. यूजर्स को नेटबैंकिंग पासवर्ड को ई-मेल पासवर्ड और दूसरे लॉगिन आई डी पासवर्ड से मिलता जुलता नहीं बनाना चाहिए।

3. कंप्यूटरों पर वर्चुअल की बोर्ड का उपयोग करते समय यह ध्यान रखें कि कोई व्यक्ति आई डी पासवर्ड का उपयोग करते समय आपकी ***की*** को देख तो नहीं रहा है अथवा मोबाइल से उसकी वीडियो तो नही बना रहा है।
4. साइबर सुरक्षा में ***फायरवॉल*** की महत्वपूर्ण भूमिका होती है। फायरवॉल वह शक्तिशाली तकनीक है जिसमें जब किसी मैसेज को नेटवर्क के माध्यम से भेजा जाता है तब वह पहले फायरवॉल से गुजरता है तथा फायरवॉल उन्हीं मैसेज को प्राप्तकर्ता को भेजता है, जो निर्धारित मानदंडों पर खरे उतरते हैं। विंडोज ऑपरेटिंग सिस्टम में फायरवॉल ऑन रहना चाहिए ताकि वह साइबर क्राइम से बचा सके और कंप्यूटर को सुरक्षित रख सके।
5. जिस प्रकार आज विभिन्न कार्यालयों और बैंकों में कर्मचारियों के कार्य करने के लिए बायोमेट्रिक व्यवस्था है, यही व्यवस्था ग्राहकों के हस्ताक्षरों के स्थान पर भी होनी चाहिए क्योंकि ज्यादातर जालसाजियां जाली हस्ताक्षरों को लेकर होती हैं। इससे ऑनलाइन बैंकिंग निगरानी सिस्टम और मजबूत होगा।
6. कार्ड लेन-देन के संबंध में अनिवार्य रूप से एसएमएस अलर्ट भेजना भी एक कारगर कदम हो सकता है।
7. ग्राहकों को साफ तौर पर आगाह किया जाए कि यदि उनके पास भारतीय रिज़र्व बैंक, बीमा नियामक आदि का फोन आए तो वे तुरंत चौकस हो जाएं कि उन्हें जालसाजी का शिकार बनाया जा रहा है क्योंकि ये संस्थान कभी किसी ग्राहक को फोन नही करते।
8. बैंकों की शाखाओं और केंद्रीय मुख्यालयों में साइबर सेल खोले जाएं जो ग्राहकों की शिकायतों पर तुरंत कार्रवाई करें।
9. एडवांस्ड एनालिटिक्स और मशीन लर्निंग पर बल दिया जाए।
10. साइबर अपराधों की जानकारी रिज़र्व बैंक और पुलिस को यथाशीघ्र दें।

यदि बैंक डिलीवरी सिस्टम से जुड़े तकनीकी जोखिमों का प्रबंधन करने में अक्षम रहते हैं तो न केवल ग्राहकों का उनमें बना विश्वास टूटता है बल्कि उनकी ओर से मुकदमेबाजी बढ़ सकती है। इतना ही नहीं, रेगुलेटर यानी भारतीय रिज़र्व बैंक से भर्त्सना और भारी जुर्माना भी झेलना पड़ सकता है। इसके लिए हमें टेक्नोलॉजी वेंडरों के साथ गहन ताल मेल बनाकर रखना होगा तथा टेलीकॉम सेवा प्रदाताओं के संपर्क में रहना होगा। सर्वोत्तम होगा कि भारत सरकार साइबर सुरक्षा को राष्ट्रीय सुरक्षा का अविभाज्य अंग बना दे। इसके अलावा, हम निम्नलिखित बातों पर भी जागरूक रहकर साइबर सुरक्षा कर सकते हैं:

1. कभी भी अपने कंप्यूटर को स्विच्ड ऑन की स्थिति में न रखें।
2. यदि **रैनसमवेयर अटैक** का संदेह है तो प्रभावित कंप्यूटर को भी सीबीएस नेटवर्क से अलग कर दें।
3. फाइल्स का नियमित बैकअप लेते रहें तथा उन्हें सुरक्षित ऑफसाइट रखें।
4. एंटीवायरस को अद्यतन करते रहें तथा कंप्यूटर में परिचालन पद्धति के पैचेज अद्यतन करते रहें।
5. ई-मेल संदेशों के आधार पर राशि का अंतरण न करें जब तक किन्ही अन्य माध्यमों से उसकी पुष्टि न कर लें।
6. लेजिटिमेट तथा फेक ई-मेल एड्रेसेज में बहुत थोड़ा अंतर होता है उसका अवश्य पता करना चाहिए।
7. फिशिंग सेल के द्वारा भेजे गए लिंक पर कभी क्लिक न करें।
8. एटीएम सुरक्षा हेतु स्पष्ट इमेज के लिए सीसीटीवी फुटेज की जांच करते रहें तथा फुटेज को सबूत के उद्देश्य से सुरक्षित करते रहें।
9. तकनीक इंजीनियर की पहचान सत्यापित करने के पश्चात ही एटीएम मेंटेनेंस के लिए अनुमति दें।

10. जब तक एटीएम मेंटेनेंस का कार्य नही हो जाता तथा मशीन सही ढंग से लॉक नही कर दी जाती, वहीं पर खड़े रहकर इंजीनियर के काम को देखते रहें।
11. एटीएम के लिए बिल्कुल नई पैन ड्राइव का प्रयोग करें तथा इस पैन ड्राइव का प्रयोग इंटरनेट पीसी पर न करें। एटीएम पर पैन ड्राइव को प्रयोग करने से पहले किसी सीबीएस नोड पर पैन ड्राइव की स्क्रीनिंग अवश्य कर लें।
12. अपना पासवर्ड, सीवीवी, ओटीपी, कार्ड नंबर आदि किसी से भी शेयर न करें।
13. शाखाओं के फोन नंबर तथा पतों का ब्यौरा बैंक की वेबसाइट से प्राप्त करें, गूगल या सर्च इंजन से कभी भी प्राप्त करने की कोशिश न करें।

दंडात्मक सुझाव : पुलिस/सीबीआई को धोखाधड़ी की रिपोर्टिंग :

धोखाधड़ी /गड़बड़ी के मामलों से निपटने में, बैंकों की प्राथमिकता नुकसान होने वाली राशि को वसूल करने में होने से अधिक दोषी व्यक्तियों को सजा दिलवाने की होनी चाहिए। वास्तव में ये सार्वजनिक हित से प्रेरित होना चाहिए क्योंकि धोखाधड़ी सिर्फ एक व्यक्ति या संस्था के साथ ही नहीं बल्कि समाज और देश के साथ भी है। धोखेबाज को सजा होने पर अन्य लोगों को ऐसा अनुकरण न करने के लिए प्रेरणा मिलती है। भारतीय रिज़र्व बैंक के दिशानिर्देशों के अनुसार, रू. 10000/* से अधिक राशि के सभी धोखाधड़ी मामलों को राज्य पुलिस/ एमएफआईओ/ ईओडब्ल्यू/ सीबीआई को नियमानुसार सौंप दिया जाना चाहिए।

धोखाधड़ी की रोकथाम करने वाले कर्मचारियों को पुरस्कृत करना:

कर्मचारियों को धोखाधड़ी की गतिविधि की रिपोर्ट करने के लिए प्रोत्साहित किया जाना चाहिए। इसके लिए उन्हें समुचित रूप से पुरस्कृत किया जाना चाहिए। बैंकों में स्पष्ट पर्दाफाश नीति यानी व्हिसलब्लोअर पॉलिसी होनी चाहिए। इस नीति के प्रति कर्मचारियों में विश्वास जगाना चाहिए। कर्मचारियों को यह विश्वास होना चाहिए कि यदि वे किसी धोखाधड़ी या होने वाली धोखाधड़ी का पर्दाफाश करेंगे तो उन्हें इसके कारण कोई नुकसान नहीं होगा बल्कि पुरस्कृत किया जाएगा, सम्मान दिया जाएगा।

अंत में **एलेन ग्रीन स्पेन** के शब्दों में:

धोखाधड़ी, गबन, भ्रष्टाचार हर जगह मौजूद है, खेद है कि यह मानव जाति की स्वभावगत कमजोरी है। किसी भी सफल अर्थव्यवस्था को बस इतना जरूर करना चाहिए कि वह इन्हें कम से कम रखे।

*****

अमित मोहन अस्थाना

पदनाम:- संकाय सदस्य

संस्था का नाम:- पंजाब एण्ड सिंध बैंक

मोबाइल नं. :- 7071301570

ई-मेल:- stc.rohini@pab.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

आज का दौर संचार क्रांति का दौर है। उदारीकरण के बाद वैश्विक ग्राम के चिंतन को काफी बल मिला, परंतु सच्चे अर्थों में वैश्विक ग्राम की परिकल्पना संचार क्रांति के बाद ही संभव हुई है। संचार क्रांति के बाद वास्तविक दुनिया के साथ-साथ एक आभासी दुनिया विकसित होने लगी है। जिसे हम साइबर स्पेस कहते हैं। आज विश्व का शायद ही कोई इंसान होगा जिसकी इस साइबर स्पेस में अपनी कोई पहचान नहीं होगी। किसी न किसी तरीके से आज हम सभी इस साइबर वर्ल्ड का हिस्सा बन चुके हैं। हमारी व्यक्तिगत जानकारी, आर्थिक जानकारी, गोपनीय जानकारी सभी प्रकार की जानकारी साइबर स्पेस में है। इसलिए साइबर स्पेस में कदम रखने से पूर्व हमें फूक-फूंककर कदम रखने की जरूरत है।

यहां हम बैंकों में बैंकिंग में साइबर अपराधों के स्वरूप एवं सुरक्षात्मक उपाय पर विशेष रूप से चर्चा कर रहे हैं। साइबर सुरक्षा के दो पहलू हैं। पहला मनोवैज्ञानिक पहलू और दूसरा तकनीकी पहलू। दोनों पहलू साइबर सुरक्षा के लिए काफी महत्वपूर्ण हैं।

ऐसा देखने में आया है कि बैंकिंग क्षेत्र में साइबर अपराधों में मनोवैज्ञानिक पहलू को मानवीय भूल या चूक के कारण सबसे ज्यादा गलतियां होती हैं। इसे कुछ उदाहरण से समझा का सकता है। साइबर धोखाधड़ी के शिकार होने वाले लोगों में सभी क्षेत्र, वर्ग एवं आयु के लोग हैं। ऐसा नहीं कहा जा सकता कि इसमें पढ़े लिखे लोगों कम और अनपढ़ या कम पढ़े लिखे लोग ज्यादा शिकार होते हैं। अधिक आयु वर्ग के लोग भी इसका शिकार हो जाते हैं जिनसे फोन पर या लिंक आदि भेजकर उनका व्यक्तिगत डेटा हासिल कर उनको साइबर धोखाधड़ी का शिकार बनाया जाता हैं। इसके लिए हम वित्तीय साक्षरता की कमी को प्रमुख कारक माना जाता है। साक्षर होना अलग बात है वित्तीय साक्षरता होना अलग। साइबर अपराध के शिकार होने से बचाव हेतु हमें प्रत्येक देशवासियों को वित्तीय रूप से साक्षर बनाने की पहल करनी चाहिए तभी हम साइबर धोखाधड़ी से बचाव हेतु एक मजबूत सुरक्षा कवच का निर्माण कर सकेंगे।

साइबर स्पेस में रहना और वहां काम करना अपने आप में एक कला और विज्ञान दोनों है। तकनीक का प्रयोग कैसे करें यह विज्ञान और छल-प्रपंच से जानकारी पर नियंत्रण हासिल करके हेरफेर, धोखा कोई न दे पाए यह कला हमें आनी चाहिए। 'मनुष्य' किसी भी सुरक्षा प्रणाली की सबसे कमजोर कड़ी होने के कारण अत्यधिक असुरक्षित है और इस प्रकार एक हैकर के लिए आवश्यक जानकारी का प्रवेश द्वार बनाता है। फ़िशिंग साइबर हमलों के लिए एक प्रयुक्त एक लोकप्रिय टूल है। फ़िशिंग अटैक - फ़िशिंग एक साइबर अपराध है जो वैध दिखने वाले ई-मेल, कॉल या टेक्स्ट संदेशों का उपयोग करता है जो स्वयं को प्रामाणिक स्रोतों से चित्रित करते हैं ताकि व्यक्तियों को व्यक्तिगत रूप से पहचान योग्य जानकारी, वित्तीय विवरण, ओटीपी या पासवर्ड जैसे संवेदनशील डेटा प्रदान करने के लिए राजी किया जा सके। लोकप्रिय सोशल वेबसाइटों, बैंकों, नीलामी साइटों, या आईटी

प्रशासकों के होने का दावा करने वाले ई-मेल के माध्यम से समान्य जनता को बरगलाने के लिए अपनाए जाने वाले सामान्य तरीके हैं।

साइबर अपराधी द्वारा भेजे गए ई-मेल, लिंक नकाबपोश होते हैं, इसलिए वे किसी ऐसे व्यवसाय द्वारा भेजे गए प्रतीत होते हैं, जिसकी सेवाओं का उपयोग प्राप्तकर्ता द्वारा किया जाता है। कभी-कभी, आधिकारिक दिखने वाले संदेश प्राप्तकर्ताओं को बताते हैं कि तकनीकी समस्याओं के कारण, उनके खातों की बिलिंग जानकारी या पासवर्ड फिर से सबमिट किए जाने चाहिए। उपभोक्ताओं को अपना व्यक्तिगत डेटा प्रदान करने के लिए मूर्ख बनाने की उम्मीद में कॉन कलाकार वैध वेबसाइटों की जानकारी का उपयोग करके पृष्ठों को फिर से बनाते हैं।

पहला फ़िशिंग मुकदमा 2004 में कैलिफोर्निया के एक किशोर के खिलाफ दायर किया गया था जिसने वेबसाइट "अमेरिका ऑनलाइन" की नकल बनाई थी। इस फर्जी वेबसाइट के साथ, वह उपयोगकर्ताओं से संवेदनशील जानकारी हासिल करने और उनके खातों से पैसे निकालने के लिए क्रेडिट कार्ड के विवरण तक पहुंचने में सक्षम था। फ़िशिंग के कुछ अन्य रूप 'विशिंग' (वॉयस फ़िशिंग), 'स्मिशिंग' (एसएमएस फ़िशिंग) आदि हैं, और साइबर अपराधी लगातार कई नई तकनीकों के साथ आते हैं। स्पीयर फ़िशिंग, एक प्रकार की फ़िशिंग है जिसमें किसी विशेष व्यक्ति या संगठन पर ई-मेल के माध्यम से किया जाता है, जिसका लक्ष्य उनके सुरक्षा में प्रवेश करना होता है। स्पीयर फ़िशिंग अटैक लक्ष्य पर शोध के बाद किया जाता है और इसमें एक विशिष्ट व्यक्तिगत घटक होता है जिसे लक्ष्य को अपने हित के विरुद्ध कुछ करने के लिए डिज़ाइन किया जाता है। गोपनीय कॉर्पोरेट डेटा को कैप्चर करने में इस तंत्र का उपयोग किया जाता है। फ़िशिंग मेल - आप फ़िशिंग ई-मेल की पहचान नीचे दिए गए विवरणों पर सत्यापित करके कर सकते हैं। प्रेषक के पते की विश्वसनीयता की जांच करें। बैंकों के नाम से अधिसूचना मेल/ लिंक से समानता से व्यक्तिगत अभिवादन की कमी, हालांकि व्यक्तिगत विवरण की उपस्थिति वैधता की गारंटी नहीं है। वास्तविक मेल आमतौर पर आपके नाम को संबोधित करते हैं। कुछ कार्य करने से पूर्व मेल में दिए गए लिंक या बटन की जांच करें। उदाहरण के रूप में “pubjabandsind@org” से ई-मेल लिंक में "गो टू " pubjabandsind@org लिंक वास्तव में एक ऐसी वेबसाइट पर जाता है जो बैंक के वेबसाइट से संबंधित नहीं होता है। ई-मेल में वर्तनी की गलतियां और लिंक में IP पता होना दोनों ही इस बात के संकेत हैं कि मेल एक फ़िशिंग प्रयास है। फ़िशिंग वेबसाइट: एक फ़िशिंग वेबसाइट (जिसे कभी-कभी "धोखाधड़ी" साइट कहा जाता है) आपको धोखा देकर आपके खाते का पासवर्ड या अन्य गोपनीय जानकारी चुराने का प्रयास करती है।

फ़िशिंग से बचाव: वेबसाइट का उपयोग करने से पहले पूरे URL को पैडलॉक चेक के साथ जांचना सबसे अच्छा अभ्यास है। हमेशा सुनिश्चित करें कि, आप वास्तविक डोमेन नाम के साथ वास्तविक URL का उपयोग कर रहे हैं। https://www.virustotal.com एक ऑनलाइन एप्लिकेशन है जिसका उपयोग यह जांचने के लिए किया जा सकता है कि कोई URL फ़िशिंग है या नहीं। फ़िशिंग का शिकार होने से बचने के लिए आप जो कुछ अन्य सावधानियां बरत सकते हैं, वे नीचे दी गई हैं: हमेशा, क्लिक करने से पहले सोचें: यादृच्छिक ई-मेल या संदेशों में दिखाई देने वाले लिंक पर क्लिक करना एक अच्छा कदम नहीं है। यदि आपको किसी मेल या लिंक की प्रामाणिकता पर संदेह हैं, तो उनकी जांच अवश्य करें। एक वैध स्रोत से होने का दावा करने वाला फ़िशिंग ई-मेल लिंक बिल्कुल वास्तविक वेबसाइट जैसा लग सकता है। हालाँकि, उनके पास व्यक्तिगत अभिवादन की कमी हो सकती है और "प्रिय ग्राहक" से शुरू हो सकते हैं, इसलिए जब आप ऐसे संदेश देखें तो सतर्क रहें। साथ ही, जब संदेह हो, तो संभावित खतरनाक लिंक पर क्लिक करने के बजाय URL पता टाइप करके सीधे स्रोत पर नेविगेट करें। साइट की सुरक्षा की दोबारा जांच करें: संवेदनशील वित्तीय जानकारी ऑनलाइन प्रदान करने के बारे में हमेशा सतर्क रहें। कोई भी जानकारी सबमिट करने से पहले, सुनिश्चित करें कि साइट का URL "https"

से शुरू होता है और एड्रेस बार और पूरे URL के पास एक क्लोज्ड लॉक आइकन होता है। यदि आपको यह संदेश मिलता है कि किसी निश्चित वेबसाइट में दुर्भावनापूर्ण फ़ाइलें हो सकती हैं, तो ऐसा न करें।

कभी भी संदिग्ध ई-मेल या वेबसाइट से फाइल डाउनलोड न करें। कई फ़िशिंग वेब पेज कम लागत वाले उत्पादों की पेशकश करने वाले उपयोगकर्ताओं को बरगलाते हैं। यदि उपयोगकर्ता ऐसी वेबसाइट पर खरीदारी करता है, तो साइबर अपराधियों द्वारा क्रेडिट कार्ड का विवरण प्राप्त किया जाएगा। अपने ऑनलाइन खातों को नियमित रूप से सत्यापित करें। नियमित रूप से अपने ऑनलाइन खातों पर जाने की आदत डालें। अपने वित्तीय खातों के मासिक विवरणों की नियमित रूप से जांच करने से बैंक फ़िशिंग और क्रेडिट कार्ड फ़िशिंग घोटालों को रोकने में मदद मिल सकती है। यह भी सुनिश्चित करता है कि आपकी जानकारी के बिना कोई भी धोखाधड़ी लेनदेन नहीं किया गया है। पासवर्ड हाइजीन- इंटरनेट सुरक्षा फर्म स्प्लैश डेटा की एक अध्ययन रिपोर्ट के अनुसार, 2018 में इस्तेमाल किया जाने वाला सबसे लोकप्रिय पासवर्ड '123456' है। दिलचस्प बात यह है कि उनके अध्ययन के अनुसार यह पिछले पांच वर्षों से नंबर एक विकल्प रहा है, इसके बाद 'पासवर्ड' आता है। जैसा कि स्पष्ट है, लोग उस पासवर्ड का उपयोग करते हैं जिसे वे आसानी से याद रख सकते हैं। पासवर्ड स्वच्छता के अच्छे स्तर को बनाए रखने के लिए अपनाई जाने वाली कुछ सर्वोत्तम प्रथाएं हैं: एक से अधिक खातों के लिए एक ही पासवर्ड का उपयोग न करें, विशेष रूप से वित्तीय खातों के लिए। आमतौर पर इस्तेमाल किए जाने वाले घर या स्थान या पालतू जानवर या कंपनी का नाम, फोन या वाहन नंबर आदि हो सकते हैं। यदि कोई हमलावर किसी भी बिंदु पर आपको लक्षित करने के लिए दृढ़ संकल्पित है, तो ऐसे पासवर्ड का उनके द्वारा आसानी से अनुमान लगाया जा सकता है। मजबूत पासवर्ड का प्रयोग करें जो अंकों, अपरकेस, लोअरकेस, विशेष वर्णों का एक संयोजन है। 'ई' के बजाय '3', 'एस' के बजाय '$', 'आई' के बजाय '1' का उपयोग करना पासवर्ड की ताकत को बेहतर बनाने के लिए कुछ सुझाव हैं। पासवर्ड की सामान्य रूप से उचित लंबाई 8 वर्ण हैं। हालाँकि, अधिकांश वेब एप्लिकेशन पासवर्ड फ़ील्ड में 25 वर्णों तक का समर्थन करते हैं। वर्णों की संख्या जितनी अधिक होगी, किसी तीसरे पक्ष द्वारा पासवर्ड का अनुमान लगाना उतना ही कठिन होगा। शब्दकोश में किसी शब्द के प्रयोग से बचें। ऐसे पासवर्ड को आसानी से पहचानने के लिए डिक्शनरी अटैक का इस्तेमाल किया जा सकता है। एप्लिकेशन द्वारा प्रदान किए गए डिफ़ॉल्ट पासवर्ड का उपयोग करने से बचें। पहले लॉगिन के बाद बदलें। अपना पासवर्ड नियमित रूप से बदलें, जैसे हर 30-45 दिनों में।

नकली वेबसाइटें:

नकली वेबसाइट और एप्लिकेशन जो COVID-19 संबंधित जानकारी साझा करने का दावा करते हैं, वास्तव में मैलवेयर इंस्टॉल करेंगे, आपकी व्यक्तिगत जानकारी चुराएंगे, या अन्य नुकसान पहुंचाएंगे। इन उदाहरणों में, वेबसाइट और एप्लिकेशन समाचार, परीक्षण परिणाम, या अन्य संसाधनों को साझा करने का दावा कर सकते हैं। हालांकि, वे केवल लॉगिन क्रेडेंशियल, बैंक खाते की जानकारी या आपके उपकरणों को मैलवेयर से संक्रमित करने के साधन की तलाश कर रहे हैं।

कपटपूर्ण चैरिटी:

फर्जी या गैर-मौजूद धर्मार्थ संगठनों के लिए दान मांगने वाली वेबसाइटों में तेजी आई है। नकली चैरिटी और डोनेशन वेबसाइट किसी की नेक इच्छा का फायदा उठाने की कोशिश करेंगी। किसी अच्छे काम के लिए पैसे दान करने के बजाय, ये नकली चैरिटी इसे अपने पास रखते हैं। अनुशंसाएं COVID-19-संबंधित विषय पंक्तियों, अनुलग्नकों, या ई-मेल, ऑनलाइन ऐप्स और वेब खोजों में हाइपरलिंक वाले किसी भी ई-मेल को संभालने में अत्यधिक सावधानी बरतें, विशेष रूप से अवांछित ई-मेल। इसके अतिरिक्त, सोशल मीडिया पोस्ट, टेक्स्ट मैसेज या समान संदेशों वाले फोन कॉल से सावधान रहें।

नीचे दी गई सावधानियों को बरतकर, आप इन खतरों से बेहतर तरीके से अपनी रक्षा कर सकते हैं –

1. अवांछित या असामान्य ई-मेल, टेक्स्ट संदेश और सोशल मीडिया पोस्ट में लिंक और अटैचमेंट पर क्लिक करने से बचें।
2. महामारी की स्थिति से संबंधित सटीक और तथ्य-आधारित जानकारी के लिए केवल विश्वसनीय स्रोतों, जैसे सरकारी वेबसाइटों का उपयोग करें।
3. कभी भी फोन या ई-मेल पर अपनी व्यक्तिगत जानकारी, बैंकिंग जानकारी या अन्य व्यक्तिगत रूप से पहचान योग्य जानकारी सहित न दें।
4. दान करने से पहले हमेशा किसी चैरिटी की प्रामाणिकता की पुष्टि करें।
5. अविश्वसनीय/अज्ञात स्रोतों से एप्लिकेशन डाउनलोड या इंस्टॉल करने से बचें।
6. एकाधिक खातों के लिए एक ही पासवर्ड का उपयोग करने से बचें।

सार्वजनिक वाई-फाई- सार्वजनिक वाईफाई का उपयोग करते समय कोई वित्तीय विवरण दर्ज न करें। यह हैकिंग के लिए प्रवृत्त है क्योंकि आप इसकी उत्पत्ति और तकनीकी के बारे में नहीं जानते हैं। मालवेयर- यह वायरस, वर्म्स, स्पाईवेयर, एडवेयर, रैंसमवेयर और ट्रोजन जैसे कई रूपों में आता है। प्रोग्राम की गई स्क्रिप्ट किसी असुरक्षित वेबसाइट, संक्रमित मेल या पेन ड्राइव आदि से किसी भी माध्यम से सिस्टम में प्रवेश कर सकती है। यह वास्तव में एक दुर्भावनापूर्ण सॉफ़्टवेयर है जो एटीएम या बैंक सर्वर पर कंप्यूटर सिस्टम को नुकसान पहुंचा सकता है और साइबर अपराधियों को गोपनीय कार्ड डेटा तक पहुंचने की अनुमति देता है। साइबर धोखाधड़ी से बचाव हेतु एवं निवारक हेतु सतर्कता ही सबसे महत्वपूर्ण और सार्थक बचाव है। इसके साथ–साथ हमें वित्तीय साक्षारता पर जोड़ देते हुए हमें साइबर धोखाधड़ी से बचाव हेतु एक सशक्त पीढ़ी तैयार करने की जरूरत है। तकनीक के विकास के साथ-साथ उसके दुष्परिणाम भी होंगे परंतु इसके लिए हम तकनीकी विकास को अस्वीकार नहीं कर सकते हैं। संचार क्रांति के इस दौर में हमें तकनीकी विकास आज की सच्चाई है हमें इसके साथ जीवन जीने की आदत बनानी होगी। अपनी क्षमता और वित्तीय साक्षारता को भी साथ-ही साथ बढ़ाना होगा।

*****

अविनाश शुक्ला

पदनाम:- उप महाप्रबंधक एवं मुख्य सूचना सुरक्षा अधिकारी
संस्था का नाम:- यूको बैंक
मोबाइल नं. :- 8016583030
ई-मेल:- shukla_avinash@rediffmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

बैंकों और उनके संघटकों द्वारा सूचना प्रौद्योगिकी का प्रयोग तेजी से बढ़ा है और यह अब बैंकों की परिचालनीय कार्यनीति का एक महत्वपूर्ण अंग है। डिजिटल तकनीक के बढ़ते प्रभाव एवं ग्राहकों की बढ़ती अपेक्षाओं के अनुरूप बैंक भी अपने को नए वातावरण में सँरेखित करने में तत्पर हैं। सरकार द्वारा डिजिटल लेन-देन को बढ़ावा दिए जाने के कारण बैंकिंग सेवाओं का डिजिटलीकरण बहुत तेजी से बढ़ रहा है। इंटरनेट की दरों में कमी एवं व्यापक उपलब्धता के कारण कहीं भी और कभी भी डिजिटल लेनदेन की सुविधा दूर-दराज के स्थानों के ग्राहकों को भी आकर्षित कर रही है। यूपीआई, वॉलेट, आईएमपीएस, एनईएफ़टी, आरटीजीएस आदि की ऑनलाइन सुविधादिन प्रतिदिन लोकप्रिय होती जा रही है।

बैंकों द्वारा तकनीक के प्रयोग में और अधिक बढ़ोतरी हुई है। दूसरी ओर, गत समय में साइबर घटनाओं/आक्रमणों की संख्या, अंतराल और प्रभाव में काफी वृद्धि हुई है, विशेष रूप से बैंक सहित वित्तीय क्षेत्र के मामले में, जो संकेत दे रहे हैं कि बैंकों में सुदृढ़ साइबर सिक्यूरिटी/आघात-सहनीयता की रूपरेखा को लागू करने की तत्काल आवश्यकता है और नियमित आधार पर बैंकों में पर्याप्त साइबर-सिक्यूरिटी की तैयारी सुनिश्चित करना आवश्यक है। आसान होते साइबर खतरे, इनका विकासरत स्वरूप, स्तर/वेग में वृद्धि, उत्प्रेरणा और बैंकिंग प्रणाली में साइबर-खतरों की उपस्थिती को ध्यान में रखते हुए, यह आवश्यक है कि साइबर जोखिमों से निपटने के लिए वर्तमान सुरक्षा में सुधार द्वारा बैंकिंग प्रणाली की आघात-सहनीयता में सुधार किया जाए। प्रतिकूल घटनाओं/बाधाओं, जब कभी घटित हों, से निपटने में अनुकूलनीय घटना प्रतिक्रिया, प्रबंध एवं पुनः प्राप्ति रूपरेखा शामिल होंगे, लेकिन ये यही तक सीमित नहीं होंगे।

एसीआई वर्ल्डवाइड (ACI Worldwide)की डिजिटल रिपोर्ट के अनुसार भारत वर्ष में 2025 तक कुल बैंकिंग लेन-देन की संख्या का 71% डिजिटल माध्यम से होगा एवं मात्र 28.3% नगद व चेक द्वारा होगा। भारत 25.5 बिलियन लेनदेन भुगतान के साथ विश्व में सबसे ऊपर हैं तथा चीन 17 बिलियन के साथ दूसरे स्थान पर है। फिनटेक के उभरने से तो डिजिटल लेन-देन की संख्या बहुत तेजी से बढ़ रही है। इसी कारण से भारतीय बैंकिंग व्यवस्था न केवल भारतीय बल्कि अंतरराष्ट्रीय हैकरों के ध्यानाकर्षण का केंद्र बन गई है।

जहां तक साइबर अपराध का प्रश्न है, कोई भी गैरकानूनी कार्य जहां कंप्यूटर या संचार उपकरण या कंप्यूटर नेटवर्क का उपयोग अपराध करने या अपराध करने की सुविधा के लिए किया जाता है, साइबर अपराध की श्रेणी में आता है। डिजिटलीकरण के प्रचार प्रसार से साइबर अपराधियों के लिए अपराध करने के अवसर भी बढ़ रहे हैं। जालसाजों द्वारा प्रयोग होने वाली तकनीकों के विकास के साथ-साथ साइबर अपराध भी उत्तरोत्तर जटिल होते जा रहे हैं। अधिकांशतः वित्तीय लाभ के उद्देश्य से आपराधिक गतिविधियां संचालित होती हैं जिससे बैंक और वित्तीय संस्थान हमेशा जालसाजों एवं घोटालेबाजों के निशाने पर होते हैं।

साइबर हमले या घटनाएं मुख्यतः दो तरह से हो रही है। एक में मासूम ग्राहकों को साइबर अपराधी मुख्यतः साइबर ठग एवं धोखेबाज या तो आधुनिक तकनीक द्वारा या फिर सोशल इंजीनियरिंग के द्वारा ठग रहे हैं। दूसरे प्रकार में साइबर अपराधी संस्थाओं को जिसमे बैंक भी शामिल हैं लक्ष्य बना रहे हैं। उनका उद्देश्य मुख्यतः बैंक के सिस्टम को भेद कर अनधिकृत वित्तीय लेनदेन करना, बैंक के सिस्टम में गड़बड़ी पैदा करके कार्य को बाधित करना या फिर संवेदनशील जानकारी चुराना है। पिछले कुछ समय से रैन्समवेयर हमले भी बहुत चर्चा में हैं। रैन्समवेयर हमले में वित्तीय हानि, कार्य में बाधा एवं डेटा की चोरी, तीनों तरह का अपराध एक साथ देखने को मिलता है।

बैंकों द्वारा बढ़ते हुए साइबर क्राइम के साथ-साथ, इन अपराधों से सुरक्षा के लिए विभिन्न उपकरणों और तकनीकों का उपयोग भी किया जा रहा है। हालांकि कानून प्रवर्तन एजेंसियों ने इन समस्याओं से निपटने के लिए कई कदम उठाए हैं, लेकिन यह समस्या खतरे के परिदृश्य के विस्तार के साथ नियमित रूप से बढ़ रही है। साइबर अपराधों को व्यापक रूप से धोखाधड़ी, बौद्धिक सम्पदा की तस्करी, व्यक्तिगत जानकारी की चोरी या गोपनीयता पर आक्रमण, बाल पोर्नोग्राफी आदि में वर्गीकृत किया जा सकता है।

यदि बैंकिंग क्षेत्र को देखें तो निम्न प्रकार के साइबर अपराध सामने आते हैं:

हैकिंग: अक्सर, सरकारी/वित्तीय संस्थानों की वेबसाइट हैकरों के लिए एक लोकप्रिय लक्ष्य होती हैं क्योंकि हैकर मौद्रिक लाभ के साथ-साथ यहां प्रचार एवं प्रसिद्धि भी पाते हैं। दूर बैठा हैकर इंटरनेट की सुविधा से बैंक के कम्प्यूटर को हैक करके अवैध लेनदेन कर सकता, गोपनीय जानकारी चुरा सकता हैतथा मैलवेयर आदि डाल सकता है।

पहचान की चोरी: नकद लेनदेन और बैंकिंग सेवाओं के लिए इंटरनेट का उपयोग करने वाले लोगों के लिए यह एक बड़ी समस्या बन गई है। इस साइबर अपराध में अपराधी, व्यक्ति के बैंक खाते, क्रेडिट कार्ड, डेबिट कार्ड और अन्य संवेदनशील सूचनाओं के बारे में जानकारी हासिल करता है ताकि पैसे की हेराफेरी की जा सके या पीड़ित के नाम पर ऑनलाइन चीजें खरीदी जा सकें। इससे बड़ा आर्थिक नुकसान हो सकता है।

कंप्यूटर वेंडेलिस्म : कंप्यूटर वेंडेलिस्म एक प्रकार का दुर्भावनापूर्ण व्यवहार है। इसमें विभिन्न तरीकों से कंप्यूटर और डेटा को नुकसान पहुँचाना और व्यवसायों को संभावित रूप से बाधित करना शामिल होता है। विशिष्ट कंप्यूटर वेंडेलिस्म में हानिकारक कार्यों को करने के लिए डिज़ाइन किए गए दुर्भावनापूर्ण प्रोग्राम बनाना शामिल है जैसे हार्ड ड्राइव डेटा मिटाना या लॉगिन क्रेडेंशियल निकालना। कंप्यूटर वेंडेलिस्म वायरस से अलग है, जो खुद को मौजूदा कार्यक्रमों से जोड़ लेता है।

दुर्भावनापूर्ण सॉफ़्टवेयर: ये इंटरनेट-आधारित सॉफ़्टवेयर या प्रोग्राम हैं जिनका उपयोग किसी नेटवर्क को बाधित करने के लिए किया जाता है। सॉफ़्टवेयर का उपयोग संवेदनशील जानकारी या डेटा चोरी करने या सिस्टम में मौजूद सॉफ़्टवेयर को नुकसान पहुंचा कर सिस्टम तक पहुंच प्राप्त करने के लिए किया जाता है।

फ्रॉड कॉल्स: केवाईसी अद्यतनकरने, खाता को अनब्लॉक करने, अस्वीकृत लेनदेन विवादका निपटान करने आदि के बहाने ग्राहकों को गोपनीय विवरण साझा करने के लिए बैंक के नाम पर फर्जी फोन कॉल्स करना एवं ग्राहक की गोपनीय जानकारी प्राप्त करना जिससे की ग्राहक के खाते से पैसा निकला जा सके।

ऑनलाइन अवैध बिक्री (डार्क वेब): इस अपराध में, एक अपराधी अवैध ऑनलाइन शॉपिंग प्लेटफॉर्म पर व्यक्ति को अवैध हथियार, ड्रग्स, तस्करी का सामान या व्यक्तिगत जानकारी बेचता है और लेनदेन भी क्रिप्टोकरेंसी के माध्यम से किया जाता है।

बैंकिंग क्षेत्र पर साइबर अपराध का प्रभाव

मोबाइल फोन और इंटरनेट के माध्यम से बड़ी संख्या में ऑनलाइन सेवाओं जैसे ऑनलाइन लेन-देन, सेवा शुल्क का भुगतान, वेब आधारित खरीदारी आदि के उपयोग से सभी वर्ग के उपयोगकर्ताओं में डिजिटलीकरण का बड़े पैमाने पर प्रसार हुआ है, तदनुसार इंटरनेट और विकसित तकनीक से साइबर अपराधियों के लिए विभिन्न पहलुओं का लाभ उठाना भी आसान हुआ है। नतीजन, कई लोग पहचान की चोरी (आइडेंटिटी थेफ़्ट), हैकिंग और दुर्भाभावनापूर्ण सॉफ़्टवेयर (मालवेयर) के शिकार हो रहे हैं। इन अपराधियों को रोकने और संवेदनशील जानकारी की रक्षा करने के सर्वोत्तम तरीकों में से एक हैऑनलाइन रहते समय सदा जागरूक रहना है।

साइबर अपराध से मुख्यतः तीन स्तरों पर निपटने की आवश्यकता है। पहला बैंक अपनी डिजिटल बैंकिंग सेवाओं तथा तकनीक में साइबर सुरक्षा का निम्नलिखित रूप से ध्यान रखे :

1. आधुनिक एवं प्रभावी साइबर सुरक्षा की व्यवस्था करना जिससे हैकिंग एवं रैंसमवेयर हमले से बचा जा सके।
2. डेटा सुरक्षा के लिए उचित एन्क्रिप्शन का उपयोग करना
3. निरंतर 24 x7 निगरानी एवं अनियमितता मिलने पर तुरंत निराकरण
4. अपने ग्राहकों को सुरक्षा प्रदान करने के लिए डिजिटल सेवाओं में पर्याप्त सुरक्षा विकल्प उपलब्ध करना
5. अपने कर्मचारियों को समय-समय पर प्रशिक्षण देना
6. ग्राहकों को साइबर सुरक्षा के क्षेत्र में जागरूक करना
7. स्वचालित धोखाधड़ी जोखिम प्रबंधन प्रणाली की मदद से पूरी सक्रियता के साथ साइबर खतरों को भांपना एवं निराकरण के लिए उचित कार्रवाई करना आदि।

दूसरा ग्राहक को सतर्क एवं सावधान रहकर निम्नलिखित बातों का ध्यान रखना चाहिए:

1. मजबूत पासवर्ड का उपयोग: अलग-अलग ऑनलाइन खाते के लिए अलग-अलग पासवर्ड बनाए रखना और अक्षरों, संख्यात्मक और विशेष वर्णों के संयोजन के साथ पासवर्ड रखना एक महत्वपूर्ण पहलू है। समय-समय पर अपनी आईडी का पासवर्ड बदलते रहें।
2. सोशल मीडिया के जानकार बनें: सोशल नेटवर्किंग प्रोफाइल (फेसबुक, ट्विटर, यूट्यूब, आदि) को उचित सुरक्षा सेटिंग्स के द्वारा रक्षा करें एवं निजता का ध्यान रखें।
3. मोबाइल उपकरणों को सुरक्षित रखें, केवल विश्वसनीय स्रोतों से एप्लिकेशन डाउनलोड करें और डिवाइस ऑपरेटिंग सिस्टम/ऐप्स को अप-टू-डेट रखें। एंटी-वायरस सॉफ़्टवेयर और सुरक्षित लॉक का उपयोग भी सुरक्षा को बढ़ाता है।
4. नवीनतम पैच और अपडेट के साथ सिस्टम को अपडेट रखें।
5. मोबाइल फोन और लैपटॉप में एंटीवायरस (Antivirus) रखें जो समय- समय पर ऑटोमैटिक वायरस को नष्ट करता रहता है।
6. अनजान मैसेज लिंक या मोबाइल पर आए नोटिफिकेशन पर बिना जानकारी के क्लिक ना करे उसे डिलीट कर दें।
7. मनी ट्रांसफर एप जैसे नेटबैंकिंग, फोन पे, गूगल पे व अन्य जो भी आप उपयोग करते होसेकाम समाप्त होने पर तुरंत लॉगआउट करें।

8. सोशल मीडिया पर सावधान रहें, सोशल मीडिया पर अपनी निजी तस्वीरें डालने से बचें, उनका कोई भी इस्तेमाल कर सकता है। अपने अकाउंट पर प्राइवेसी सेटिंग को पब्लिक न करें। अगर किसी समस्या में फंस जाते हैं, तो घबराए नहीं। पुलिस को इसकी जानकारी दें।
9. क्रेडिट कार्ड से निकासी की सीमा रखें- अगर आपके क्रेडिट कार्ड की कभी क्लोनिंग हो जाए या चोरी हो तो भी आप ज्यादा नुकसान से बच सकते हैं। लेकिन इसके लिए जरूरी है कि आप क्रेडिट कार्ड से शॉपिंग नगद निकासी की सीमा 10-20 हजार रुपए से ज्यादा न रखें। इससे फायदा यह होगा कि चोरी करने वाला कम से कम रकम निकाल पाएगा और आप बहुत बड़े नुकसान से बच सकते हैं।

तीसरे स्तर पर साइबर अपराध से प्रभावी ढंग से निपटने के लिए, कानून प्रवर्तन एजेंसियों, सूचना प्रौद्योगिकी उद्योग, सूचना सुरक्षा संगठनों, इंटरनेट कंपनियों और वित्तीय संस्थानों के बीच सार्वजनिक-निजी सहयोग का बहुआयामी प्रयास एक महत्वपूर्ण पहलू है। यदि कानून प्रवर्तन एजेंसियां साइबर अपराधियों को समय से पकड़ कर उचित सजा दिलवा पायें तो अपने आप ही इस तरह की घटनाएं कम हो जाएंगी। अंतर्राष्ट्रीय स्तर पर भी साइबर अपराधों को रोकने के लिए सहयोग की आवश्यकता है। सरकार को समय- समय पर क़ानून की समीक्षा करके उचित एवं जरूरी बदलाव लाते रहना चाहिए।

साइबर अपराध रिपोर्टिंग

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://cybercrime.gov.in) गृह मंत्रालय, भारत सरकार द्वारा राष्ट्रीय मिशन के तहत पीड़ितों/शिकायतों को सायबर-अपराध की शिकायतों की ऑनलाइन रिपोर्ट करने की सुविधा प्रदान करने की एक पहल है। यह पोर्टल महिलाओं, बच्चों के विरुद्ध अपराधों और अन्य साइबर अपराधों जैसे पहचान की चोरी, ऑनलाइन और सोशल मीडिया अपराध, ऑनलाइन वित्तीय धोखाधड़ी, रैंसमवेयर, हैकिंग, क्रिप्टोकरेंसी अपराध और ऑनलाइन साइबर तस्करी के खिलाफ अपराधों पर विशेष ध्यान देने के साथ ऑनलाइन शिकायत दर्ज करने की सुविधा प्रदान करता है। हाल ही में गृह मंत्रालय ने 1930 हेल्प लाइन शुरू की है जिसपर भी साइबर क्राइम की शिकायत की जा सकती है।

निष्कर्ष

जैसे-जैसे खतरे का परिदृश्य विकसित हो रहा है, नए उपकरण और दृष्टिकोण नियमित रूप से उभर रहे हैं। लेकिन एक चीज स्थिर रहती है। वह है मानवीय कारक। वित्तीय संस्थाओं एवं ग्राहकों में साइबर अपराध के प्रति बढ़ती जागरूकता बहुत कारगर साबित हो सकती है। सतर्क एवं जागरूक कर्मचारी एवं ग्राहक साइबर सुरक्षा की पहली पंक्ति हैं।साइबर सुरक्षा का महत्व एवं जागरूकता की जितनी आवश्यकता कर्मचारियों एवं ग्राहकों को है उससे कहीं ज्यादा शीर्ष प्रबंधन को है। शीर्ष प्रबंधन के जुड़ाव से संगठन के भीतर बेहतर साइबर संस्कृति उत्पन्न हो सकती है। साइबर क्राइम दिनप्रतिदिन अपने पैर फैलाता जा रहा है। साइबर सुरक्षा को सदैव चुस्त एवं अद्यतनित रखना होगा। बैंकों को नियामक दिशानिर्देशों का अक्षरशः पालन करना होगा। इसके दुष्प्रभाव के शिकार बनने से सुरक्षित रहने का सबसे उचित तरीका सुरक्षा के उपायों का पालन करना है क्योंकि 'रोकथाम इलाज से हमेशा बेहतर होता है।

*****

ए अरुणा ज्योति

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 7696029275
ई-मेल:- zoddnraj@pnb.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

आज वैकल्पिक डिलीवरी चैनलों का जमाना है। बैंकिंग के नवोन्मेषी तरीके ग्राहकों में काफी लोकप्रिय होते जा रहे हैं। आज बैंकों द्वारा बढ़ते सूचना प्रौद्योगिकी के विकास के क्रम में आधुनिक कम्प्यूटर, इंटरनेट बैंकिंग, जमा मशीनों, एटीएम, टेली बैंकिंग, डेबिट एवं क्रेडिट कार्ड, प्लास्टिक मनी स्मार्ट कार्ड, आदि का उपयोग किया जा रहा है। सूचना प्रौद्योगिकी के इस युग में ग्राहक की अनेक अपेक्षाएं हो सकती हैं। इलेक्ट्रॉनिक बैंकिंग के अंतर्गत इलेक्ट्रॉनिक निधि अंतरण, इंटरनेट आधारित बैंकिंग लेनदेन, कार्ड बैंकिंग काफी बढ़ रही है। आज हमारे सामने अनेक ऐसे मुद्दे/ चुनौतियां उभर कर आ रही हैं जिनके बारे में कभी सोचा नहीं गया था। चिंता के प्रमुख विषय हैं–इंटरनेट बैंकिंग का गलत प्रयोग/ दुष्प्रयोग, एटीएम से जुड़ी सेवाओं में कमियां, क्रेडिट/ डेबिट कार्ड खो जाना तथा इस स्थिति में कार्डधारक की जिम्मेदारी इत्यादि। ग्राहकों को अपने अधिकारों, बैंकिंग उत्पादों के सेवा प्रभार, धोखाधड़ी के विरूद्ध अपनी सुरक्षा इत्यादि से संबंधित जागरूक होना चाहिए।

सुपुर्दगी (Delivery) चैनल में जोखिम :

आज आधुनिक एवं तकनीक आधारित सुपुर्दगी (Delivery) चैनल का यद्यपि स्वागत किया जा रहा है, परंतु समय की मांग यह भी है कि इससे जुड़े जोखिम के प्रति सजग एवं सर्तक रहा जाए। ई-बैंकिंग, प्लास्टिक कार्डों का दुरूपयोग, धोखाधड़ी एवं साइबर अपराध जैसे जोखिमों से आज ग्राहक भयभीत हैं।

ऑनलाइन बैंकिंग अपनाने का चलन जोर पकड़ रहा है। इसके बावजूद कई बैंक व इंटरनेट सुविधा का इस्तेमाल करने वाले ग्राहक सुरक्षा से जुड़े मुद्दों को लेकर काफी चिंतित नज़र आ रहे हैं। ग्राहकों के लिए ऑनलाइन बैंकिंग में चिंता की सबसे बड़ी वजह सुरक्षा से जुड़े पहलू हैं। बैंकरों एवं आईटी जानकारों का मानना है कि पर्याप्त सिक्योरिटी सिस्टम के नहीं होने तथा ग्राहकों के बीच समुचित जानकारी और जागरूकता के अभाव के कारण इंटरनेट असुरक्षा बनी रहती है तथा हैकिंग जैसी घटनाएं होती हैं।

सूचना सुरक्षा

सूचना सुरक्षा का अर्थ है सूचना को सुरक्षित रखना एवं सूचना प्रणालियों को अनधिकृत पहुंच से बचाना तथा उनके दुरूपयोग, प्रकटीकरण, विघटन, संशोधन, अवलोकन, निरीक्षण, रिकॉर्डिंग अथवा उनको नष्ट होने से सुरक्षित रखना। सूचना की सुरक्षा का मुख्य उद्देश्य सूचना की गोपनीयता, अखंडता एवं आंकड़ों (चाहे इलेक्ट्रॉनिक, प्रिंट या अन्य किसी भी रूप में हों) की उपलब्धता को सुरक्षित रखने के संबंध में है।

साइबर खतरे कई प्रकार के होते हैं जिनमें से कुछ इस प्रकार हैं:-

- *फ़िशिंग (Phishing)

- स्निफर (Sniffer)
- पासवर्ड की चोरी (Password Cracking)
- पहचान हमला आईपी स्पूफिंग (IP Spoofing)
- इनपुट मान्यकरण हमला (Input Validation Attack)
- एसक्यूएल इंजेक्शन हमला (SQL Injection Attack)
- सेवा बाधित करने वाले हमले (Denial of Service Attack)
- एस्मर्फ हमला (Smurf Attack)
- एसवाईएन फ़्लड (SYN Flood)
- मैन-इन-मिडिल हमला (Man-in-Middle Attack),
- सोशल इंजीनियरिंग हमला (Social Engineering Attack,
- सीएसआरएफ हमला (Cross Site Request Forgery (CSRF) attack,
- क्रॉस साइट स्क्रिप्टिंग (Hijack of user session via XSS (Cross site) Screpting,
- ई-मेल फॉर्जिंग (Email forging),
- स्वचालित हमले : साइट पर कैप्चा (CAPTCHA) का अभाव

ज्वलंत उदाहरण – 27 जून, 2017 को हुई साइबर सुरक्षा हमला- PETYA RANSOMWARE/ MALWARE.

कंप्यूटर सुरक्षा के क्षेत्र में, **फ़िशिंग** एक आपराधिक धोखाधड़ी की प्रक्रिया है जिसके द्वारा नकली पहचान बनाकर संवेदनशील जानकारी जैसे उपयोगकर्ता का नाम, पासवर्ड, क्रेडिट कार्ड का विवरण आदि की चोरी का प्रयास किया जाता है। हमलावर अवांछनीय एवं दुर्भावनापूर्ण तरीकों का प्रयोग करके संवेदनशील फाइलों, क्रेडिट कार्ड विवरणों इत्यादि की चोरी कर सकता है। इस तरह के हमले में, एक अपराधी बड़ी मात्रा में पिंग ट्रैफिक (ping traffic) भेजते हैं जिसमें स्रोत आईपी एड्रेस नकली होते हैं। अत्यधिक मात्रा में पिंग ट्रैफिक होने के कारण नेटवर्क के कार्य में बाधा उत्पन्न हो जाती है। **एन्क्रिप्शन** का अभाव होने के कारण महत्वपूर्ण सूचनाओं की चोरी संभव हो जाती है। अगर ब्राउजर में "save password" के विकल्प का प्रयोग किया जाता है, तो पासवर्ड का पता किया जा सकता है। ई-मेल के सबसे आम खतरे हैं: अपमानजनक ई-मेल, जाली ई-मेल और स्पैम. **70% ई-मेल संदेश स्पैम होते हैं.** 'गोपनीय सूचनाओं' की सुरक्षा न केवल व्यावसायिक आवश्यकता है, अपितु कई मामलों में यह नैतिक एवं कानूनी आवश्यकता भी है। व्यक्ति विशेष के संदर्भ में, सूचना की सुरक्षा जीवन के गोपनीय पहलुओं पर महत्वपूर्ण प्रभाव डालती है। हाल के वर्षों में सूचना की सुरक्षा का क्षेत्र काफी विस्तृत तथा प्रभावी रूप से विकसित हुआ है।

कैशलेस अर्थव्यवस्था:

विमुद्रीकरण के समय सरकार ने लोगों को प्रोत्साहित करने तथा विभिन्न डिजिटल तरीकों को अपनाने के प्रति ध्यान आकर्षित करने के लिए निम्नलिखित कदम उठाएं :

- **डिजिटल लॉटरी योजनाओं :**

लकी ग्राहक योजना के अंतर्गत डिजिधन व्यापार योजना की शुरूआत की गई ताकि ऐसे प्रोत्साहन योजनाओं से डिजिटल इंडिया के सपने को साकार करके देश के आर्थिक व्यवस्था को सुदृढ़ बनाया जा सकें। रूपे कार्ड, यूएसएसडी, यूपीआई, आधार समर्थित भुगतान प्रणालियां इन योजनाओं का हिस्सा है.

- **भारत इंटरफेस फॉर मनी (BHIM) :**

ऑनलाइन लेन-देन को आसान बनाने के लिए BHIM नामक ई-वॉलेट ऐप की शुरूआत प्रधानमंत्री द्वारा 30 दिसम्बर, 2016 को किया गया। इस आधार समर्थित मोबाइल भुगतान ऐप्लिकेशन के जरिए कोई भी व्यक्ति अपने बैंक खाते से सीधे भुगतान कर सकता है। केवल आपका मोबाइल नंबर बैंक खाते से जुड़ा होना चाहिए और धन अंतरण के लिए बस एक क्लिक (one click) की ही देरी है।

- **आधार भुगतान ऐप :**

यह ऐप एक बायोमैट्रिक रीडर से जुड़ा होता है। उपभोक्ता को अपनी आधार संख्या दर्ज करने के उपरांत अंतरण के लिए किसी बैंक का चुनाव करना होगा। इस ऐप की विशेषता यह है कि भुगतान करने के लिए बिना फोन के इसका इस्तेमाल किया जा सकता है।

हालांकि, त्वरित भुगतान वाले इलेक्ट्रॉनिक लेन-देन ऐप, मोबाइल–वॉलेट की बढ़ोत्तरी में इजाफा अर्थव्यवस्था के लिए अच्छी बात है मगर वहीं दूसरी ओर स्टाफ सदस्यों एवं ग्राहकों को साइबर ज्ञान/ जानकारी (Cyber literate) के अभाव में आए दिन धोखाधड़ी के मामले बढ़ते जा रहे हैं।

चिप-आधारित कार्ड

धोखाधड़ी के बढ़ते मामलों के मद्देनजर भारतीय रिजर्व बैंक ने ग्राहकों/ बैंकों की सुरक्षा के लिए एटीएम कार्ड को चिप-आधारित बनाने जैसे कई कदम उठाए हैं। अब तक प्रचलित डेबिट या क्रेडिट कार्ड को क्लोन करना बेहद आसान है। सूचना सुरक्षा कंपनी इनफाइसेक के संस्थापक विनोद सेंथिल कहते हैं "अमेजन या फ्लिपकार्ट से कोई भी कार्ड रीडर-राइटर खरीद सकता है। इसके बाद किसी भी कार्ड की नकल कर लेना बेहद आसान है। "बैंकर भी इससे सहमत हैं कि डेबिट कार्ड की नकल कर क्लोन तैयार करना सबसे आसान है। रिज़र्व बैंक पहले ही 31 दिसंबर, 2018 तक मैग्नेटिक स्ट्रिप आधारित तमाम कार्डों का प्रचलन बंद करने का निर्देश दे चुका है। लेकिन मुश्किल यह है कि ज्यादातर एटीएम चिप-आधारित कार्डों को पढ़ नहीं सकते। उनको मैग्नेटिक स्ट्रिप वाले कार्डों को पढ़ने के लिए बनाया गया है। रिजर्व बैंक की नई नीति से नेशनल पेमेंट्स कॉर्पोरेशन ऑफ इंडिया की सहायता से एटीएम मशीनों को अपग्रेड करने पर ग्राहक/ बैंकर राहत की सांस ले सकते हैं।

ई-मेल सुरक्षा

बैंक कभी भी आपकी गोपनीय सूचना जानने के लिए मेल नहीं भेजते हैं। यदि आपको कोई मेल प्राप्त होती है जिसमें आपके इंटरनेट बैंकिग विवरण जैसे आपका पिन, पासवर्ड, खाता संख्या आदि पूछे गए हों तो इसका जवाब न दें। **"फिशर्स"** में प्राय: परेशान करने वाली या उत्तेजक (किंतु, झूठी) सूचना होती है जिससे लोग इसका जवाब तुरंत दें। ई-मेल संदेश में ऐसे फार्म न भरें जिसमें निजी वित्तीय जानकारी मांगी गई हो। कभी भी पॉप-अप विंडों में लॉग इन तथा संवेदनशील जानकारियों की प्रविष्टि न करें। अपने यूजर आईडी/ पासवर्ड/ कार्ड नंबर/ सीवीवी आदि को अद्यतन या सत्यापित करने की मांग करने वाले ई-मेल/ एम्बेडेड लिंक पर क्लिक न करें।

डिजिटल हस्ताक्षर का सुरक्षित उपयोग :-

साइबर सुरक्षा से संबंधित बढ़ते जोखिम को ध्यान में रखते हुए साइबर स्पेस में सुरक्षा सुनिश्चित करने हेतु समुचित उपायों की आवश्यकता है। डिजिटल हस्ताक्षर प्रमाणपत्र का प्रयोग करना, एक ऐसा ही उपाय है। इसके प्रयोग करने की प्रक्रिया को उपयुक्त रूप से समझना जरूरी है:

✓ डिजिटल सर्टिफिकेट एक ऐसा इलेक्ट्रॉनिक "पासपोर्ट" है जो एक व्यक्तिगत कम्प्यूटर या संगठन को पब्लिक की- इन्फ्रास्ट्रक्चर (पीकेआई) का उपयोग करते हुए इंटरनेट पर सुरक्षित जानकारी के आदान-प्रदान करने की अनुमति देता है।

- ✓ हस्तलिखित हस्ताक्षर के समान, डिजिटल हस्ताक्षर भी प्रत्येक हस्ताक्षरकर्ता के लिए अलग-अलग है जो प्रमाणन प्राधिकरण नियंत्रक (सीसीए) के तहत लाइसेंस प्रमाणन प्राधिकरण (सीए) द्वारा जारी किए जाते हैं।
- ✓ इलेक्ट्रॉनिक दस्तावेजों के डिजिटल हस्ताक्षर का उद्देश्य प्रमाणिकता, गैर-निराकरण, अखंडता की आवश्यकता को पूरा करना है.
  - यह कि प्राप्तकर्ता, भेजने वाले की पहचान का सत्यापन कर सकता है **(प्रमाणिकता)**
  - यह कि भेजने वाला इस बात से इंकार नहीं कर सकता कि उसने दस्तावेजों पर हस्ताक्षर नहीं किए हैं. **(गैर-निराकरण)**
  - यह कि प्राप्तकर्ता किसी अन्य द्वारा हस्ताक्षित दस्तावेज को परिवर्तित या संशोधित नहीं कर पाएगा.

इस प्रकार के कई पी.के.आई. सक्षम ऐप्लिकेशन हैं जिनके लिए डिजिटल प्रमाणपत्र की आवश्यकता होती है। कुछ पी.के.आई सक्षम ऐप्लिकेशन के उदाहरण निम्नानुसार है :

1) आरटीजीएस (RTGS)
2) एसएफएमएस (SFMS)
3) पीडीओ-एनडीएस (PDO-NDS)
4) एनईएफटी (NEFT)
5) ई-निविदा (E-TENDERING)
6) कंपनी रजिस्ट्रार (ROC)
7) सरसाई (CERSAI)

डिजिटल हस्ताक्षर निम्न के लिए प्रयोग किए जाते हैं:

- ➢ साइबर की दुनिया में अपने आप को प्रमाणित करना.
- ➢ अपने डेटा एवं लेन-देनों को छेड़-छाड़ से बचाना.
- ➢ ऑनलाइन लेन-देनों की कानूनी वैधता सुनिश्चित करना.
- ➢ हस्ताक्षर का सत्यापन करना.
- ➢ **साइबर धोखाधड़ी को कम करना.**

कुशल जोखिम प्रबंधन की आवश्यकता

उन्नत सूचना प्रौद्योगिकी के बढ़ते प्रयोग के मिले-जुले प्रभाव से आधुनिक कंप्यूटरीकृत बैंकिंग कारोबार में जोखिम प्रबंधन के विकास में तेजी आई है। पहले बैंकों के कारोबार के दौरान मुख्यत: साख के संदर्भ में ही जोखिम उठाना पड़ता था। लेकिन अब निवेश बैंकिंग, यूनिवर्सल बैंकिंग आदि के आगमन से बैंकिंग कारोबार में जोखिम की परिधि का काफी ज्यादा फैलाव हो चुका है। कम्प्यूटरीकृत बैंकिंग वातावरण में तीव्र गति से विकास होने के चलते बैंकों में कई नए जोखिमों का सामना करना पड़ता है। सूचना प्रौद्योगिकी की उन्नति के साथ ही आजकल बैंकिंग कारोबार में धोखाधड़ी व जालसाजी के नए-नए तरीके विकसित हो रहे हैं जो साख जोखिम के अतिरिक्त बाज़ार जोखिम व परिचालन जोखिम के कुशल प्रबंध की आवश्यकता की ओर इशारा कर रहे हैं। आंतरिक व बाह्य लेखापरीक्षकों द्वारा प्रस्तुत लेखापरीक्षा रिपोर्टों में कम्प्यूटरीकृत वातावरण में कार्य संबंधी गंभीर विसंगतियों/ चूकों का उल्लेख किया जाता है जिससे कारोबार संबंधी लेनदेन करते समय सुरक्षा का उल्लंघन हो सकता है जिसके परिणामत: बैंक को वितीय जोखिम उठाना पड सकता है। **अत: समय की मांग 'कुशल जोखिम प्रबंधन' है.**

साइबर सुरक्षा के व्यावहारिक सतर्कता पहलू:

डिजिटल बैंकिंग के नए युग में बैंकिंग कार्य को सरल, सुगम एवं साइबर हमले से इसे बचाने व सुरक्षित रखने के लिए निम्न व्यावहारिक सतर्कता पहलूओं को अपनाया जाए:-

1) सबसे पहले अपने आप को शिक्षित करें.
   फिशिंग घोटालों के बारे में जानकारी प्राप्त करें। फिशिंग के तहत हैकर आपकी व्यक्तिगत जानकारी का खुलासा करने के लिए आपको प्रेरित करता है।
2) अपने सिस्टम को अद्यतन रखें तथा सुरक्षित सॉफ्टवेयर का प्रयोग करें।
   सुरक्षा कंट्रोल पैनल पर स्वत: अद्यतन फंक्शन का चयन करें ताकि सुरक्षा सॉफ्टवेयर अद्यतन होते रहें।
3) फायरवॉल का प्रयोग करें.
   फ़र्स्ट स्टेप साइबर हमले से बचाव के लिए फायरवॉल होता है। अत: यह सुनिश्चित करना आवश्यक हो जाता है कि वाई-फाई के मामले में राऊटर के साथ फायरवॉल सक्रिय कर लें।
4) सुरक्षित सर्फिंग करें.
   नकली साइट के प्रयोग से बचें। साइट एडवाइजर सॉफ्टवेयर का प्रयोग करें जो सर्च परिणाम के समय ही बता देता है कि साइट सुरक्षित है या नहीं, क्लिक करने से पूर्व चेतावनी दे देता है।
5) मजबूत पासवर्ड का प्रयोग करें.
6) कॉमन सेंस (Common sense) का प्रयोग करें.
   व्यक्तिगत/ संवेदनशील जानकारी किसी भी साइट/ इंटरनेट पर साझा न करें.
7) सुरक्षित खरीदारी करें एवं सावधानी के साथ क्लिक करें.
   भुगतान के लिए डेबिट कार्ड के बजाय क्रेडिट कार्ड का उपयोग करें.
   - https:// पेज हो, http:// पेज नहीं होना चाहिए.
   - ब्राउजर के दाईं ओर नीचे की तरफ लॉक का चिह्न तथा सत्यापन प्राधिकारियों द्वारा प्रस्तुत प्रमाण पत्र भी देखें.
8) वायरलेस नेटवर्क को सुरक्षित(secure) करें.
   अपने कंप्यूटर पर फायरवॉल सक्रिय करें तथा इस प्रकार राउटर को स्थापित करें जिससे किसी को एन्क्रिप्टेड पासवर्ड (Encrypted Password) के साथ ही उपयोग की अनुमति प्रदान करें.
9) जागरूक व सतर्क रहें.
   अपने बिल का ब्यौरा हर माह जांच करें। किसी भी कोरे क्रेडिट कार्ड रसीद पर हस्ताक्षर न करें। अपने कार्ड की जानकारी देने से बचें। उन सभी चीजों के टुकड़े कर दें जिन पर क्रेडिट कार्ड की संख्या दर्ज हो। कार्ड के गुम एवं चोरी होने की तत्काल सूचना दें।
10) नियमित रूप से डेटा का बैक-अप लेते रहें।
    समय-समय पर अपने खातों एवं क्रेडिट रिपोर्ट की जांच करते रहें।

निष्कर्ष

आज के दौर में सभी बैंकों के सामने धोखाधड़ी, जोखिम प्रबंधन एवं उनकी रोकथाम एक ज्वलंत समस्या है। ग्राहक अपने धन का विशेष ध्यान रखते हुए इन सेवाओं को हैकिंग/ वायरस प्रूफ बनाना चाहिए। सजग रहना हर ग्राहक के हित में है। यह जरूरी है कि ग्राहकों को बैंकिंग प्रौद्योगिकी का सुरक्षित इस्तेमाल करना सिखाया जाए। सूचना-सुरक्षा आज की जरूरत है। किसी भी प्रणाली की सुरक्षा तभी मजबूत होगी जब उसकी सूचना-सुरक्षा पुख्ता और मजबूत हो। इस संबंध में निरंतर जांच, प्रशिक्षण, निरीक्षण और समय-समय पर उसकी मरम्मत

जरूरी है। सूचना-सुरक्षा की आवश्यकता से इंकार नहीं किया जा सकता, लेकिन यह एक निरंतर प्रक्रिया है। इसके लिए समय-समय पर आकलन, जांच एवं समीक्षा किए जाने की आवश्यकता होती है ताकि सूचना को अनधिकृत घुसपैठ/ पहुंच/ संशोधन/ विघटन/ व्यवधान से बचाया जा सके। कभी न समाप्त होने वाली इस प्रक्रिया को सक्रिय एवं उद्देश्यपरक बनाए जाने के लिए यह आवश्यक है कि समय-समय पर इसके लिए प्रशिक्षण कार्यक्रम चलाए जाएं जिनमें सूचना-सुरक्षा को मजबूत एवं अभेद्य बनाए रखने संबंधी जानकारी संबंधित व्यक्तियों/ ग्राहकों/ कर्मचारियों को दी जाए। अत: ऑन दी जॉब ट्रेनिंग (On the Job Training) क्लास रूम ट्रेनिंग (Class Room Training) से ज्यादा कारगर सिद्ध हो सकता है। अत: कंप्यूटरीकृत बैंकिंग वातावरण में सूचना प्रौद्योगिकी एवं सूचना सुरक्षा समय की मांग एवं आवश्यकता है। सूचना सुरक्षा संबंधी नीति को अपनाते हुए कंप्यूटरीकृत बैंकिंग/ डिजिटल बैंकिंग वातावरण से संबंधित प्रौद्योगिकी जोखिम को आसानी से सतर्क रहकर निपटाया जा सकता है।

*****

कृष्ण कुमार

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- केनरा बैंक
मोबाइल नं. :- 9416284380
ई-मेल:- krishankumar2@canarabank.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

बैंकिंग क्षेत्र को अर्थव्यवस्था की रीढ़ माना जाता है। हम अपने दैनिक व्यावसायिक लेन-देन का संचालन करने के लिए नकदी, चेक और ड्राफ्ट का उपयोग करते हैं। हालांकि, इस पैटर्न ने डेबिट या क्रेडिट कार्ड स्वाइप करने के आधार पर एक नई भुगतान प्रणाली का मार्ग प्रशस्त किया है। नरसिम्हन समिति (1991-1998) जो वित्तीय मामलों पर सिफारिश के पक्ष में थी, ने सुझाव दिया कि आईटी का उपयोग बैंकिंग क्षेत्र में भी किया जाएगा ताकि इसे कामकाज में अधिक कुशल बनाया जा सके।

बैंकिंग उद्योग में साइबर अपराध : -

साइबर अपराध शब्द कंप्यूटर पर या इंटरनेट पर की जाने वाली किसी भी आपराधिक गतिविधि को संदर्भित करता है। दूसरे शब्दों में, डिजिटल कदाचार को साइबर अपराध के रूप में संदर्भित किया जाता है जहां अपराधी कंप्यूटर या किसी भी अन्य इलेक्ट्रॉनिक उपकरणों और इंटरनेट का उपयोग करके अनधिकृत पहुंच के माध्यम से धन अंतरण और निकासी जैसे कई गलत कामों को अंजाम देता है। आज की वैश्वीकृत दुनिया में परिदृश्य को संकीर्ण करने के लिए, बैंकिंग उद्योग अपने ग्राहकों और उपभोक्ताओं को कई डिजिटल सेवाएं प्रदान करता है, जैसे कि ऑनलाइन बैंकिंग और क्रेडिट कार्ड सेवाएं, डेबिट कार्ड के साथ ऑनलाइन भुगतान आदि। ग्राहक दिन में 24 घंटे सभी प्रकार की बैंक सुविधाओं का उपयोग कर सकते हैं और वे इंटरनेट और सेल फोन का उपयोग करके दुनिया में कहीं से भी आसानी से अपने खातों मे लेन-देन कर सकते हैं। जैसा कि हम सभी जानते हैं, ये सेवाएं ग्राहकों के लिए उपयोगी हैं, लेकिन इसका एक नकारात्मक पक्ष भी हैं, जिसमें हैकिंग और साइबर डकैती शामिल हैं। वे बैंकिंग वेबसाइटों और ग्राहकों के खातों में सेंध लगाकर, खातों में गड़बड़ी पैदा करके और ग्राहकों के खातों से पैसे की चोरी करके उन सेवाओं का लाभ उठाते हैं, इसका सबसे अच्छा उदाहरण था "जिसमें एक हैकर ने प्रत्येक खाते से एक रुपया लिया, लेकिन उस एक रुपये से एक बड़ी राशि प्राप्त की।

1. **साइबर अपराधों का प्रभाव: -**

बैंकिंग में साइबर अपराधों के परिणाम अत्यंत गंभीर एवं दीर्घकालिक होते हैं। इन साइबर हमलों के परिणाम निम्नलिखित रूप में हमारे सामने आते हैं : -

i. वित्तीय नुकसान
ii. गोपनीय जानकारी प्रकट होना
iii. कानूनी दुष्परिणाम
iv. पहचानने - योग्य जानकारी की चोरी और उसके उपयोग में अवरोध उत्पन्न करना
v. प्रतिष्ठा- जोखिम का खतरा
vi. परिचालन-जोखिम

2. साइबर अपराधों के कारण: -

साइबर अपराधों के अनेक कारण हैं, जिनमें से कुछ निम्नानुसार हैं :-

i. **डेटा तक आसान पहुंच:** एक बार जब कोई साइबर अपराधी कंप्यूटर सिस्टम में पहुंच प्राप्त करने में सक्षम हो जाता है, तो उनकी ग्राहकों के निजी वित्तीय जानकारी सहित व्यक्तिगत डेटा तक पहुंच हो सकती है, जिसे एक छोटे से रिमूवेबल डिवाइस में कॉपी या स्थानांतरित किया जा सकता है। चूंकि सूचना प्रौद्योगिकी बैंकों, व्यक्तियों, निगमों, सरकारी एजेंसियों आदि के संचालन को शक्ति देती है, इसलिए उनके कंप्यूटर पर संसाधित गोपनीय डेटा और जानकारी का असुरक्षित भंडारण एक गंभीर खतरा पैदा करता है।

ii. **उपयोगकर्ता की लापरवाही:** कंप्यूटर सिस्टम का उपयोग करने वाले सभी अधिकारियों को कंप्यूटर में संग्रहीत अपने गोपनीय डेटा और जानकारी की सुरक्षा के लिए बहुत सावधान और सतर्क रहना चाहिए। पासवर्ड और व्यक्तिगत पहचान संख्या (पिन) के उचित उपयोग के माध्यम से वे पहुंच को सीमित कर सकते हैं। उनकी ओर से कोई भी लापरवाही साइबर अपराधियों को कुछ उपकरणों और रिकॉर्ड तक आसान पहुंच प्रदान कर सकती है।

iii. **संगठनों और बैंकों में आंतरिक नियंत्रण की कमी:** बैंक अपनी दिन-प्रतिदिन की गतिविधियों के लिए विभिन्न प्रकार के ऑपरेटिंग सिस्टम का उपयोग करते हैं; इसलिए बैंकों को यह सुनिश्चित करना चाहिए कि उनके पास आंतरिक नियंत्रण और आईटी ऑडिट सिस्टम मौजूदा हैं। अन्यथा इसके परिणामस्वरूप अक्षम सॉफ़्टवेयर और हार्डवेयर सिस्टम की उपलब्धता के कारण कंप्यूटरीकृत सुरक्षा में चूक हो सकती है।

बैंकिंग क्षेत्र से जुड़े साइबर अपराधों के प्रकार निम्नानुसार हैं :-

i. **हैकिंग:-** हैकिंग एक साइबर क्राइम है जिसमें एक व्यक्ति को सिस्टम तक अवैध पहुंच प्राप्त करना या ग्राहकों के खातों या बैंकिंग साइटों में हैकिंग करके सुरक्षा तंत्र को दरकिनार करने का प्रयास करना शामिल है।

ii. **की लॉगिंग:-** इसे 'keystroke logging या keyboard captureing' के रूप में जाना जाता है। यह कीबोर्ड पर दबाई गई चाबियों को गुप्त रूप से रिकॉर्ड करने (लॉगिंग) की प्रक्रिया है ताकि इसका उपयोग करने वाला व्यक्ति इस बात से अनजान हो कि उनकी गतिविधियों को ट्रैक किया जा रहा है और ये बैंकिंग विवरण आदि जैसी गोपनीय जानकारी चुराने के लिए अविश्वसनीय रूप से हानिकारक हैं।

iii. **वायरस:-** एक प्रकार का स्व-प्रतिकृति प्रोग्राम है जो निष्पादन योग्य कोड या दस्तावेजों को स्वयं की प्रतियां सम्मिलित करके संक्रमित करता है। वायरस एक प्रोग्राम है जो एक निष्पादन योग्य फ़ाइल को संक्रमित करता है और संक्रमण के बाद फाइल को असामान्य रूप से व्यवहार करने का कारण बनता है। यह प्रोग्राम फाइलों और ऑपरेटिंग सिस्टम जैसी निष्पादन योग्य फाइलों से खुद को जोड़कर फैलता है। निष्पादन योग्य फाइल लोड करने के परिणामस्वरूप वायरस की नई प्रतियां बनाई जा सकती हैं।

iv. **स्पाईवेयर:-** स्पाईवेयर ऑनलाइन बैंकिंग क्रेडेंशियल्स चोरी करने और धोखाधड़ी के उद्देश्यों के लिए उनका उपयोग करने का सबसे आम तरीका है। स्पाइवेयर कंप्यूटर और वेबसाइटों के बीच जानकारी एकत्र करने या प्रसारित करके संचालित होता है। यह ज्यादातर फर्जी 'पॉप अप' विज्ञापनों द्वारा सॉफ्टवेयर डाउनलोड करने के लिए स्थापित किया गया है। मानक एंटीवायरस मुख्य रूप से पीसी को संक्रमित करने से पहले डाउनलोड और इंस्टॉलेशन को अवरुद्ध करके, इस प्रकार के सॉफ्टवेयर का पता लगाते हैं और उन्हें हटा देते हैं।

v. **फिशिंग-** फिशिंग एक प्रकार की धोखाधड़ी है जिसमें डेबिट / क्रेडिट कार्ड नंबर ग्राहक आईडी, आईपीआईएन, सीवीवी नंबर, कार्ड समाप्ति की तारीख और इसी तरह की निजी जानकारी ई-मेल के माध्यम से चोरी हो जाती है जो वास्तविक स्रोत से प्रतीत होती है। फिशिंग को त्वरित संदेश और ई-मेल

स्पूफिंग के उपयोग के माध्यम से पूरा किया जाता है। इस प्रकार के अपराध में, धोखेबाज़ बैंकों के अधिकारियों की तरह कार्य करते हैं और वे एक सीधा लिंक बनाते हैं जो लक्षित ग्राहकों को एक नकली पृष्ठ पर निर्देशित करता है, जो वास्तविक बैंक वेबसाइट के समान दिखता है। तब अधिग्रहीत गोपनीय जानकारी का उपयोग ग्राहक के खाते पर धोखाधड़ी लेन-देन करने के लिए किया जाता है। फिशर इन दिनों इस तरह के अपराधों को अंजाम देने के लिए एसएमएस (स्मिशिंग) और मोबाइल (वॉयस फिशिंग) का भी उपयोग करते हैं।

vi. **फार्मिंग**–फार्मिंग इंटरनेट के माध्यम से की जाती है। जब कोई ग्राहक बैंक की वेबसाइट पर लॉग इन करता है, तो हमलावर यूआरएल को इस तरह से हाइजैक करते हैं कि उन्हें किसी अन्य वेबसाइट पर भेजा जाता है, जो झूठी है लेकिन बैंक की मूल वेबसाइट की तरह दिखाई देती है।

vii. **एटीएम स्कीमिंग और पॉइंट ऑफ सेल क्राइम**:- स्कीमिंग डिवाइस के लिए एक असली कीपैड या एक ऐसी डिवाइस का इस्तेमाल किया जाता है जो कार्ड रीडर के साथ एक मशीन के एक हिस्से के रूप में दिखाई देती है। इसे एटीएम मशीनों या पीओएस सिस्टम से धोखाधड़ी करने के लिए बनाया जाता है। सीधे क्रेडिट कार्ड डेटा चुराने वाले मैलवेयर को भी इन उपकरणों पर स्थापित किया जा सकता है। एटीएम मशीनों में सफलतापूर्वक स्थापित किए गए स्किमर व्यक्तिगत पहचान संख्या (पिन) कोड और कार्ड नंबर चुरा लेते हैं, जिन्हें फिर धोखाधड़ीपूर्ण लेन-देन के लिए इस्तेमाल किया जाता है।

viii. **मैलवेयर आधारित हमले**:- इलेक्ट्रॉनिक बैंकिंग सेवाओं के लिए सबसे खतरनाक साइबर खतरों में से एक मैलवेयर-आधारित हमले हैं। ऐसे हमलों में एक दुर्भावनापूर्ण कोड बनाया जाता है। बैंकिंग इंडस्ट्री में इन दिनों मालवेयर अटैक की संख्या बढ़ रही है। ज़ीउस, Spyeye, Carbep, KINS, और Tinba, सबसे प्रसिद्ध बैंकिंग मैलवेयर में से कुछ हैं। लगभग हर वायरस की दो विशेषताएं होती हैं: एक, यह सिस्टम में बैकडोर से एंट्री करता है, और दूसरा, यह उपयोगकर्ता की क्रेडेंशियल जानकारी चुराता है।

साइबर अपराध को रोकने के तरीके :-

बैंकिंग उद्योग में साइबर अपराधों में बेतहाशा वृद्धि हुई है जिसके परिणामस्वरूप महत्वपूर्ण आर्थिक नुकसान हुआ है। जैसा कि हम सभी जानते हैं कि बैंकिंग हमारी अर्थव्यवस्था का सबसे महत्वपूर्ण मुख्य आधार है, इसलिए इसे साइबर हमलों से रोका जाना चाहिए। इसमें शामिल जोखिम और साइबर हमले से निपटने के लिए सुरक्षा उपायों के बारे में बैंकों और ग्राहकों को जागरूक किया जाना चाहिए। साइबर सुरक्षा नीति के सभी मामलों के प्रभावी कार्यान्वयन के लिए, सरकार ने नोडल एजेंसी के रूप में राष्ट्रीय सुरक्षा परिषद के साथ एक "अंतर-विभागीय सूचना सुरक्षा टास्क फोर्स (आईएसटीएफ)" की स्थापना की है। राष्ट्रीय नोडल एजेंसी 'भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन)' है जिसे कंप्यूटर सुरक्षा की घटनाओं की जांच करने का काम सौंपा गया है।

साइबर अपराध के सुरक्षात्मक उपाय:

1. उपयोग करने से पहले साइट डोमेन आईडी की जांच करें। हमेशा प्रामाणिक साइट का उपयोग करें।
2. https:// मे 's' चेक करें, हरा और पैड लॉक साइन देखें, यह इंगित करता है कि वेबसाइट हैकर से बचाने के लिए सुरक्षित है।
3. किसी भी अनौपचारिक लिंक, जो ओटीपी/ बैंक विवरण मांगता है, पर क्लिक न करें क्योंकि बैंक कभी भी यह जानकारियां साझा करने के लिए नहीं कहता है।
4. फर्जी योजनाओं से सावधान रहें। केवल उन्हीं वेबसाइट का उपयोग करें जिन की प्रामाणिकता स्थापित की गई है।

5. ऑपरेटिंग सिस्टम को उसके नवीनतम संस्करण में नियमित रूप में अपडेट करें। किसी भी प्रतिष्ठित प्रदाता के सुरक्षा सॉफ्टवेयर का उपयोग करें और इसे नियमित अंतराल पर अपडेट करें।
6. नियमित अंतराल पर पासवर्ड बदलें।
7. हैकर्स तक आसान पहुंच प्रदान करने के लिए अपनी सारी जानकारी सार्वजनिक डोमेन पर साझा ना करें।
8. किसी भी अनधिकृत लेन-देन की तुरंत रिपोर्ट करें।
9. बैंक और साइबर सेल को और अधिक नुकसान होने से बचाने के लिए डोमेन विवरण देखने हेतु whois.com जैसे खोज इंजन का उपयोग करें।
10. दो स्तरीय प्रमाणीकरण का उपयोग करना सुनिश्चित करें और देखें की पासवर्ड अनुमान लगाने वाले हमलों से कैसे बचा जाए।
11. नियंत्रण पहुंच :सुनिश्चित करें कि व्यक्ति केवल उन्हीं डेटा और सेवाओं तक पहुंच सकते हैं जिसके लिए वह अधिकृत हैं।
12. अनधिकृत उपयोगकर्ताओं तक पहुंच को प्रतिबंधित करें।
13. आवेदन नियंत्रण के माध्यम से डेटा या सेवाओं तक पहुंच को सीमित करें।
14. जो भी जानकारी सिस्टम से नकल कर स्टोरेज डिवाइस में सहेजा जा सकता है, उसे प्रतिबंधित करें।
15. ई-मेल अटैचमेंट भेजने और प्राप्त करने को सीमित करें।
16. जब आपको अपने कार्य संबंधी कर्तव्यों का निर्वहन करने की आवश्यकता होती है तो नेटवर्क से कनेक्ट करने के लिए हमारे वीपीएन का उपयोग करें।
17. कार्यस्थल पर केवल अपने कंप्यूटर पर कार्य करें और अपने घर के कंप्यूटर या व्यक्तिगत उपकरणों के साथ कार्य संबंधी डेटा और जानकारी साझा न करें।
18. सुनिश्चित करें कि आपके कंप्यूटर में नवीनतम अनुप्रयोग, ऑपरेटिंग सिस्टम, नेटवर्क टूल और आंतरिक सॉफ्टवेयर स्थापित हैं।
19. अपने कंप्यूटर पर मैलवेयर सुरक्षा और anti-spam सॉफ्टवेयर को अक्षम न करें।
20. जानकारी साझा करने के बारे में हमारी नीतियों का पालन करें। केवल स्वीकृत क्लाउड- शेयरिंग टूल का उपयोग करें। यदि आप इस संबंध में किसी भी बात से पूरी संतुष्ट नहीं है तो अवश्य पूछें।
21. अपने पासवर्ड को सुरक्षित करें, जहां आप उन्हें दर्ज करते हैं, उस पर ध्यान दें और कई सिस्टम का एक ही पासवर्ड पुन: उपयोग न करें।
22. आवश्यक साइबर सुरक्षा सर्वोत्तम प्रथा को याद रखें। सभी अवांछित ई-मेल, पाठ संदेश, सोशल मीडिया चैट और अटैचमेंट से सतर्क रहें। संदेह होने पर, क्लिक न करें।
23. सभी मोबाइल उपकरणों पर ब्लूटूथ auto-discovery बंद करें।
24. कभी भी ऐसे सार्वजनिक वाई-फाई नेटवर्क से कनेक्ट न करें जो पासवर्ड सुरक्षित न हो।
25. यहां तक कि जब आप घर पर कार्य कर रहे हों -अपने लैपटॉप को अनलॉक और उपेक्षित न छोड़ें, किसी भी मुद्रित दस्तावेजों को सुरक्षित रूप में स्टोर करें (उन्हें अपनी डेस्क पर न छोड़ें) और हमेशा जागरूक रहें।

निष्कर्ष :-

निष्कर्षत: कहा जा सकता है कि साइबर अपराध इस तकनीकी युग की सर्वाधिक महत्वपूर्ण सुरक्षा संबंधी चिंताओं में से एक है। साइबर सुरक्षा के प्रति हमें सतत रूप से जागरूक रहने के साथ-साथ साइबर सुरक्षा के लिए निर्धारित मानकों का कड़ाई से अनुपालन करने की आवश्यकता है। साइबर अपराधों के तरीकों और उनसे बचने के उपायों के बारे में लोगों को शिक्षित करके साइबर अपराधों से बचा जा सकता है।

*****

गुलशन पंवार

पदनाम:- लिपिक
संस्था का नाम:- केनरा बैंक
मोबाइल नं. :- 7888462508
ई-मेल:- gulshanpanwar261@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

बैंकिंग को किसी भी देश की अर्थव्यवस्था की रीढ़ की हड्डी कहा जाता है। इक्कीसवीं सदी को इंटरनेट का युग कहा जाये तो इसमें कोई अतिश्योक्ति नहीं होगी। दुनिया की लगभग 466 करोड़ आबादी इंटरनेट का उपयोग करती है। इसमें भी 432 करोड़ लोग केवल मोबाइल के द्वारा ही इंटरनेट का उपयोग करते हैं, दुनिया की इतनी अधिक आबादी इंटरनेट का उपयोग करती है। बैंको का डिजिटलीकरण भी काफी तेजी से बढ़ रहा है। अत: कई षडयन्त्रकारी एवं धोखेबाज लोग इसका दुरूपयोग करते हैं जैसे कि निजी जानकारी चुराकर दूसरों के बैंक खातों से पैसे निकालना, क्रेडिट कार्ड की जानकारी चोरी करना आदि। बैंकिंग उद्योग बहुत पुराना है और उदारीकरण के बाद से इस उद्योग में कई बदलाव लाए गए हैं। बैंकिंग प्रणाली अच्छी तरह से विनियमित और पर्यवेक्षित है, इसमें नैतिक अभ्यास, वित्तीय संकट और कंपनी शासन शामिल हैं। VMware कार्बन ब्लैक संस्था की रिपोर्ट के अनुसार, फरवरी 2020 और अप्रैल 2020 के बीच COVID-19 संकट के बीच वैश्विक स्तर पर बैंकों और वित्तीय संस्थानों के खिलाफ साइबर हमले में 238 प्रतिशत की वृद्धि हुई।

बैंकिंग में साइबर अपराध एवं उनके स्वरूप :-

साइबर अपराध पर उपलब्ध आंकड़ों से पता लगता है कि दुनिया भर में साइबर अपराध में बढ़ोत्तरी हो रही है। बैंकिंग क्षेत्र में, विभिन्न खातों में अवैध रूप से धन निकालने या स्थानांतरित करने के लिए ऑनलाइन तकनीकों का उपयोग करने वाले अपराधों को बैंकिंग धोखाधड़ी के रूप में चिह्नित किया जाता है। डिजिटल उल्लंघनों को कई रूपों में व्यवस्थित रूप से वर्गीकृत किया जा सकता है जैसे कि -डिजिटल उत्पीड़न, प्रोग्रामिंग डकैती, थोक धोखाधड़ी, ई-मेल स्पैम, ऑनलाइन डकैती। साइबर अपराधों ने विभिन्न उद्योगों को प्रभावित किया है और बैंकिंग क्षेत्र उनमें से एक है जिसने एटीएम धोखाधड़ी, फ़िशिंग, पहचान की चोरी, सेवा से इनकार जैसे साइबर अपराधों के विभिन्न रूपों को देखा है। टेक्नोलॉजी ने कॉरपोरेट गवर्नेंस और राज्य प्रशासन से लेकर छोटी दुकानों, जो हम अपने आस-पास देखते हैं, तक अपना प्रभाव बनाया है।

बैंकिंग में साइबर अपराध के विभिन्न स्वरूप निम्नलिखित हैं:-

1. **फ़िशिंग** एक प्रकार का ई-मेल हमला है जिसमें हमलावर किसी संबंधित विश्वसनीय संगठन से होने का इरादा करके इलेक्ट्रॉनिक संचार के माध्यम से उपयोगकर्ताओं की संवेदनशील जानकारी को धोखाधड़ी के तरीके से खोजने का प्रयास करता है। हमलावर किसी समूह को लक्षित करने के लिए ई-मेल को सावधानीपूर्वक डिज़ाइन करते हैं और लिंक पर क्लिक करने से कंप्यूटर पर दुर्भावनापूर्ण कोड इंस्टॉल हो जाता है। जैसे कि इंटरनेट बैंकिंग धोखाधड़ी एक धोखाधड़ी या चोरी है जो किसी बैंक खाते से अवैध रूप से धन निकालने और/या किसी भिन्न बैंक के खाते में धन अंतरित करने के लिए ऑनलाइन तकनीक का

उपयोग करके की जाती है। इंटरनेट बैंकिंग धोखाधड़ी पहचान की चोरी का एक रूप है और इसे आमतौर पर फ़िशिंग जैसी तकनीकों के माध्यम से संभव बनाया जाता है

2. **विशिंग** एक प्रकार का साइबर हमला है जिसमें वॉयस कम्युनिकेशन का उपयोग लोगों के समूह से गोपनीय डेटा चोरी करने के लिए किया जाता है। विशिंग में, हमलावर संबंधित और विश्वसनीय फर्म का कर्मचारी होने का नाटक करते हुए वॉयस कॉल के माध्यम से संवेदनशील जानकारी देने के लिए लक्ष्य को चकमा देता है। जैसे की OTP या PIN की जानकारी एकत्रित करना।
3. **हैकिंग**: यह किसी भी जानकारी को देखने के लिए सिस्टम तक एक गैरकानूनी पहुंच है।
4. **स्पैमिंग** एक अवांछित संदेश (स्पैम), विशेष रूप से विज्ञापन भेजने के साथ-साथ एक ही साइट पर बार-बार संदेश भेजने के लिए मैसेजिंग सिस्टम का उपयोग है।
5. **स्किमिंग**: यह कीपैड पर एक गैजेट पेश करके एटीएम मशीन या पीओएस को ट्रैक करने का सबसे विकसित तरीका है जो एक ही चीज़ की प्रतिलिपि बनाता है। एटीएम मशीनों के माध्यम से स्किमर्स का प्रभावी निष्पादन कार्ड नंबर और व्यक्तिगत जानकारी एकत्र करता है जिसे बाद में नकली लेन-देन करने के लिए दोहराया जाता है।
6. **क्रेडिट कार्ड फ्रॉड**:- क्रेडिट कार्ड धोखाधड़ी का अपराध वह होता है जब कोई व्यक्ति या तो क्रेडिट या डेबिट कार्ड चुरा लेता है, या कार्ड नंबर और कार्ड के सफलतापूर्वक उपयोग के लिए आवश्यक अन्य खाता जानकारी धोखाधड़ी से प्राप्त करता है जबकि क्रेडिट कार्ड की वास्तविक भौतिक चोरी होती है, आधुनिक तकनीक से इलेक्ट्रॉनिक रूप से खाते की जानकारी को घात लगाने वाली घटनाओं में भारी वृद्धि देखी है। खाते के स्वामी, जिस व्यापारी से कार्ड की जानकारी चोरी या इंटरसेप्ट की गई थी, वह और यहां तक कि कार्ड जारीकर्ता भी समझौते से अनजान हो सकता है जब तक कि जानकारी वास्तव में खरीदारी करने के लिए उपयोग नहीं की जाती है।
7. **ई- मनी लॉन्डरिंग** :- यह कोई नई अवधारणा नहीं है, बल्कि यह तो मनी लॉन्ड्रिंग के "गैर आमने सामने के (Non Face-to-Face) लेन-देन के रूप में या वायर ट्रान्सफर प्रणाली का उपयोग करके अपराधिक लाभों को धनशोधन करने की प्रक्रिया है।
8. **DOS Attack**:- इस हमले का उपयोग कर हैकर द्वारा किसी नेटवर्क या मशीन को उस इस्तेमाल करने वाले उपयोगकर्ता के लिए अनुपलब्ध करा दिया जाता है। इस हमले का मुख्य उदेश्य किसी इन्टरनेट उपयोगकर्ता को इन्टरनेट की पहुंच से दूर रखना। DOS हमले में हैकर नेटवर्क या मशीन को ओवरलोड कर देता है जिससे उपयोगकर्ता उस साइट पर नही पहुंच पाता है। एक DOS हमला बैंक के डेटा या लेन-देन प्रणाली केवल नेटवर्क को खतरे में नहीं डालेगा, बल्कि बैंकों की लोकाभिमुख वेबसाइटों और पोर्टलों को अस्थायी रूप से अक्षम कर देगा।
9. **मालवेयर** शब्द का तात्पर्य ऐसे सॉफ्टवेयर से है जो उपकरणों को नुकसान पहुंचाता है, डेटा चुराता है और अराजकता का कारण बनता है। मालवेयर कई प्रकार (वायरस, ट्रोजन, स्पाईवेयर, रैंसमवेयर) के होते हैं और ये विभिन्न प्रकार से बैंको को नुकसान पहुंचाते हैं।

   जेसे कि -रैनसमवेयर, एक प्रकार का मालवेयर है जो उपयोगकर्ताओं को उनके सिस्टम या व्यक्तिगत फाइलों तक पहुंचने से रोकता है और पहुंच प्राप्त करने के लिए फिरौती के भुगतान की मांग करता है। रैंसमवेयर: ये रैंसमवेयर हमले मुख्य रूप से छोटे बैंकों को प्रभावित करते हैं क्योंकि उनके पास आईटी संसाधनों, पुरानी सुरक्षा तकनीक और साइबर सुरक्षा पर प्रोटोकॉल की कमी है।
10. **पहचान की चोरी**- यह अपराध काफी ज्यादा देखने को मिलता है। आज कल समाचारपत्रों में आप पढ़ते होंगे कि आज कल लोग बैंक जाने की अपेक्षा ऑनलाइन ट्रांजेक्शन करते हैं जिसमें आप किसी ट्रांजेक्शन ऐप या बैंको की ऑनलाइन सर्विस का उपयोग करते हैं। ऐसे क्राइम में, साइबर अपराधी कोई न कोई गैर

कानूनी तरीके (जो ऊपर बिंदु 1 से 9 में दिए गये हैं) से ऑनलाइन आपका पर्सनल डेटा जैसे आपके लेन-देन प्लेटफार्म का लॉग-इन ID या पासवर्ड, व्यक्तिगत जानकारी, इन्टरनेट बैंकिंग डिटेल्स, क्रेडिट कार्ड/डेबिट कार्ड डिटेल्स चुरा लेता है।

बैंको में साइबर हमलों से बचने के सुरक्षात्मक उपाय:-

1. बैंकों को साइबर हमलों से निपटने के लिए अपने कर्मचारियों को तैयार करने हेतु एक व्यापक प्रशिक्षण मॉड्यूल अपनाने की आवश्यकता है। साइबर सुरक्षा पेशेवर बैंकरों हेतु डेटा सुरक्षा के सभी पहलुओं को कवर करके उन्हें अप-टू-डेट रखते हुए अपनी साइबर-जागरूकता की प्रासंगिक जानकारी और परीक्षणों में अपने कौशल को बढ़ाने के लिए साइबर सुरक्षा प्रशिक्षण आवश्यक है।
2. ऐप्लीकेशन और सिस्टम को नियमित रूप से अद्यतन करना चाहिए।
3. सिस्टम में फायरवाल इनस्टॉल करें तथा अपने सिस्टम तक पहुंच को नियंत्रित करें।
4. अपने पासवर्ड को सुरक्षित रखें एवं किसी के साथ साझा न करें तथा नियमित अन्तराल के बाद इसे बदलते रहें। **("क्रिस पिरिलो के अनुसार "पासवर्ड एक अंत:वस्त्र की तरह होता है, इसे किसी को देखने न दें एवं नियमित रूप से बदलते रहें, इसे किसी के साथ साझा न करें।")**
5. एंटीवायरस का उपयोग करें एवं इसको समय-समय पर अद्यतन करते रहें एवं वाईफाई-सुरक्षा सुनिश्चित करें।
6. इंटरनेट का उपयोग किसी सुरक्षित ब्राउजर से करें जो कि एनक्रिप्टेड हो, जेसे की HTTPS इत्यादि।
7. अपने डेटा का उचित प्रबंधन करना और अपने डेटा का बैकअप सुनिश्चित करें। (जैसे बैकअप बीसी – डीरपी में बहुत मददगार होता है।)
8. स्पैम मेल खोलकर न देखें एवं इन्हें तुरंत डिलीट कर दें और स्पैम फ़िल्टर का उपयोग करें। ललचाने वाले अज्ञात विज्ञापनों पर क्लिक न करें।
9. साइबर अपराध करने वाले लोगों के लिए क़ानूनी सजा या भारी जुर्माना लगाने का प्रावधान किया जाए। क्लाउड सुरक्षा का आकलन करें, अपने क्लाउड इन्फ्रास्ट्रक्चर की अक्सर समीक्षा करें ताकि यह सुनिश्चित हो सके कि यह अद्यतित है। अपनी क्लाउड सुरक्षा की वर्तमान स्थिति, सर्वोत्तम प्रथाओं और अनुपालन मानकों का आकलन करें। क्लाउड प्लेटफॉर्म और इंफ्रास्ट्रक्चर को सुरक्षित करने के लिए मल्टीफैक्टर ऑथेंटिकेशन का इस्तेमाल किया जा सकता है तथा क्लाउड सुरक्षा की निगरानी करें।
10. दो-तरफा या बहु-कारक प्रमाणीकरण:- हैकर्स को बैंक खाते में झांकने से दूर रखने के लिए उपयोगकर्ता को दो-तरफा या बहु-कारक प्रमाणीकरण का उपयोग करना चाहिए। इस तरह के कृत्यों के खिलाफ एक प्रभावी रक्षा रणनीति के रूप में बहु-कारक प्रमाणीकरण तकनीक का उपयोग किया जाता है।
11. स्व-जागरूकता:- बैंको में साइबर अपराधों को रोकने का सबसे महत्वपूर्ण उपाय है - स्वयं की जागरूकता। यह जागरूकता बैंक के कर्मचारियों के साथ-साथ बैंक के उपभोक्ताओं के लिए भी अतिआवश्यक हैं। बैंक के कर्मचारियों को यह जागरूकता विभिन्न परिपत्रों, समय-समय पर प्रशिक्षण देकर और बैंक के उपभोक्ताओं को सोशल मीडिया, टीवी पर प्रसारित विज्ञापन, रेडियो एवं बैंकों तथा भारतीय रिज़र्व बैंक द्वारा बताये गये दिशा निर्देशों का पालन कर के साइबर अपराधों से सुरक्षित रहने हेतु जागरूक करें।

बैंक साइबर अपराध के प्रति इतने संवेदनशील क्यों हैं?

इसका उत्तर सरल है, साइबर अपराधी वहीं जाते हैं जहां पैसा होता है, और बैंकों के पास अन्य संगठनों की तुलना में अधिक पैसा होता है।

बैंक में साइबर अपराध एक भयंकर खतरे के रूप में सम्पूर्ण विश्व में अपने पैर पसार रहा है। साइबर अपराध के संबंध में जागरुक करने के लिए किसी न किसी तरह ज्ञान देना। प्रौद्योगिकी ने साइबर अपराध को पारंपरिक

गतिविधियों की तुलना में अपराधी के लिए अधिक फायदेमंद और कम जोखिम भरा बना दिया है। बैंक को एक बुनियादी ढांचे द्वारा अपने नेटवर्क और सुरक्षा टीमों को समय-समय पर सुरक्षा घटनाओं पर प्रतिक्रिया करने की अनुमति देनी चाहिये और विकासशील साइबर से बचाने के लिये एक समान सिस्टम रख-रखाव, कॉन्फिगरेशन और सॉफ्टवेयर पैचिंग प्रदान करनी चाहिए।

डिजिटल बैंकिंग में प्रौद्योगिकी की गति के साथ खतरा विकसित हो रहा है। एक ठोस साइबर सुरक्षा अभ्यास के रूप में, बैंकों एवं वित्तीय संस्थानों को नियमित अंतराल पर साइबर सुरक्षा अभ्यास के रूप में विभिन्न प्रकार की साइबर सुरक्षा उल्लंघन स्थितियों का अनुकरण करना चाहिए। इससे संगठनों को साइबर सुरक्षा क्षेत्र में चुनौतियों का सामना करने और उनका मुकाबला करने के लिए तैयार होने में मदद मिलेगी। इसके अतिरिक्त, संगठनों को कुछ सुरक्षा उल्लंघनों पर जोर देना चाहिए जो अतीत में उचित एंड-टू-एंड विश्लेषण के साथ हुए थे और सुरक्षा उल्लंघनों के अपने डेटाबेस का निर्माण करते रहें। प्रत्येक उल्लंघन का उचित विश्लेषण कार्रवाई करने के लिए अंतर्दृष्टि प्रदान करेगा। जबकि आरबीआई और सरकार बैंको के साइबर हमलों से लड़ने के लिए सक्रिय कदम उठा रहे हैं, वे क्रिप्टोकरेंसी और ब्लॉकचेन जैसी नई प्रौद्योगिकी प्रवृत्तियों के साथ भी विकसित हो रहे हैं। बैंकों, भुगतान बैंकों, वॉलेट में हो रहे साइबर अपराधों से सावधानी बरतने और इनको रिपोर्ट करने के लिए हेल्पलाइन 155260 है और इसके रिपोर्टिंग प्लेटफॉर्म को गृह मंत्रालय के तहत भारतीय साइबर अपराध समन्वय केंद्र (I4C) द्वारा भारतीय रिजर्व बैंक (RBI), सभी प्रमुख बैंकों, भुगतान बैंकों, वॉलेट, और ऑनलाइन व्यापारी के सक्रिय समर्थन और सहयोग से चालू किया गया है।

निष्कर्षत: कहा जा सकता है कि आज के तकनीकी युग में जहां दिन-प्रतिदिन उन्नत होती तकनीक हमें लाभ पहुंचा रही है, वहीं जरा सी चूक से एक क्षण में हमें यह इतना नुकसान भी दे सकती है, जिसकी हम कल्पना भी नही कर सकते । अत: बैंकिंग के सम्पूर्ण क्रियाकलापों में अत्यंत जागरुकता, सावधानी और सतर्कता की आवश्यकता है । एक ऐसी व्यवस्था बनाये जाने की आवश्यकता है जिसमें साइबर अपराध के किसी भी हमले को तुरंत नेस्तनाबूद किया जा सके और अपरधियों तक पहुंच कर उन्हें कानून के अनुरूप दण्डित किया जा सके।

*****

चंचल लाम्बा

पदनाम:- एस. डब्लयू. ओ. –ए. क्लर्क
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 8527036756
ई-मेल:- chanchallamba8527@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

परिचय:-

वित्तीय क्षेत्र को सुदृढ़ बनाने के लिए लेन-देन और संचार के डिजिटल माध्यमों का महत्व तेजी से बढ़ रहा है जिससे समाज और अर्थव्यवस्था दोनों सशक्त हो रही है। तथापि, इलेक्ट्रॉनिक लेन-देनों में हुई अभूतपूर्व वृद्धि और तेजी से विकसित होती डिजिटल अर्थव्यवस्था के चलते साइबर हमले गंभीर चिंता का विषय बन गए हैं। इस प्रकार, डिजिटीकरण ने न केवल अवसर उपलब्ध कराए हैं; अपितु अर्थव्यवस्था को ऐसे जोखिमों के समक्ष ला खडा़ किया है जिनमें बैंकिंग और अन्य वित्तीय संस्थानों के परिचालनों में गंभीर व्यवधान उत्पन्न करने की क्षमता है।

वित्तीय सेवाएं उपलब्ध कराने के लिए सूचना प्रौद्योगिकी (आईटी) का उपयोग तेजी से बढा़ है और वर्तमान में यह सभी बैंको और वित्तीय संस्थानों की परिचालन रणनीति का एक अभिन्न अंग है। इंटरनेट बैंकिंग और नवीनतम तकनीकयुक्त वित्तीय सेवाओं के बढ़ते उपयोग के साथ ही साइबर जोखिमों में वृद्धि हुई है। ऐसे हमले करने वालों में हैकिटविस्ट्स, साइबर अपराधी और आतंकवादी शामिल हैं जो राजनीतिक और वित्तीय अस्थिरता पैदा करने तथा वित्तीय अवसंरचना को ठप्प करने के लिए वित्तीय प्रलोभनों से प्रेरित होते हैं।

राष्ट्रीय सीमाओं की तरह, साइबर स्पेस की सीमाएं सुपरिभाषित नहीं हैं। इसकी भौगोलिक अथवा संस्थागत सीमाएं भी नहीं हैं। ऐसे परिदृश्य में प्रौद्योगिकी को सावधानीपूर्वक अपनाने की आवश्यकता है ताकि साइबर जोखिमों की संभावनाओं को कम से कम किया जा सके। आज, साइबर हमलों की बारम्बारिता और प्रभाव कई गुणा बढ़ गए हैं और प्रमुख रूप से वित्तीय क्षेत्र में ऐसा हुआ है जो बैंकों और वित्तीय संस्थानों द्वारा सतत् आधार पर पर्याप्त साइबर सुरक्षा की तैयारी सुनिश्चित करने की आवश्यकता को रेखांकित करता है।

हाल ही में राष्ट्रीय स्तर पर हुए साइबर हमले संबंधी कुछ उदाहरण:

1. **फिलिपींस**: हैकरों ने 04 और 05 फरवरी, 2016 को जब बांग्लादेश कार्यालय बंद थे, फैडरवल रिज़र्व बैंक ऑफ़ न्यूयार्क में बांग्लादेश सेंट्रल बैंक के खाते से 951,000,000 अमरीकी डॉलर की चोरी करने के लिए स्विफ्ट नेटवर्क के माध्यम से अनुदेश जारी किए और वे 101,000,000 अमरीकी डॉलर की चोरी करने में सफल भी रहे।
2. **यूनाईटेड किंग्डम**: हैकरों ने जनवरी, 2016 में एच. एस. बी. सी. यूनाईटेड किंग्डम की वेबसाइट को हैक कर लिया था जिसके बाद वहां कई घंटों के लिए इंटरनेट बैंकिग सेवा को ब्लॉक कर दिया गया।

3. **ग्रीस**: जनवरी, 2016 में अज्ञात एक्टिविस्ट हैकर ग्रुप ने बैंक ऑफ़ ग्रीस को कई मिनटों के लिए ऑफलाइन कर दिया था। तत्पश्चात, बैंक के सुरक्षा दस्ते ने इस पर तुरंत कार्रवाई की और डेटा को किसी प्रकार का नुक्सान नहीं होने दिया।

4. **कतर**: अप्रैल, 2016 में कतर नैशनल बैंक पर एक अज्ञात साइबर हमला हुआ जिसके परिणामस्वरूप ग्राहकों के लगभग 1.4 जीबी तक के डेटा की हानि हुई थी। चोरी हुए डेटा में अल जजीरा के कर्मचारियों, कतर पर शासन करने वाले अल-थानी परिवार के सदस्यों और सूचना तथा रक्षा विभाग के अधिकारियों से संबंधित फाइलें शामिल थीं।

5. **वियतनाम**: मई, 2016 में हैकरों ने वियतनाम के ताइन फोंग बैंक से 1,100,000 मिलियन अमरीकी डॉलर चुराने की कोशिश की। इस हमले में स्विफ्ट नेटवर्क के माध्यम से जारी अनुदेशों का प्रयोग किया गया था। तथापि, बैंक के साइबर सुरक्षा दस्ते ने इस पर तुरंत कार्रवाई की और कोई हानि नहीं हुई।

भारत में बैंकिंग क्षेत्र में साइबर खतरों के प्रकार:-

भारत में मोटे तौर पर निम्न प्रकार के साइबर खतरे हैं-

(क) **एटीएम जैकपॉटिंग/ स्पिटिंग मालवेयर अटैक्स**: मालवेयर ग्रीन डिसपेंसर पुराने सॉफ्टवेयर से संचालित एटीएम की श्रृंखला की लोकलाइज्ड हैकिंग को सुगम बनाता है। यह हमलावरों को किसी व्यापक नेटवर्क संक्रमण को शामिल किए बिना एटीएम तक पहुंचने, वहां से आसानी से नकदी निकालने की सुविधा प्रदान करता है। यह हैक भौतिक (फिज़िकल) मालवेयर हमला होता है जिसमें डिस्पेंसर के यूएसबी पोर्ट में लैपटॉप, फोन अथवा पेन ड्राइव जैसा कोई भी यंत्र लगाकर उसमें कोई संक्रमित फाइल अथवा वायरस डाला जाता है जिससे मशीन अनियमित ढंग से कार्य करने लगती है। जब इन्हें लगाया जाता है तब ग्रीन डिस्पेंसर एटीएम पर "सेवा में नहीं है" (आउट ऑफ सर्विस) संदेश प्रदर्शित कर सकता है परंतु मशीन को वर्चुअल की-बोर्ड द्वारा दूर से नियंत्रित किया जा सकता है तथा इसे नकदी बाहर निकालने का अनुदेश दिया जा सकता है।

(ख) **एटीएम स्कीमिंग और प्वाइंट ऑफ सेल क्राइम**: इसमें एटीएम मशीन अथवा पीओएस सिस्टम की सुरक्षा में सेंध लगाई जाती है और मशीन के कीपैड के ऊपर एक स्किमिंग यंत्र लगाया जाता है ताकि वह असली कीपैड जैसा प्रतीत हो अथवा कार्ड रीडर से एक यंत्र लगाया जाता है ताकि वह मशीन का ही एक हिस्सा दिखे। स्किमर्स के सफल कार्यान्वयन से एटीएम मशीन से कार्ड नंबर और निजी पहचान संख्या कोड (पीआईएन) एकत्रित करके कपटपूर्ण लेन-देन करने के लिए इनका बाद में फिर से उपयोग किया जाता है।

फिशिंग घोटाले:

फिशिंग सामाजिक इंजीनियरिंग का एक ऐसा रूप है जिसमें ई-मेल अथवा इंसटैंट मैसेज जैसे ऊपरी तौर पर अधिकृत प्रतीत होते इलेक्ट्रॉनिक संप्रेषण में एक विश्वस्त व्यक्ति अथवा व्यापार का छद्म वेश धारण करके धोखे से पासवर्ड, यूजरनेम, लॉगिन आईडी, एटीएम पिन और क्रेडिट कार्ड के ब्यौरे जैसी संवेदनशील जानकारी प्राप्त कर ली जाती है। फिशिंग हमलावर संदेश प्राप्तकर्ता को एक वेब पेज (प्रतिरूप वेब पेज) की ओर निदेशित करता है जिसे पूर्णतः इस ढंग से तैयार किया जाता है कि वह किसी संगठन (अक्सर बैंक और वित्तीय संस्थान) की अपनी वेबसाइट की तरह दिखता है और तत्पश्चात् वे चालाकी से उपभोक्ता की निजी सूचना एकत्र कर लेते है और पीड़ित व्यक्ति को अक्सर इस हमले के बारे में पता भी नहीं होता है।

विशिंग घोटाले:-

इस प्रकार के फिशिंग घोटाले में साइबर अपराधी विक्टिम को मोबाइल पर फोन करता है और पेमेंट की गलत जानकारी देता है।

स्पूफिंग घोटाले:-

इस प्रकार के साइबर अपराध में अपराधी विक्टिम को एक नकली ई-मेल आईडी से ई-मेल भेजता है या फोन कॉल करता है और ये ई-मेल एवं फोन कॉल बिलकुल सही प्रतीत होते हैं।

एडवान्सड परसिसटेंट थ्रेट (एपीटी) अटैक्स: इसमें बैंक के डेटा में सीधे परिवर्तन करने, मिटाने और/ अथवा उन्हें चोरी करने के लिए बैंक की प्रणालियों को सीधे निशाना बनाया जाता है। इसकी विशेषता यह है कि इसे सम्मिश्र, गुप्त और चल रही कम्पयूटर हैकिंग प्रक्रियाओं के सेट के रूप में किया जाता है जिसमें एक विशिष्ट समयावधि में बेइमानी से संवेदनशील लक्षित सूचना निकालने के लिए, पहचान से बचने के लिए, नेटवर्क में प्रवेश के लिए किसी विशिष्ट निकाय को लक्ष्य बनाया जाता है। एटीपी में विशिष्ट रूप से अनेक चरण शामिल हैं-

1. ऐसे संगठन का चयन करने के लिए व्यापक रिसर्च करना जो ऐसी सूचना प्रोद्योगिकी का इस्तेमाल करते हैं जिसका अनुचित लाभ उठाया जा सकता है।
2. प्रिविलेज्ड क्रेडेन्शियल की चोरी और चोरी किए गए डेटा के वांछित प्रवाह के लिए गुप्त व्यवस्था करना और अधिक संख्या में सिस्टम को संकट में डालने के लिए अधिक मालवेयर डालना।
3. हैक, अनधिकार प्रवेश, संकट में डालने और चोरी के डिजिटल प्रमाण को मिटाने के लिए ट्रैक को कवर करना।

इनसाइडर साइबर अपराध:-

इनसाइडर साइबर अपराध विभिन्न संगठनात्मक नेटवर्क संसाधनों के एक्सेस के अधिकारों को दुरूपयोग, सामग्रियों की चोरी और भौतिक उपकरणों को गलत ढंग से चलाकर किया जाता है। जानबूझकर तोड-फोड़, चोरी, जासूसी, छल-कपट और प्रतिस्पर्द्धात्मक लाभ सहित इनसाइडर जोखिमों के कारण बैंकों में कई घटनाएं घटित होती है।

साइबर सुरक्षा समस्या का समाधान करने हेतु भारत सरकार द्वारा की गई पहलें:-

सुरक्षित ऑनलाइन भुगतान प्रणालियों के लिए भारत सरकार ने कई कदम उठाए हैं। वर्ष 2016 में साइबर नियमों के उल्लंघन की घटना के बाद भारतीय रिज़र्व बैंक (आरबीआई) ने भी बैंकों को क्या करें और क्या न करें की एक सूची जारी की है।

राष्ट्रीय साइबर सुरक्षा नीति-2013

राष्ट्रीय साइबर सुरक्षा नीति-2013 की मुख्य विशेषताएं इस प्रकार हैं-

1. सूचना पर निगरानी रखने एवं उसके संरक्षण तथा साइबर हमलों से सुरक्षा तंत्र को मजबूत करने के उद्देश्य से 2 जुलाई, 2013 को भारत सरकार द्वारा राष्ट्रीय साइबर सुरक्षा नीति, 2013 जारी की गई थी। इस प्रारूप दस्तावेज का उद्देश्य नागरिकों, व्यवसायों और सरकार के लिए एक सुरक्षित और लचीला साइबर स्पेस सुनिश्चित करना है।
2. व्यापक अर्थो में इस नीति का उद्देश्य एक सुरक्षित साइबर स्पेस इकोसिस्टम का सृजन करना तथा नियामक ढांचे को मजबूत करना है। राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र {नेशनल क्रिटिकल इंफार्मेशन

प्रोटेक्शन सेंटर} (एनसीआईआईपीसी) के माध्यम से साइबर जोखिमों का सामना करने के लिए एक राष्ट्रीय और क्षेत्रीय चौबीस घंटे (24* 7) वाले तंत्र पर बल दिया गया है।

3. संकट प्रबंधन प्रयासों के समन्वय हेतु एक नोडल अभिकरण प्रतिक्रिया दल (सीईआरटी-इन) का गठन किया गया है। यह सीईआरटी-इन, क्षेत्रीय सीईआरटी-इन के समन्वय और संचालन के लिए मुख्य संगठन के रूप में भी कार्य करेगा।
4. इस नीति में शिक्षण और प्रशिक्षण कार्यक्रमों के माध्यम से मानव संसाधन विकसित करने, सरकारी-निजी साझेदारी के माध्यम से साइबर सुरक्षा प्रशिक्षण अवसंरचना की स्थापना करने और कानून प्रवर्तन अभिकरणों के लिए क्षमता निर्माण हेतु संस्थागत तंत्र की स्थापना करने की अपेक्षा की गई है।

डिजिटल भुगतान के प्रति सुरक्षा चिंताओं का समाधान करने के लिए सरकार द्वारा हाल ही में निम्नलिखित प्रमुख पहलें की गई हैं-

1. सचिव, इलेक्ट्रॉनिकी और सूचना प्राद्योगिकी की अध्यक्षता में तथा सचिव, दूरसंचार विभाग की सह अध्यक्षता में डिजिटल भुगतान सुरक्षा समिति की स्थापना की गई है। इस समिति की प्रथम बैठक 31 मार्च, 2017 को आयोजित की गई थी।
2. प्रीपेड पेमेंट इंस्ट्रूमेंटस की सुरक्षा संबंधी नियमों का प्रारूप तैयार किया है। इस प्रारूप नियम में इलेक्ट्रॉनिक प्रीपेड पेमेंट इंस्ट्रूमेंट के लिए शिकायत समाधान तंत्र हेतु प्रावधान हैं। इस प्रारूप नियम को इलेक्ट्रॉनिक और सूचना प्रौद्योगिकी मंत्रालय की वेबसाइट पर प्रकाशित किया गया है और जनता एवं सभी पक्षकारों से टिप्पणियां मांगी गई हैं।
3. चुनौतियों का सामना करने और डिजिटल पेमेंट इकोसिस्टम की साइबर सुरक्षा स्थिति के सुधार हेतु मंत्रालय में डिजिटल भुगतान प्रभाग की स्थापना की गई है।

विनिमायकों द्वारा की गयी पहलें:

1. भारतीय रिज़र्व बैंक (आरबीआई)

भारत में बैंकों पर साइबर हमलों की घटनाओं में हुई वृद्धि को देखते हुए, आरबीआई ने बैंकों में साइबर सुरक्षा की तैयारियों को सुदृढ़ करने के लिए अनेक मुख्य पहलें की हैं और महत्वपूर्ण कदम उठाए हैं।

1) बैंकों के जोखिम को चार श्रेणियों- कम, माध्यम, उच्च और बहुत अधिक के रूप में वर्गीकृत करना होगा तथा अपने सर्वर/ नेटवर्क में किसी असामान्य व्यवहार की सूचना अनिवार्य रूप से तुरंत भारतीय रिज़र्व बैंक को देनी होगी।
2) निरंतर निगरानी और साइबर खतरों से संबंधित नवीनतम जानकारी हेतु बैंकों को सुरक्षा संचालन केन्द्र (एसओसी) की स्थापना करनी होगी।
3) न्यूनतम साइबर सुरक्षा और आवश्यक लचीलेपन तथा सुरक्षा संचालन केन्द्र के गठन और संचालन हेतु दिशानिर्देश स्पष्ट कर दिए गए हैं।

2. भारतीय प्रतिभूति एवं विनिमय बोर्ड (सेबी)

सेबी द्वारा साइबर सुरक्षा संबधी एक उच्च स्तरीय निगरानी समिति का गठन किया गया है।

1) सेबी और संपूर्ण पूंजी बाजार की साइबर सुरक्षा पहलों की निगरानी करना और उन्हें संपूर्ण मार्गदर्शन प्रदान करना।
2) साइबर लचीलेपन और संबंधित कार्यों तथा भारतीय प्रतिभूति बाजार में आपदा रिकवरी प्रक्रिया में सुधार हेतु उपाय खोजना।

3) समय-समय पर एसओसी (सुरक्षा संचालन केन्द्र) के अधिदेश और कार्यकरण की समीक्षा करना और प्रतिभूति बाजार हेतु साइबर प्रयोगशाला/ साइबर उत्कृष्टता केन्द्र की स्थापना करने में सेबी का मार्गदर्शन करना।

निष्कर्ष:-

एक व्यापक साइबर सुरक्षा संदर्भ में, वित्तीय क्षेत्र में साइबर सुरक्षा सुनिश्चित करना वित्तीय और बैंकिंग क्षेत्र जो हमारे जैसी विकासशील और बदलती हुई अर्थव्यवस्था के महत्वपूर्ण स्तम्भ हैं, में सुरक्षा व्यवस्था को बढाने और मजबूत करने की दिशा में एक निर्णायक कदम है। जैसा कि पूरे विश्व में हुई विभिन्न घटनाओं से पता चलता है कि साइबर खतरों की कोई भौगोलिक अथवा संस्थागत सीमाएं नहीं होती हैं। इसके अलावा, लोगों को पासवर्ड प्रबंधन और साइबर सुरक्षा संबधी जानकारी के बारे में जागरूक करना भी आवश्यक है। विशेषज्ञों ने भी भारत के नाभिकीय निवारण सिद्धान्त के अनुसार एक साइबर निवारण सिद्धान्त तैयार करने का सुझाव दिया है।

सन्दर्भ:-

1. लोक सभा सचिवालय शोध और सूचना प्रभाग, सं. लार्डिस (ई एंड एफ) 2017/आईबी-2 अगस्त 2017 वित्तिय क्षेत्र में साइबर-सुरक्षा।
2. पंजाब नैशनल बैंक एफ. आर.एम.डी परिपत्र सं. 04/2022।

*****

डॉ. सत्येंद्र कुमार

पदनाम:- मुख्य प्रबंधक
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 8866780305
ई-मेल:- satyendra.khampariya@bankofbaroda.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

परिचय:-

'डिजिटल बैंकिंग' के अभूतपूर्व विकास ने बैंकिंग के पारंपरिक तरीकों को बदल दिया है और करोड़ों ग्राहक बैंकिंग लेन-देन करने के इन तरीकों का उपयोग कर लाभांवित हो रहे हैं। भारत दुनिया में दूसरी सबसे बड़ी इंटरनेट आबादी वाला देश है। अधिक से अधिक कनेक्टिविटी जहां विश्व की अर्थव्यवस्थाओं के लिए एक वरदान है, वहीं दूसरी ओर इसके नकारात्मक पहलू भी हैं। हमारा डिजिटल समाज साइबर अपराधों के प्रति अधिक संवेदनशील हो गया है। सरल शब्दों में, "साइबर अपराध" ऐसा अपराध है जिसमें एक कंप्यूटर और एक नेटवर्क शामिल होता है। इंटरनेट और मोबाइल बैंकिंग का उपयोग करने वाले लोगों की संख्या में वृद्धि के कारण साइबर अपराध पिछले कुछ वर्षों में लगातार बढ़ रहे हैं। साइबर अपराध की घटनाओं में क्रेडिट कार्ड धोखाधड़ी, स्पैमिंग, स्पूफिंग, ई-मनी लॉन्ड्रिंग, एटीएम धोखाधड़ी, फ़िशिंग, पहचान की चोरी आदि शामिल है। रिपोर्ट किए गए साइबर अपराधों में से अधिकांश मामले एटीएम धोखाधड़ी के हैं और इसके बाद ऑनलाइन बैंकिंग धोखाधड़ी के मामले दर्ज किए गए हैं। नकदी और उपभोक्ता डेटा के विशाल भंडार के कारण बैंकिंग उद्योग साइबर सुरक्षा अपराधियों के लिए शीर्ष लक्ष्य है।

खरीदारी, किराना ऑर्डर, बिल भुगतान आदि जैसी सभी आवश्यक गतिविधियां डिजिटल स्पेस में स्थानांतरित हो गई हैं। इससे भारतीय अर्थव्यवस्था तेजी से नकदी से डिजिटल लेन-देन की ओर बढ़ रही है जिससे देश साइबर हमलों की चपेट में आ रहा है। ग्राहकों के लिए लेन-देन को और सुविधाजनक बनाने हेतु बैंकों ने डिजिटल भुगतान के विभिन्न डिजिटल प्लेटफॉर्म को एकीकृत किया है, जिसने बैंकिंग क्षेत्र में साइबर धोखाधड़ी की संख्या में और अधिक वृद्धि की है। बैंकिंग क्षेत्र में तकनीकी प्रगति ने ग्राहकों को एक सुविधाजनक बैंकिंग का अनुभव प्रदान किया है। हालांकि, जैसे-जैसे तकनीक का विस्तार होता जा रहा है, ऑनलाइन बैंकिंग में धोखाधड़ी का दायरा तेजी से बढ़ रहा है। इसके अलावा, ऑनलाइन लेन-देन की बढ़ती संख्या और सुदृढ़ साइबर सुरक्षा प्रणालियों की कमी धोखाधड़ीकर्ताओं को दुर्भावनापूर्ण कार्य करने के लिए जगह देती हैं। कोविड-19 महामारी के प्रकोप ने लोगों को डिजिटल अपनाने के लिए मजबूर किया है। एक ओर जहां आम जनता को अपने घरों से ऑनलाइन लेन-देन करने में आराम मिला है, वहीं दूसरी ओर साइबर अपराधियों को प्रौद्योगिकी पर हमारी निर्भरता से लाभ उठाने का अवसर भी मिला है। बैंक और अन्य वित्तीय संस्थान साइबर अपराधियों के लिए आकर्षक लक्ष्य हैं क्योंकि उनके पास मूल्यवान व्यक्तिगत डेटा होता है जोकि विशेष वित्तीय या आर्थिक जरूरतों को पूरा करने में महत्वपूर्ण भूमिका निभाते हैं। साइबर अपराध विशेष रूप से एक वैश्विक समस्या बन गई है, जोकि लगातार बढ़ रही है। साइबर हमलों की प्रवृत्ति किसी भी अन्य क्षेत्र की तुलना में वित्तीय क्षेत्र में काफी अधिक है। इससे ग्राहक और बैंक को धन की भारी हानि होती है, बैंक की प्रतिष्ठा में कमी आती है और उपयोगकर्ताओं के बीच बैंकों के प्रति विश्वास में कमी आती है।

बैंक अपने उपयोगकर्ताओं को एक सुरक्षित ऑनलाइन बैंकिंग वातावरण प्रदान करने के लिए बाध्य हैं। हालांकि बैंकों ने अपनी संपत्ति की अतिरिक्त सुरक्षा के लिए बहुत सारे उपाय किए हैं, फिर भी ये पारंपरिक सुरक्षा तंत्र अब पर्याप्त नहीं हैं क्योंकि हमलावर इन सुरक्षा तंत्रों को बाईपास करने में सक्षम हैं। बैंकों को अपनी सुरक्षा तंत्र को मजबूत करने के लिए निरंतर प्रयत्न करने होंगे और बैंक की मूल्यवान संपत्तियों की सुरक्षा और गोपनीयता सुनिश्चित करने के लिए उचित पहल करनी होगी।

बैंकिंग में साइबर अपराधों के स्वरूप:-

ग्राहकों द्वारा ऑनलाइन बैंकिंग के उपयोग में वृद्धि के साथ बैंकिंग क्षेत्र में साइबर अपराधों की संख्या असाधारण रूप से बढ़ गयी है। बैंकों में सामान्यत: होने वाले कुछ साइबर हमलों के स्वरूप निम्नानुसार हैं।

फिशिंग:- फ़िशिंग एक ऐसा हमला है जिसमें इलेक्ट्रॉनिक संचार में ट्रस्टेड बॉडी होने का नाटक करके हमलावर द्वारा उपयोगकर्ता के नाम, पासवर्ड, क्रेडिट कार्ड विवरण इत्यादि जैसे संवेदनशील जानकारी प्राप्त करने का प्रयास किया जाता है। फ़िशिंग आमतौर पर ई-मेल स्पूफ़िंग या इंस्टेंट मैसेजिंग द्वारा की जाती है, जिसमें उपयोगकर्ताओं को आमतौर पर अपने खातों को सुरक्षित करने के लिए लिंक पर क्लिक करने के लिए कहा जाता है। जैसे ही उपयोगकर्ता इन्हें क्लिक करता है उसे धोखाधड़ी वाली वेबसाइटों के लिए निर्देशित किया जाता है जो मूल बैंकिंग वेबसाइट की तरह दिखते हैं। फिशर्स कई प्रकार के टूल और तकनीक का उपयोग करते हैं जो उन्हें ई-मेल डिलीवरी, फ़िशिंग साइट होस्टिंग और विशेष मैलवेयर समेत विभिन्न प्रकार के फंक्शन प्रदान करती हैं। इन टूल और तकनीकों में बॉटनेट, फ़िशिंग किट, डोमेन नाम सेवा (डीएनएस) का दुरुपयोग, तकनीकी डेसीट और विशिष्ट मैलवेयर शामिल हैं।

क्रॉस साइट स्क्रिप्टिंग - क्रॉस-साइट स्क्रिप्टिंग (एक्सएसएस) एक प्रकार का विशिष्ट साइबर अपराध है जो कि आमतौर पर अतिसंवेदनशील वेब ऐप्लिकेशन को नुकसान पहुंचाने के उद्देश्य से किया जाता है। क्रॉस-साइट स्क्रिप्टिंग (एक्सएसएस) दुर्भावनापूर्ण वेब उपयोगकर्ताओं द्वारा वेब पृष्ठों में कोड इंजेक्शन की अनुमति देते हैं जो अन्य उपयोगकर्ताओं द्वारा देखी जाती हैं। इस तरह के कोड के उदाहरणों में क्लाइंट-साइड स्क्रिप्ट, एचटीएमएल कोड इत्यादि शामिल हैं।

विशिंग:- विशिंग एक साइबर हमला है, जिसमें इनाम (लॉटरी) प्राप्त करने के लिए लोगों से निजी और वित्तीय जानकारी तक पहुंचने के लिए सोशल इंजीनियरिंग और वॉयस ओवर आईपी (वीओआईपी) का उपयोग किया जाता है। यह "आवाज (वॉइस)" और फिशिंग को जोड़ती है। विशिंग एक अवैध अभ्यास है जहां एक हमलावर उपयोगकर्ता को कॉल करता है और उस बैंक से होने का नाटक करता है जिसमें उपयोगकर्ता का खाता होता है। आमतौर पर उपयोगकर्ता के खाते की जानकारी (यह बताते हुए कि उपयोगकर्ता का खाता निलंबित कर दिया गया है, आदि) को सत्यापित करने के लिए कहा जाता है।

बॉट नेटवर्क (बॉटनेट):- बॉट ऐसे प्रोग्राम होते हैं जो रिमोट कमांड प्रदान करने के लिए सिस्टम को संक्रमित करते हैं और विभिन्न प्रोटोकॉल जैसे एचटीटीपी, इंस्टेंट मैसेजिंग और पीयर-टू-पीयर प्रोटोकॉल के माध्यम से कमांड को नियंत्रित करते हैं। इस तरह के बॉट्स को आमतौर पर बॉटनेट के रूप में जाना जाता है।

मैलवेयर:- मैलवेयर एक दुर्भावनापूर्ण रूप से तैयार किया गया सॉफ्टवेयर प्रोग्राम होता है जो उपयोगकर्ता या मालिक की सहमति के बिना कंप्यूटर सिस्टम को एक्सेस करता है। मैलवेयर में वायरस, ट्रोजन हॉर्स, वर्म्स इत्यादि शामिल हैं। मैलवेयर बैंकिंग प्रणाली की गोपनीयता, अखंडता और उपलब्धता पर भारी प्रभाव डालता है। इसमें बैंकिंग सिस्टम के डेटा की गोपनीयता भंग करने की क्षमता होती है और बैंक के लाखों लोगों को इससे हानि हो सकती है। मैलवेयर उपयोगकर्ता के सिस्टम और बैंक दोनों को लक्षित कर सकते हैं।

बैंकिंग ट्रोजन मैलवेयर:- ट्रोजन मैलवेयर स्वयं को वास्तविक ऐप्लिकेशन के साथ छिपाता है, ये ट्रोजन विशेष रूप से पूरे बैंकिंग नेटवर्क को स्कैन करने और वित्तीय डेटा चोरी करने के लिए बनाए जाते हैं। कुछ मैलवेयर जैसे अर्न्सिफ, ड्राइडेक्स, ट्रिकबॉट, ज्युस, रेमिट इत्यादि हैं जिन्होंने पिछले कुछ वर्षों में बड़े वित्तीय नुकसान किए हैं।

एटीएम/ पीओएस मैलवेयर:- एटीएम और पीओएस सिस्टम साइबर आपराधियों के लिए आसान लक्ष्य माना जाता है, साइबर अपराधियों द्वारा ओपन यूएसबी पोर्ट, सीडी ड्राइव, बीआईओएस बूट अनुक्रम तक पहुंच और ओएस फर्मवेयर का शोषण किया जाता है। आजकल एटीएम और पीओएस सिस्टम पर लगातार मैलवेयर हमले बढ़ रहे हैं जैसे प्लूटस, ट्यूपकिन, कारबानक, कार्डस्टेलर, वीएसकिमर, चेवबाका, पॉसीडन और फाइंडपॉस इत्यादि।

डीओएस हमले (डिनायल ऑफ़ सर्विस):- डीओएस एक ऐसा हमला है जिसमें उपयोगकर्ता या संगठन को ऑनलाइन संसाधन तक पहुंचने से रोका जाता है। इसमें बॉटनेट के एक बड़े समूह द्वारा सिस्टम को लक्षित किया जाता है और लक्षित उपयोगकर्ताओं की सेवाओं को उनके लिए अनुपलब्ध बना दिया जाता है।

डीडीओएस हमले (डिस्ट्रीब्युटेड डिनाइल ऑफ़ सर्विस) :- डीडीओएस एक ऐसा हमला है जहां बड़ी संख्या में सेवा अनुरोधों के साथ लक्षित प्रणाली में बाढ़ लाई जाती है जो सिस्टम दुर्घटना और नेटवर्क जैमिंग का कारण बनता है, अंततः सेवाओं को अनुपलब्ध बनाते हैं।

एसएमएस स्पूफिंग:- यह एक अपेक्षाकृत नई तकनीक है जिसमें उपयोगकर्ता को फोन पर एक एसएमएस संदेश प्राप्त होता है जो एक वैध बैंक से आया हुआ प्रतीत होता है। इस एसएमएस में मूल मोबाइल नंबर (प्रेषक आईडी) को अल्फान्यूमेरिक टेक्स्ट द्वारा प्रतिस्थापित किया जाता है। यहां उपयोगकर्ता को उसके ऑनलाइन प्रमाणपत्र देने के लिए उनके साथ धोखाधड़ी की जाती है और उनका पैसा चोरी कर लिया जाता है।

टीसीपी / आईपी स्पूफिंग:- आईपी स्पूफिंग में, ग्राहक को एक ई-मेल संदेश भेजकर उसके सिस्टम पर गैरकानूनी तरीके से पहुंचने का प्रयास किया जाता है जो कि एक भरोसेमंद मशीन के आईपी पते से आती हुई प्रतीत होती है। आईपी एड्रेस स्पूफिंग एक शक्तिशाली तकनीक है जो किसी हमलावर को फ़ायरवॉल द्वारा अवरुद्ध किए बिना नेटवर्क को भेदने में सक्षम कर सकती है। यहां मुख्य लक्ष्य बैंकिंग सिस्टम के सर्वर तक रूट प्राप्त करना है, जो लक्षित सिस्टम में बैकडोर एंट्री पाथ की एंट्री देता है।

फार्मिंग:- इस हमले में जब भी कोई उपयोगकर्ता किसी वेबसाइट तक पहुंचने का प्रयास करता है तो उसे नकली साइट पर रीडायरेक्ट कर दिया जाता है। फार्मिंग दो संभावित तरीकों से किया जा सकता है: एक पीड़ित के कंप्यूटर पर होस्ट की फाइलों को बदलकर और दूसरा अन्य तरीकों से डीएनएस सर्वर सॉफ़्टवेयर में भेद्यता का शोषण कर।

अंदरूनी सूत्र धमकी (इनटर्नल सोर्स थ्रेट) :- बैंकों के अंदरूनी सूत्र व कर्मचारी भी बैंक के डेटा के लिए एक बड़ा सुरक्षा जोखिम है जो अवैध रूप से जानकारी का खुलासा, संशोधन या उपयोग कर सकते हैं। कर्मचारियों द्वारा अनजानी त्रुटियों के विनाशकारी परिणाम भी हो सकते हैं।

ओटीपी पर हमले:- ओटीपी (वन टाइम पासवर्ड) दो कारक प्रमाणीकरण विधि है जिसमें उपयोगकर्ता मोबाईल में प्राप्त हुए ओटीपी और पासवर्ड का उपयोग करने के बाद ही पेमेंट कर सकता है। अपराधी ओटीपी संरक्षित खातों पर हमले कर ग्राहकों के ओटीपी प्राप्त कर उन्हें वित्तीय नुकसान पहुंचाते है जिन्हें एमआईटी-एक्स विधियों (मैन-इन-द-एक्स) के रूप में जाना जाता है। ये निम्नानुसार हैं:

- **मैन-इन-द-मिडल हमले (एमआईटीएम):** यहां डेटा के ट्रांसमिशन पाथ का उपयोग किया जाता है और लेन-देन के बीच में जानकारी को आसानी से चुरा लिया जाता है।
- **मैन-इन-द-ब्राउज़र हमला (एमआईटीबी):** यहां वेब ब्राउज़र में दुर्भावनापूर्ण तरीके से कोड को मौजूद किया जाता है जोकि उपयोगकर्ताओं को प्रमाणपत्र और अन्य महत्वपूर्ण जानकारी दर्ज करने के लिए प्रेरित करता है।
- **मैन-इन-द-पीसी हमला (एमआईटीपीसी):** एमआईटीपीसी सिस्टम संबंधित कमजोरियों का शोषण करता है।

स्विफ्ट संबंधित हमले:- अंतर्राष्ट्रीय लेन-देन सोसाइटी फॉर वर्ल्डवाइड इंटरबैंक फाइनेंशियल टेलीकम्युनिकेशंस (एसडब्ल्यूआईएफटी) के अधीन है दुनिया भर में इन पर नियमित रूप से हमले हो रहे हैं और प्रवृत्ति बढ़ रही है।

उदाहरण: हैकर्स ने पिछले कुछ वर्षों में बांग्लादेश सेंट्रल बैंक से $ 81 मिलियन और रूस के ग्लोबैंक्स बैंक से $ 9.4 मिलियन की धोखाधड़ी की। दक्षिण भारत स्थित बैंक में से एक पर फरवरी 2018 में साइबर अपराधियों ने हमला कर इसके सिस्टम को हैक कर लिया और बैंक की स्विफ्ट प्रणाली में समझौता कर इसके माध्यम से भेजे

गए तीन अनधिकृत प्रेषणों के द्वारा करीब 2 मिलियन डॉलर दुबई, तुर्की और चीन के बैंक खातों में स्थानांतरित किए।

रैंसमवेयर हमले :- रैंसमवेयर सिस्टम के शोषण के बाद उसके डेटा को एन्क्रिप्ट करता है और इसे उपयोगकर्ता के लिए अनुपलब्ध बना डेटा है। वानाक्राय पेट्या, बद्रीबिट, लोकी, नोटपेट्या कुछ रैंसमवेयर वेरिएंट हैं जो वित्त, ऊर्जा और हेल्थकेयर जैसे महत्वपूर्ण क्षेत्रों को प्रभावित करते हैं। मई 2017 में विश्वभर में वनाक्राय रैंसमवेयर हमले ने हजारों लोगों को प्रभावित किया 230,000 से अधिक कंप्यूटरों पर डेटा एन्क्रिप्ट कर बिटकॉइन के रूप में फिरौती का भुगतान करने की मांग पीड़ितों से की गई।

सुरक्षात्मक उपाय:- बैंकों को ग्राहकों के डेटा की सुरक्षा के लिए अपनी रक्षा विधियों को और अधिक मजबूत करने की आवश्यकता है तथा इन हमलों के लिए बैंकिंग प्रणाली को अधिक सुरक्षित बनाने के लिए नई तकनीक अपनानी चाहिए।

निरंतर जोखिमों का आकलन:- बैंकों को अपने आकार, भौगोलिक सेटअप, व्यापार परिचालन क्षेत्र इत्यादि के आधार पर अपनी जोखिम प्रोफाइल का आकलन करते हुए सुरक्षा नियंत्रण में प्रभाव डालने वाले, कमियों और जोखिमों की पहचान कर सुरक्षा नियंत्रण को लागू करने के लिए पर्याप्त कार्रवाई करनी चाहिए जो इन जोखिमों का निवारण कर सके।

1. **कीलॉगिंग हमलों के विरुद्ध उपाय :-** बैंक कीलॉगर्स का लक्ष्य बन गए हैं, कीलॉगिंग हमलों से बचने के लिऐ तीन विधियां अपनाई जा सकती हैं: एंटी-कीलॉगर, कर्नेल स्तर कीलॉगिंग और उपयोगकर्ता स्तर कीलॉगिंग।
2. **वेब ब्राउज़र हमलों के विरुद्ध उपाय:-** सुरक्षित ऑनलाइन बैंकिंग के लिए हमें वेब ब्राउज़र तकनीक की आवश्यकता है जो हमलावरों द्वारा रिवर्स इंजीनियरिंग और डिबगिंग के विरुद्ध स्वयं को बचाने में सक्षम हो और इसकी मेमोरी को एक्सेस या संशोधित करने के किसी भी प्रयास को अवरुद्ध करने में सक्षम हो।
3. **क्रॉस साइट स्क्रिप्टिंग के विरुद्ध उपाय :-** एक्सएसएस हमलों को रोकने के लिए दो मुख्य उपाय हैं: फ़िल्टरिंग और एस्केपिंग।
4. **बॉटनेट्स से हमलों के विरुद्ध उपाय :-** ये दो श्रेणियों के अंतर्गत आते हैं, क्लासिकल काउंटरमेजर्स एवं आपत्तिजनक उपाय जैसे: मिटीगेशन, मेनीपुलेशन और एक्स्प्लॉएटेशन।
5. **डीओएस और डीडीओएस हमलों के विरुद्ध उपाय:-** परिनियोजन के आधार पर डीडीओएस के लिए रक्षा तंत्र का वर्गीकरण उस स्थान पर आधारित है जहां रक्षा तंत्र लागू किया गया है और इसे तीन प्रकार से वर्गीकृत किया जा सकता है: स्रोत आधारित, गंतव्य आधारित एवं नेटवर्क आधारित।
6. **ग्राहक जागरूकता अभियान:-** उपयोगकर्ता किसी भी क्षेत्र की कुंजी है और कुछ मामलों में सबसे कमजोर लिंक भी। एक बैंक नवीनतम सुरक्षा तकनीकों को नियोजित कर सकता है लेकिन सभी बेकार हैं, यदि ग्राहक नहीं जानते हैं कि उनका उपयोग कैसे किया जाए। बैंकों को अंततः उपयोगकर्ताओं के लिए बैंक द्वारा पेश की गई नवीनतम सुरक्षा सुविधाओं और उनके खातों को सुरक्षित करने के लिए उनका उपयोग करने के बारे में सूचित करने के लिए सतत् जागरूकता कार्यक्रम चलाए जाने चाहिए।

उपयोगकर्ताओं के लिए सुरक्षात्मक उपाय	
क्या करें	**क्या न करें**
1. अपने कंप्यूटर या मोबाइल फोन पर नवीनतम एंटी-वायरस/ एंटी स्पाइवेयर/ फ़ायरवॉल/ सुरक्षा पैच	1. ज्ञात या अज्ञात उपयोगकर्ताओं द्वारा अग्रेषित आपके ई-मेल में किसी भी संदिग्ध लिंक या

इंस्टाल करें और नियमित रूप से अपडेट व स्कैन करें। 2. केवल लाइसेंस प्राप्त सॉफ्टवेयर और ऐप्लिकेशन का उपयोग करें। 3. विश्वसनीय एवं विविधतापूर्ण पासवर्ड बनाएं आपका पासवर्ड आपकी पहचान है। 4. पासवर्ड जो अप्रत्याशित हो, इसे बनाने के लिए अक्षरों, संख्याओं और विशेष कैरेक्टर का मिश्रण करें। 5. पासवर्ड में कम से कम आठ वर्ण होने चाहिए, जितना लंबा पासवर्ड होगा उतना ही मुश्किल उसमें सेंध लगाना होगा। 6. जब आप कंप्यूटर का उपयोग न कर रहें हों तो अपनी कंप्यूटर स्क्रीन लॉक करें। 7. हमेशा समय-समय पर बाहरी हार्ड डिस्क में अपने डेटा का बैकअप लेते रहें। 8. हमेशा वेब साइट यूआरएल पता सावधानी से जांचें । पता "https" से शुरू होना चाहिए जो सुरक्षित संचार का प्रतिनिधित्व करता है। 9. लॉग इन करने के लिए सीधे लिंक पर क्लिक किए बिना अपने वेब ब्राउज़र पता बार में वेबसाइट पता टाइप करें, वेबपृष्ठ यूआरएल के ऊपरी या निचले दाएं कोने पर 'ऑन' और हरे रंग के रंग के लिए हमेशा पैडलॉक आइकन की जांच करें।	यूआरएल पर क्लिक न करें, यह आपको फ़िशिंग साइट पर ले जा सकता है। 2. ज्ञात या अज्ञात उपयोगकर्ताओं द्वारा अग्रेषित अप्रत्याशित ई-मेल अनुलग्नक या तत्काल संदेश डाउनलोड लिंक न खोलें, यह मैलवेयर इंस्टाल कर सकते हैं। 3. जंक ई-मेल या किसी श्रृंखला में आए सवालों का जवाब न दें ये आपके सिस्टम पर अनधिकृत नियंत्रण प्राप्त कर अपको हानि पहुंचा सकते हैं। 4. कभी भी अपना पासवर्ड संगठन या बाहर भीतर किसी से भी साझा न करें। 5. कभी भी एवं कहीं भी जैसे अपने डेस्क के पास अपना पासवर्ड न लिखें। 6. एक से अधिक स्थानों के लिए एक ही पासवर्ड का उपयोग न करें। 7. सोशल मीडिया में कोई आधिकारिक या अपमानजनक पोस्ट न करें। 8. ई-मेल के माध्यम से कोई गोपनीय जानकारी प्रदान न करें, भले ही यह अनुरोध आयकर विभाग के अधिकारियों, वीजा या मास्टरकार्ड और बैंक के अधिकारियों द्वारा किए जाएं। 9. साइबर कैफे जैसे सार्वजनिक स्थानों में ऑनलाइन लेन-देन न करें।

संदर्भ:-

1. https://www.byteacademy.co/blog/banking-cyber-security
2. https://financialservicesblog.accenture.com/cybercrime-in-banking-and-capital-markets-technology-and-human-vulnerabilities
3. https://www.jigsawacademy.com/rise-of-cyber-crimes-how-are-banks-fighting-back/
4. https://www.financialexpress.com/money/how-to-secure-your-banking-transactions-from-cyber-frauds/2235437/
5. https://www.legalserviceindia.com/legal/article-3073-cyber-frauds-in-the-indian-banking-industry.html

*****

डॉ. साकेत कुमार सहाय

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 8800556043
ई-मेल:- hindisewi@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

पृष्ठभूमि:

आज साइबर अपराध भारत ही नहीं बल्कि पूरे विश्व में एक केंद्रीय विषय बना हुआ है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) के अनुसार वर्ष 2020 में भारत में साइबर अपराध के 50,035 मामले सामने आए थे जो एक वर्ष पहले की तुलना में 11.8 फीसदी से अधिक है। सरकार, भारतीय रिज़र्व बैंक सहित सभी बैंक इस विषय पर सतर्क हैं। भारतीय रिज़र्व बैंक भी उपभोक्ताओं को साइबर अपराधों के प्रति सजग रहने का आह्वान करता रहता है।

जून, 2021 की भारतीय रिज़र्व बैंक की वित्तीय स्थिरता रिपोर्ट के अनुसार कोरोना महामारी के बाद बैंकिंग प्रणाली के लिए साइबर अपराध को ज्यादा बड़ा खतरा माना जा रहा है। रिपोर्ट के मुताबिक अक्तूबर, 2020 से ही यह क्षेत्र उच्च जोखिम क्षेत्र में शामिल है। उल्लेखनीय है कि भारतीय रिज़र्व बैंक समय-समय पर साइबर धोखाधड़ी को लेकर आम आदमी को आगाह करता रहा है। भारतीय रिज़र्व बैंक के पूर्व गवर्नर श्री रघुराम राजन ने अपने कार्यकाल में बड़ी बेबाकी से यह कहा था कि ''साइबर ठग भारतीय रिज़र्व बैंक के गर्वनर को भी आम ग्राहक समझकर लुभावनी पेशकश करते हैं।''

इस रिपोर्ट के मुताबिक

- **भारत में रोजाना साइबर धोखाधड़ी के 3137 मामले दर्ज हो रहे हैं।**
- **25 हजार करोड़ रूपये साइबर धोखाधड़ी के सालाना मामले हैं।**
- **लोगों ने वर्ष 2019 में 1.25 लाख करोड़ रुपये साइबर धोखाधड़ी से गंवाया है।**
- **कोरोना के बाद डिजिटल भुगतान बढ़ने से ऐसे मामलों में 41% की वृद्धि हुई है।**

(स्रोत-हिंदुस्तान, पटना, 03 जुलाई, 2021)

आंकड़े बताते हैं कि ऑनलाइन तकनीक के प्रयोग में बढ़ोत्तरी के साथ ही बैंकिंग क्षेत्र में साइबर आक्रमणों की संख्या, अंतराल एवं प्रभाव में भी वृद्धि हुई है।

बैंकिंग में साइबर अपराधों का स्वरूप एवं सुरक्षात्मक उपाय

आए दिन समाचार पत्रों में प्रकाशित रिपोर्टों से यह स्पष्ट है कि वर्तमान में बैंक इलेक्ट्रॉनिक एवं पेपर दोनों ही माध्यमों में मौजूद धोखाधड़ी से जूझ रहे हैं, पर इससे भी बड़ी समस्या है साइबर धोखाधड़ी, क्योंकि इसमें सब कुछ आभासी है। बैंकिंग प्रणाली में साइबर अपराधों के स्वरूप को यथाशीघ्र समझना जरूरी है एवं इस हेतु यथासंभव सुरक्षात्मक उपाय भी अपनाया जाना आवश्यक है ताकि साइबर अपराध के गंभीर खतरों से बैंकिंग प्रणाली को सुरक्षित रखा जा सके।

हालांकि, इस चुनौती से निपटने हेतु बैंकों ने साइबर जोखिम प्रबंधन की ओर विशेष ध्यान दिया है। जी. गोपाल कृष्ण समिति के निर्देशों के अनुरूप सुरक्षा, इलेक्ट्रॉनिक बैंकिंग, तकनीकी जोखिम प्रबंधन एवं साइबर धोखाधड़ी से निपटने हेतु उपाय भी लागू किए हैं, फिर भी यह कहा जा सकता है कि बैंकों द्वारा अपनाए गए ये उपाय फिलहाल शुरूआती दौर में ही हैं, क्योंकि जिस प्रकार से डिजिटल बैंकिंग अपनाने वालों की संख्या तथा इससे जुड़े साइबर अपराध के खतरे बढ़ते जा रहे हैं उसको देखते हुए यह आवश्यक है कि बैंकों को अपने स्तर पर नए संवर्धन एवं विकास और इस क्षेत्र में हर दिन उत्पन्न नई कठिनाइयों के आधार पर अपनी नीतियों, प्रणालियों एवं तकनीक को सक्रिय रूप से तैयार एवं संशोधित करना होगा।

यह ज्ञात तथ्य है कि धोखाधड़ी के अधिकांश मामलों के पीछे शक्ति, लोभ, प्रचार, बदला, आनंद अथवा विध्वंसात्मक सोच की ही प्रवृत्ति पाई गई है। निश्चय ही अपराधी मानसिकता से निपटना दुरूह कार्य है और इसकी दुरूहता तब ज्यादा बढ़ जाती है जबकि यह ऑनलाइन हो। ऐसे में संस्थागत, वैयक्तिक, आभासी माध्यमों से की जाने वाली साइबर अपराधों से निपटने का एकमात्र उपाय है- **सुदृढ़ एवं सुरक्षात्मक प्रबंधन।**

बैंकिंग में साइबर अपराधों का स्वरूप

साइबर अपराधों की चुनौती इसलिए भी ज्यादा बड़ी है क्योंकि वित्तीय लाभ लेने के लिए कोई भी प्रेरित हो सकता है और इस क्षेत्र में लाभ प्राप्ति की संभावना सबसे अधिक है। सामान्यत: बैंकिंग प्रणाली में धोखाधड़ी के अंतर्गत निम्नलिखित शामिल किए जाते हैं- अपने ग्राहक को जानिए तथा अपने कर्मचारियों को जानिए नीति का ठीक से पालन नहीं होना, निर्धारित आंतरिक एवं बाह्य प्रक्रियाओं का पालन नहीं करना, अति विश्वास, धोखाधड़ी की रिपोर्टिंग नहीं करना, ग्राहकों का जागरूक नहीं होना आदि एवं डिजिटल धोखाधड़ी में ए.टी.एम. डेबिट/ क्रेडिट कार्ड से संबंधित धोखाधड़ी, स्किमिंग, कार्ड क्लोनिंग, ऑनलाइन पासवर्ड या पिन की चोरी, मोबाइल धोखाधड़ी, फिशिंग, विशिंग आदि शामिल हैं। **सहज, सुरक्षित एवं विश्वसनीय डिजिटल बैंकिंग सेवा प्रदान करने के बीच एक बड़ी चुनौती के रूप में उपस्थित है- साइबर धोखाधड़ी।**

विचारणीय तथ्य यह भी है कि बढ़ते साइबर अपराध की वजह से देश की बड़ी आबादी डिजिटल लेन-देन से आज परहेज कर रही है। सरकार के लिए हाल के दिनों में घटित रैनसमवेयर जैसे बड़े साइबर हमले, आधार कार्ड, डेबिट कार्ड का डेटा लीक होना आदि बड़ी चुनौती हैं। जब से ऑनलाइन बैंकिंग पर जोर बढ़ा है तब से हर दिन ऐसे मामले सामने आने लगे हैं। उदाहरण के लिए कोरोना महामारी के दौरान कुछ लोगों ने बैंक शाखाओं तक जाना बंद कर दिया जिससे धोखेबाजों को 'अपने ग्राहक को जानिए" (केवाईसी) संबंधी दस्तावेजों को अद्यतन कराने जैसे बहाने धोखाधड़ी के एक मौके के रूप में मिल गया। इस प्रक्रिया में धोखेबाज ग्राहक को एसएमएस के माध्यम से यह चेतावनी संदेश भेजता है कि उसका कार्ड या बैंक खाता ब्लॉक कर दिया जाएगा। यह संदेश पाने वाला ग्राहक उसकी वैधता पर विचार किए बगैर कदम उठा लेता है। जब वह एसएमएस में दिए गए नंबर पर कॉल करता है तो उसे अपनी केवाईसी जानकारी की पुष्टि के नाम पर निजी विवरण देने को कहा जाता है। इसके अलावा, अन्य कई प्रकार के धोखे हैं यथा: सिम स्वैप, यूपीआई से जुड़ी धोखाधड़ी आदि जिसमें फंसकर ग्राहक धोखेबाजों के चक्कर में आ जाते हैं।

बैंकिंग में साइबर अपराधों की रोकथाम हेतु सुरक्षात्मक उपाय

बैंकिंग प्रणाली से जुड़ें अधिकांश साइबर अपराध के मामलों को देखा जाए तो यह कहा जा सकता है कि बैंकिंग क्षेत्र में साइबर सुरक्षा प्रबंधन की तीन स्तरों पर जरूरत है- बैंक, विनियामक एवं ग्राहक। साइबर अपराध के समुचित निपटान, कार्रवाई, समाधान एवं नियंत्रण में बैंक, हितधारक एवं विनियामक तीनों की महत्वपूर्ण भूमिका है। ग्राहक स्तर पर यदि देखें तो पहला उपाय यह है कि अपने डेटा को सुरक्षित रखें और उससे भी महत्वपूर्ण है

'थोड़े अविश्वासी बनें'। आज के दौर में यह कहा जा सकता है कि अपनी डिजिटल गतिविधियों को लेकर जितने सतर्क और जागरूक हम खुद होंगे, उतना ही ज्यादा हम सुरक्षित रह सकेंगे।

साइबर सुरक्षा प्रबंधन हेतु बैंकों एवं विनियामकों (भारत सरकार, भारतीय रिज़र्व बैंक) तथा भारत सरकार द्वारा की गई कार्रवाई

- **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन या आईसीईआरटी)**

भारत सरकार साइबर खतरों के प्रति सचेत है। इसी के तहत सीईआरटी-इन (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल) गठित है। यह संगठन साइबर सुरक्षा को दुरूस्त करने की दिशा में सक्रिय एवं प्रतिक्रियात्मक सेवाओं के साथ-साथ दिशानिर्देश भी प्रदान करती है।

साइबर संकट प्रबंधन योजना

बैंक साइबर संकट प्रबंधन योजना (सीसीएमपी) को प्रभावी रुप से अपना रहे हैं। सी.सी.एम.पी. के तहत बैंक के साइबर धोखाधड़ी कक्ष निम्नलिखित चार पहलूओं पर कार्रवाई सुनिश्चित करते हैं: (i) पहचानना (ii) जवाबी कार्रवाई (iii) सुधार तथा (iv) नियंत्रण, आदि।

साथ ही बैंकों के लिए यह जरूरी है कि विभिन्न प्रकार के साइबर खतरों, जैसे सेवा से इंकार, डिस्ट्रीब्यूटेड डिनायल ऑफ़ सर्विसेस (डीडीओएस), रैनसमवेयर/ क्रिप्टोवेयर, घातक मालवेयर, व्यवसाय ई-मेल धोखाधड़ी जैसे - स्पैम, ई-मेल फिशिंग, स्पियर फिशिंग, व्हेलिंग, विशिंग धोखाधड़ी, ड्राइव-बाय डाऊनलोड, ब्राउज़र गेटवे धोखाधड़ी, घोस्ट एडमिनिस्ट्रेटर एक्सप्लॉइट्स, पहचान संबंधी धोखाधड़ी, मेमोरी अपडेट धोखाधड़ी, पासवर्ड संबंधी धोखाधड़ी से निपटने हेतु आवश्यक सुरक्षात्मक तथा सुधारात्मक उपाय प्रबंधित करें।

- **एसओसी (सिक्यूरिटी ऑपरेशन सेंटर) केंद्र**

बैंकों द्वारा गठित सिक्यूरिटी ऑपरेशन सेंटर (एसओसी) से रीयल टाइम में साइबर जोखिमों की निगरानी तथा प्रबंधन सुनिश्चित की जा रही है। बैंकों के समामेलन के बाद बड़े बैंकों को देखते हुए इन केंद्रों को मजबूत किया जाना और भी आवश्यक है।

- **साइबर सुरक्षा मुस्तैदी संकेतक**

बैंक साइबर खतरों से अपने डेटा को सुरक्षित करने हेतु साइबर रेजिलिएन्स फ्रेमवर्क के तहत साइबर सुरक्षा मुस्तैदी संकेतक भी अपना रहे हैं।

- **साइबर-सुरक्षा घटनाओं से संबंधित सूचनाओं को भारतीय रिज़र्व बैंक के साथ साझा करना**

बैंकों द्वारा उनके संगठन में पायी गई साइबर–घटनाओं को भारतीय रिज़र्व बैंक के साथ साझा करने से (चाहे वे सफल हों या असफल प्रयास के रूप में हों) सामूहिक खतरे की आसूचना, समय पर अलर्ट्स तथा सक्रिय साइबर सुरक्षा उपायों को अपनाने में सहायता मिलती है।

- **हितधारकों/ शीर्ष प्रबंधन/ बोर्ड के बीच साइबर-सुरक्षा जागरूकता**

साइबर-सुरक्षित माहौल बनाने के लिए संपूर्ण संगठन की प्रतिबद्धता आवश्यक है। यह आवश्यक है कि बैंक अपने ग्राहकों, वेंडरों, सेवा-प्रदाताओं तथा अन्य संबंधित हितधारकों के बीच साइबर रेजिलिएन्स उद्देश्यों की समझ सक्रियता के साथ पैदा करें। यह भी महत्वपूर्ण है कि हितधारकों (ग्राहकों, कर्मचारियों, भागीदारों तथा वेंडरों) को साइबर-हमले से होने वाले संभाव्य प्रभाव के बारे में जानकारी दी जाए।

साइबर अपराध से बचाव हेतु अन्य उपाय

- **ग्राहक सूचना की सुरक्षा सुनिश्चित करना**

जब से बैंकिंग उद्योग ने प्रौद्योगिकी आधारित सेवाएं देना शुरू किया है तब से इस क्षेत्र में साइबर खतरे बढ़ गए हैं। इसका बड़ा कारण है कि देश में प्रौद्योगिकी आधारित सेवाओं के प्रति लोगों की अनभिज्ञता के कारण आज भी बहुत लोगों को ए.टी.एम. कार्ड का उपयोग नहीं आता है, अत: वे पैसा निकालने के लिए ए.टी.एम में जाकर अपना कार्ड किसी दूसरे के हवाले कर देते है और अपने कार्ड पर या डायरी में लिखी पिन संख्या भी उन्हें दिखा देते हैं जिसके परिणामस्वरूप उनके कार्ड का दुरूपयोग करना बेहद आसान हो जाता है। इन घटनाओं की गंभीरता को देखते हुए बैंकों द्वारा इस हेतु वित्तीय साक्षरता अभियान भी चलाया जा रहा है।

- **भारत में आम आदमी के स्तर पर सूचना प्रौद्योगिकी इंफ्रास्ट्रक्चर संबंधी जागरूकता व जानकारी**

आम तौर पर उपभोक्ताओं को जानकारी के अभाव, इन्टरनेट की खराब स्पीड के कारण ऑनलाइन लेन-देन में काफी दिक्कतें होती हैं। अत: यह जरूरी है कि बैंक इन आंकड़ों के कस्टोडियन (अभिरक्षक) के रूप में, इसकी गोपनीयता, सत्यनिष्ठा तथा उपलब्धता को संरक्षित करने के लिए समुचित प्रबंधन तंत्र बनाएं।

- **वित्तीय साक्षरता, जागरूकता एवं सतर्कता संबंधी उपाय**

कार्ड क्लोनिंग, फिशिंग, स्किमिंग, ऑनलाइन पासवर्ड की चोरी, विशिंग इत्यादि को पर्याप्त सतर्कता एवं जागरूकता के माध्यम से काफी हद तक कम किया जा सकता है।

साइबर अपराध से बचाव हेतु आवश्यक नियम एवं उपाय -

- ए.टी.एम. के प्रयोग से पूर्व ग्राहक इसकी सुरक्षा स्थिति यथा ए.टी.एम कार्ड स्लॉट आदि की जांच कर लें।
- कार्ड एवं पिन नंबर किसी भी व्यक्ति को न दें।
- पासवर्ड कठिन बनाएं जिसमें कई तरह के चिन्हों एवं अंकों का इस्तेमाल हो और वह छोटा न हो।
- वेबसाइट का इस्तेमाल करते समय उसके यूआरएल पर जरूर गौर करें।
- निजी लैपटॉप पर कार्यालय का काम करते समय एक अलग यूजर खाता बनाएं।
- सिस्टम एवं सॉफ्टवेयर को हमेशा अपडेट रखें।
- अपने घर की वाई-फ़ाई की डिफ़ॉल्ट सेटिंग एवं पासवर्ड को बदल दें।
- सोशल मीडिया पर साझा करने वाली सामग्री पर विशेष ध्यान रखें।
- फोन पर संवेदनशील जानकारी मांगे जाने पर मना कर दें।
- कार्ड प्राप्ति के तुरंत बाद पीछे या चेकबुक पर दर्ज नंबर पर कॉल कर इसकी पुष्टि करें।

उपसंहार

निष्कर्षत: साइबर सुरक्षा को कारगर बनाने हेतु सरकार, भारतीय रिज़र्व बैंक, बैंक, भुगतान कंपनियां एवं साइबर सुरक्षा तंत्र सभी को एक टीम की तरह कार्य करना होगा। साइबर अपराध से जुड़े अधिकांश मामलों में यह देखा गया है कि अधिकांश अपराध पेमेंट कार्ड की जानकारी चुराने और एटीएम ढांचे के जरिए नुकसान पहुंचाने जैसी चीजों से जुड़ा रहा है। सरकार ने धोखाधड़ी का पता लगाने और जांच करने के लिए एक राष्ट्रीय हेल्पलाइन नंबर 155260 भी शुरू किया है। यह कदम साइबर अपराध नियंत्रण में बेहद उपयोगी साबित होगा। बैंक साइबर सुरक्षा जोखिम प्रबंधन हेतु बीमा भी ले सकते हैं। साइबर अपराध से निपटने हेतु सभी हितधारकों में एक संतुलित एवं दूरगामी सोच विकसित करना अत्यन्त आवश्यक है और यह कार्य सबके सहयोग से ही संभव है।

संदर्भ स्रोत:

दैनिक हिंदुस्तान, बिजनेस स्टैंडर्ड के विभिन्न अंक, भारतीय रिज़र्व बैंक की वेबसाइट

*****

डॉ. सुनील कुमार

पदनाम:- वरिष्ठ प्रबंधक (राजभाषा)
संस्था का नाम:- यूको बैंक
मोबाइल नं. :- 9689924355
ई-मेल:- vmsunilk78@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

भूमिका

न्यूटन की गति के तृतीय नियम के अनुसार 'प्रत्येक क्रिया के बराबर विपरीत प्रतिक्रिया होती है।' अर्थात् जब कभी एक वस्तु किसी दूसरी वस्तु पर बल लगाती है तो दूसरी वस्तु भी पहली वस्तु पर बराबर और विपरीत बल लगाती है। प्रयोग किए गए दोनों बल परिमाण में बराबर होते हैं परंतु दिशा में विपरीत होते हैं। प्रायः ऐसा देखा गया है कि जितनी तीव्र गति से तकनीक का विकास होता है उतनी ही तीव्रता से साइबर अपराधी भी उसमें कुछ त्रुटियां व कमियां निकालकर साइबर अपराध को अंजाम देते हैं।

वर्तमान परिप्रेक्ष्य में बैंकिंग क्षेत्र में लेनदेन संबंधी कपट की घटनाएं आम सी हो गई हैं। आज पूरी दुनिया इंटरनेट और कम्प्यूटर के माध्यम से एक दूसरे से जुड़ी हुई है जिसके बहुत सारे लाभ है और उसके साथ ही बहुत सारे खतरे भी हैं। इससे सिर्फ आम ग्राहक ही नहीं बल्कि बैककर्मी भी साइबर अपराध जैसी घटना के शिकार हो रहे हैं। भारत में बैंकिंग, एटीएम/डेबिट कार्ड और ऑनलाइन बैंकिंग खाते के माध्यम से बड़े पैमाने पर साइबर हमले हो रहे हैं। ग्लोबल स्तर पर अध्ययन करने वाली रिसर्च फर्म के ताजा सर्वे के अनुसार वित्तीय सेवा क्षेत्र (फाइनेंशियल सर्विसेज सेक्टर) में साइबर अपराध का खतरा सबसे अधिक है।

ऑनलाइन बैंकिंग और वित्तीय लेनदेन के लिए मोबाइल का उपयोग बढ़ने से साइबर अपराध का खतरा और बढ़ गया है। साइबर अपराधी अपनी तकनीक को लगातार विकसित और अपग्रेड कर रहे हैं। इसके अलावा अब वे वित्तीय सूचनाओं की चोरी के बजाय कारोबारी जासूसी और सरकारी सूचनाएं हासिल करने की वारदातों को अंजाम देने पर ज्यादा ध्यान दे रहे हैं।

क्या है साइबर अपराध ?

साइबर अपराध के तहत आधुनिक दूरसंचार नेटवर्क (इंटरनेट, मोबाइल फोन) का अवैध रूप से उपयोग किया जाता है जिससे अनभिज्ञ व अनजान व्यक्ति शारीरिक या मानसिक रूप से प्रताड़ित होते हैं एवं उनके मान-सम्मान और प्रतिष्ठा को नुकसान पहुँचता है। साइबर अपराध किसी व्यक्ति या राष्ट्र की सुरक्षा एवं वित्तीय स्वास्थ्य के लिए खतरा हो सकता है। साइबर अपराध एक अवैध कार्य है जहां कंप्यूटर को साधन या लक्ष्य या दोनों ही तरीके से उपयोग किया जाता है। लोगों को धोखा देने और अपने चंगुल में फंसाने के लिए अधिकतर घोटाले बाज जाली/नकली साइट को उपयोग करते हैं ताकि लोगों को पता भी न चले और उनका काम भी आसानी से हो जाए।

आज दुनिया भर में लोग ऑनलाइन इंटरनेट के माध्यम से डेटा फेच कर घर बैठे लोगों की निजी जानकारियों की चोरी कर रहे हैं जिसे साइबर अपराध कहते हैं। आज के अत्याधुनिक तकनीकी युग में लोग अपने जीवन को

सरल बनाने के लिए कई उपकरणों का प्रयोग करते हैं। वैश्वीकरण के माध्यम से दुनिया भर के लोग एक दूसरे से आसानी से जुड़ पाने में सक्षम हुए हैं। तकनीक का आसानी से उपलब्ध होना एवं इसका लगातार प्रयोग, लोगों के संवाद के तरीकों एवं जीवन के संचालन पर गहरा प्रभाव डालता है।

साइबर क्राइम को कम्प्यूटर क्राइम या इंटरनेट क्राइम के नाम से भी जाना जाता है। कम्प्यूटर और इंटरनेट के माध्यम से की गई किसी भी तरह की आपराधिक गतिविधियां साइबर क्राइम की श्रेणी में आती है। साइबर क्राइम के माध्यम से कहीं दूर बैठाकर आपके सरकारी या महत्वपूर्ण कारोबारी दस्तावेजों या आपकी निजी महत्वपूर्ण जानकारी को इंटरनेट और कम्प्यूटर के माध्यम से चुरा सकता है। साइबर क्राइम में गैर-निधि अपराध भी शामिल है।

बैंकिंग में साइबर अपराध की एक सच्ची घटना

ग्राहकों की शिकायतें सुनते-सुनते हमें कभी-कभी ऐसे कॉल भी आते हैं :-

" हलऊ सर ! हमार खतवा से पचास हजार रूपइयवा कट गया है सर ! पईसवा कटने का मेरे मोबइलवा पर मैसेज आया है ! एटीएम कार्डवा तअ हमरे लागे ही है सर! हम तअ डेढ़- दू-महीना भर से एटीएम मशीनवा में गइबे नहीं किए हैं ! पर हमरा खतवा से पईसवा कईसे कट गया सर ! बैंकवा में पईसवा रखले-रखले उड़ जाता है काअ ? हमरा पईसवा लौटा दीजिए सर, नहीं तअ हम पुलिस टिशनी में आपका कांपलेंट (शिकायत) करेंगे ! हमनी सबन बड़ी मेहनत से पईसवा जोड़-जोड़ के जमा करअ हिला सर ! दू महीना बाद हमर बेटिया के शादी है सर। हमर बेटवा दिल्ली में पढ़ता है। ओकरा ला भी पईसवा भेजना है। हमर ई पईसवा कब तलक आ जाईगा सर ? हलऊ सर ! हम काअ करें सर ? हमरा मदद कीजिए सर ! नहीं तअ हम कहीं के नहीं रहेंगे सर !

यह व्यथा एक बैंक खाताधारक (ग्राहक) की है जो मगही और हिंदी (भाषा) मिलाकर बोल रहा है और बैंक में अपनी शिकायत बयां कर रहा है कि उसके खाते से पचास हजार रुपए (रु. 50,000/-) कट गए हैं जबकि उसके संबंधित खाते का एटीएम उसके पास है। यह शिकायत आज आम शिकायत सी हो गई है। एटीएम कार्ड की क्लोनिंग कर धोखाधड़ीकर्ता आसानी से बैंक खाताधारकों के पैसे को निकाल लेते हैं और इसका पता तब चलता है जब खाताधारक के मोबाइल पर इसका संदेश जाता है।

आजकल ऐसे ही लॉटरी के नाम पर ठगी का धंधा काफी तेजी से चल रहा है। केबीसी के स्टाइल में मोबाइल पर एक आसान सा प्रश्न (संकेत / clue के साथ) चार विकल्प के साथ भेज दिया जाता है और ग्राहक उसका जवाब आसानी से दे देता है तुरंत ही एक मैसेज आता है। बधाई हो ! (Congratulations!) आप काफी भाग्यशाली हैं। पूरे भारत में यह प्रश्न भेजा गया था जिसमें करोड़ों लोगों ने भाग लिया परंतु इसका सही जवाब सिर्फ आपने दिया है। आप सात लाख रुपए (रु. 7.00 लाख) का इनाम जीत गए हैं। आपके इनाम की राशि आपके खाते में भेज दी जाएगी। तुरंत ही एक कॉल आता है बधाई हो सर ! / मैडम ! आप हमारे इस प्रश्न के विजेता हैं। कृपया आप अपने खाते का विवरण हमें भेज दें ताकि हम पुरस्कार की राशि को आपके खाते में जमा कर सकें। आप चाहे तो अपने खाते का विवरण हमें अपने मोबाइल से भी बता सकते हैं ताकि हम संबंधित राशि को तुरंत ही आपके खाते में जमा कर सकें।

कॉल सेंटर पर बैठे धोखाधड़ीकर्ता फोन करता है कि सर मैं आपके बैंक से बोल रहा हूं। आपके एटीएम कार्ड का अंतिम चार अंक (xxxxxxxxx4xx2) ये है। कृपया अपने एटीएम कार्ड का पूरा नंबर, एक्सपायरी डेट और सीवीवी नंबर बताएं। ग्राहक बता देता है। फिर धोखाधड़ीकर्ता कहता है कि आपके मोबाइल पर एक ओटीपी नंबर आया होगा कृपया उसे बताएं। फिर ग्राहक को याद आता है कि सीवीवी नंबर, पासवर्ड, पिन नंबर, ओटीपी आदि किसी को भी नहीं बताना चाहिए। ग्राहक धोखाधड़ीकर्ता से कहता है कि ये सब तो किसी को

नहीं बताना चाहिए। फिर धोखाधड़ीकर्ता चालाकी से कहता है कोई बात नहीं, आप मत बताइये फिर आप के इनाम के सात लाख रुपए (रु. 7.00 लाख) आने में दो से तीन महीने लग जाएंगे। अगर आप अभी ओटीपी नंबर बता दें तो आपके इनाम का पैसा अभी आ जाएगा। ग्राहक धोखाधड़ीकर्ता के चंगुल में आ जाता है और ओटीपी बता देता है। फिर कुछ ही मिनटों में ग्राहक के खाते से नब्बे हजार रुपये साँय-साँय (तुरंत-तुरंत) निकलने के मैसेज आने लगते हैं और ग्राहक ठगी का शिकार हो जाता है।

साइबर अपराध की घटना घटित होने पर क्या करें ?

ऐसी घटना घटित होने पर हमें साइबर क्राइम हेल्पलाइन नंबर 1930 पर तुरंत कॉल करना चाहिए और अपनी शिकायत को https://cybercrime.gov.in दर्ज करनी चाहिए। संबंधित शिकायत दर्ज करने में निम्नलिखित जानकारी दी जानी चाहिए : -

- ✓ शिकायतकर्ता का पंजीकृत मोबाइल नंबर
- ✓ बैंक का नाम और खाता संख्या जिससे संबंधित राशि (पैसे) निकाली गई है
- ✓ लेनदेन का पूर्ण विवरण (आईडी और लेनदेन की तिथि)
- ✓ डेबिट / क्रेडिट कार्ड के नंबर जिसे कार्ड का उपयोग कर धोखाधड़ी / साइबर अपराध किया गया है
- ✓ लेनदेन की स्क्रीनशॉर्ट या धोखाधड़ी (साइबर अपराध) संबंधी कोई अन्य तस्वीर (इमेज), यदि उपलब्ध हो

शिकायत दर्ज करने के उपरांत शिकायतकर्ता को एसएमएस / ई-मेल के माध्यम से सिस्टम जनरेटेड लॉगिन आईडी / पावती संख्या प्राप्त होगी। उपर्युक्त सिस्टम जनरेटेड लॉगिन आईडी / पावती संख्या का उपयोग करते हुए शिकायतकर्ता को 24 घंटे के अंदर नैशनल साइबर क्राइम रिपोर्टिंग पोर्टल (www.cybercrime.gov.in) पर अपनी शिकायत दर्ज करनी चाहिए।

सुगमता के साथ सावधानी भी जरूरी

आजकल इंटरनेट के माध्यम से हम सारी दुनिया के साथ जुड़ गए हैं। आज अधिकांश लोग इंटरनेट पर आश्रित हैं। दुनिया की अधिकांश चीजों को इंटरनेट ने एक प्लेटफॉर्म पर ला दिया है। मानो सारी दुनिया मुट्ठी में समाहित हो गई हो ! आज हमारी दिनचर्या की अधिकांश जरूरत की चीजों को इंटरनेट ने सुलभ व सुगम बना दिया है। सामाजिक नेटवर्किंग, ऑनलाइन ख़रीदारी, जानकारी का आदान-प्रदान, गेमिंग, ऑनलाइन पढ़ाई, ऑनलाइन नौकरियां आदि जिसके बारे में भी मनुष्य कल्पना कर सकता है, वे सारी चीजें बस इंटरनेट पर एक क्लिक से उपलब्ध हो जाती हैं। परंतु जो चीजें हमें आसानी से मिल जाती हैं उसके साथ हमें काफी सावधानी से और संभलकर चलना चाहिए।

साइबर अपराध एक गंभीर खतरे के रूप में विकसित हो रहा है। दुनिया भर की सरकारों, पुलिस विभागों और गुप्तचर इकाइयों ने साइबर अपराध के खिलाफ प्रतिक्रिया देना शुरू कर दिया है। सीमा पार साइबर खतरों पर अंकुश लगाने के लिए अंतर्राष्ट्रीय स्तर पर भी कई प्रयास किए जा रहे हैं।

वर्तमान में, इंटरनेट का उपयोग अधिकांश क्षेत्रों में किया जा रहा है। इंटरनेट के बढ़ते फायदों के साथ साइबर अपराध जैसे भयावह मुद्दे भी उभर कर आए हैं। साइबर अपराध अलग-अलग तरीकों से घटित होते हैं। कुछ वर्षों पहले तक इन सारी चीजों के बारे में इतनी जागरुकता नहीं थी। अन्य देशों के साथ-साथ भारत में भी साइबर अपराध की घटनाएं दिन-प्रतिदिन बढ़ती जा रही हैं।

साइबर अपराध को दो तरह से वर्गीकृत किया गया है : -

1. पहला, ऐसे अपराध जिनमें कंप्यूटर को लक्ष्य के रूप में उपयोग किया जाता है।

2. दूसरा, ऐसे अपराध जिनमें कंप्यूटर/लैपटॉप को हथियार की तरह इस्तेमाल किया जाता है।

अनधिकृत उपयोग एवं हैकिंग

अनधिकृत उपयोग एक ऐसा अपराध है जिसमें कंप्यूटर के मालिक की अनुमति के बिना कंप्यूटर का किसी भी प्रकार से अवैध उपयोग किया जाता है। हैकिंग एक ऐसा अपराध है जिसमें कंप्यूटर प्रणाली में अवैध घुसपैठ करके उसको नुकसान पहुंचाया जाता है।

वेब हाईजैकिंग

यह एक ऐसा अपराध है जिसमें किसी व्यक्ति की वेबसाइट पर अवैध रूप से सशक्त नियंत्रण कर लिया जाता है। इस प्रकार वेबसाइट का मालिक उस वेबसाइट पर नियंत्रण एवं ज़रूरी जानकारी खो देता है।

साइबर स्टॉकिंग

यह एक ऐसा अपराध है जिसके माध्यम से किसी व्यक्ति को बार-बार उत्पीड़न का शिकार बनाया जाता है; पीड़ित का पीछा करके, तंग करके, कॉल द्वारा परेशान करके, संपत्ति के साथ छेड़छाड़ करके आदि। स्टॉकिंग के उपरांत पीड़ित को मानसिक एवं शारीरिक रूप से हानि पहुंचाना मकसद होता है। अपराधी पीड़ित की सारी जानकारी अवैध रूप से इकट्ठा करके एवं इंटरनेट पर उनकी गलत छवि दिखाकर हानि पहुंचाने का लक्ष्य रखते हैं, ताकि भविष्य में भयादोहन करके उनका अनुचित लाभ उठा सकें।

सॉफ्टवेयर पायरेसी

यह एक ऐसा अपराध है जिसमें वास्तविक प्रोग्राम की अवैध प्रतिलिपि बनाकर जालसाजी द्वारा वितरित किया जाता है। इसमें और भी अपराध शामिल है, जैसे- सत्वाधिकार उल्लंघन, ट्रेडमार्क उल्लंघन, कंप्यूटर सोर्स कोड की चोरी आदि शामिल हैं।

सलामी अटैक / हमला

यह एक तरीके का वित्तीय अपराध है। ठगी इतनी छोटी होती है कि पकड़ पाना बहुत मुश्किल होता है। उदाहरण के लिए अगर कोई बैंक कर्मचारी इस प्रकार की धोखाधड़ी कर और हर खाताधारक के बैंक खाते से हर माह केवल रु.5 की कटौती करें तो कोई भी इतनी थोड़ी धनराशि के कटने पर पकड़ नहीं पाएगा तथा अपराधी के पास महीने के अंत में काफी अच्छी मात्रा में धन राशि इकट्ठी हो जाती है।

सर्विस अटैक

यह एक ऐसा अपराध है, ऐसा हमला है जिसमें पीड़ित के नेटवर्क या विद्युत संदेश पात्र को बेकार यातायात एवं अन्य संदेशों से भर दिया जाता है। यह सब इसलिए किया जाता है ताकि पीड़ित को जानबूझकर तंग किया जा सके या पीड़ित अपना ई-मेल उपयोग ना कर पाए।

वायरस अटैक

वायरस ऐसे प्रोग्राम को कहा जाता है जो कंप्यूटर के अन्य प्रोग्राम को संक्रमित करने की क्षमता रखते हैं अथवा अपनी प्रतियां बना कर दूसरे प्रोग्राम में फैल जाते हैं। यह दुर्भावनापूर्ण सॉफ़्टवेयर होते हैं जो अपने आप को किसी दूसरे सॉफ्टवेयर से जोड़ लेते हैं अथवा कंप्यूटर को हानि पहुंचाते हैं। ट्रोजन हॉर्स, टाइम बम, लॉजिक बम, रैबिट आदि यह सभी दुर्भावनापूर्ण सॉफ़्टवेयर हैं। वायरस कंप्यूटर पर कुछ इस तरीके से प्रभाव डालते हैं कि या तो कंप्यूटर में मौजूद जानकारी को बदल देते हैं या नष्ट कर देते हैं ताकि वह इस्तेमाल करने लायक ना रह पाए।

क्या होती है जाली/ नकली साइट ?

जाली/ नकली साइट के नाम से ही प्रतीत हो जाता है कि यह एक झूठी वेबसाइट है, जो हू-ब-हू आपके बैंक के वेबसाइट, खरीदारी करने वाली साइट या पेमेंट गेटवे इंटरफेस जैसा होता है। ऑनलाइन ख़रीदारी या कोई भी ऑनलाइन लेन-देन करने के लिए जैसे ही आप वहां अपने क्रेडिट कार्ड, डेबिट कार्ड, इंटरनेट बैंकिंग का यूजर नेम, लॉगिन पासवर्ड, ट्रांजेक्शन पासवर्ड या ओ.टी.पी दर्ज करते हैं, वो इस विवरण को कॉपी कर लेता है और बाद में इसका प्रयोग गलत तरीके से गलत कार्यों के लिए कर सकता है। जाली/ नकली वेबसाइट का संचालन एक संगठित ग्रुप के अपराधियों द्वारा किया जाता है।

साइबर अपराध रोकने के सुरक्षात्मक उपाय :-

- अपने इंटरनेट की बैंकिंग और बैंकिंग लेन-देन का इस्तेमाल कभी भी सार्वजनिक स्थान जैसे- साइबर कैफे, ऑफिस, पार्क, सार्वजनिक मीटिंग और किसी भीड़-भाड़ वाले स्थान पर न करें। किसी भी प्रकार के बैंकिंग लेन-देन के लिए आप अपने पर्सनल कम्प्यूटर या लैपटॉप का ही इस्तेमाल करें।
- जब कभी भी आप अपने इंटरनेट बैंकिंग या किसी भी जरुरी अकाउंट में लॉगिन करें, तो काम खत्म कर अपने अकाउंट को लॉगआउट करना न भूलें और जब आप लॉगिन कर रहे हो तब इस बात पर जरूर धयान दें कि पासवर्ड टाइप करने के बाद कम्प्यूटर द्वारा पूछे जा रहे ऑप्शन रिमेंबर पासवर्ड या कीप लॉगिन में क्लिक न करें।
- कभी भी आप अपने बैंकिंग यूजर नेम, लॉगिन पासवर्ड, ट्रांजेक्शन पासवर्ड, ओ. टी.पी, गोपनीय प्रश्नों या गोपनीय उत्तर को अपने मोबाइल, नोटबुक, डायरी, लैपटॉप या किसी कागज पर न लिखें।
- हमेशा आप ऐसा पासवर्ड सेट करें जो आपको आसानी से याद रहे और आपको इसे कहीं लिखने की आवश्यकता न पड़े।
- अपना पासवर्ड कभी भी अपने नाम, पता, गली नंबर, जन्म तिथि, परिवार के सदस्यों के नाम, विद्यालय के नाम या अपने वाहनों के नंबर पर न बनाएं जिसका दूसरों द्वारा आसानी से अनुमान न लगाया जा सके।
- अगर किसी वेबसाइट पर कोई पॉपअप खुले और आपको कुछ आकर्षक गिफ्ट या इनाम ऑफर करे तब आप अपनी पर्सनल जानकारी या बैंक अकाउंट नंबर या बैंक से संबंधित कोई भी जानकारी न भरें।
- आप अपने कम्प्यूटर में अगर इंटरनेट का प्रयोग करते हैं तो सबसे पहले आप अपने पर्सनल कम्प्यूटर को पासवर्ड से सुरक्षित कीजिए ताकि कोई दूसरा व्यक्ति बिना आपके जानकारी के आपका कम्प्यूटर प्रयोग न कर सकें।
- अगर आपका कम्प्यूटर सुरक्षित नहीं होगा, तो अपराधी या कोई भी व्यक्ति आपके कम्प्यूटर से जरूरी जानकारियां चुरा सकता है और गलत कार्यों के लिए आपके कम्प्यूटर का इस्तेमाल भी कर सकता है। साथ ही यह भी चेक करें कि आपका एंटी वायरस और एंटी स्पाई वेयर सॉफ्टवेयर ठीक से काम कर रहा है या नहीं और उसके वेंडर से जरुरी अपडेट्स आ रहें हैं या नहीं।
- हमेशा बहुत स्ट्रांग पासवर्ड का प्रयोग करें, जिससे आसानी से किसी को पता न चले, क्योंकि साइबर क्रिमिनल प्रोग्रामर ऐसे सॉफ्टवेयर प्रोग्राम का निर्माण करते हैं जो कि आपके साधारण से पासवर्ड को आसानी से गेस कर सकते हैं। ऐसे में आप ऐसा पासवर्ड सेट करें जिसका कोई दूसरा अनुमान न लगा सके और आप आसानी से याद भी रख सकें।
- आपका पासवर्ड कम से कम आठ कैरेक्टर का हो जो कि लोअर केस लेटर्स, अपर केस लेटर्स, नंबर्स और स्पेशल कैरेक्टर्स का मिश्रण हो। अगर आप एक से अधिक अकाउंट्स का प्रयोग करते हैं, तो सभी के लिए अलग- अलग पासवर्ड का प्रयोग करें।

- ❖ अपने सोशल मीडिया अकाउंट को देखते रहें, अगर कभी आप अपने सोशल साइट्स के अकाउंट को डिलीट कर रहे हैं, तो उससे पहले आप अपनी सारी पर्सनल जानकारी को डिलीट कर दें और फिर उसके बाद आप अपना अकाउंट डीएक्टिवेट या डिलीट करें। किसी भी स्पैम ई-मेल का उत्तर न दें।
- ❖ अज्ञात ई-मेल में आए अटैचमेंट्स को कभी खोल कर न देखें या उस पर मौजूद लिंक पर क्लिक न करें। इसमें वायरस या ऐसा प्रोग्राम हो सकता है जिसको क्लिक करते ही आपका कम्प्यूटर उनके कंट्रोल में जा सकता है या आपके कम्प्यूटर में वायरस के प्रभाव से कोई जरूरी फाइल डिलीट हो सकती है और आपका ऑपरेटिंग सिस्टम करप्ट हो सकता है।
- ❖ अगर हम किसी ऑफर का लाभ लेना चाहते हैं तो आप सीधे रिटेलर के वेबसाइट, रीटेल आउटलेट या अन्य जायज साइट से संपर्क करें। आज के दौर मे इंटरनेट हमारे लिए काफी महत्वपूर्ण है, लेकिन इंटरनेट पर जरा सी ना समझी स्कैमर्स को साइबर क्राइम के लिए खुला निमंत्रण देता है।
- ❖ कंप्यूटर उपयोगकर्ताओं को हैकर्स से अपने कंप्यूटर की सुरक्षा के लिए एक फ़ायरवॉल का उपयोग करना चाहिए।
- ❖ कंप्यूटर उपयोगकर्ताओं को एंटी वायरस सॉफ्टवेयर जैसे McAfee या Norton एंटी वायरस के रूप में स्थापित करना चाहिए।
- ❖ यूजर्स को केवल सुरक्षित वेबसाइट्स पर ही खरीदारी करनी चाहिए और अपने क्रेडिट कार्ड की जानकारी संदिग्ध या अजनबियों के साथ कभी भी साझा नहीं करनी चाहिए।
- ❖ उपयोगकर्ताओं को अपने खातों पर मजबूत पासवर्ड विकसित करने चाहिए, अर्थात अक्षरों और संख्याओं को पासवर्ड में शामिल करें एवं लगातार पासवर्ड और लॉगिन विवरण का अद्यतन करते रहना चाहिए।
- ❖ फेसबुक, ट्विटर, यूट्यूब की सुरक्षा सेटिंग्स की जांच करें, बच्चों पर नजर रखें एवं उनके द्वारा इंटरनेट के उपयोग को सीमित रखें।
- ❖ हैकिंग से बचने के लिए जानकारी सुरक्षित रखें। अधिकांश संवेदनशील फ़ाइलों या वित्तीय रिकॉर्ड के लिए एंक्रिप्शन का उपयोग करें, सभी महत्वपूर्ण जानकारी के लिए नियमित बैक-अप बनाएं और इसे किसी अन्य स्थान पर संग्रहीत कर लें।
- ❖ उपयोगकर्ताओं को सार्वजनिक वाई-फाई हॉटस्पॉट का उपयोग करते समय सचेत रहना चाहिए। इन नेटवर्क पर वित्तीय लेनदेन के संचालन से बचें।
- ❖ उपयोगकर्ताओं को इंटरनेट पर नाम, पता, फोन नंबर या वित्तीय जानकारी जैसे व्यक्तिगत जानकारी देते समय सावधान रहना चाहिए। सुनिश्चित करें कि वेबसाइट्स सुरक्षित हैं।
- ❖ कोई लिंक या अज्ञात मूल के फ़ाइल पर क्लिक करने से पहले सभी चीजों का बुद्धिमता से आकलन करना चाहिए। इनबॉक्स में कोई भी ई-मेल न खोलें। संदेश के स्रोत की जांच करें। यदि कोई संदेह हो, तो स्रोत सत्यापित करें। कभी उन ई-मेल का जवाब न दें जो उनसे जानकारी सत्यापित करने या उपयोगकर्ता के पासवर्ड की पुष्टि करने के लिए कहें।

निष्कर्ष

साइबर अपराध को रोकने के लिए हमें साइबर जागरूकता के तहत अपने ग्राहकों और कर्मचारियों को विशेष रूप से अवगत कराना होगा। सीमा पार साइबर खतरों पर अंकुश लगाने के लिए अंतर्राष्ट्रीय स्तर पर उचित कार्रवाई की जानी चाहिए। निरंतर सतर्कता, मजबूत डिजिटल आंतरिक नियंत्रण, बैंक के सॉफ्टवेयर को नियमित रूप से अद्यतित करते हुए मजबूत अनुपालन की संस्कृति को अपनाना चाहिए।

भारतीय पुलिस ने देश भर में विशेष साइबर सेल की शुरूआत की है और लोगों को शिक्षित भी कर रहे हैं, ताकि जरूरी जानकारी हासिल कर वे ऐसे अपराधो से खुद को बचा सकें। आज हर एक व्यक्ति को अपने स्तर पर साइबर अपराधों के विरोध में आवाज उठानी पड़ेगी और इसके लिए सबसे ज्यादा जरूरत है - साइबर शिक्षा की। वर्तमान में युवापीढ़ी तकनीक का ज्यादा उपयोग कर रही है। आज फिनटेक बैंकिंग का जमाना है। साइबर शिक्षा को स्कूल, महाविद्यालय और विश्वविद्यालय के पाठ्यक्रम में शामिल कर नई पीढ़ी में जागरुकता लाने से इस अपराध को कम किया जा सकता है। विद्यार्थी ही हमारे देश के भविष्य हैं। अतः वे जितने जागरूक होंगे हमारा देश भी उतना ही तरक्की की राह पर विराजमान होगा।

हमें कभी भी किसी की लालच में नहीं आना चाहिए। हमारी नैतिकता इतनी मजबूत हो कि हम अपने धन को ही अपना धन समझें। हम अपनी मेहनत को ही अपना इमान बनाएं। कभी भी किसी लॉटरी या रातोरात अमीर बनाने के सपनों से दूर रहें। कहा जाता है कि सतर्कता से ही शांति संभव है। हर पल जागरुक और सतर्क रहने से हमारे जीवन में उन्नति और खुशहाली आ सकती है।

*****

तरुण चंद

पदनाम:- अधिकारी
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 7992202014
ई-मेल:- ttt.tarunchand@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

प्रस्तावना

आज का युग सूचना प्रौद्योगिकी का युग है। उभरती हुई प्रौद्योगिकी का फायदा बैंकिंग क्षेत्र को भी हुआ है। यह प्रौद्योगिकी का ही असर है कि आज बैंक शाखा कंप्यूटरीकृत बैंकिंग से मोबाइल एवं वर्चुअल बैंकिंग तक जा पहुंची है।

प्रौद्योगिकीजनित इन बदलावों से बैंकों के समक्ष कई चुनौतीयां भी उत्पन्न हुई हैं जिनमें सबसे बड़ी चुनौती आज "साइबर अपराध" के रूप में है। पिछले दो दशकों के दौरान बैंकिंग की अवधारणा के वैश्विक स्वरूप अख्तियार करने, बैंकिंग लेन-देन के तरीकों में आए आमूलचूल परिवर्तनों, नित्य नए वित्तीय उत्पादों के सामने आने, अंतर्राष्ट्रीय लेन-देन के कई गुना बढ़ जाने, ऑनलाइन और डिजिटल बैंकिंग में हुई अभूतपूर्व वृद्धि आदि के कारण बैंकिंग तंत्र में साइबर अपराधों के मामले सुरसा के मुख की तरह बढ़ते जा रहे हैं।

बैंकिंग जगत में साइबर अपराधों के स्वरूप

साइबर अपराधों को सामान्यतः साइबर आतंकवाद, सॉफ्टवेयर चोरी, पहचान की चोरी, ऑनलाइन चोरी और धोखाधड़ी, ई-मेल स्पैम और फिशिंग जैसे कई अन्य श्रेणियों में वर्गीकृत किया जा सकता है। हालांकि, बैंकिंग उद्योग को प्रभावित करने वाले वित्तीय साइबर अपराध के प्रमुख प्रकार निम्नलिखित हैं:

1. **हैकिंग** :-
   यदि कोई व्यक्ति कहीं दूर बैठकर आपके कंप्यूटर, वेबसाइट या प्रोफाइल पर किसी कमजोरी का फायदा उठाकर या इंटरनेट की सुरक्षा को तोड़कर उसमें लॉगिन करने में सक्षम होता है तो इसका मतलब उस व्यक्ति ने आपके कंप्यूटर, वेबसाइट या सोशल मीडिया प्रोफाइल को हैक कर लिया है और अब वह उसका गलत इस्तेमाल कर सकता है। इंटरनेट बैंकिंग जैसी आधुनिक सुविधाओं का दुरुपयोग साइबर अपराधी हैकिंग के जरिए करते हैं। इससे बैंक के ग्राहकों को आर्थिक हानि होती है।

2. **फ़िशिंग**:-
   जिस प्रकार मछली पकड़ने के लिए कांटे में चारा लगाकर डाला जाता है और चारा खाने के लालच या धोके में आकर मछली कांटे में फंस जाती है। उसी प्रकार फ़िशिंग भी आपराधिक तत्वों द्वारा इंटरनेट पर नकली वेबसाइट या ई-मेल के माध्यम से इंटरनेट का प्रयोग करने वाले बैंक ग्राहकों की निजी जानकारी चुराकर उनके साथ की गई आर्थिक धोखेबाजी को कहते हैं।

3. **विशिंग**:-
   विशिंग अपराध टेलीफोन की मदद से किया जाता है। इसमें साइबर अपराधी वित्तीय लाभ अर्जित करने के लिए बैंक के ग्राहकों को फोन कर आंतरिक सूचना मांगता है एवं उसका गलत इस्तेमाल करते हुए आर्थिक

अपराध को अंजाम देता है। वर्तमान में भारतीय बैंकिंग क्षेत्र में इस प्रकार का अपराध बहुत ज्यादा हो रहा है।

4. **ई-मेल स्पूफिंग** :-

इस प्रकार के साइबर अपराध में एक जाली प्रेषक पते के माध्यम से ई-मेल संदेश भेजा जाता है। ऐसा करना आसान है क्योंकि आंतरिक प्रोटोकॉल में इसके प्रमाणन के लिए कोई तंत्र नहीं है। यह आम तौर पर संदेश की उत्पत्ति के बारे में प्राप्तकर्ता को गुमराह करता है जिसका लाभ आर्थिक अपराधी उठाते हैं।

5. **स्पैमिंग** :-

स्पैम उस प्रकार के ई-मेल संदेश को कहते हैं जो थोक में भेजे जाते हैं, ये बिना मांगे या बुलाए आ जाते हैं जिसमें प्रायः विज्ञापन भरे होते हैं। एक अध्ययन से पता चलता है कि हर रोज कम से कम एक अरब स्पैम भेजी जाती हैं। इन स्पैम संदेशों में एक लिंक होता है जिसे खोलने से गोपनीय जानकारी को चुरा लिया जाता है और आर्थिक नुकसान उठाना पड़ सकता है।

6. **सेवा से इनकार आक्रमण (डिनायल ऑफ सर्विस अटैक)**:-

यह इंटरनेट की दुनिया में किसी सर्वर या वेबसाइट पर किया जाने वाला ऐसा साइबर हमला है जिससे किसी भी सर्वर या वेबसाइट को बंद कर दिया जाता है या फिर उस वेबसाइट को उपयोगकर्ताओं के लिए अनुपलब्ध कर दिया जाता है। इस आक्रमण के जरिए अपराधी आर्थिक धोखाधड़ी को अंजाम देते हैं।

7. **सलामी अटैक** :-

इस साइबर हमले में गुपचुप तरीके से आर्थिक अपराध को अंजाम दिया जाता है। ये अपराध बैंकों मे ज्यादा होते हैं। उदाहरणस्वरूप कोई व्यक्ति यदि बैंक सर्वर में ऐसा प्रोग्राम डाल दे जिससे हर खाते से इतना कम धन कटता है कि वह नजरअंदाज होता रहता है। इस तरह के आक्रमण से साइबर अपराधी सीधे बैंक के मुख्य सर्वर को निशाना बनाते हैं।

8. **एटीएम स्किमिंग**:-

क्रेडिट अथवा डेबिट कार्ड की जानकारी की चोरी को स्किमिंग कहते हैं। इस प्रक्रिया में अपराधी एक छुपाए गए कार्ड रीडर (स्किमर) और छोटे कैमरे को एटीएम में स्थापित कर, ग्राहक के क्रेडिट अथवा डेबिट कार्ड की जानकारी को एक रिक्त कार्ड में स्थानांतरित कर उसका प्रयोग धोखे से नकदी आहरण में करता है। अनभिज्ञ ग्राहकों को इससे काफी आर्थिक नुकसान झेलना पड़ता है।

9. **सोशल इंजीनियरिंग हमले**:-

सोशल इंजीनियरिंग के जरिए एक साइबर अपराधी, प्राकृतिक मानव प्रवृत्ति पर भरोसा उत्पन्न कर चालाकी और हेरफेर से उसके डेबिट अथवा क्रेडिट कार्ड का नंबर, खाता संख्या, पासवर्ड, गोपनीय पिन, सीवीवी संख्या, मोबाइल पर प्राप्त ओटीपी आदि प्राप्त कर उसका अनधिकृत उपयोग वित्तीय धोखाधड़ी हेतु करता है।

10. **पहचान संबंधी धोखाधड़ी (आइडेंटिटी थेफ्ट)**:-

बैंक के सभी ग्राहकों की जानकारी अब डेटा सेंटर में उपलब्ध होती है। बैंकों एवं बाहर के सेवाप्रदाता कंपनियों के लोगों को यह डेटा आसानी से उपलब्ध हो जाता है जिसका प्रयोग आपराधिक प्रवृत्ति के लोग पहचान संबंधी धोखाधड़ी में करते हैं और कई आर्थिक आपराधिक घटनाओं को अंजाम देते हैं।

11. **फॉर्मजैकिंग तथा क्रिप्टोजैकिंग** :-

फॉर्मजैकिंग साइबर हमलों की अपेक्षाकृत नया तरीका है जिसके माध्यम से ऑनलाइन बैंकिंग अथवा ई-वाणिज्य वेबसाइट पर उपभोक्ताओं द्वारा दर्ज किए जाने वाले क्रेडिट/ डेबिट कार्ड अथवा बैंकिंग खाते संबंधी विवरण को चुरा लिया जाता है। वर्ष 2021 में प्रति माह 4818 वेबसाइट पर फॉर्मजैकिंग हमले किए गए। इन हमलों से प्राप्त विभिन्न गोपनीय विवरण की खरीद-फरोख्त भी संदिग्ध बाज़ारों में की जाती है। दूसरी ओर क्रिप्टोजैकिंग का आशय किसी की जानकारी के बिना उसके कंप्यूटर का प्रयोग क्रिप्टो-करेंसी की माइनिंग के लिए किया जाना है। क्रिप्टो-करेंसी के बढ़ते प्रयोग के मद्देनजर ये हमले बैंकों के साइबर सुरक्षा के लिए नई चुनौती हैं।

भारतीय बैंकों द्वारा साइबर सुरक्षा हेतु उठाए गए कदम

1. **ग्राहक सूचना की सुरक्षा सुनिश्चित करना**:-

बैंक अपने सुचारु कामकाज के लिए ही नहीं बल्कि अपने ग्राहकों को उन्नत एवं नवीन डिजिटल उत्पाद उपलब्ध कराने के लिए, विभिन्न व्यक्तिगत तथा संवेदनशील सूचनाओं को एकत्र करने के लिए, प्रौद्योगिकी पर पूरी तरह से निर्भर होते हैं। बैंकों ने इस प्रकार के डेटा अभिरक्षक के रूप में, इसकी गोपनीयता, सत्यनिष्ठा तथा उपलब्धता को संरक्षित करने के लिए उचित उपाय किए हैं। बैंकों को चाहिए कि भले ही डेटा उनके पास हो, ट्रांजिट में हो या ग्राहकों या तृतीय पक्ष वेन्डर के पास हो। ऐसे भंडारित सूचना की गोपनीयता के साथ किसी भी अवस्था में समझौता नहीं किया जाना चाहिए तथा डेटा के आदान-प्रदान में उचित प्रणालियों एवं प्रक्रियाओं को लागू करने की आवश्यकता है।

2. **हितधारकों/ शीर्ष प्रबंधन / बोर्ड के बीच साइबर सुरक्षा जागरूकता**:-

साइबर जोखिम का प्रबंधन और साइबर-सुरक्षित माहौल बनाने के लिए सम्पूर्ण बैंकिंग संगठन की प्रतिबद्धता आवश्यक है। इसके लिए सभी स्तरों पर स्टाफ के बीच एक उच्च स्तर की जागरूकता की आवश्यकता होगी। बैंक के शीर्ष प्रबंधन एवं बोर्ड के पास भी साइबर खतरों की सूक्ष्मतम जानकारी होनी चाहिए ताकि बैंक अपने ग्राहकों, सेवा प्रदाताओं तथा अन्य हितधारकों के बीच साइबर सुरक्षा को लेकर जागरूकता उत्पन्न कर सकें।

3. **वित्तीय साक्षरता, जागरूकता एवं सतर्कता संबंधी उपाय**:-

हैकिंग, फ़िशिंग, विशिंग, स्पूफिंग, कार्ड क्लोनिंग एवं सोशल इंजीनियरिंग जैसे साइबर आपराधिक हमलों को पर्याप्त सतर्कता एवं जागरूकता के माध्यम से काफी हद तक कम किया जा सकता है। इसके लिए आवश्यक है कि बैंक भी साइबर सुरक्षा के प्रति अपने ग्राहकों को जागरूक करें एवं साइबर साक्षर बनाएं।

4. **बैंककर्मियों को साइबर सुरक्षा हेतु समुचित प्रशिक्षण**:-

बैंकिंग कार्यप्रणाली के अंतर्गत आने वाले संवेदनशील विभाग के कर्मियों जहां साइबर हमले की संभावना अधिक होती है, को साइबर सुरक्षा संबंधी ज्ञान से सुसज्जित करना बैंक की प्राथमिकता है। इन कार्य क्षेत्रों में कार्यरत बैंक कर्मियों को सघन प्रशिक्षण प्रदान कर साइबर सुरक्षा प्रबंधन संबंधी निर्देशों की अद्यतन जानकारी देना अत्यंत आवश्यक है, तभी वे साइबर हमलों की पहचान करने एवं उन्हें रोकने में सक्षम हो पाएंगे। बैंकों को चाहिए कि वो साइबर सुरक्षा पेशेवरों की भी नियुक्ति करें।

5. **साइबर बीमा**:-

साइबर जोखिम को कारोबार हेतु एक गंभीर खतरे के रूप में देखते हुए बैंकों को साइबर सुरक्षा जोखिम प्रबंधन हेतु साइबर बीमा को अपनाना चाहिए। भारत में साइबर बीमा निवेश बहुत निम्न स्तर का है। वैश्विक स्तर पर जहां साइबर बीमा बाज़ार 4 अरब डॉलर का है, वहीं भारत में साइबर बीमा का बाज़ार मात्र 90 करोड़ रुपए है, चूंकि भविष्य में साइबर हमलों की संख्या बढ़ने की आशंका है, इसलिए भारतीय बैंकों को साइबर बीमा अपनाना चाहिए।

6. **व्यापक रूप से नेटवर्क तथा डेटाबेस सुरक्षा पर ध्यान**:-

साइबर अपराध की बढ़ती घटनाओं के मद्देनजर प्रत्येक बैंकों में नेटवर्क सुरक्षा की बेहतर तरीके से समीक्षा करने की आवश्यकता पर ध्यान केंद्रित किया जाना चाहिए। नेटवर्क तथा डेटाबेस में अप्राधिकृत रूप से पहुंच पाने की अनुमति नहीं दी जानी चाहिए तथा जब कभी अनुमति दी जाए तो निर्धारित प्रक्रियाओं का अनिवार्य रूप से पालन किया जाए।

7. **नियमित चौकसी हेतु साइबर सिक्योरिटी ऑपरेशन सेंटर (एसओसी) की व्यवस्था**:-

साइबर-आक्रमण का स्वरूप इस प्रकार है कि वे कभी भी घटित हो सकते हैं और अनुमान से परे भी हो सकते हैं। अतः इसे ध्यान में रखते हुए बैंकों को साइबर सिक्योरिटी ऑपरेशन सेंटर (एसओसी) की स्थापना को महत्व देना चाहिए।

8. **साइबर सुरक्षा मुस्तैदी संकेतक**:-

बैंक साइबर खतरों से अपने डेटा को सुरक्षित करने हेतु साइबर रेजिलिएन्स (समुत्थानशक्ति) फ्रेमवर्क के तहत साइबर सुरक्षा मुस्तैदी संकेतक को भी अपना रहे हैं। इन संकेतकों का इस्तेमाल स्वतंत्र अनुपालन जांच तथा लेखापरीक्षा में भी किया जाता है। साथ ही, कर्मचारियों के साथ-साथ हितधारकों के बीच जागरूकता को भी इस मूल्यांकन का भाग बनाया जाता है।

9. **बैंकों द्वारा साइबर जोखिम सुरक्षा व्यय में करनी होगी बढ़ोत्तरी**:-

भारतीय बैंक कुल बजट का अनुमानतः10% भी साइबर जोखिम सुरक्षा प्रबंधन पर व्यय नहीं करते हैं जबकि संभावित खतरों को देखते हुए साइबर सुरक्षा पर सालाना खर्च बढ़ाने की जरूरत है क्योंकि साइबर सुरक्षा में कमी के कारण ही भारतीय बैंकों को अरबों रुपए का सालाना नुकसान होता है।

10. **'साइबर हायजीन' का अभ्यास**:-

बैंकों से अपेक्षा है कि वो सुरक्षा संस्कृति में परिवर्तन कर 'साइबर हायजीन' का अभ्यास करें। साइबर खतरों को भी उसी प्रकार गंभीरता से लिया जाए जैसे बैंक अन्य जोखिमों (क्रेडिट, परिचालन आदि) को लेते हैं। हार्डवेयर, मिडलवेयर, सॉफ्टवेयर, ऑपरेटिंग सिस्टम, एंटी-वायरस, ऐप्लीकेशन, नेटवर्क डिवाइस के उचित रखरखाव एवं उन्हें अद्यतन रखने की आवश्यकता है। बैंकों को साइबर हायजीन के संदर्भ में साइबर सुरक्षा के व्यापक पहलुओं को समाहित करना चाहिए जैसे आईटी इंफ्रास्ट्रक्चर, अंतिम बिन्दु सुरक्षा, सुरक्षा निगरानी, आउटसोर्सिंग सुरक्षा आदि।

उपसंहार

यह सर्वमान्य सत्य है कि प्रत्येक सिक्के के दो पहलू होते हैं, जैसे-जैसे तकनीक का विकास होता जा रहा है वैसे-वैसे साइबर अपराध भी बढ़ रहे हैं। साइबर अपराध को पूरी तरह से खत्म नहीं किया जा सकता है लेकिन इसके खतरे को सतर्कता एवं जागरूकता से कम जरूर किया जा सकता है। इसके लिए जरूरी है कि बैंक समय-समय पर भारत सरकार एवं विभिन्न विनियामकीय संस्थाओं द्वारा साइबर सुरक्षा संबंधी दिशानिर्देशों का अनुपालन सुनिश्चित करें। हालांकि भारतीय रिज़र्व बैंक और भारत सरकार द्वारा साइबर सुरक्षा के लिए उठाए गए सक्रिय कदम सामयिक और बहुत जरूरी हैं लेकिन साइबर हमलों के विरुद्ध बैंकिंग ढांचे की आघात सहनीयता सभी हितधारकों की समन्वित कार्यवाही पर निर्भर करेगी।

बैंकों को चाहिए कि वो पूरी सक्रियता से अपने ग्राहकों, सेवा प्रदाताओं एवं हितधारकों के बीच साइबर सुरक्षा के महत्व की समझ पैदा करें एवं दुर्भेद्य सुरक्षा प्रणाली के साथ साइबर सुरक्षा प्रबंधन की नीतियों और कार्यविधियों का अनुपालन करें। तभी भारतीय बैंक विश्व में अपनी विशिष्ट पहचान स्थापित कर सकती हैं और ग्राहकों का विश्वास प्राप्त कर सकती हैं।

"हेयम् दुःखं अनागतं"

अर्थात् आने वाले संकट को टाल दें–पूर्वोपाय करें

*****

दीपक कुमार

पदनाम:- सहायक प्रबन्धक
संस्था का नाम:- यूनियन बैंक ऑफ इंडिया
मोबाइल नं. :- 9598384832
ई-मेल:- deepak.kumar5@unionbankofindia.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

वर्तमान समय में मानव की सम्पूर्ण गतिविधियां साइबर आधारित हो गयी हैं। खाना मंगाना हो या हवाई जहाज की टिकट बुक करनी हो, सब कुछ पलक झपकते ही अपने मोबाइल, कंप्यूटर या लैपटॉप के माध्यम से कर सकते हैं। इन सभी के फलस्वरूप हमारे जीवन की गति बहुत तीव्र और सरल हो गयी है। इन सभी व्यवहारों के दौरान हम कहीं न कहीं पर डेटा संबंधी लापरवाही करते हैं और साइबर अपराध का शिकार हो जाते हैं। वास्तव में वर्तमान युग सूचना विस्फोट और डेटा का युग है जिसके पास जितनी अद्यतित और समसामयिक सूचना एवं डेटा है वह उतना ही शक्तिशाली तथा सक्षम माना जाता है।

साइबर अपराध में ऐसी ही व्यक्तिगत जानकारियों का दुरुपयोग किया जाता है और यह ऐसा अपराध है जिसमें डिजिटल उपकरण जैसे- कंप्यूटर, लैपटॉप, नोटपैड, मोबाइल और इंटरनेट आदि शामिल हैं। किसी भी डिजिटल उपकरण का उसके नियत स्थान पर न मिलना या फिर किसी आपराधिक स्थान पर मिलना, किसी उपकरण से डेटा चोरी करना या फिर डेटा से छेड़-छाड़ करना अथवा डिलीट करना अथवा इंटरनेट के विभिन्न माध्यमों जैसे ई-मेल, सोशल मीडिया साइटों आदि के माध्यम से व्यक्तिगत जानकारी चुराना या मांगना आदि साइबर अपराध की श्रेणी में आते हैं। "थ्री इडियट्स" मूवी में आमिरखान ने चतुर के भाषण में परिवर्तन कर दिया था जिसके फलस्वरूप पूरे भाषण का स्वरूप ही बदल गया था। यहां पर यह ध्यान देने वाली बात है कि यदि कंप्यूटर लॉक होता तो यह परिवर्तन रोका जा सकता था।

पूरा विश्व बहुत तेजी से बदल रहा है और नित नवीन आविष्कार हो रहे हैं और मनुष्य का प्रायः सम्पूर्ण जीवन ही साइबर आधारित हो रहा है जिसके कारण साइबर अपराध के स्वरूप में भी लगातार परिवर्तन हो रहा है। साइबर अपराध के प्रमुख स्वरूप निम्न प्रकार से हैं:

बैंकिंग में साइबर अपराधों के विविध स्वरूप;

साइबर अपराध का गहन विश्लेषण करें तो हमें पता चलता है कि ये प्रमुखतः तीन प्रकार के होते हैं:

1. **मालवेयर :-**

सॉफ़्टवेयर या कोड स्निपेट्स जिन्हें आपके कंप्यूटर और/या नेटवर्क सुरक्षा को नुकसान पहुंचाने के लिए डिज़ाइन किया गया है।

- **वायरस और कृमि -** गड़बड़ी या क्षति पहुंचाने के दुर्भावनापूर्ण इरादे वाला सॉफ़्टवेयर। जब सॉफ़्टवेयर निष्पादित होता है तो वायरस स्वयं को आपके कंप्यूटर/नेटवर्क संचालन को नुकसान पहुंचाने के उद्देश्य से सिस्टम फाइलों को संक्रमित करने और पूरे सिस्टम में फैलने के लिए आपके सिस्टम के प्रोग्राम/फ़ाइल से जोड़ लेता है।

- ❖ **ट्रोजन हॉर्स -** ऐसा सॉफ़्टवेयर जो या तो दूसरे सॉफ़्टवेयर के अंदर छिपा हो सकता है या वैध सॉफ्टवेयर प्रतीत होता है। एक वायरस या कृमि के विपरीत, एक ट्रोजन हॉर्स पुनरुत्पादन या आत्म-प्रतिकृति नहीं करता है लेकिन संक्रमित ई-मेल, अटैचमेंट या इंटरनेट फ़ाइलें खोलने/लॉन्च करने से फैलता है।
- ❖ **रिमोट एक्सेस ट्रोजन (RAT) -** एक मैलवेयर प्रोग्राम है जिसमें एक लक्षित कंप्यूटर पर प्रशासनिक नियंत्रण के लिए गुप्त रूप से प्रवेश कराया जाता है। RAT आमतौर पर उपयोगकर्ता द्वारा अनुरोधित प्रोग्राम के साथ अदृश्य रूप से डाउनलोड किए गए होते हैं।
- ❖ **स्पाइवेयर -** दुर्भावनापूर्ण सॉफ़्टवेयर जो उपयोगकर्ता की जानकारी के बिना कंप्यूटर या नेटवर्क पर किसी व्यक्ति या संस्था की निगरानी करता है।
- ❖ **रैनसमवेयर -** ऐसा सॉफ़्टवेयर जो उपयोगकर्ताओं को उनके सिस्टम या कुछ फाइलों तक उनकी पहुंच को सीमित या प्रतिबंधित करता है, जब तक कि फिरौती का भुगतान नहीं किया जाता है। प्रायः हैकर भुगतान होने तक फ़ाइलों तक पहुँच को रोकने के लिए एन्क्रिप्शन का उपयोग करते हैं।

2. सोशल इंजीनियरिंग :-

जोड़-तोड़ विधियों के उपयोग या अनधिकृत तरीकों से सूचना (गोपनीय जानकारी) प्राप्त करना,

- ❖ **स्पूफिंग -** यह एक ऐसी तकनीक को संदर्भित करता है जिसमें किसी व्यक्ति के कंप्यूटर तक अनधिकृत पहुंच होती है जिससे अपराधी आईपी पते के साथ नेटवर्क वाले कंप्यूटर को संदेश भेजता है।
- ❖ **फ़िशिंग (ई-मेल) -** यह एक तरह का कपटपूर्ण प्रयास है जो व्यक्तिगत और वित्तीय जानकारी प्राप्त करने के लिए ई-मेल के माध्यम से किया जाता है। स्पीयर फ़िशिंग, विशिंग और स्मिशिंग भी फ़िशिंग के ही स्वरूप हैं।
- ❖ **फ़ार्मिंग -** आपकी सहमति या जानकारी के बिना कपटपूर्ण वेबसाइटों पर पुनर्निर्देशन।
- ❖ **बैटिंग** – बैटिंग भी कई मायनों में फ़िशिंग हमलों के समान है। हालांकि, एक वस्तु या उपहार जिसका उपयोग हैकर पीड़ितों को लुभाने के लिए करते हैं वही उन्हें अन्य प्रकार की सोशल इंजीनियरिंग से क्या अलग करता है। बैटर उपयोगकर्ताओं को अपने लॉगिन क्रेडेंशियल किसी निश्चित साइट पर दर्ज करने के बदले डाउनलोड करने की पेशकश करता है।
- ❖ **प्रीटेक्स्टिंग -** प्रीटेक्स्टिंग सोशल इंजीनियरिंग का दूसरा रूप है जिसमें हमलावर एक अच्छा बहाना या एक मनगढ़ंत परिदृश्य बनाकर पीड़ितों की व्यक्तिगत जानकारी प्राप्त करने का प्रयास करते हैं। इस तरह के हमलों में हमलावर आपसे कुछ सूचनाओं की पुष्टि करने की बात करता है जिससे पीड़ित की पहचान की जा सके।

3. सुभेद्यता/शोषण हेतु हमले :-

क्षमता आधारित हमले प्रौद्योगिकी में मौजूद कमजोरियों का लाभ उठाते हैं। उदाहरणार्थ:

- ❖ **सेवा से इनकार (डीओएस) हमला -** एक सर्वर या नेटवर्क पर सेवा के लिए इतने अधिक अनुरोध आ जाते हैं कि वह धीमा या क्रैश हो जाता है। परिणामस्वरूप वैध ग्राहकों / उपयोगकर्ताओं की उस सर्वर या नेटवर्क तक पहुँच बाधित हो जाती है।
- ❖ **डिस्ट्रिब्यूटेड डिनायल ऑफ़ सर्विस अटैक्स (DDoS)** – इसके अंतर्गत एक ही समय पर कई कम्प्यूटरों से हमले किए जाते हैं जिससे वेबसाइट/नेटवर्क बंद पड़ जाता है। (बोटनेट / जॉम्बी इसी तरह के हमलों के लिए उपयोग किए जाते हैं।)
- ❖ **मैन इन द मिडल (MITM)** – यह एक ऐसा हमला है जिसका इस्तेमाल दो उपयोगकर्ताओं के बीच सम्प्रेषण की निगरानी और संदेश को संशोधित करने के लिए किया जाता है। मैन इन द ब्राउज़र भी इसी तरह का एक हमला है, यद्यपि इसमें हमले के लिए ट्रोजन हॉर्स का उपयोग किया जाता है।

उपर्युक्त साइबर अपराधों के स्वरूप का अवलोकन करने से हमें यह प्रतीत होने लगता है कि इंटरनेट का प्रयोग करने का मतलब है साइबर अपराधों का शिकार होना। परंतु जहां समस्या होती है वहीं समाधान भी होता है। निम्नलिखित कुछ सुरक्षात्मक उपायों को अपनाकर हम साइबर अपराधों का शिकार होने से बच सकते हैं।

बैंकिंग में साइबर अपराधों से बचने के उपाय;

1. **ग्राहकों /हितधारकों /शीर्ष प्रबंधन /बोर्ड को साइबर-सुरक्षा के संबंध में जागरूक करना :-**
   बैंक और बैंक के स्टाफ के साथ-साथ यह बेहद आवश्यक है कि उसके ग्राहक भी साइबर अपराध के तरीकों और उससे निपटने की युक्तियों के प्रति जागरूक रहें अर्थात जागरूक किया जाए जिससे साइबर सुरक्षा संबंधी चूक न हो और व्यक्तिगत या संस्थागत हानि से बचा जा सके। साथ यह भी आवश्यक है कि बैंक के शीर्ष प्रबंधन तथा बोर्ड के पास सूक्ष्मतम जानकारी हो जिससे वे समय पर उचित कार्यवाही कर सकें।
2. **ग्राहकों से संबन्धित सूचना की सुरक्षा सुनिश्चित करना :-**
   बैंक अपने सुचारु कामकाज के लिए ही नहीं बल्कि अपने ग्राहकों को उन्नत डिजिटल उत्पाद देने तथा विभिन्न व्यक्तिगत तथा संवेदनशील सूचनाओं को एकत्र करने की प्रक्रिया के लिए प्रौद्योगिकी पर पूरी तरह से निर्भर होते हैं। बैंकों को इस प्रकार के डेटा के अभिरक्षक के रूप में इसकी गोपनियता, सत्यनिष्ठा तथा उपलब्धता को संरक्षित करने के लिए उचित उपाय करने चाहिए, भले ही डेटा उनके पास हो/ ट्रांजिट में हो या ग्राहकों या तृतीयपार्टी वेंडर के पास हो; इस प्रकार की भंडारित सूचना की गोपनीयता के साथ किसी भी अवस्था में समझौता नहीं किया जाना चाहिए तथा इस प्रयोजन हेतु, बैंकों द्वारा समूचे डेटा/सूचना के जीवनचक्र में उचित प्रणालियों तथा प्रक्रियाओं को लागू करने की आवश्यकता है।
3. **साइबर संकट प्रबंधन योजना :-**
   बैंकों में जनता की मेहनत की कमाई जमा रहती है। चूंकि बैंक धन का लेन-देन करते हैं, इसलिए साइबर अपराधियों के अधिक निशाने पर रहते हैं। अतः यह आवश्यक है कि बैंकों के पास साइबर संकट प्रबंधन के लिए योजना तैयार रहे। इस क्रम में साइबर संकट प्रबंधन के क्रमशः चार पहलुओं (i) संकट की पहचान (ii) जवाबी कार्यवाई (iii) सुधारात्मक कार्यवाई और (iv) नियंत्रण पर विशेष ध्यान दिया जाना चाहिए ताकि आकस्मिक संकट से कुशलतापूर्वक निपटा जा सके।
4. **सतर्कतापूर्ण व्यवस्था की जांच :-**
   जिस तरह से हम अन्य कार्यविधि का निरीक्षण और निगरानी करते हैं उसी तरह से समय-समय पर साइबर सुरक्षा संबंधी संवेदनशीलताओं की जांच करना बहुत ही महत्वपूर्ण है। साइबर-आक्रमण का स्वरूप इस प्रकार है कि वे कभी भी घटित हो सकते हैं और अनुमान से परे भी हो सकते हैं। अतः यह अत्यावश्यक है कि साइबर सुरक्षा व्यवस्था की नियमित और सुव्यवस्थित निगरानी की जाए।
5. **अलग साइबर सुरक्षा नीति का निर्माण :-**
   हम सभी इस बात से अनभिज्ञ नहीं हैं कि किसी एक काम को पूर्ण समर्पण के साथ करने से सफलता की संभावना सर्वाधिक होती है। यही बात साइबर सुरक्षा पर भी लागू होती है। अतः साइबर सुरक्षित माहौल में सम्पूर्ण बैंक के योगदान की आवश्यकताओं पर ध्यान देने हेतु साइबर सुरक्षा नीति, विस्तृत सूचना प्रौद्योगिकी नीति और आईएस सुरक्षा नीति से भिन्न एवं अलग होनी चाहिए ताकि यह साइबर खतरों के जोखिमों और इन जोखिमों से निपटने / कम करने के उपायों पर अपना पूर्ण ध्यान लगा सके।
6. **सुरक्षा के लिए सहायक आईटी आर्किटेक्चर :-**
   आईटी आर्किटेचर इस तरह से बनाया जाए कि वह सदैव लागू किए जाने वाले सुरक्षा उपायों की सुविधा का ध्यान रखे। बोर्ड की आईटी उप समिति द्वारा इसकी समीक्षा की जाए और यदि आवश्यक हो तो इसके जोखिम मूल्यांकन के अनुसार इसे चरणबद्ध तरीके से अद्यतन किया जाए।

7. **मुस्तैदी संकेतक :-**

बैंकों में साइबर सुरक्षा मुस्तैदी संकेतकों की स्थापना की जानी चाहिए जिससे सुरक्षा में कोई चूक या कमी की जानकारी समय से हो सके। इन संकेतकों को स्वतंत्र अनुपालन जांच तथा योग्य एवं सक्षम पेशेवरों द्वारा की गई लेखा परीक्षाओं द्वारा व्यापक जांच के लिए इस्तेमाल किया जाना चाहिए। कर्मचारियों के साथ-साथ हितधारकों के बीच जागरूकता को भी इस मूल्यांकन का भाग बनाया जाना चाहिए।

8. **साइबर-सुरक्षा घटनाओं से संबंधित सूचनाओं को आरबीआई के साथ साझा करना :-**

बैंकों को उनके यहां घटित साइबर अपराध की घटनाओं को भारतीय रिज़र्व बैंक से समय पर साझा करना चाहिए जिससे साइबर – घटनाओं को साझा करने में संस्थाओं के बीच परस्पर सहयोग तथा निर्धारित प्रक्रियाओं से साइबर-जोखिमों को रोकने के लिए समय पर उपाय लागू किए जा सकें। इस प्रकार के समन्वयित प्रयासों से सामूहिक खतरे की आसूचना, समय पर अलर्ट्स तथा सक्रिय साइबर सुरक्षा उपायों को अपनाने में बैंकों को मदद मिलेगी।

9. **बोर्ड द्वारा अनुमोदित साइबर सुरक्षा नीति की आवश्यकता :-**

बैंकों को अपने बोर्ड द्वारा विधिवत अनुमोदित साइबर सुरक्षा नीति को तत्काल लागू करना चाहिए जिसमें साइबर खतरों से लड़ने के लिए उचित उपायों की रणनीति तथा कारोबार की जटिलताओं का स्तर और जोखिम का स्वीकार्य स्तर स्पष्ट होने चाहिए।

वस्तुतः इंटरनेट ने दुनिया के परिवर्तन की गति अत्यधिक तीव्र कर दिया है। नित-नवीन नई तकनीक आ रही है और लोग दिल खोलकर नई चीजों को अपना रहे हैं, इससे जहां उनका जीवन सरल होता है वहीं उनके साइबर अपराध के शिकार होने की संभावनाएं भी बढ़ जाती हैं। ऐसी परिस्थितियों में हम साइबर अपराध से बचने के लिए सुरक्षात्मक उपायों को अपनाकर साइबर संबंधी किसी भी धोखाधड़ी से बच सकते हैं। तथापि कभी-कभी हम सारी सावधानियां बरतने के बाद भी साइबर अपराध के शिकार हो जाते हैं। ऐसी स्थिति में "साइबर बीमा" हमारे जीवन निर्णायक भूमिका का निर्वाह कर सकता है। भारतीय रिजर्व बैंक ने समय-समय पर कंपनियों और बैंकों के दायित्वों का निर्धारण किया है जो एक सराहनीय कदम है, लेकिन कंपनियां भी यह दलील दे सकती हैं कि साइबर हमलों में यदि उनका ही पैसा डूब गया तो वे कैसे अन्य हितधारकों का ख्याल रखें? इसी समस्या का समाधान 'साइबर बीमा' है। यद्यपि अभी साइबर बीमा का अधिक प्रचार-प्रसार नहीं है, परंतु यह आशा है कि साइबर जागरूकता बढ़ने के साथ इस क्षेत्र में भी पर्याप्त वृद्धि देखने को मिलेगी। फलस्वरूप हम सभी संस्थागत और व्यक्तिगत स्तर पर अधिक सुरक्षित और खुशहाल होंगे।

स्रोत-

1. साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम
2. बैंकों की साइबर सुरक्षा नीति
3. www.rbi.org.in
4. www.drishtiias.com
5. www.wikipedia.org

*****

नीलेश कुमार

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- बैंक ऑफ महाराष्ट्र
मोबाइल नं. :- 9051069869
ई-मेल:- nilesh.kumar@mahabank.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

आज इंटरनेट हमारी दिनचर्या का अभिन्न हिस्सा बन चुका है। प्रत्येक दूसरा व्यक्ति इसका लाभ बैंकिंग, ई-कॉमर्स, शिक्षा, मनोरंजन आदि के लिए उठा रहा है। देश की अधिकतर सेवाएं ऑनलाइन उपलब्ध कराई जा रही हैं। विमुद्रीकरण के बाद देश में डिजिटलीकरण को विशेष प्रोत्साहन मिला है। नकदी का स्थान डेबिट कार्ड, क्रेडिट कार्ड, ऑनलाइन बैंकिंग, यूपीआई आदि ले रहे हैं। समय के साथ कई पेमेंट बैंक भी सामने आए हैं और देश को डिजिटल बनाने में सहयोग प्रदान कर रहे हैं। कोरोना महामारी के दौरान डिजिटलीकरण को अतिरिक्त गति मिली है। इससे लोगों के समय की बचत हो रही है और महामारी में शारीरिक दूरी एवं अन्य सुरक्षात्मक उपायों को अपनाने में मदद मिल रही है। कंप्यूटर और इंटरनेट प्रौद्योगिकी के तेजी से विस्तार के साथ साइबर अपराधों की संख्या में भी बढ़ोत्तरी देखी जा रही है। नैशनल क्राइम रिकॉर्ड ब्यूरो (एनसीआरबी) की एक रिपोर्ट के अनुसार वर्ष 2020 में भारत में साइबर अपराध के 50,035 मामले सामने आए जो विगत वर्ष की तुलना में 11.8% अधिक पाए गए। वर्ष 2020 में ऑनलाइन बैंकिंग धोखाधड़ी के 4,047 मामले, ओटीपी धोखाधड़ी के 1093 मामले, डेबिट/ क्रेडिट धोखाधड़ी के 1,194 मामले और एटीएम धोखाधड़ी के 2,160 मामले सामने आए। साइबर अपराधों की दर (प्रति लाख जनसंख्या पर घटनाओं) में भी बढ़ोत्तरी देखी गई। वर्ष 2019 में यह 3.3% थी जो वर्ष 2020 में बढ़कर 3.7% हो गई।

साइबर अपराध की परिभाषा :

साइबर अपराध एक ऐसा अपराध है जिसमें किसी की निजी जानकारी बिना अनुमति के ऑनलाइन चोरी की जाती है और उसे आर्थिक क्षति पहुंचाई जाती है। इसमें कंप्यूटर और नेटवर्क शामिल होता है। साइबर अपराध कई प्रकार से किए जाते हैं यथा - जानकारी चोरी करना, जानकारी में फेरबदल करना, जानकारी नष्ट करना, किसी की जानकारी को किसी अन्य को देना आदि। साइबर अपराध भी कई प्रकार के होते हैं, जैसे स्पैम ई-मेल, हैकिंग, फिशिंग, विशिंग, स्पैमिंग आदि।

बैंकिंग में साइबर अपराधों का स्वरूप :

उभरती हुई प्रौद्योगिकी का सबसे अधिक लाभ बैंकिंग क्षेत्र को मिला है। यह प्रौद्योगिकी का ही असर है कि आज शाखा कंप्यूटरीकृत बैंकिंग से मोबाइल एवं वर्चुअल बैंकिंग तक जा पहुंची है। प्रौद्योगिकी जनित इन बदलावों से बैंकों के समक्ष कई चुनौतियां भी उत्पन्न हुई हैं जिसमें एक प्रमुख चुनौती साइबर जोखिम के रूप में है। बदलते समय के साथ साइबर अपराधों की घटनाओं का पैटर्न भी अधिक चुनौतीपूर्ण और जटिल बनता जा रहा है।

वर्ष 2017 में रैनसमवेयर वायरस के आने के पहले तक माना जाता था कि वायरस का उद्देश्य कंप्यूटर का डेटा चुराना या फिर उसे मिटाना होता है। रैनसमवेयर वायरस के आने के बाद यह सोच बदल गई। रैनसमवेयर

वायरस एक ऐसा वायरस है जो सिस्टम में घुसकर डेटा लॉक कर गिरफ्त में आए लोगों एवं कंपनियों से फिरौती की मांग करता है। रैनसमवेयर जैसे साइबर हमले डिजिटल बैंकिंग अभियान के लिए खतरा साबित हो सकते हैं। समय के साथ ऐसे हमलों में तेजी से बढ़ोत्तरी भी हो रही है। आईटी विशेषज्ञों के मुताबिक फिरौती मांगने वाले, जासूसी करने वाले (स्पाईवेयर) और दूसरे के कंप्यूटर का गलत इस्तेमाल करने वाले (ट्रोजन) हमलों में भारत सहित पूरी दुनिया में तेजी से वृद्धि हो रही है। जुनिपर रिसर्च ने एक अध्ययन में अनुमान लगाया है कि 2024 तक डेटा ब्रीच की लागत प्रति वर्ष 11% की वृद्धि के साथ 3 ट्रिलियन डॉलर से बढ़कर 5 ट्रिलियन डॉलर हो सकती है।

साइबर अपराध में निम्नलिखित श्रेणियां प्रमुख हैं –

1) हैकिंग : यदि कोई व्यक्ति कहीं दूर बैठकर इंटरनेट की सुरक्षा में सेंध हमारे कंप्यूटर, वेबसाइट या प्रोफाइल में लॉग-इन करने में सक्षम होता है तो इसका मतलब उस व्यक्ति ने हमारे कंप्यूटर, वेबसाइट या सोशल मीडिया प्रोफाइल को हैक कर लिया है। इसके बाद वह हमारे कंप्यूटर, वेबसाइट या प्रोफाइल का गलत इस्तेमाल भी कर सकता है। इसे हैंकिंग कहा जाता है।

2) फिशिंग : फिशिंग वह तकनीक है जिसमें लॉगिन आईडी और पासवर्ड, डेबिट/ क्रेडिट कार्ड विवरण, पिन, जन्मतिथि और मोबाइल नंबर आदि निजी जानकारी धोखे से प्राप्त की जाती है। आजकल होने वाले सोशल इंजीनियरिंग हमलों में सबसे ज्यादा मामले फिशिंग के होते हैं। अधिकांश फिशिंग हमले निम्नलिखित उद्देश्य से किए जाते हैं:

- ❖ संक्षिप्त या भ्रामक लिंक का उपयोग कर व्यक्तिगत जानकारी जैसे नाम, पता, बैंक खाता विवरण, पैन, आधार आदि प्राप्त करना।
- ❖ उपयोगकर्ता को भय, लोभ तथा जल्दबाजी के लिए उकसा कर तुरंत कार्रवाई करने के लिए मजबूर करना।

फ़िशिंग हमलों से बचने के उपाय

- ❖ किसी भी अनजान हाइपरलिंक या मेल अटैचमेंट पर क्लिक न करें।
- ❖ भेजने वाले की पहचान या प्रामाणिकता की जांच करें।
- ❖ वैध वेबसाइट की पुष्टि के लिए यूआरएल की जांच अवश्य करें।
- ❖ मेल से प्राप्त संदेश में टाइपिंग और व्याकरण की अशुद्धियों पर ध्यान दें।
- ❖ हमेशा याद रखें, बैंक कभी भी आपकी निजी जानकारी नहीं मांगता है।
- ❖ लुभावने ऑफरों से सावधान रहें।

3) विशिंग : विशिंग धोखाधड़ी टेलीफोन के माध्यम से की जाती है। इसमें अपराधी वित्तीय लाभ अर्जित करने के लिए लोगों को फोन कर निजी जानकारी मांगता है और गलत इस्तेमाल करते हुए आर्थिक अपराध को अंजाम देता है। विशिंग से संबंधित धोखाधड़ी में दिन-प्रतिदिन वृद्धि देखी जा रही है।

विशिंग हमलों से बचने के उपाय :

- ❖ हमेशा फोन करने वाले के पहचान की पुष्टि करें।
- ❖ अपने मोबाइल पर कोई भी अनजान सॉफ्टवेयर इंस्टॉल न करें।
- ❖ अवांछित बिक्री, मार्केटिंग या अन्य संदेशों का जवाब न दें।
- ❖ फोन पर ओटीपी, एटीएम पिन, सीवीवी शेयर न करें।

4) स्पैमिंग: स्पैमिंग थोक में भेजे जाने वाले ई-मेल को कहते हैं। इसमें प्राय: विज्ञापन होते हैं। इंटरनेट सुरक्षा के लिए कार्यरत कंपनी ट्रेड माइक्रो के अनुसार भारत एशिया का सातवां सबसे बड़ा देश है जहां स्पैमिंग भारी मात्रा में की जाती है।

5) डिनायल ऑफ़ सर्विस अटैक : यह इंटरनेट की दुनिया में किसी सर्वर या वेबसाइट पर किया जाने वाला ऐसा आक्रमण है जिससे किसी भी सर्वर या वेबसाइट को बॉटनेट के जरिए डाउन कर दिया जाता है या बंद कर दिया जाता है या फिर उस वेबसाइट के यूजर के लिए वेबसाइट को अनुपलब्ध कर दिया जाता है। इस पूरी प्रक्रिया के पीछे सिर्फ एक ही आदमी का ही हाथ नहीं होता है बल्कि हैकर्स की एक पूरी टीम होती है जो मिलकर इसे अंजाम देती है।

6) एटीएम स्किमिंग और प्वाइंट ऑफ सेल अपराध : क्रेडिट या डेबिट कार्ड की चोरी को स्किमिंग कहते हैं। इस तरीके में चोर अपने शिकार के क्रेडिट कार्ड का नंबर, रसीदों की फोटोकॉपी कर या और अधिक विकसित तरीकों से जैसे एक छोटे से इलेक्ट्रॉनिक उपकरण (स्किमर) का उपयोग करके सैकड़ों क्रेडिट कार्ड नंबर अपने पास संग्रहित कर सकते हैं। स्किमिंग एटीएम/ पीओएस में किया जाता है। इसमें अपराधी हमारे डेटा की स्किमिंग करने के बाद धोखाधड़ी करते हैं।

भारत सरकार द्वारा उठाए गए कदम

1) सीईआरटी-इन (कंप्यूटर आपात कार्रवाई टीम-भारत) एवं सीसीबी (साइबर सुरक्षित भारत)

भारत सरकार साइबर खतरों के प्रति सचेत है। इसी के तहत सीईआरटी-इन गठित की गई है। यह संगठन साइबर सुरक्षा को बेहतर करने की दिशा में सक्रियता से कार्रवाई कर रहा है। इसके द्वारा राष्ट्रीय साइबर संकट प्रबंधन योजना तथा साइबर सुरक्षा मूल्यांकन फ्रेमवर्क भी तैयार किया गया है।

2) साइबर संकट प्रबंधन योजना :

साइबर संकट को देखते हुए बैंक में साइबर संकट प्रबंधन योजना (सीसीएमपी) को प्रभावी रूप से अपनाया जा रहा है। सीसीएमपी के तहत बैंक के साइबर धोखाधड़ी कक्ष निम्नलिखित 4 पहलुओं पर कार्रवाई कर रहे हैं –

क) पहचान
ख) जवाबी कार्रवाई
ग) सुधार
घ) नियंत्रण

इससे किसी भी अनहोनी की स्थिति में बैंक नियंत्रणात्मक कार्रवाई कर पाने में सक्षम बन रहे हैं।

3) एसओसी (सिक्यूरिटी ऑपरेशन सेंटर) केन्द्र

साइबर आक्रमण कभी भी घटित हो सकते हैं, अतः ऐसी स्थिति में बैंकों द्वारा स्थापित एसओसी केन्द्र साइबर जोखिम प्रबंधन में काफी सहायक सिद्ध हो रहे हैं। इन केन्द्रों के लिए आवश्यक है कि वे नियमित चौकसी को सुनिश्चित करें तथा आगामी साइबर खतरों के स्वरूपों को नियमित आधार पर अद्यतन करें।

4) भारतीय साइबर अपराध समन्वय केंद्र की स्थापना

जनवरी 2020 में गृह मंत्रालय द्वारा साइबर क्राइम से निपटने के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' की शुरूआत की गई है। इस योजना को संपूर्ण भारत में लागू किया गया है। साइबर क्राइम से बेहतर तरीके से

निपटने के लिये तथा I4C को समन्वित और प्रभावी तरीके से लागू करने हेतु इस योजना के निम्नलिखित सात प्रमुख घटक है –

- नेशनल साइबर क्राइम थ्रेट एनालिटिक्स यूनिट
- नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल
- संयुक्त साइबर अपराध जांच दल के लिये मंच
- राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र
- राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र
- साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट
- राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र

भारतीय रिज़र्व बैंक द्वारा जारी दिशानिर्देश :

भारतीय रिज़र्व बैंक द्वारा समय-समय पर साइबर अपराध के संबंध में दिशानिर्देश जारी किए जाते हैं। साइबर सुरक्षा के खतरों से निपटने के लिए भारतीय रिज़र्व बैंक ने श्री जी. गोपालकृष्ण की अध्यक्षता में एक वर्किंग ग्रुप का गठन किया। समिति की अनुशंसा के आधार पर बैंकों को इंन्फॉरमेशन सिक्यूरिटी, इलेक्ट्रॉनिक बैंकिंग, तकनीकी जोखिम प्रबंधन और साइबर धोखाधड़ी के संबंध में दिशानिर्देश जारी किए गए। कुछ महत्वपूर्ण दिशानिर्देश निम्नानुसार हैं –

1) साइबर सुरक्षा नीति – साइबर सुरक्षित माहौल बनाने हेतु एक साइबर सुरक्षा नीति बनाई जानी चाहिए। यह विस्तृत आईटी नीति/ आई.एस सिक्यूरिटी नीति से भिन्न होनी चाहिए ताकि यह साइबर खतरों के जोखिमों और इन जोखिमों से निपटने के उपायों पर प्रकाश डाल सकें।

2) नियमित निगरानी की व्यवस्था – साइबर अपराधों से बचने के लिए बैंकों को निर्देश दिया गया है कि एसओसी (सिक्यूरिटी ऑपरेशन सेंटर) स्थापित किया जाए।

3) व्यापक रूप से नेटवर्क तथा डेटाबेस सुरक्षा पर ध्यान देना – बढ़ती घटनाओं के कारण प्रत्येक बैंक में नेटवर्क सुरक्षा की बेहतर तरीके से समीक्षा करने की आवश्यकता पर ध्यान केन्द्रित किया गया है। नेटवर्क तथा डेटाबेस में अप्राधिकृत रूप से एक्सेस करने की अनुमति नहीं दी जानी चाहिए तथा जब कभी भी अनुमति दी जाए तो निर्धारित प्रक्रियाओं का अनिवार्य रूप से पालन किया जाए।

सुरक्षात्मक उपाय

लॉगिन सिक्योरिटी:

- हमेशा मजबूत और जटिल पासवर्ड का प्रयोग करें।
- पासवर्ड को समय-समय पर बदलें।
- अपनी यूजर आईडी, पासवर्ड या पिन कभी किसी को न बताएं, न ही कहीं स्टोर करें अथवा लिखें।
- यूजर आईडी और पासवर्ड को स्टोर होने से बचाने के लिए अपने कंप्यूटर में ऑटो सेव या ऑटो रिमेम्बर फ़ंक्शन को निष्क्रिय करें।

इंटरनेट सिक्योरिटी:

- बैंकिंग साइट के एड्रेस बार में हमेशा "https" देखें।
- सार्वजनिक वाई-फाई नेटवर्क का उपयोग कर ऑनलाइन बैंकिंग लेनदेन न करें।

- अपना काम समाप्त करने के बाद हमेशा लॉगआउट करें।

यूपीआई सिक्योरिटी:

- अपना मोबाइल पिन और यूपीआई पिन अलग-अलग रखें।
- संदिग्ध अनुरोध का जवाब न दें। रिपोर्ट करें।
- अगर आपके जानकारी के बिना कोई यूपीआई ट्रांजेक्शन हुआ है तो अपने अकाउंट पर यूपीआई सर्विस को तुरंत डिसेबल करें।

डेबिट/ क्रेडिट कार्ड सिक्योरिटी:

- एटीएम मशीनों या पीओएस के माध्यम से लेनदेन/ पिन डालते समय की-पैड को कवर करें।
- लेनदेन करने से पहले हमेशा ई-कॉमर्स वेबसाइटों की प्रामाणिकता सुनिश्चित करें।
- घरेलू और अंतर्राष्ट्रीय दोनों तरह के लेन-देन के लिए ई-कॉमर्स प्लेटफॉर्म, पीओएस और एटीएम पर कार्ड लेनदेन की सीमा निर्धारित करें।

मोबाइल बैंकिंग सिक्योरिटी:

- आपके फोन, टैबलेट पर मजबूत पासवर्ड/ बायोमेट्रिक प्रमाणीकरण लागू होनी चाहिए।
- अपना मोबाइल पिन किसी से साझा न करें, जहां भी संभव हो बायोमेट्रिक प्रमाणीकरण का उपयोग करें।
- अनजान लोगों की सलाह पर कोई भी ऐप इंस्टॉल न करें। मोबाइल ऐप केवल विश्वसनीय स्टोर के माध्यम से ही डाउनलोड करें।

सोशल मीडिया सिक्योरिटी:

- आप जिसके साथ बातचीत कर रहे हैं, उस व्यक्ति के पहचान की पुष्टि करें।
- किसी भी सोशल मीडिया प्लेटफॉर्म पर अपनी व्यक्तिगत/वित्तीय जानकारी साझा न करें।

उपसंहार

समग्रतः हम कह सकते हैं कि तकनीक के बढ़ने के साथ-साथ साइबर अपराधों में भी बढ़ोत्तरी हो रही है। साइबर अपराध को पूरी तरह से खत्म करना कठिन है लेकिन इसके खतरे को कम जरूर किया जा सकता है। इसके लिए जरूरी है कि हम भारत सरकार और विभिन्न विनियामकों द्वारा समय-समय पर जारी दिशानिर्देशों का अनुपालन सुनिश्चित करें। इसके अतिरिक्त व्यापक उपभोक्ता शिक्षा और जागरूकता फैलाना भी अत्यंत आवश्यक है।

संदर्भ

1) http://www.internetworldstats.com
2) भारतीय रिज़र्व बैंक के विभिन्न परिपत्र

*****

नेहा मुझाल्दा

पदनाम:- एडीसी अधिकारी
संस्था का नाम:- बैंक ऑफ इंडिया
मोबाइल नं. :- 7440446026
ई-मेल:- Neha.Muzalda@bankofindia.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

प्रस्तावना :- एक फोन कॉल या SMS से खाली हो सकता है आपका बैंक अकाउंट, फिशिंग के जरिए नेट बैंकिंग में सेंध जैसे समाचार आपको न्यूज़ पेपर, इन्टरनेट, न्यूज़ आदि में पढ़ने, देखने एवं सुनने को मिलती रहती हैं। अपराधी बैंक फ्रॉड करने के लिए तरह-तरह के तरीकों का इस्तेमाल कर रहे हैं। वे व्यक्ति को झांसे में फंसाकर कुछ मिनटों में उनका अकाउंट खाली कर देते हैं। आज कल अपराधों की श्रेणी में नए प्रकार के अपराध मिल रहे हैं - साइबर अपराध। साइबर अपराध में नेट बैंकिग का इस्तेमाल करके लोगों को लुटने के लिए नए-नए तरीको का उपयोग किया जाता है। जैसे क्लोनिंग, हैकिंग, मैलवेयर आदि। साइबर अपराधियों ने नेट बैंकिग का इस्तेमाल करने वाले लोगों को लुटने के लिए नए- नए तरीके निकाल रहे हैं। फिशिंग अटैक करके खातों से पैसे निकालने वाला गिरोह बैंक या दूसरे वित्तीय संस्थानों से मिलती- जुलती वेबसाइट तैयार करने के बाद लोगों को ई-मेल या स्पैम भेजकर फंसाता है।

बैकिंग सेक्टर भी साइबर अपराधियों की नजर में है, इसमें निशाना इंटरनेट बैंकिंग और ब्रोकरेज सेवाएं हैं। ऑनलाइन बैंक खातों पर फिशिंग अटैक और एटीएम/डेबिट कार्ड की क्लोनिंग की घटनाएं आम हैं। ऑनलाइन बैंकिंग और फाइनेंशियल ट्रांजेक्शन के लिए मोबाइल का उपयोग बढ़ने से साइबर अपराध का खतरा और बढ़ गया है।

साइबर सुरक्षा के बारे में गहन जानकारी और ज्यादा परिष्कृत तकनीक से लैस साइबर अपराधियों के कारण भारत बड़े पैमाने पर साइबर अपराध के खतरे का सामना कर रहा है। हाल के वर्षों में भारत बड़े पैमाने पर साइबर हमले का शिकार रहा है। इससे सवाल उठता है कि आपके सभी बैंकिंग, एटीएम/डेबिट कार्ड और ऑनलाइन बैंकिंग खाते वास्तव में कितने सुरक्षित हैं।

साइबर अपराध क्या है? :- साइबर अपराध को साइबर क्राइम या कंप्यूटर क्राइम भी कहा जाता है। साइबर अपराध एक प्रकार की गैर कानूनी गतिविधि है जिसे इंटरनेट या डिजिटल माध्यमों की सहायता से अंजाम दिया जाता है। सामान्य शब्दों में डिजिटल या इंटरनेट माध्यमों से होने वाला कोई भी अपराध साइबर अपराध कहलाता है। जैसे-जैसे सूचना और प्रौद्योगिकी का क्षेत्र बढ़ता जा रहा है वैसे-वैसे साइबर अपराधों की संख्या भी बढ़ती जा रही है और देश का लगभग हर व्यक्ति इसका शिकार हो रहा है साइबर अपराध एक बहुत ही बड़ा अपराध है जिससे सुरक्षित रहने के लिए सबसे जरूरी जागरूकता और सतर्कता है।

साइबर अपराध के प्रकार:- साइबर अपराध कई प्रकार के होते हैं जैसे हैकिंग, साइबर स्टॉकिंग और थेफ़्ट, DDos हमले, पहचान की चोरी आदि।

1- **हैकिंग**:- हैकिंग एक प्रकार का साइबर अपराध है जिसमें एक व्यक्ति के कंप्यूटर के अंदर उसकी व्यक्तिगत या संवेदनशील जानकारी को प्राप्त करने के उद्देश्य से उस तक पहुंच बनायी जाती है। अर्थात

किसी व्यक्ति की अनुमति के बिना उसके कंप्यूटर की सभी महत्वपूर्ण जानकारियों को चुराना **हैकिंग** कहलाता है। हैकिंग करने वाले व्यक्ति को हैकर कहा जाता है। हैकिंग में अपराधी विभिन्न सॉफ्टवेयर के माध्यम से व्यक्ति के कंप्यूटर में प्रवेश करने का प्रयास करता है और पीड़ित व्यक्ति को यह पता भी नहीं चलता है कि उसके कंप्यूटर को कोई एक्सेस कर रहा है।

2- **साइबर स्टॉकिंग और थेफ़्ट** : साइबर स्टॉकिंग एक प्रकार का ऑनलाइन उत्पीड़न है पीड़ित को ऑनलाइन संदेशों और मेल के माध्यम से परेशान किया जाता है। इसके अलावा थेफ़्ट भी एक प्रकार का अपराध है। जब कोई व्यक्ति ऑनलाइन व डिजिटल माध्यमों से कॉपीराइट के नियमों का उल्लंघन करता है जैसे गैर कानूनी तरीके से कोई गाना, मूवी या गेम आदि डाउनलोड करता है उसे थेफ्ट कहा जाता है।

3- **DDos हमले**:- DDos एक प्रकार का ऐसा साइबर अपराध है जिसमें अपराधी द्वारा ऑनलाइन सेवा को अनुपलब्ध बनाने का प्रयास किया जाता है तथा साइट पर कई स्रोतों से ट्रैफिक लाकर साइट को डाउन किया जाता है। DDos को बोटनेट्स नामक संक्रमित उपकरणों के बड़े नेटवर्क के माध्यम से उपयोगकर्ताओं के कंप्यूटर पर मैलवेयर जमा करके बनाया जाता है और नेटवर्क के डाउन होते ही हैकर सिस्टम को हैक कर लेता है।

4- **Malicious सॉफ्टवेयर**:- ऐसे बहुत से इन्टरनेट बेस्ड सॉफ्टवेयर या प्रोग्राम्स हैं जो की किसी भी नेटवर्क को ख़राब कर सकते हैं। ऐसे सॉफ्टवेयर को यदि किसी नेटवर्क में एक बार इनस्टॉल कर दिया जाये तब ये हैकर्स बड़ी ही आसानी से उस नेटवर्क में स्थित डेटा को भी ख़राब कर सकते हैं।

5- **पहचान की चोरी:-** यह क्राइम आज के समय में सबसे ज्यादा देखा जा रहा है। ये ज्यादातर उन लोगों को टारगेट करते हैं जो लोग ज्यादातर इन्टरनेट के माध्यम से कैश लेनदेन और बैंकिंग सर्विसेज का उपयोग करते हैं। इस साइबर अपराध के अंतर्गत एक अपराधी किसी व्यक्ति के बैंक के खाते, क्रेडिट कार्ड, डेबिट कार्ड, पूरा नाम आदि की जानकारी प्राप्त करने का प्रयास करता है ताकि व्यक्ति से पैसे प्राप्त किए जा सके या पीड़ित के नाम पर ऑनलाइन खरीदी की जा सके।

6- **साइबर टेरेरिज्म** :- बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं लेकिन यूजर्स उनके इरादें समझ नहीं पाते हैं और जाने-अनजाने में ऐसे लिंक्स को शेयर करते रहते हैं, लेकिन यह भी साइबर अपराध और साइबर-आतंकवाद की श्रेणी में आता है।

साइबर क्राइम के कारण:-

- डिजिटल जागरूकता की कमी होना
- कानूनों का अभाव
- तकनीकी अधिकारियों और कर्मचारियों की कमी
- क्राइम के दायरों का अधिक विस्तृत ना होना
- साइबर क्राइम से संबंधित शिकायत प्रणाली का अभाव

साइबर क्राइम को खत्म करने या उससे सुरक्षित रहने के लिए भारत सरकार द्वारा किए गए प्रयास:-

- भारत में साइबर अपराध को रोकना और उससे सुरक्षित होना बहुत कठिन कार्य है क्योंकि भारत में आधारभूत संरचना का अभाव है परन्तु फिर भी भारत सरकार साइबर अपराध को दूर करने के लिए ठोस प्रयास कर रही है।
- सूचना प्रौद्योगिकी अधिनियम 2000 (आईटी एक्ट 2000) की धाराएं 43, 43A, 66, 67, 67A, 70, 72, 72A और 74 हैकिंग और साइबर अपराधों से संबंधित है ये सभी धाराएं लागू की गई है।

- साइबर अपराध से सुरक्षा के लिए सरकार द्वारा राष्ट्रीय साइबर नीति 2013 जारी की गई जिसके तहत सरकार ने अति संवेदनशील सूचनाओं के संरक्षण एवं सुविधा के लिए राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical information Infrastructure Protection Centre - NCIIPC) का गठन किया। इस नीति के तहत अपराधी को 2 वर्ष से लेकर उम्रकैद व दंड और जुर्माने का प्रावधान किया गया है।
- भारत सरकार द्वारा कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-in) की स्थापना की गई। यह कंप्यूटर सुरक्षा के लिए राष्ट्रीय स्तर की मॉडल एजेंसी है।
- भारत सरकार द्वारा देश में साइबर अपराधों से समन्वित और प्रभावी ढंग से निपटने के लिए साइबर स्वच्छता केंद्र की स्थापना की गई है। इसके अलावा भारत साइबर अपराधों को खत्म करने के लिए सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्यप्रणाली अपनाने के लिए अमेरिका, चीन और ब्रिटेन जैसे देशों के साथ समन्वय स्थापित कर रहा है।
- भारतीय रिज़र्व बैंक ने मास्टर कार्ड पर सख्त कार्रवाई की है। केन्द्रीय बैंक के नियमों का पालन नहीं करने की वजह से मास्टर कार्ड के नए डेबिट-क्रेडिट कार्ड जारी करने पर रोक लगा दी है।
  भारतीय रिज़र्व बैंक के नियमानुसार सभी पेमेंट सर्विस प्रोवाइडर कंपनियों द्वारा ग्राहकों का डेटा, भुगतान लेनदेन संबंधी विवरण आदि आंकड़ों का स्टोरेज सिर्फ भारत में किया जाना था। इसके लिए भारतीय रिज़र्व बैंक ने इन्हें 6 माह का समय भी दिया था परन्तु भारतीय रिज़र्व बैंक के नियमों का पालन न होने के कारण 22 जुलाई, 2022 को भारत में मास्टर कार्ड पर रोक लगा दिया गया है।

<u>बैंकिंग में साइबर अपराधों से बचने के सुरक्षात्मक उपाय :-</u>

जामताड़ा झारखण्ड का एक छोटा जिला है लेकिन इसने भारत के अलावा कई दूसरे देशो के भी कान खड़े कर रखे हैं। जामताड़ा ठगों की बस्ती के रूप में कुख्यात हो चुका है। कहने को यहां के ज्यादातर युवा कम पढ़े-लिखे है। कोई पांचवी फेल, तो कोई चौथी फेल है। लेकिन दिमाग इतना शातिर की सारे देश को ठगने में लगे हैं जामताड़ा पर सिर्फ विभिन्न राज्यों की साइबर क्राइम पुलिस ही नजर नहीं रखती, बल्कि अब अमेरिका की एक एजेंसी भी इस पर रिसर्च करेगी। वे यह पता लगाएंगे कि आखिर यहां के युवा ठगी इस प्रकार के विचार लाते कहां से हैं? कैसे छोटे से शहर के बेरोजगार युवा ठगी के जरिये लखपति बन गए? जामताड़ा के ठग बकायदा कॉल सेंटर के जरिये ठगी करते हैं। ये विभिन्न प्रकार के ऐप डाउनलोड करवाकर लोगों का पैसा उड़ा देते हैं।

यहां के ठग किसी को नहीं छोड़ते, चाहे वो अमीर हो या गरीब। पुलिस वाला हो या कोई नेता-अभिनेता।

बैंकिंग में साइबर अपराधों से बचने के सुरक्षात्मक उपाय निम्नलिखित हैं:-

- पी.पी.एस.(पॉजिटिव पे सिस्टम) 1 जनवरी, 2021 से सभी बैंकों में यह सिस्टम लागू किया गया है। इस सिस्टम के अनुसार 5.00 लाख या इससे अधिक राशि वाले सभी चेकों की सूचना बैंक में दिया जाना आवश्यक है।
- मास्टर कार्ड के माध्यम से भारतीय रिज़र्व बैंक के नियमों का उल्लंघन किया जिसके कारण भारतीय रिज़र्व बैंक ने मास्टर कार्ड पर रोक लगा दी है।
- ग्राहक अपना एटीएम कार्ड, इन्टरनेट बैंकिंग आदि के पासवर्ड एवं ओटीपी किसी अनजान व्यक्ति को भी ना बताये।
- ग्राहक अपना एटीएम कार्ड, क्रेडिट कार्ड एवं पिन किसी भी रिश्तेदार या मित्र आदि को ना बताये।
- किसी भी प्रकार की जानकारी फोन कॉल, मेल, एसएमएस के माध्यम से किसी को भी नहीं देना चाहिए एवं इसकी सूचना अपनी शाखा में अवश्य दें।

- ग्राहक को अपने पासवर्ड में अपना नाम, जन्म तारीख, रिश्तेदारों का नाम आदि नहीं रखना चाहिए। पासवर्ड में अपर केस, लोअर केस, स्पेशल कैरैक्टर, संख्यात्मक होनी चाहिए। पासवर्ड कहीं लिखना नहीं चाहिए और न ही किसी को बताना चाहिए।
- इन्टरनेट बैंकिंग का प्रयोग अपने मोबाइल फोन या कंप्यूटर में करना चाहिए। किसी दूसरे का कंप्यूटर कभी प्रयोग करना पड़े तो उसकी हिस्ट्री क्लियर कर देनी चाहिए।
- अपना एटीएम कार्ड, क्रेडिट कार्ड आदि गूम होने पर सर्वप्रथम इसे ब्लॉक करवाना चाहिए एवं इसकी सूचना शाखा में देनी चाहिए।
- एटीएम मशीन से पैसे निकलते समय इस बात का ध्यान रखें कि कोई अन्य व्यक्ति साथ में ना हो एवं अपना लेन-देन पूर्ण होने के बाद ही एटीएम से बाहर जाना चाहिए।
- ऑनलाइन विश्वसनीय साइट से ही खरीदारी करनी चाहिए। कई नकली साइट कम दाम एवं नकली माल बेच कर ग्राहकों को ठगते हैं।

निष्कर्ष:- कोरोना महामारी के दौर में ज्यादातर लोग अपने बैंक से जुड़ा कामकाज इन्टरनेट या स्मार्टफोन के जरिए कर रहे हैं। ऐसे में साइबर क्राइम के मामलों में लगातार बढ़ोत्तरी हो रही है। इनमें साइबर अपराधी अलग-अलग तरीके अपनाते हैं। इनमें से दो तरीके विशिंग और स्मिशिंग भी हैं। साइबर अपराध के मामले बढ़ने से कारोबारी इसका प्रभाव न सिर्फ वित्तीय मोर्चे पर महसूस कर रहे हैं, बल्कि इससे उनके ब्रांड और साख को भी नुकसान हो रहा है। रिपोर्ट के अनुसार साइबर अपराधी अपनी तकनीक को लगातार विकसित और अपग्रेड कर रहे हैं। इसके अलावा अब वे वित्तीय सूचनाओं की चोरी के बजाय कारोबारी जासूसी और सरकारी सूचनाएं हासिल करने की वारदातों को अंजाम देने पर ज्यादा ध्यान दे रहे हैं। यदि आपके बैंक अकाउंट से धोखाधड़ी हुई है तो यदि आप 3 दिन के अन्दर बैंक में शिकायत करते हैं तो आपको आपका पूरा पैसा वापस मिल सकता है। पिछले कुछ वर्षों के दौरान साइबर अपराध के हमलों की संख्या तेजी से बढ़ी है।

स्त्रोत:- नेट, समाचार पत्रों में प्रकाशित आर्टिकल, भारतीय रिज़र्व बैंक की वेबसाइट आदि

******

नौशाबा हसन

पदनाम:- सहायक महाप्रबंधक
संस्था का नाम:- भारतीय स्टेट बैंक
मोबाइल नं. :- 7389905035
ई-मेल:- naushaba.hasan@sbi.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

सम्पूर्ण विश्व में अब तक हुए विकास में प्रौद्यौगिकी का कार्यान्वयन तथा विस्तार सबसे बड़े प्रेरक के रूप में उभर कर सामने आया है। साइबर स्पेस की उन्नत तकनीकों के दुरूपयोग के फलस्वरूप अलग-अलग तरह के साइबर अपराध भी अस्तित्व में आते चले गए हैं। विभिन्न प्रणालियों जैसे कंप्यूटर, इंटरनेट आदि पर अवैधानिक तरीके से किये गए ऐसे कार्य जिसमें:

- प्रणालियों में व्यवधान उत्पन्न किया जाए,
- लोगों/ संस्थाओं को किसी भी रूप में हानि पहुंचाई जाए,
- संस्थाओं या ग्राहकों की राशि का कपटपूर्ण आहरण/ दुरुपयोग किया जाए साइबर अपराध कहलाते हैं।

साइबर अपराधों को निम्नानुसार दो तरह से वर्गीकृत किया जाता है:-

- ऐसे अपराध जिनमें कंप्यूटर/ डिवाईस को एक लक्ष्य के रूप में इस्तेमाल किया जाता है, उदाहरण हैकिंग, मालवेयर आदि।
- ऐसे अपराध जिनमें कंप्यूटर/ डिवाईस को एक हथियार की तरह इस्तेमाल किया जाता है, उदाहरण साइबर आतंकवाद, क्रेडिट कार्ड धोखाधड़ी आदि।

आइये संक्षेप में चर्चा करें इन विभिन्न प्रकार के साइबर अपराधों की:

- **मालवेयर/ मेलेशियस कोड-** दुर्भावनापूर्ण सॉफ्टवेयर, जिसमें उल्लेखनीय हैं:
  - **वाइरस** (वाईटल इन्फर्मेशन रिसोर्सेस अंडर सीज) प्रोग्राम जो सिस्टम फाईलों को नष्ट करता है।
  - **वर्म** मेलेशियस कोड जो अपनी प्रतिलिपि बनाते रहते हैं ताकि सिस्टम धीमा हो जाए।
  - **ट्रोजन हार्स** अपनी पहचान छुपाकर कंप्यूटर सिस्टम को ठप्प कर देता है। लॉजिक बॉम्ब इसी का एक रुप है।
  - **रैनसमवेयर** में कंप्यूटर फाईलों को एन्क्रिप्ट कर देते हैं जिसके डिक्रिप्शन हेतु फिरौती मांगी जाती है।
- **सोशल इंजीनियरिंग-** अपराधी, ग्राहकों को प्रलोभन देकर या भय दिखाकर धोखे से उनकी बैंकिंग संबंधी संवेदनशील जानकारी प्राप्त कर उनके खाते से कपटपूर्ण आहरण कर लेते हैं।
- **फ़िशिंग-** खातों के लॉग-इन क्रिडेन्शियल लेने हेतु ग्राहकों को नकली वेबसाइट के यूआरएल भेजे जाते हैं। इसके लिए की-लागर, स्क्रीन-लागर जैसे सॉफ्टवेयर का प्रयोग करते हैं।
- **विशिंग**- वाईस ओवर टेलीफोन सर्विस में इनका प्रयोग होता है। ग्राहकों को फोन करके गोपनीय बैंकिंग जानकारी प्राप्त कर उनके खातों से रकम पार कर ली जाती है।
- **स्मिशिंग-** संक्षिप्त संदेश सेवा (एसएमएस) पद्धति का उपयोग छलपूर्ण टेक्स्ट संदेश भेजने के दुर्भावनापूर्ण उद्देश्य हेतु किया जाता है।

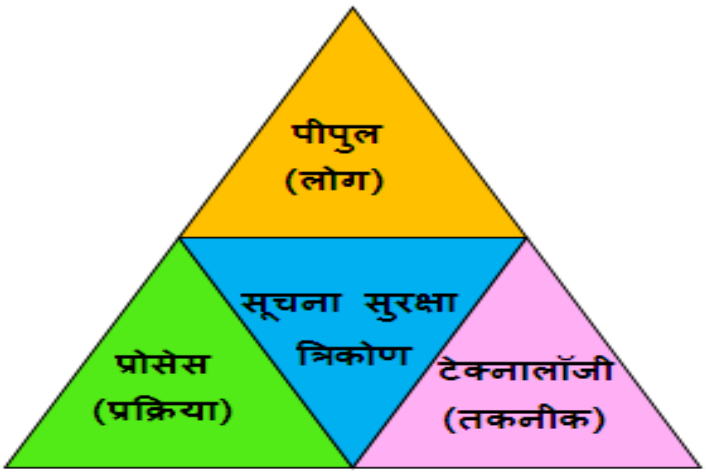
- **स्पूफिंग-** 'पहचान की चोरी' के उद्देश्य से किया गया हमला। ई-मेल स्पूफिंग में छद्मरूपी ई-मेल से अनुचित तरीके से लाभ प्राप्त किया जाता है। स्पैम (अनचाहे ई-मेल) संदेश की उत्पत्ति के बारे में प्राप्तकर्ता को गुमराह करते हैं।
- **हैकिंग-** सिस्टम में किसी की व्यक्तिगत/ गोपनीय जानकारी को प्राप्त करने के उद्देश्य से अनधिकृत पहुंच बनायी जाती है।
- **डिनायल ऑफ सर्विस (डीओएस/ DoS)-** विभिन्न स्रोतों से ट्रैफिक लाकर साइट को डाउन कर ऑनलाइन-सेवा को अनुपलब्ध बना दिया जाता है। डिस्ट्रिब्यूटेड डिनायल आफ सर्विस (डीडीओएस/ DDoS) इन्ही हमलों का अधिक परिमार्जित/ वृहद रूप होते हैं।
- **कार्ड क्लोनिंग-** एक कार्ड की जानकारी दूसरे कार्ड में डालकर मूल-कार्ड का प्रतिरूप/ क्लोन तैयार किया जाता है। इसमें स्किमिंग तकनीक का प्रयोग होता है, जिसके लिए अलग कार्ड-रीडर आता है। पिन की चोरी, पिन-होल कैमरे की सहायता से की जाती है।

साइबर सुरक्षा और बैंकिंग: आधुनिक बैंकिंग मूलरूप से सूचना-प्रौद्योगिकी पर अवलम्बित प्रणाली है। जिस तेजी से देश में डिजिटल माध्यमों का प्रसार हो रहा है, उतनी ही तेजी और व्यापकता से साइबर अपराध भी बढ़ रहे हैं। कई बैंकों में हो रही साइबर अपराध के अनेकों प्रकरण आइसबर्ग के टिप की मिसाल से बन गए हैं। विभिन्न साइबर अपराधों ने बैंकों पर अनेकों दुष्प्रभाव छोड़े हैं जैसे:

विशेषज्ञों ने बैंकिंग में साइबर अपराध के बढ़ते मामलों के पीछे निम्नलिखित कारण बताए हैं:

बाधाएं	बैंकिंग प्रणाली में प्रवेश हेतु कम बाधाएं
रुझान	उभरती अपराधिक प्रवृतियां उदा- लालच, प्रतिशोध आदि
मनोवृति	प्रणाली में व्यवधान पैदा करने की इच्छा
प्रौद्योगिकी सीमाएं	विश्लेषणात्मक मॉडलिंग हेतु असमर्थ सिस्टम एवं धीमी प्रक्रिया
विविध डेटा सोर्स	ग्राहकों/ व्यवसाय की सहजता से उपलब्ध जानकारी
कुशलता	परिष्कृत तकनीकें
अनुपालन	विनियामक आवश्यकताओं के अनुपालन में शिथिलता

साइबर सुरक्षा के विभिन्न आयाम: आज कोई भी बैंक तीव्र प्रौद्योगिकी एवं उन्नत साइबर तकनीकों के बिना जीवित नहीं रह सकता है। अब जहां साइबर सुविधाएं हैं तो वहां साइबर जोखिम भी होंगे हैं! *'सिक्योरिटी-थ्रू-डार्कनेस'* के सिद्धांत पर साइबर सुरक्षा को ना तो भाग्य के भरोसे ही छोड़ा जा सकता है और ना ही उसे शून्य किया जा सकता है, हां सतर्कता के विभिन्न उपाय अपनाकर उसे न्यून अवश्य किया जा सकता है। किसी भी संगठन में पीपीटी अर्थात् पीपुल (लोग), प्रोसेस (प्रक्रिया) एवं टेक्नोलॉजी (तकनीक) सूचना सुरक्षा के आधार माने जाते हैं:



- **लोग:** किसी जोखिम का सामना करने हेतु लोग अग्रिम-पंक्ति की सुरक्षा की व्यवस्था करते है। साइबर अपराधों से निपटने में सतर्क ग्राहक एवं जागरूक कर्मचारी सबसे महत्वपूर्ण कड़ी हैं।
- **प्रक्रिया:** उच्च-प्रबंधन द्वारा सूचना सुरक्षा नीति, जिसमे निम्नलिखित 6'S' शामिल हों बनाई जाए-

1'S'	**स्ट्रैटेजी**	दीर्घावधि उद्देश्य
2'S'	**सर्विलेंस**	बाह्य/ आंतरिक सतर्कता
3'S'	**शेयरिंग**	अनुभव साझेदारी
4'S'	**सेंसिटाईजेशन**	साइबर सुरक्षा जागरूकता
5'S'	**सिमुलेशन**	संवेदनशीलताओं का आकलन
6'S'	**सेफगार्डिंग**	सभी पणधारियों के हितों की सुरक्षा

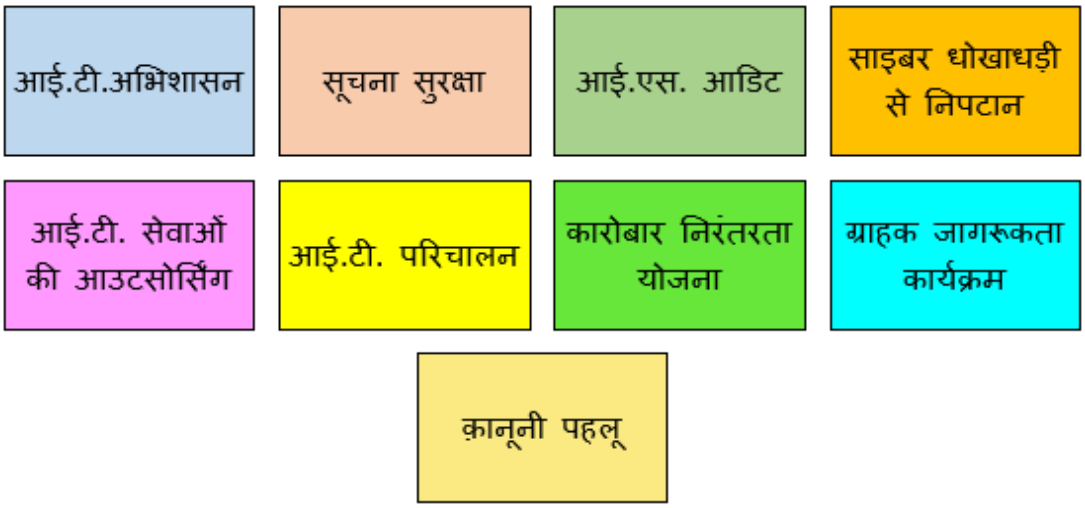
- **तकनीक** सुरक्षा के 3'D' आधार अर्थात् डिटर (सीसीटीवी, अलार्म्स), डिटेक्ट (इंट्रूशन डिटेक्शन सिस्टम) व डिनायल (प्रिवेंशन सिस्टम) को अपनाकर साइबर सुरक्षा सुनिश्चित की जा सकती है।

बैंकिंग क्षेत्र में साइबर सुरक्षा की आवश्यकता विनियामक, बैंक एवं ग्राहक तीनों ही स्तरों पर अनिवार्य होती है। इन तीनों ही स्तरों पर साइबर सुरक्षा के निम्नलिखित आयाम देखने को मिलते हैं:

1. **साइबर सुरक्षा परिप्रेक्ष्य में भारत सरकार द्वारा की गई नीतिगत पहलें:**
   - **आईटी अधिनियम, 2000 तथा आईटी (संशोधन) विधेयक, 2008** पारित कर साइबर अपराधों को दंडनीय अपराधों की श्रेणी में रखा गया है।
   - संस्थागत ढांचे के रूप में भारतीय कंप्यूटर आपात-कालीन प्रतिक्रिया दल **(सीईआरटी-इन)** को स्थापित किया गया है।
   - सरकार द्वारा साइबर सुरक्षा हेतु सार्वजनिक-निजी भागीदारी के तहत कदम उठाए जा रहे हैं। इस हेतु सरकार ने **साइबर सुरक्षित भारत (सीसीबी)** प्रारंभ किया है।

2. साइबर सुरक्षा में भारतीय रिज़र्व बैंक द्वारा उठाये गए कदम:

- भारतीय रिज़र्व बैंक द्वारा **श्रीमती मीना हेमचंद्रा की अध्यक्षता में** एक साइबर सुरक्षा विशेषज्ञ पैनल गठित किया गया था। पैनल की अनुशंसाओं के आधार पर भारतीय रिज़र्व बैंक ने **साइबर सुरक्षा फ्रेमवर्क** संबंधी एक व्यापक परिपत्र जारी किया है, जिसमें बैंकों को निम्नलिखित निर्देश दिए गए हैं:
  - बैंकों में साइबर सुरक्षा को केवल सूचना-प्रौद्योगिकी से जुड़ा मुद्दा ना मानते हुए सामरिक व्यापार नीति सा महत्व दिया जाए।
  - बैंक सर्वर/ नेटवर्क में किसी असामान्य व्यवहार की सूचना तुरंत भारतीय रिज़र्व बैंक को दी जाए।
  - साइबर खतरों से निपटने हेतु **सुरक्षा संचालन केन्द्र (एसओसी)** की स्थापना की जाए।
  - सुरक्षा खामियों का सतत् रूप से आकलन किया जाए।
  - **साइबर संकट/ आपदा-प्रबंधन योजना (सीसीएमपी)** लागू की जाए।
- अनाधिकृत डिजिटल बैंकिंग लेन-देन में ग्राहक की देयता को सीमित किया गया है। बैंक की लापरवाही के मामलों में ग्राहकों की शून्य-देयता अर्थात् ज़ीरो-लायबिलिटी का प्रावधान तक किया गया है।
- साइबर सुरक्षा परिप्रेक्ष्य में भारतीय रिज़र्व बैंक ने **श्री गोपालकृष्ण की अध्यक्षता में एक कार्यसमूह** बनाया है, जिसने निम्नलिखित नौ क्षेत्रों में सिफारिशें दी हैं:



बैंकों द्वारा साइबर सुरक्षा सुनिश्चित करने के उपाय:

- बैंक साइबर खतरों से अपने डेटा को सुरक्षित करने हेतु **साइबर रेसिलिएन्स फ्रेमवर्क** के तहत साइबर सुरक्षा मुस्तैदी संकेतक अपना रहे हैं, जिसमे निम्नलिखित बातों को सुनिश्चित किया जाता है:
  - डेटा बैकअप व्यवस्था,
  - सक्रिय सुरक्षा सूचना-तंत्र,
  - आऊटसोर्स सर्विसेस का सुपरविज़न,
  - डिजास्टर रिकवरी एवं बिज़नेस कंटीन्यूटी योजना,
  - साइबर सिक्युरिटी ऑडिट (सुरक्षा-लेखापरीक्षा) फ्रेमवर्क,
  - सूचना सुरक्षा से सम्बन्धित ISO-27001 व ISO-27002 सर्टिफिकेट,
  - भौतिक सुरक्षा बिंदु जैसे डायल-अप सुरक्षा, बाहरी तत्वों के आक्रमण एवं प्राकृतिक आपदाओं से मुख्य सर्वर की सुरक्षा आदि।

साइबर सुरक्षा जागरूकता एवं इसमें बैंकों की भूमिका:

- डिजिटल बैंकिंग में एंड-यूज़र अर्थात् ग्राहक सबसे महत्वपूर्ण एवं सबसे कमज़ोर कड़ी होते हैं। विभिन्न साइबर अपराधों में जो बात प्रमुखता से सामने आती है, वह है ग्राहकों का अति-विश्वास, भूल-चूक, प्रलोभन अर्थात् लालच, जो दर्शाता है कि साइबर सुरक्षा के बारे में लोगों में विवेक एवं सतर्कता का अनुपात लगभग शून्य ही है। हमारे देश में डिजिटल माध्यम से समव्यवहारों के बारे में जागरूकता काफी कम है जिसके कारण लोग धोखाधड़ी का शिकार बनते रहते हैं। साइबर सुरक्षित वातावरण बनाने हेतु सभी स्तरों की प्रतिबद्धता एवं जागरूकता अत्यंत आवश्यक होती है। अशिक्षित एवं ग्रामीण ग्राहकों की ओर विशेष ध्यान देने की आवश्यकता होती है क्योंकि प्रौद्योगिकी से भली-भांति परिचित नहीं होने के कारण इनके ठगे जाने का खतरा बढ़ जाता है।
- बैंकों द्वारा ग्राहकों को इस बारे में जागरूक बनाना होगा कि यूज़र-आईडी एवं पासवर्ड डिजिटल बैंकिंग की दुनिया के प्रवेश द्वार हैं इसलिए उनकी गोपनीयता सर्वाधिक महत्वपूर्ण होती है। किसी भी संस्था का कोई भी अधिकारी फ़ोन, ई-मेल या किसी अन्य तरीके से कभी भी उनका यूज़र-आईडी अथवा पासवर्ड नहीं मांग सकता है। ग्राहक यह भी सतर्कता बरतें कि प्रत्येक सिस्टम का यूज़र-आईडी एवं पासवर्ड अचूक रूप से भिन्न-भिन्न हो।

साइबर सुरक्षा में ग्राहकों की भूमिका:

साइबर स्पेस एक ऐसी जगह है जिसमें अनेक प्रॉक्सी सर्वर होते हैं जिन पर दुनिया की कोई भी सरकार हमेशा नज़र नहीं रख सकती। सतर्कता, जो जागरूकता, सावधानी तथा विवेक का सम्मिश्रण होती है, इन अपराधों से बचने का एक प्रभावी हथियार है। डिजिटल बैंकिंग के विभिन्न उत्पादों के प्रयोग के दौरान ग्राहकों द्वारा अपनाई जाने वाली सामान्य सतर्कता को निम्नलिखित टेबल के माध्यम से समझा जा सकता है-

साधन	क्या करें	क्या न करें
मोबाईल बैंकिंग	1. अपने हैंडसेट, टैब्स आदि की सुरक्षा पासवर्ड से करें। हैंडसेट खोने/ बदलने की दिशा में बैंक को अविलंब सूचित करें। 2. मोबाइल ऐप हमेशा विश्वसनीय साईटों से ही डाउनलोड करें एवं उसे अद्यतन रखें। 3. सिम-कार्ड अचानक बंद हो जाए तो तत्काल बैंक/ पुलिस/ टेलिकॉम सेवा-प्रदाता को इसकी सूचना दें।	1. अपना एम पिन न तो किसी को बताएं न ही इसे फोन में सहेजें। 2. किसी आईएसडी नंबर से मिस्ड-कॉल मिलने पर उस नंबर पर कॉल कभी न करें।
	1. नियमित अंतराल में अपना पासवर्ड बदलें। पासवर्ड जटिल एवं कम से कम आठ कैरेक्टर का हो जो लोअर एवं अपर केस-लेटर्स, नंबर्स और स्पेशल कैरेक्टर्स का मिश्रण हो। 2. अद्यतन एन्टी-वाइरस/ एन्टी-मालवेयर/ सिक्यूरिटी पैचेस का प्रयोग करें। 3. सिक्योर प्रोटोकॉल यूआरएल https:// का प्रयोग करें, जिसमे "s" सिक्योर्ड को दर्शाता है। 4. इंटरनेट बैंकिंग का प्रयोग वेरीसाइन व पैडलोक के चिन्ह देख कर ही करें। एसएसएल की वैधता एवं	1. सार्वजनिक स्थानों में शेयर्ड वाई-फाई का प्रयोग न करें। 2. ई-मेल पर कभी भी अपने क्रिडेंशियल्स जैसे आईडी अथवा पासवर्ड साझा न करें। 3. किसी अपरिचित लिंक अथवा ई-मेल अटेंचमेंट में क्लिक न करें। ऑनलाइन एड्रेस का यूआरएल स्वयं टाईप करें। 4. पासवर्ड याद रखने के विकल्प

इंटरनेट बैंकिंग	एन्क्रिप्शन स्टेंडर्डस भी जांच लें। 5. हमेशा विश्वसनीय साईट से ही लेनदेन करें। अकाउंट स्टेटमेंट/ एसएमएस अलर्ट की हमेशा जांच करें। 6. की-लॉगिंग से बचने वर्चुअल की-बोर्ड का प्रयोग करें। 7. नेट बैंकिंग का प्रयोग केवल प्राधिकृत एप्लीकेशन में ही करें और वह भी यथासंभव अपने निजी उपकरणों में ही। 8. कार्य खत्म हो जाने पर लॉग-आउट कर दें।	रिमेंबर मी को क्लिक न करें।
डेबिट/ क्रेडिट कार्ड	1. एटीएम मशीन को जांच लें कि कहीं उसमें कुछ असामान्य परिवर्तन तो नहीं है जैसे कार्ड-रीडर में कुछ उभरा हुआ (स्किमिंग मशीन) तो नहीं लगा है? 2. मैग्नीटिक स्ट्रिप कार्ड के बदले ईएमवी चिप कार्ड का प्रयोग करें। डेबिट/ क्रेडिट कार्ड्स के बजाए प्री-पेड/ वर्चुअल कार्ड्स का उपयोग करें। 3. पिन दर्ज करते समय उसे छुपा कर डालें। 4. ट्रांजेक्शन पूरा होने के बाद कार्ड लेना याद रखें। 5. यदि कार्ड गुम/ चोरी हो जाए तो तुरन्त कॉल सेंटर/ शाखा को रिपोर्ट कर उसे हॉटलिस्ट करवाएं।	1. पिन और कार्ड एक साथ न रखें। अपना पिन कार्ड के पीछे न लिखें। 2. किसी से अपना कार्ड नंबर, सीवीवी, पिन आदि शेयर न करें। 3. एटीएम में किसी दूसरे की सहायता न लें, न ही किसी अन्य व्यक्ति की उपिस्थति में एटीएम का प्रयोग करें।
पीओएस	1. कार्ड अपने सामने स्वाइप करवाएं। 2. कार्ड वापस लेते समय जांच लें कि वह आपका ही कार्ड है।	1. मर्चेंट लोकेशन में कार्ड को अपनी नज़रों से दूर न जाने दें।
पीसी/ लैपटॉप	1. फ़ायरवॉल का उपयोग करें। 2. फ़ाइलों के लिए एंक्रिप्शन का प्रयोग करें। 3. महत्वपूर्ण जानकारी के लिए नियमित बैक - अप बनाएं।	1. अनलाइसेंस्ड सॉफ्टवेयर का प्रयोग न करें। 2. फ्री गेम्स/ सॉन्ग्स की लिंक को डाउनलोड न करें।

निष्कर्ष: हमारे प्रधानमंत्री का कहना है कि *मैं ऐसे भारत का स्वप्न देखता हूं, जहां पर साइबर सुरक्षा हमारी राष्ट्रीय रक्षा का ही एक अभिन्न अंग हो जाती है"*। $5 ट्रिलियन की राह में अग्रसर होती भारतीय अर्थव्यवस्था में बेहतर साइबर सुरक्षा संस्कृति एवं डिजिटल साक्षरता के माध्यम से ग्राहकों को इस प्रकार जागरूक करने की आवश्यकता है कि वह प्रौद्योगिकी का लाभ तो उठाएं पर उसकी सुरक्षा के साथ समझौता कदापि न करें क्योंकि यदि हमारे ग्राहकों के डिजिटल अनुभव हितकारी नहीं होंगे तो वह तकनीकी नवोन्मेषों को कभी नही अपना पाएंगे। इस प्रयोजन से बैंकों द्वारा अपने ग्राहकों को ऐसे सरल एवं सुरक्षित डिजिटल समाधान उपलब्ध कराये जाने चाहिए जो भारत में निर्मित और भारत के लिए निर्मित का पर्याय हों बैंकों में परिचालनीय कार्यकुशलता एवं लाभप्रदता बढ़ाने, अंशधारकों के मूल्यों में संवर्धन करने, ग्राहकों के विश्वास को सुदृढ़ करने तथा भारत को एक डिजिटल राष्ट्र बनाने की दृष्टि से साइबर सुरक्षा के विभिन्न आयामों का निश्चित रूप से कोई स्थानापन्न नहीं है।

*****

पम्मी कुमारी

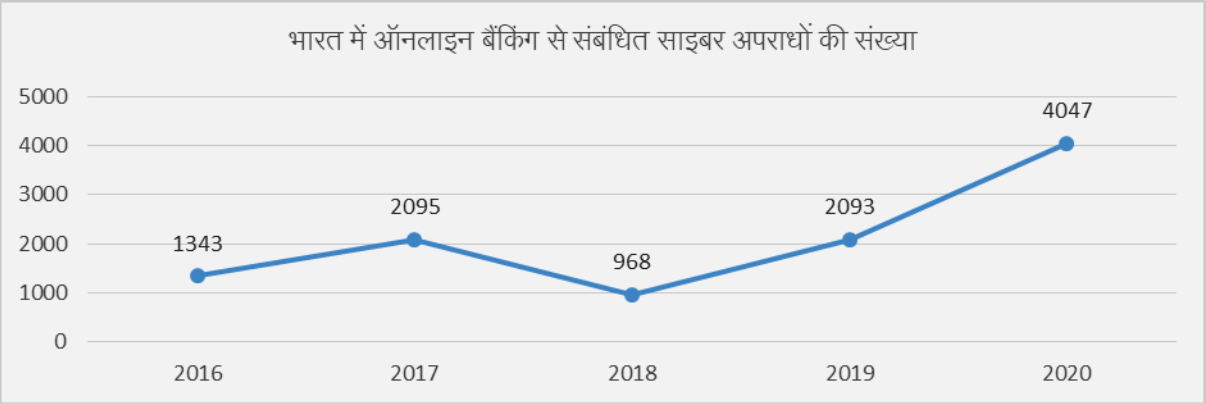
पदनाम:- लिपिक
संस्था का नाम:- बैंक ऑफ इंडिया
मोबाइल नं. :- 9142401685
ई-मेल:- kumaripummy81@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

बदली दुनिया तकनीक नई, मोबाइल में है बैंक खुला।
बदले हैं तेवर चोरों के, डिजिटल लूटों का दौर चला॥

आदिकाल से ही धन, स्वर्ण, जमीन, सौन्दर्य और सत्ता शक्ति को लेकर मनुष्य की आसक्ति ने कई छोटे-बड़े सामाजिक असंतुलनों को उत्पन्न किया है। धन किसी भी रूप में हो, सदैव ही सुरक्षा चाहता है - 'सुरक्षा हटी, दुर्घटना घटी'। इसमें कोई शक नहीं है कि 21 वीं सदी में विज्ञान और तकनीक ने बेहतरीन सुरक्षा व्यवस्थाओं को विकसित किया है, किन्तु मनुष्य, उसके विचार, लोभ और तृष्णा आदि तो आज भी वैसे ही हैं। एक तरफ डिजिटल तकनीकों के आशातीत विकास ने विश्व की अर्थव्यवस्थाओं, संस्कृतियों और लोगों को आपस में जोड़ा है, तो दूसरी तरफ इन्ही प्रौद्योगिकियों ने नए आपराधिक अवसर भी उत्पन्न किए हैं। साइबर अपराध, कंप्यूटर के माध्यम से किए जाने वाले ऐसे अपराध हैं जिनमें कंप्यूटर का उपयोग एक उपकरण के रूप में अवैध उद्देश्यों को पूरा करने के लिए किया जाता है। जैसे- हैकिंग, पैसों की धोखाधड़ी, चाइल्ड पोर्नोग्राफ़ी, बौद्धिक संपदा की तस्करी, पहचान की चोरी या गोपनीयता का उल्लंघन आदि। इंटरनेट आज घर-घर में कम्प्यूटरों और मोबाइलों तक अपनी पहुंच बना चुका है। ये डिवाइसेज़ वाणिज्य, मनोरंजन, सरकारी योजनाओं व सामाजिक जुड़ाव के केंद्र बन गए हैं। इस डिजिटल प्रगति से चीज़ें आसान तो हुई हैं, मगर साइबर अपराधों में वृद्धि भी हुई है। लोगों को यह समझना होगा कि उनके हाथ में रखा एक छोटा सा मोबाइल अगर उनके लिए सभी बैंकिंग सुविधाओं को घर तक ला सकता है, तो वही मोबाइल एक छोटी सी गलती से उनका बैंक अकाउंट साफ भी करवा सकता है। इंटरनेट और मोबाइल बैंकिंग के उपयोगकर्ताओं में वृद्धि के साथ, बैंकिंग संबंधी साइबर अपराध की घटनाएं भी पिछले कुछ वर्षों से लगातार बढ़ रही हैं। इन घटनाओं में क्रेडिट कार्ड धोखाधड़ी, स्पैमिंग, स्पूफिंग, ई-मनी लॉन्ड्रिंग, एटीएम धोखाधड़ी, फ़िशिंग आदि शामिल हैं। आइए, बैंकिंग में साइबर अपराधों के विभिन्न स्वरूप एवं उसके सभी संभावित सुरक्षात्मक उपायों को आगे विस्तार से समझते हैं:-

बैंकिंग में साइबर अपराधों का बढ़ता ग्राफ़: आज दुनिया में शायद ही कोई ऐसा गांव बचा हो, जिसे किसी न किसी तरह के बैंकिंग साइबर अपराध ने न छुआ हो। डिजिटल लेन-देन में वृद्धि के साथ, देश में बैंकिंग धोखाधड़ी की संख्या में भी वृद्धि हुई है। भारतीय रिज़र्व बैंक के आंकड़ों के अनुसार, भारत में वित्त वर्ष 2020-21 में प्रति दिन औसतन 229 बैंकिंग धोखाधड़ी की घटनाएं रिकॉर्ड की गई हैं, जिनमें 1 प्रतिशत से भी कम राशि की वसूली हो पाई है। भारत में वर्ष 2020 में कुल साइबर अपराध के मामलों में 11.8% की वृद्धि हुई है। इस तरह के अपराधों का बढ़ता ट्रेंड देश के लिए भयावह स्थिति की सूचना देता है। इसे नीचे दिए गए ग्राफ से समझा जा सकता है: -



हालिया वर्षों में बैंकिंग संबंधी साइबर अपराध तेजी से बढ़ने के कुछ कारण इस प्रकार हैं- ग्राहकों में जागरूकता का अभाव, पर्याप्त बजट और संस्थागत प्रबंधन का अभाव, रैंसमवेयर बढ़ना, मोबाइलों में असुरक्षित ऐप्स, सोशल मीडिया के माध्यम से फिशिंग तथा इस मद में अंतर्राष्ट्रीय क़ानूनों का अभाव आदि।

बैंकिंग संबंधी साइबर क्राइम के प्रकार

बैंकिंग संबंधी साइबर क्राइम का एक पूरा स्पेक्ट्रम है, जिसमें कई तरह की आपराधिक गतिविधियां शामिल हैं। एक तरफ ऐसे अपराध हैं, जिनमें व्यक्तिगत या कॉर्पोरेट स्तर पर सेंसिटिव डेटा लीक करने से लेकर पहचान की चोरी, फर्म या व्यक्ति को ब्लैकमेल करने के लिए अवैध रूप से प्राप्त डिजिटल जानकारी का उपयोग, स्पैमिंग, फिशिंग आदि मामले शामिल हैं, तो दूसरी तरफ हैकिंग, एटीएम संबंधी धोखाधड़ी, डिजिटल पाइरेसी, मनी लॉन्ड्रिंग और जालसाजी तक के मामले शामिल हैं। इन ऑनलाइन अपराधों को कुछ इस प्रकार वर्गीकृत किया जा सकता है:

I. **पहचान की चोरी:** इस डिजिटल युग में प्रत्येक चल-अचल या सजीव-निर्जीव इकाई की पहचान 0-1 की एक बाइनरी संख्या भर में सिमट कर रह गयी है। भारत में आधार नंबर हो या अमेरिका में सोशल सिक्योरिटी नंबर, सबका उद्देश्य नागरिकों के वास्तविक पहचान को स्थापित करना ही है। ये नंबर्स सामाजिक प्रबंधन, वित्तीय समावेशन, सुविधाएं बढ़ाने तथा जन-केंद्रित शासन को बढ़ावा देने के लिए अत्यधिक उपयोगी हैं, मगर इन पर बढ़ रही हमारी निर्भरता हमें पहचान की चोरी और गोपनीयता के हनन जैसे डिजिटल खतरों के तरफ भी बढ़ा रही है। किसी व्यक्ति की इस डिजिटल पहचान संख्या तक हैकरों की पहुंच उन्हें उस व्यक्ति की नागरिकता से संबंधित सभी दस्तावेजों को इकट्ठा करने का साधन बन रही है - यानी, इसके माध्यम से वह हैकर उस व्यक्ति की पहचान को मास्क करके उसके क्रेडिट कार्ड, बैंक खाता या अन्य सेंसिटिव वित्तीय जानकारियां जुटाकर उनका गलत उपयोग करता है।

II. **एटीएम धोखाधड़ी व एटीएम स्किमिंग:** ऐसे धोखाधड़ी के लिए अपराधी, शॉपिंग सेंटर तथा अन्य स्टोर आदि में फ्री-स्टैंडिंग एटीएम मशीनें स्थापित करते हैं, जो बिलकुल असली और वैध मशीनों की तरह ही दिखती हैं। परंतु पैसे देने के बजाय ये मशीनें उपयोगकर्ताओं के बारे में जानकारी एकत्र करती हैं और उन्हें केवल यह बताती हैं कि उनके द्वारा अपना पिन टाइप करने के बाद मशीन खराब हो गई है। ऐसी जानकारियों के माध्यम से नकली एटीएम कॉपी बनाकर लेन-देन किए जाते हैं।

III. **हैकिंग:** हैकिंग के माध्यम से किसी सिस्टम तक गैर-कानूनी रूप से पहुंच कर मनचाहे काम किए जाते हैं। यद्यपि इससे सुरक्षा हेतु कई स्तर पर फायरवॉल सिस्टम, एंटीवाइरस सॉफ्टवेयर, एंटीस्पाइवेयर तथा एंटीमैलवेयर आदि इंस्टाल किए जाते हैं, मगर आज भी यह एक बड़ी चुनौती के रूप में देखा जा रहा है।

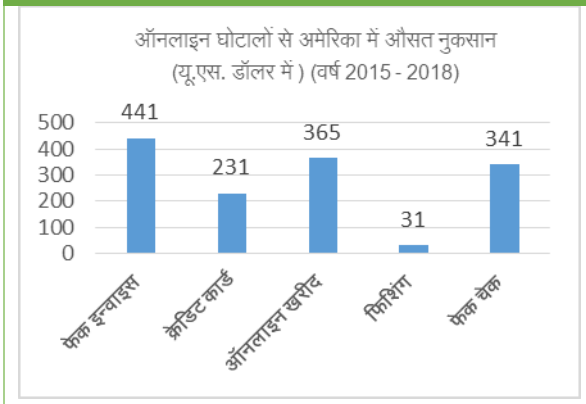
IV. **फिशिंग:** जिस प्रकार मछली पकड़ने के लिए कांटे में चारा लगाकर डाला जाता है और चारा खाने के लालच में आकर मछली कांटे में फंस जाती है, ठीक उसी प्रकार हैकर्स द्वारा इंटरनेट पर नकली वेबसाइट या ई-मेल के माध्यम से इंटररनेट यूजर्स को लुभावने ऑफर या अन्य लिंक्स देकर की गयी धोखेबाजी को फ़िशिंग कहते हैं। ऐसे नकली वेब साइटों या संक्रमित वेबसाइटों के लिंक्स पर क्लिक करते ही हमारे सेंसिटिव डेटा तक पहुँचकर कई तरह के अपराध किए जा सकते हैं।

V. **स्पैमिंग:** इंटरनेट पर हर काम को करने के लिए अलग-अलग नियम बने हैं और इन नियमों का उल्लंघन करके किया गया काम स्पैम कहलाता है। वैसे तो इंटरनेट पर अनेकों प्रकार से स्पैमिंग की जाती है, लेकिन वर्तमान में सबसे ज्यादा ई-मेल, फेसबुक, व्हाट्सऐप तथा यूट्यूब आदि बहुप्रचलित प्लेटफॉर्मों पर स्पैमिंग की जा रही है। स्पैमिंग में अवांछित ई-मेल भेजना भी शामिल है और इसे अक्सर जंक ई-मेल कहा जाता है। स्पैम का अधिकांश हिस्सा वाणिज्यिक विज्ञापन से संबंधित होता है जो संदिग्ध उत्पादों या सेवाओं को बढ़ावा देता है। इसकी ओट में कई तरह के वित्तीय धोखाधड़ियों को अंजाम दिया जाता है।

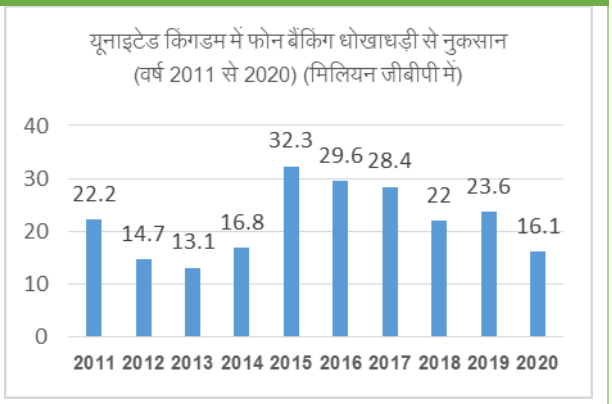
साइबर अपराधों का अंतर्राष्ट्रीय पक्ष

साइबर अपराध का एक महत्वपूर्ण पहलू इसका नॉन-लोकल कैरेक्टर है- अर्थात् विश्व के एक कोने में बैठ कर किसी भी दूसरे कोने में अपराध को अंजाम दिया जा सकता है। इससे सबसे बड़ी समस्या यह उत्पन्न होती है कि अपराध करने वाला व्यक्ति, स्थानीय क़ानूनों या सरकार के क्षेत्राधिकार से बाहर होता है। उदाहरण के लिए, यदि कोई व्यक्ति किसी ऐसे देश में कंप्यूटर पर चाइल्ड पोर्नोग्राफ़ी अपलोड करता है जहां इस पर प्रतिबंध नहीं है, तो क्या वह व्यक्ति उस देश के दृष्टिकोण से अपराध कर रहा है ? या हम इस बात की गंभीरता को यूं भी समझ सकते हैं-यदि कोई साइबर अपराधी किसी अफ्रीकन देश में बैठकर किसी ऐसे देश के बैंक पर साइबर क्राइम करता है, जिसके साथ उस अफ्रीकन देश की एक्सट्राडीशन ट्रीटी (प्रत्यर्पन संधि) नहीं है, तो सोचिए कि अपराधी तक पहुंचना कितना मुश्किल हो जाएगा? राष्ट्रीय सीमाओं के पार से होने वाले इस तरह के अपराधों को रोकने के लिए अंतर्राष्ट्रीय साइबर अपराध संधियों का क्रियान्वयन आवश्यक है.

विश्व भर में हो रहे वित्तीय साइबर अपराधों के कुछ आंकड़े:-



स्रोत: बीबीबी स्कैम ट्रैकर



स्रोत: https://www.statista.com/

साइबर अपराध ना केवल भारतीय बैंकिंग के लिए बल्कि पूरे वैश्विक बैंकिंग समुदाय के लिए एक बड़ी चुनौती बन चुके हैं। इसके रोकथाम हेतु पैसा पानी की तरह बहाया जा रहा है। निश्चय ही साइबर सुरक्षा कंपनियां एक स्वर्णिम भविष्य की तरफ अग्रसर हैं। वर्ष 2022 में दुनिया भर में साइबर सुरक्षा पर होने वाला कुल खर्च लगभग

133.7 अरब डॉलर तक पहुंचने का अनुमान है। इन आंकड़ों से हम साइबर अपराधों के आयाम एवं उसके विध्वंसकारी परिणामों का आंकलन कर सकते हैं।

साइबर अपराधों के प्रतिरोधार्थ सुरक्षात्मक उपाय

आंतरिक साइबर सुरक्षा नीतियों को लागू करना: ग्राहक डेटा को नियमित रूप से सुरक्षित और बैकअप किया जाना चाहिए, नियमित अंतराल पर पासवर्ड बदलना चाहिए। व्यवस्थापकों को कर्मचारियों द्वारा अनधिकृत सॉफ़्टवेयर डाउनलोड और इंस्टॉल करने से प्रतिबंधित करना चाहिए।

मशीनों का अपडेशन: बैंक के आईटी विभाग को यह सुनिश्चित करना चाहिए कि उपयोग किए जा रहे प्रत्येक वर्कस्टेशन और इंटरनेट-सक्षम डिवाइसों में अपडेटेड सक्षम फ़ायरवॉल हों। इसके साथ ही सभी पीसी पर एंटी-वायरस और एंटी-स्पाइवेयर सॉफ़्टवेयर आदि भी इन्सटॉल होने चाहिए। सभी वायरलेस नेटवर्क की सुरक्षा भी सुनिश्चित की जानी चाहिए।

एडवांस्ड औथेंटिकेसन तकनीकों का उपयोग: आजकल केवल जटिल यूजर-आईडी और पासवर्ड सेट करना पर्याप्त नहीं है, क्योंकि हैकर्स गोपनीय क्रेडेंशियल्स को क्रैक करने के लिए लगातार नए-नए तरीके खोज रहे हैं। बैंकों को ऐसी एडवांस्ड औथेंटिकेसन तकनीकों का उपयोग करना चाहिए, जो वेबसाइट नेविगेशन या लेन-देन में पाए गए पैटर्न के आधार पर साइबर अपराध का पता लगा सकें। इनमें स्मार्ट कार्ड, पिन, चेहरे की पहचान, फिंगरप्रिंट सेंसर आदि शामिल किए जा सकते हैं।

ग्राहक जागरूकता बढ़ाएं: साइबर खतरों से सभी स्तरों पर लड़ा जाना चाहिए और इसमें सबसे महत्वपूर्ण कड़ी है- ग्राहक। ग्राहकों में आवश्यक जागरूकता की कमी अनेक साइबर अपराधों का मुख्य कारण बनती हैं। खासकर ग्रामीण इलाकों के भोलेभाले या अल्पशिक्षित ग्राहकों को ऐसी वारदातों का शिकार बनाना आसान होता है। ग्राहकों को कभी भी अपना कार्ड नंबर, सीवीवी, पिन, कार्ड समाप्ति की तारीख, ओटीपी, इंटरनेट बैंकिंग यूजर आईडी, पासवर्ड या यूआरएन आदि किसी के साथ साझा नहीं करना चाहिए, भले ही कॉलर बैंक कर्मचारी होने का दावा करता हो। विशेषकर युवा मोबाइल उपयोगकर्ता ग्राहकों को अज्ञात स्रोतों से प्राप्त ई-मेल अटैचमेंट खोलने या डाउनलोड करने के खतरों से अवगत कराया जाना चाहिए।

भारत में साइबर अपराधों की रिपोर्ट कैसे करें ?

बैंकिंग ग्राहकों को किसी भी प्रकार के साइबर अपराध का शिकार होने की स्थिति में शीघ्रातिशीघ्र इसकी शिकायत नजदीकी थाने में दर्ज करानी चाहिए। यदि कोई पुलिस अधिकारी प्राथमिकी दर्ज नहीं करता है, तो सीधे मजिस्ट्रेट से भी शिकायत की जा सकती है। लिखित शिकायत दर्ज कराने हेतु कुछ आवश्यक दस्तावेज़ साथ रखने चाहिए, जैसे- बैंक स्टेटमेंट, कथित लेन-देन से संबंधित प्राप्त एस.एम.एस, अपने आईडी प्रूफ और एड्रेस प्रूफ की कॉपी आदि।

भारत में साइबर अपराध दो निम्नांकित अधिनियमों - आईटी अधिनियम और भारतीय दंड संहिता (आईपीसी) के तहत पंजीकृत किए जाते हैं : -

आईटी अधिनियम के तहत दर्ज मामलों की कुछ धाराएं	आईपीसी के तहत दर्ज मामलों की कुछ धाराएं
▪ **कंप्यूटर दस्तावेजों से छेड़छाड़ (धारा 65)** ▪ **कंप्यूटर संसाधन/ उपयोगिता की क्षति (धारा 66(1))**	▪ झूठे इलेक्ट्रॉनिक साक्ष्य (धारा 193 आईपीसी) ▪ इलेक्ट्रॉनिक साक्ष्य की क्षति (धारा 204, 477 आईपीसी)

- **हैकिंग (धारा 66 (2))**
- **इलेक्ट्रॉनिक रूप में अश्लील प्रकाशन/ प्रसारण (धारा 67)**
- **संरक्षित कंप्यूटर सिस्टम तक अनधिकृत पहुंच का प्रयास (धारा 70)**
- **झूठे डिजिटल हस्ताक्षर का उपयोग (धारा 73)**

- जालसाजी (धारा 463, 465, 477ए आईपीसी)
- आपराधिक विश्वास का उल्लंघन (धारा 405, 406, 408, 409 आईपीसी)
- जाली मुद्रा / टिकटें (धारा 489ए से 489ई आईपीसी)

वर्ष	**आईटी अधिनियम के तहत**		**भारतीय दंड संहिता (आईपीसी) के तहत**	
	दर्ज किए गए मामले	गिरफ्तार किए गए लोग	दर्ज किए गए मामले	गिरफ्तार किए गए लोग
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
कुल	9023	4804	2360	2198

निष्कर्ष

साइबर अपराधी लगातार वैश्विक अर्थतंत्र को लूटने के लिए नए-नए तकनीकों का सहारा ले रहे हैं। इंटरनेट उनके लिए सोने के अंडे देने वाली मुर्गी बन चुकी है। लेख में ऊपर वर्णित संदर्भों से स्पष्ट है कि साइबर अपराध बैंकिंग व्यवस्था के लिए कोढ़ बनता जा रहा है, जिसका निवारण केवल निर्धारित साइबर सुरक्षा नियमों के पालन, सुरक्षा तकनीकों में लगातार अपडेशन तथा इसके प्रति ग्राहकों में आवश्यक जागरूकता के प्रसार से ही संभव है। इसके साथ ही इसे एक वैश्विक समस्या समझा जाना चाहिए तथा इसके रोकथाम हेतु अंतर्राष्ट्रीय सहयोग एवं क़ानूनों का कार्यान्वयन किया जाना चाहिए। इस डिजिटल कुरुक्षेत्र में विजय हेतु ग्राहकों को भी यह बात गांठ बांध लेनी चाहिए कि – "सतर्कता में ही है भलाई, बचाएं अपने जीवन भर की कमाई"

*****

प्रणय कुन्दन

पदनाम:- अधिकारी
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 9419162866
ई-मेल:- prannoypicean18@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

साइबर अपराध से तात्पर्य एक ऐसी आपराधिक गतिविधि से है जिसमें कंप्यूटर या किसी अन्य उपकरण या इंटरनेट की मदद से धोखाधड़ी, चोरी, जालसाजी से किसी व्यक्ति को आर्थिक व मानसिक नुकसान पहुँचने जैसी आपराधिक गतिविधियां आती हैं। यह भारतीय दंड संहिता व सूचना एवं प्रौद्योगिकी अधिनियम के अंतर्गत अपराधों की श्रेणी में आती है।

"पासवर्ड अंतरवस्त्र की तरह होते हैं: लोगों को इसे देखने न दें, इसे बार-बार बदलें और आपको इसे अजनबियों के साथ साझा नहीं करना चाहिए।"

- क्रिस पिरिलो

नई तकनीकों के आगमन, स्मार्टफोन के बढ़ते उपयोग और हाई-स्पीड नेटवर्क के प्रसार के साथ साइबर अपराधों की घटनाओं में बढ़ोतरी हुई है। चूंकि साइबर से जुड़ी तकनीक अपेक्षाकृत कम समझ में आती है, इसलिए लोग साइबर अपराधियों के नापाक मंसूबों का आसान शिकार बन रहे हैं। युवा, स्कूल जाने वाले बच्चे अपनी जिज्ञासा व साइबर अपराधों के प्रति अपर्याप्त जागरूकता के कारण साइबर अपराधों के प्रति अधिक संवेदनशील होते हैं। वरिष्ठ नागरिक भी नई तकनीकों एवं कार्यप्रणाली की अनभिज्ञता, सीमित जीवन, एकल जीवन, दूसरों पर निर्भरता आदि के कारण साइबर धोखाधड़ी के अधिक शिकार होते हैं। अतः बैंकिंग प्रणाली में होने वाले विभिन्न साइबर अपराध, धोखाधड़ी, उनसे बचने के लिए विभिन्न सावधानियों एवं दंडनीय प्रवाधानों का विवरण निम्न है:-

1. सिम स्वैप

"सिम स्वैप" साइबर अपराध के अंतर्गत जालसाज मोबाइल सेवा प्रदाता के माध्यम से पीड़ित व्यक्ति के पंजीकृत मोबाइल नंबर के बदले एक नया सिम कार्ड जारी करने का प्रबंधन करते हैं। इस नए सिम कार्ड की मदद से, धोखेबाज व्यक्ति, पीड़ित व्यक्ति के बैंक खाते से वित्तीय लेन-देन करने के लिए आवश्यक वन टाइम पासवर्ड (ओटीपी) और अलर्ट प्राप्त करते हैं।

सिम स्वैप साइबर अपराध की कार्य प्रणाली

- जालसाज फ़िशिंग, विशिंग, स्मिशिंग या किसी अन्य माध्यम से ग्राहक की व्यक्तिगत जानकारी एकत्र करते हैं।
- फिर वे मोबाइल ऑपरेटर से संपर्क करते हैं और सिम को ब्लॉक करवा देते हैं। इसके बाद, वे ग्राहक के रूप में फर्जी आईडी प्रूफ के साथ मोबाइल ऑपरेटर के रिटेल आउटलेट पर जाते हैं।

- मोबाइल ऑपरेटर असली सिम कार्ड को निष्क्रिय कर देता है और जालसाज को एक नया सिम कार्ड जारी करता है।
- धोखेबाज व्यक्ति तब वन टाइम पासवर्ड (ओटीपी) उत्पन्न करता है जो लेन-देन की सुविधा के लिए आवश्यक है। यह ओटीपी जालसाज के पास रखे नए सिम पर आता है।

सिम स्वैप साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. अगर आपका मोबाइल नं। सामान्य अवधि से अधिक समय से बंद है, तो मोबाइल ऑपरेटर से संपर्क कर यह सुनिश्चित करें कि कहीं आप धोखाधड़ी के शिकार तो नहीं हुए हैं।
2. अपने बैंक खाते में गतिविधियों के बारे में सूचित रहने के लिए एसएमएस और ई-मेल अलर्ट के लिए पंजीकरण करें।
3. किसी भी तरह की अनियमितता के लिए अपने बैंक स्टेटमेंट और ट्रांजेक्शन विवरणी की नियमित जांच करें।

2. विशिंग

"विशिंग" साइबर अपराध एक ऐसा अपराध है जहां धोखाधड़ीकर्ता व्यक्ति ग्राहक की आईडी, नेट बैंकिंग पासवर्ड, एटीएम पिन, ओटीपी, एटीएम कार्ड की समाप्ति तिथि, सीवीवी, आदि जैसी व्यक्तिगत जानकारी फोन कॉल के माध्यम से प्राप्त करने का प्रयास करते हैं।

विशिंग साइबर अपराध की कार्य प्रणाली

- इसमें जालसाज व्यक्ति बैंक, आरबीआई या किसी सरकारी/ वित्तीय संस्थान का कर्मचारी बनकर विभिन्न कारणों का हवाला देते हुए ग्राहकों से उनकी व्यक्तिगत जानकारी मांगता है। उदाहरण के लिए मुख्यता जालसाजों द्वारा कहा जाता है कि उन्हे ग्राहकों के निष्क्रय खाते को फिर से सक्रिय करना है, रिवॉर्ड पॉइंट का रिडीम करना है, नया एटीएम कार्ड भेजना, खाते को आधार से जोड़ना आदि।
- इस प्रकार प्राप्त किए गए ग्राहकों के व्यक्तिगत विवरणों का उपयोग, ग्राहक के खाते से उनकी जानकारी के बिना लेन-देन करने के लिए किया जाता है।

विशिंग साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. फोन, एसएमएस या ई-मेल पर कभी भी कोई भी व्यक्तिगत जानकारी जैसे कि ग्राहक आईडी, एटीएम पिन, ओटीपी आदि साझा नहीं करनी चाहिए।
2. संदेह होने पर अपने बैंक शाखा के फोन नंबर पर कॉल कर संपर्क करें। हालांकि, गूगल से बैंक के फोन नंबर सर्च न करें। बैंक शाखा के संपर्क नंबर के लिए बैंक की आधिकारिक वेबसाइट पर जाएं।

3. स्मिशिंग

"स्मिशिंग" साइबर अपराध के अंतर्गत धोखाधड़ीकर्ता पीड़ित व्यक्तियों को धोखाधड़ी वाले फोन नंबर पर कॉल करने, धोखाधड़ी वाली वेबसाइटों पर जाने या फोन या वेब के माध्यम से दुर्भावनापूर्ण सामग्री डाउनलोड करने हेतु लुभाने के लिए मोबाइल फोन, टेक्स्ट संदेशों का उपयोग करता है।

स्मिशिंग साइबर अपराध की कार्य प्रणाली

- धोखाधड़ीकर्ता ग्राहकों को पुरस्कार राशि, लॉटरी, नौकरी का लालच आदि के बारे में एसएमएस भेजते है और उनसे अपना कार्ड या खाता विवरणी साझा करने का अनुरोध करते हैं।

- ग्राहक धोखाधड़ी वाली वेबसाइट पर जाने, फोन नंबर पर कॉल करने या खाते, पिन, क्रेडिट कार्ड नंबर, सीवीवी, पासवर्ड आदि के बारे में संवेदनशील जानकारी मांगने वाली दुर्भावनापूर्ण सामग्री डाउनलोड करने के निर्देशों का पालन करते हैं।
- इस प्रकार एसएमएस भेजने वाले धोखाधड़ीकर्ता के साथ साझा किए गए विवरण का उपयोग ग्राहक के खाते में धोखाधड़ी से लेन-देन करने के लिए किया जाता है, जिससे उन्हें वित्तीय नुकसान होता है।

स्मिशिंग साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. अपनी व्यक्तिगत या वित्तीय जानकारी एसएमएस, कॉल, ई-मेल या एसएमएस के माध्यम से प्राप्त लिंक पर कभी साझा न करें।
2. गैर-विश्वसनीय स्रोत से भेजे गए एसएमएस तुरंत हटा दें।

4. फ़िशिंग

"फ़िशिंग" एक प्रकार की साइबर धोखाधड़ी है जिसमें वैध स्रोत से प्रतीत होने वाले ई-मेल के माध्यम से व्यक्तिगत जानकारी जैसे कि ग्राहक आईडी, आई-पिन, क्रेडिट/ डेबिट कार्ड नंबर, कार्ड समाप्ति की तारीख, सीवीवी नंबर इत्यादि की चोरी करना शामिल है। आजकल, इस प्रकार की धोखाधड़ी में फ़िशर फ़ोन (वॉयस फ़िशिंग) और एसएमएस (स्मिशिंग) का भी उपयोग किया जा रहा है।

फ़िशिंग साइबर अपराध की कार्य प्रणाली

- धोखाधड़ीकर्ता स्वयं को बैंक अधिकारी बता कर ग्राहकों को फर्जी ई-मेल भेजते हैं, उनसे ई-मेल में एक लिंक पर क्लिक करके अपने खाते की जानकारी को तत्काल सत्यापित या अपडेट करने के लिए कहते हैं।
- लिंक पर क्लिक करने से ग्राहक एक जाली वेबसाइट पर पहुंच जाता है जो बैंक की आधिकारिक वेबसाइट की तरह दिखती है, जिसमें ग्राहक की व्यक्तिगत जानकारी भरने के लिए एक वेब फॉर्म होता है।
- इस प्रकार वेब फॉर्म से अर्जित की गई जानकारी का उपयोग ग्राहक के खाते में धोखाधड़ी करने के लिए किया जाता है।

नकली/ जाली फ़िशिंग वेबसाइट की पहचान कैसे करें:

1. वेबपेज का यूआरएल सत्यापित करें। 'https://' के अंत में 's' का अर्थ 'सुरक्षित' है – अर्थात् उक्त वेब-पृष्ठ एक एन्क्रिप्शन के साथ सुरक्षित है। अधिकांश नकली वेब-पृष्ठ 'http://' से शुरू होते हैं। ऐसी वेबसाइटों से ग्राहकों को सावधान रहना चाहिए।
2. वेबसाइटों के एड्रेस बार में वेबसाइट के नाम से पहले एक छोटा लॉक सिंबल जिसे पैडलॉक (🔒) कहते हैं पैडलॉक को चेक करने से वेबसाइट का सुरक्षित होना प्रमाणित होता है।
3. वेबसाइट की प्रामाणिकता स्थापित करने के लिए डिजिटल प्रमाणपत्र को सत्यापित करके जांचा जा सकता है। ऐसा करने के लिए फ़ाइल > प्रोपर्टीज़ > सेर्टिफिकेटस पर जाएं या अपनी ब्राउज़र विंडो के ऊपरी दाएं या निचले कोने में पैडलॉक बटन पर डबल क्लिक करें, जिससे वेबसाइट की प्रामाणिकता स्थापित की जा सकती है।

फ़िशिंग साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. हमेशा वेब एड्रेस को ध्यान से देखें।
2. लॉग इन करने के लिए हमेशा अपने वेब ब्राउजर एड्रेस बार में वेबसाइट एड्रेस टाइप करें।
3. वेबपेज के ऊपरी या निचले दाएं कोने में पैडलॉक आइकन के हमेशा 'चालू' होने की जांच करें।

4. अपने कंप्यूटर या मोबाइल फोन पर नवीनतम एंटी-वायरस/ एंटी-स्पाइवेयर/ फ़ायरवॉल/ सुरक्षा पैच स्थापित करें।
5. अपने कंप्यूटर पर नियमित कार्य के लिए हमेशा गैर-व्यवस्थापक उपयोगकर्ता आईडी का उपयोग करें।
6. अपने ई-मेल में किसी भी संदिग्ध लिंक पर क्लिक न करें।
7. ई-मेल के माध्यम से कोई भी गोपनीय जानकारी प्रदान न करें, भले ही अनुरोध आयकर विभाग, आरबीआई, वीज़ा या मास्टरकार्ड आदि जैसे अधिकारियों से ही हो।
8. अनपेक्षित ई-मेल अटैचमेंट या संदेश डाउनलोड लिंक न खोलें।
9. सार्वजनिक स्थानों जैसे साइबर कैफे या यहां तक कि असुरक्षित मोबाइल फोन से भी नेट बैंकिंग एक्सेस न करें व न ही अपने क्रेडिट/ डेबिट कार्ड का उपयोग करके भुगतान करें।

5. ट्रोजन

"ट्रोजन" एक हानिकारक सॉफ़्टवेयर है जिसे आमतौर पर उपयोगकर्ताओं को अपने कंप्यूटर पर लोड करने और निष्पादित करने के लिए धोखे से प्रेरित किया जाता है। इसके स्थापित और सक्रिय होने के बाद ट्रोजन कंप्यूटर पर आक्रमण करता है, जिससे फाइलों का विलोपन, डेटा की चोरी या वायरस सक्रियण हो जाता है। हैकर्स को आपके कंप्यूटर की एक्सेस देने के लिए ट्रोजन बैक डोर भी बना सकते हैं।

ट्रोजन साइबर अपराध की कार्य प्रणाली

- धोखाधड़ीकर्ता कई अनजान लोगों को ई-मेल भेजने के लिए स्पैमिंग तकनीकों का इस्तेमाल करते हैं।
- जो ग्राहक इन ई-मेल में अटैचमेंट खोलते या डाउनलोड करते हैं, उनके कंप्यूटर ट्रोजन जैसे हानिकारक सॉफ़्टवेयर से संक्रमित हो जाते हैं।
- जब ग्राहक खाता या कार्ड से संबंधित लेन-देन करते हैं, तो ट्रोजन व्यक्तिगत जानकारी चुरा लेता है और उन्हें जालसाज़ों को भेज देता है।
- इस माध्यम से प्राप्त इन व्यक्तिगत विवरणों का उपयोग ग्राहक के खाते से धोखाधड़ी करने के लिए किया जाता है।

ट्रोजन साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. अज्ञात प्रेषकों से प्राप्त ई-मेल या अटैचमेंट कभी भी न खोलें अथवा डाउनलोड करें व ऐसी प्राप्त ईमेलों को डिलीट कर दें।
2. ट्रोजन साइबर अपराध से बचने के लिए एंटीवायरस इंस्टॉल करने से भी काफी मदद मिलती है। एंटीवायरस आपके द्वारा डाउनलोड की जाने वाली प्रत्येक फ़ाइल को स्कैन करता है और आपके कंप्यूटर को संक्रमित फ़ाइलों से बचाता है।
3. अपने ऑपरेटिंग सिस्टम को हानिकारक साइबर आक्रमणों से बचाने हेतु "स्वचालित ओएस अपडेट" सक्षम करें या "ओएस पैच अपडेट" नियमित रूप से डाउनलोड करें।
4. जैसे ही नए सॉफ़्टवेयर वितरित होते हैं वैसे ही सॉफ़्टवेयर-निर्माताओं से पैच स्थापित करें या फ़ायरवॉल लगाकर ट्रोजन साइबर आक्रमणों से बचा जा सकता है।
5. अपने ब्राउज़र का नवीनतम संस्करण डाउनलोड करने व उसका उपयोग करने से भी ट्रोजन साइबर आक्रमण से बचा जा सकता है।
6. यदि आपका कंप्यूटर ट्रोजन से संक्रमित हो जाता है, तो अपने इंटरनेट कनेक्शन को वियोजित करें और किसी एंटीवायरस प्रोग्राम से संबंधित फ़ाइलों को हटा दें या अपने ऑपरेटिंग सिस्टम को फिर से इंस्टॉल करें। यदि आवश्यक हो, तो अपने कंप्यूटर की सर्विस करवाएं।

6. सलामी साइबर अपराध

"सलामी साइबर अपराध" का इस्तेमाल आर्थिक अपराधों के लिए किया जाता है। यदि कोई प्रोग्रामर, सिस्टम में छोटा सा परिवर्तन करता है जो कि इतना महत्वहीन है कि किसी के संज्ञान में भी न आ पाये।

सलामी साइबर अपराध की कार्य प्रणाली

उदाहरण के लिए, यदि कोई प्रोग्रामर बैंक के सर्वर में एक प्रोग्राम डाल दे जो प्रत्येक ग्राहक के खातों से एक महीने में 10 पैसे की एक छोटी से राशि काटता है, जिसे शायद कोई भी खाताधारक इस अनधिकृत डेबिट को नोटिस नहीं करेगा, लेकिन ऐसा प्रोग्रामर हर महीने एक बड़ी राशि कमाएगा। इसलिए सलामी हमले को "कलेक्ट-द-राउंड ऑफ" के नाम से भी जाना जाता है।

सलामी साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. नियमित रूप से साइबर ऑडिट आयोजित की जाए, जिसमें कम्प्युटर व अन्य उपकरणों को होने वाले जोखिमों को उजागर कर सुधारा जा सके।
2. फ़ायरवॉल लगाकर सलामी साइबर आक्रमणों से बचा जा सकता है।

7. मैन-इन-द-मिडल साइबर अपराध

"मैन-इन-द-मिडल" साइबर अपराध में हमलावर, संभवत: दो पक्षों के बीच हो रहे सीधे संवाद संचार में, गुप्त रूप से अतिक्रमण कर, अपने निजी इस्तेमाल के लिए प्रसारण को बदल देता है।

मैन-इन-द-मिडल साइबर अपराध की कार्य प्रणाली

मैन-इन-द-मिडल साइबर अपराध में, धोखेबाज व्यक्ति एक अस्थायी डिवाइस के माध्यम से बैंक के सर्वर से प्रेषित रिस्पांस कोड को धोखे से बदलकर लेन-देन को प्रभावित कर देता है और इस तरह धोखाधड़ी से एटीएम मशीन / कैश रिसाइक्लर मशीन से नकदी निकाल लेता है।

मैन-इन-द-मिडल साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. वेबसाइटों को एन्क्रिप्ट और प्रमाणित करके, डेटा और वेबसाइटों के अवरोधन को रोका जा सकता है।
2. एटीएम और कैश रिसाइकिलर्स के सभी ढीले तारों को कंसीलर का उपयोग करके ठीक से बंद करने से हैकर्स अपने अस्थायी उपकरणों को आरोपित करने से प्रतिबंधित किया जा सकता है।

8. कार्ड स्किमिंग साइबर अपराध

"कार्ड स्किमिंग" साइबर अपराध के अंतर्गत धोखेबाज व्यक्ति क्रेडिट या एटीएम कार्ड की चुंबकीय पट्टी से जानकारी की अवैध प्रतिलिपि बनाकर उससे प्राप्त व्यक्तिगत व वित्तीय जानकारी से एटीएम मशीन/ कैश रिसाइक्लर मशीन से नकदी निकाल लेता है।

कार्ड स्किमिंग साइबर अपराध की कार्य प्रणाली

कार्ड स्किमिंग साइबर अपराध में, धोखेबाज व्यक्ति बैंक की एटीएम मशीन पर एक अस्थायी उपकरण लगा देता है व जब ग्राहक अपने बैंक खाते से लेन-देन करने के लिए उक्त एटीएम मशीन पर अपना एटीएम कार्ड स्वाइप करता है तब वह अस्थायी उपकरण एटीएम कार्ड की चुंबकीय पट्टी से व्यक्तिगत एवं वित्तीय जानकारी की अवैध प्रतिलिपि प्राप्त कर लेता है।

कार्ड स्किमिंग साइबर अपराध से बचने के लिए विभिन्न सावधानियां

1. एटीएम मशीन का उपयोग करने से पहले यह जांच लें कि मशीन में कोई संदिग्ध उपकरण तो नहीं है।

2. जहां कमी न तो बैंक के पक्ष पर है और न ही ग्राहक के पक्ष पर है बल्कि "तृतीय पक्ष उल्लंघन" या सिस्टम में कहीं और कमी है और ग्राहक ऐसे अनधिकृत लेन-देन के बारे में बैंक को तीन कार्यदिवस में सूचित करता है, जो ऐसे में ग्राहक नुकसान की पूर्ण भरपाई के लिए हकदार होगा।

9. सुरक्षित नेट-बैंकिंग युक्तियां

- अपने बैंक ग्राहक-आईडी और पासवर्ड को गोपनीय रखें और किसी को भी इसकी जानकारी न दें।
- अपना नेट बैंकिंग पासवर्ड प्राप्त होते ही, नेट बैंकिंग खाते में लॉग-इन करके तुरंत उसे बदल दें। अपना पासवर्ड याद रखें, इसे कहीं भी न लिखें।
- सार्वजनिक कंप्यूटर नेटवर्क जैसे साइबर कैफे या सार्वजनिक वाई-फाई नेटवर्क जैसे होटल/ हवाई अड्डे आदि से इंटरनेट बैंकिंग का उपयोग करने से बचें।
- अपने नेट बैंकिंग वेबपेज तक पहुंचने के लिए अपने बैंक की आधिकारिक नेट बैंकिंग वेबसाइट के अलावा अन्य किसी ई-मेल या साइटों के लिंक पर क्लिक न करें। इसके लिए ब्राउजर के एड्रेस बार पर बैंक की वेबसाइट का पता टाइप करके हमेशा बैंक के होम पेज के माध्यम से बैंक की नेट बैंकिंग साइट पर जाएं।
- हमेशा बैंक के नेट बैंकिंग वेबपेज के यूआरएल और ब्राउज़र के निचले कोने पर पैड-लॉक (🔒) सिंबल की जांच करके उसकी प्रामाणिकता को सत्यापित करें।
- "प्रपत्रों पर उपयोगकर्ता का नाम और पासवर्ड" को हटाने हेतु "क्लियर पासवर्ड" कर अपनी व्यक्तिगत जानकारी सुरक्षित करें। अन्यथा अपने इंटरनेट बैंकिंग खाते में लॉग-इन करते समय वर्चुअल कीबोर्ड सुविधा का उपयोग करें।
- किसी भी अनधिकृत लॉगिन की निगरानी के लिए प्रत्येक लॉगिन पर नेट बैंकिंग पर उपलब्ध अपनी अंतिम लॉगिन जानकारी को क्रॉस चेक करें।
- हमेशा अपनी गोपनीय खाता जानकारी टाइप करें। इसे कभी भी कॉपी पेस्ट न करें।
- अपने लेन-देन खातों की नियमित निगरानी करें। बैंक की एसएमएस अलर्ट सेवा का उपयोग करें और किसी भी धोखाधड़ी वाले लेन-देन को बैंक के संज्ञान में लाएं।
- नेट बैंकिंग से बाहर निकलने पर ब्राउज़र को सीधे बंद न करें बल्कि हमेशा 'लॉगआउट' बटन का प्रयोग करें।

Disposal of Persons Arrested for Cyber Crime Cases (Crime Head-wise) - 2020 (Continued)

SL	Crime Head	Persons Arrested			Persons Charge sheeted		
		Male	Female	Total	Male	Female	Total
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
1	Cyber Stalking/Bullying of Women/Children	36	3	39	24	1	25
2	Data theft	8	0	8	0	0	0
3	Fraud	99	0	99	87	0	87
3.1	Credit Card/Debit Card	5	0	5	3	0	3
3.2	ATMs	26	0	26	16	0	16
3.3	Online Banking Fraud	44	0	44	44	0	44
3.4	OTP Frauds	6	0	6	6	0	6
3.5	Others	18	0	18	18	0	18
4	Cheating	82	6	88	61	4	65
5	Forgery	15	0	15	15	0	15
6	Defamation/Morphing	0	0	0	0	0	0

7	Fake Profile	5	3	8	5	3	8
8	Counterfeiting	0	0	0	0	0	0
9	Cyber Blackmailing/ Threatening	40	0	40	20	0	20
10	Fake News on Social Media	7	0	7	7	0	7
11	Other Offences	103	2	105	73	1	74
	Total Offences under IPC	395	14	409	292	9	301

10. दंडनीय प्रावधान

अगर उक्त सावधानियां एवं सुरक्षात्मक उपाय साइबर अपराधों की जांच एवं और नियंत्रण करने में अपर्याप्त पाये जाते हैं या फिर उक्त सभी उपायों के बावजूद भी विशिष्ट साइबर अपराध कारित किया जाता है तो उक्त साइबर अपराधों की रिपोर्ट साइबर सेल में दर्ज करें जिसके हेतु प्रावधान भारतीय दंड संहिता एवं सूचना और प्रौद्योगिकी अधिनियम दोनों में पाये जाते हैं:

भारतीय दंड संहिता - चोरी के मोबाइल/ कंप्यूटर या चोरी किए गए डेटा का उपयोग करके किए गए साइबर अपराधों के लिए तीन वर्ष तक की सजा और/ या जुर्माना के लिए प्रावधान देती है (धारा 379), फर्जी वेबसाइट बनाने, पासवर्ड चोरी, साइबर धोखाधड़ी और बेईमानी से संपत्ति की सुपुर्दगी जैसे साइबर अपराध इस धारा के अंतर्गत सात वर्ष की जेल और/ या जुर्माना के साथ दंडनीय हैं (धारा 420), झूठे दस्तावेज या झूठे इलेक्ट्रॉनिक रिकॉर्ड बनाना या ई-मेल स्पूफिंग जैसे अपराध इस धारा के अंतर्गत सात वर्ष तक के कारावास और/या जुर्माने के साथ दंडनीय हैं (धारा 463, 468)।

भारतीय दंड संहिता के अतिरिक्त **सूचना और प्रौद्योगिकी अधिनियम** के अंतर्गत भी विभिन्न प्रकार के साइबर अपराध दंडनीय हैं, जैसे कि कंप्यूटर स्रोत व दस्तावेजों के साथ छेड़छाड़ (धारा 65 सूचना और प्रौद्योगिकी अधिनियम), कंप्यूटर सिस्टम के साथ हैकिंग या कंप्यूटर सिस्टम और नेटवर्क का अनधिकृत उपयोग (धारा 66), धोखाधड़ी के उद्देश्यों के लिए पासवर्ड, डिजिटल हस्ताक्षर, बायोमेट्रिक अंगूठे या किसी अन्य व्यक्ति की पहचान की अन्य विशेषताओं का उपयोग करके पहचान की चोरी (धारा 66 सी), कंप्यूटर संसाधनों का उपयोग कर व्यक्ति द्वारा धोखाधड़ी (धारा 66 डी), किसी व्यक्ति की सहमति के बिना निजी क्षेत्रों की तस्वीरें लेना व उन्हें प्रकाशित या प्रसारित करना (धारा 66 ई), साइबर आतंकवाद फैलाने हेतु अपराध इसमें किसी वित्तीय संस्थान को धमकी भरा ई-मेल भेजाना शामिल हो जिससे आतंकी हमले को रोकने की चुनौती उत्पन्न हो (धारा 66 एफ़), इलेक्ट्रॉनिक रूप में अश्लील सूचना का प्रकाशन (धारा 67) आदि।

अंतत: उपर्युक्त सुरक्षात्मक सावधानियों एवं उपायों का प्रयोग कर बैंकिंग प्रणाली में होने वाले विभिन्न साइबर अपराधों, धोखाधड़ी से बचा जा सकता है जिससे आर्थिक एवं राष्ट्रीय सुरक्षा सुनिश्चित की जा सकती है।

"मैं एक डिजिटल इंडिया का सपना देखता हूं जहां साइबर सुरक्षा हमारी राष्ट्रीय सुरक्षा का एक अभिन्न अंग बन जाए।"

- नरेंद्र मोदी

*****

प्रदीप गुप्ता

पदनाम:- मुख्य प्रबंधक
संस्था का नाम:- यूको बैंक
मोबाइल नं. :- 8423633305
ई-मेल:- pradeep.gupta@ucobank.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

हमारे देश की बैंकिंग व्यवस्था, देश की आर्थिक मेरुदंड के समान है । **बैंकिंग उद्योग अति महत्वपूर्ण व्यवस्था होने के साथ-साथ एक विश्वास की व्यवस्था है ।** बैंक ग्राहकों की महत्वपूर्ण एवं अतिसंवेदनशील जानकारी रखते तथा उनका संचरण करते हैं । बैंक के डेटाबेस में ग्राहकों से संबंधित यह सभी जानकारियां एवं उनसे संबंधित समस्त ट्रांजैक्शन का संपूर्ण विवरण रखा जाता है । **संवेदनशीलता, गोपनीयता एवं महत्व बैंकिंग डेटाबेस की संरचना का मुख्य आधार है ।** किसी भी प्रकार की गोपनीयता में चूक ना केवल बैंक के ग्राहक को वित्तीय नुकसान पहुंचा सकती है बल्कि बैंक के लिए भी एक अति संवेदनशील एवं घातक वित्तीय हानि, एवं खराब छवि में परिवर्तित हो सकती हैं । जिसके फलस्वरूप ग्राहकों का बैंक के प्रति विश्वास कम होने के साथ-साथ, बैंक के लिए अति हानिकारक एवं घातक सिद्ध हो सकती है । यही वजह है कि **बैंकिंग में साइबर अपराधों के विभिन्न स्वरूप से सुरक्षा का महत्व अत्यधिक है ।जैसा कि कहा जाता है कि इलाज से बेहतर बचाव है ।**

बैंकिंग में भी यह कहना सर्वदा उचित है कि साइबर अपराधों के विभिन्न स्वरूपों से निपटने के लिये सुदृढ़ सुरक्षात्मक उपायों एवं सुनियंत्रित प्रणाली का होना अति आवश्यक है ।

बैंकिंग व्यवस्था में तकनीकी रूप से विकसित एवं सुदृढ़ होने के साथ ही कई चुनौतियां स्वाभाविक रूप से उत्पन्न होने लगती हैं । इन्हीं चुनौतियों में से एक जटिल एवं महत्वपूर्ण चुनौती है **'बैंकों में साइबर अपराध'**, एवं इन अपराधों के नियंत्रण हेतु अत्यावश्यक है सुरक्षात्मक उपाय, जिसके बिना ना केवल बैंकों या बैंक के ग्राहकों को वित्तीय नुकसान हो सकता है, बल्कि बैंक की छवि खराब होने (Market Risk) की स्थिति भी उत्पन्न हो सकती है । वैश्विक प्रतिस्पर्धा के इस समय में बैंकों को अनुकूलतम वृद्धि के साथ ही **साइबर अपराध रोकने के नवोन्मेषी सुरक्षात्मक उपायों** की अति आवश्यकता है ।

भारत की अधिक जनसंख्या, वैश्विक स्तर पर सभी संस्थाओं के विभिन्न उत्पादों का वृहद बाज़ार का केंद्र बनाती है । इसलिये **भारत में ऑनलाइन बैंकिंग एवं लेनदेन में उल्लेखनीय** वृद्धि होने पर बैंकिंग धोखाधड़ी की संख्या में भी काफी वृद्धि हुई है। ऑनलाइन बैंकिंग से सम्बंधित साइबर अपराध के स्वरूप सामान्यत: अधिक संख्या में घटित होते हैं, उदाहरण के तौर पर, फोन पर ओटीपी पूछकर किये गये अपराध, डेबिट कार्ड का दुरुपयोग/क्लोनिंग इत्यादि ।

रिजर्व बैंक ऑफ इंडिया (RBI) की पिछले वर्ष में प्रकाशित वार्षिक रिपोर्ट के अनुसार वित्त वर्ष 2019 में 71,500 करोड़ की तुलना में वित्त वर्ष 2020 में 1,00,000 और उससे अधिक की बैंक धोखाधड़ी दोगुने से

अधिक 1.85 करोड़ हो गई। इसी प्रकार वित्त वर्ष 2021 में बैंकिंग धोखाधड़ी के 83,638 मामले (लगभग1.38 लाख करोड़ राशि) दर्ज किये गये।

बैंकिंग व्यवस्था के साइबर अपराध के स्वरूपों में यह देखा गया है कि **केवल उपभोक्ता या ग्राहक ही ऑनलाइन धोखाधड़ी के शिकार नहीं है, बल्कि खुदरा विक्रेता और विभिन्न संगठन भी डेटा उल्लंघन और धोखाधड़ी वाले विभिन्न घटनाओं के शिकार बन रहे हैं।** सभी विक्रेता एवं संगठन किसी न किसी बैंक के ग्राहक होते हैं।

साइबर अपराध एवं धोखाधड़ी से संबंधित कॉल, मैसेज एवं ई-मेल की संख्या में भी काफी वृद्धि हुई है। इस तरह की धोखाधड़ी का निशाना बनने का शिकार होने से **ना केवल व्यवसायिक कार्य में व्यवधान आता है, बल्कि यह बैंक को ग्राहकों के विश्वास, ब्रांड प्रतिष्ठा एवं संवेदनशील डेटा की हानि का कारण भी बनता है।** इसलिए यह महत्वपूर्ण है कि बैंक इन घटनाओं की रोकथाम के लिए मजबूत साइबर सुरक्षा प्रणाली एवं उपायों को अपनाएं।

विभिन्न **ऑनलाइन बैंकिंग एवं ई-कॉमर्स चैनलों के प्रसार से बैंकिंग में सर्वोत्तम साइबर सुरक्षा प्रणाली का होना भी अति आवश्यक** हो गया है।

बैंकिंग में सुदृढ़ साइबर सुरक्षा प्रणाली होने के बावजूद साइबर अपराधों की एक बड़ी संख्या है। अत: उपरोक्त सभी **डिजिटल बैंकिंग के माध्यम को सार्थक स्वरूप देने हेतु सुदृढ़ करने एवं दंड का प्रावधान करने हेतु नियम एवं कानून भी अति आवश्यक, महत्वपूर्ण घटक एवं अनिवार्य सुरक्षात्मक उपाय है।**

भारतीय संविधान में साइबर सुरक्षा की दृष्टि से मजबूती प्रदान करने एवं दंड का प्रावधान करने हेतु **विभिन्न साइबर अपराधों हेतु नियम एवं कानून भारत सरकार द्वारा आईटी एक्ट 2000 के माध्यम से अधिनियमित किए गए हैं।** इस कानून के माध्यम से **डिजिटल ट्रांजैक्शन एवं डिजिटल मोड से किए गए धोखाधड़ी एवं अपराध हेतु नियमानुसार आर्थिक दंड एवं अन्य कठोर प्रावधान हैं**, जो ना केवल बैंकिंग व्यवस्था में निर्णायक भूमिका हेतु आवश्यक है बल्कि साइबर सुरक्षा की दृष्टि से बैंकिंग व्यवस्था को सहयोग प्रदान करने हेतु सबसे महत्वपूर्ण स्तंभ हैं।

बैंकिंग व्यवस्था में डिजिटल रूप का अत्यधिक उपयोग होने के कारण बैंकिंग में साइबर सुरक्षा के सफल निष्पादन हेतु **आईटी एक्ट 2000 सर्वाधिक महत्वपूर्ण माध्यम** है। आईटी एक्ट 2000 एक ऐसा अधिनियम है, जो इलेक्ट्रॉनिक डेटा इंटरचेंज और इलेक्ट्रॉनिक संचार के अन्य माध्यमों से किए गए लेनदेन के लिए कानूनी मान्यता प्रदान करता है। आईटी एक्ट 2000 इलेक्ट्रॉनिक सामान सरकारी एजेंसियों के साथ **दस्तावेजों की इलेक्ट्रॉनिक फाइलिंग**, **भारतीय साक्ष्य अधिनियम**, **भारतीय दंड संहिता, भारतीय साक्ष्य अधिनियम 1872, बैंकर बुक्स एविडेंस एक्ट 1891 और भारतीय रिजर्व बैंक अधिनियम 1934** में इलेक्ट्रॉनिक डेटा इंटरचेंज एवं इलेक्ट्रॉनिक संचार एवं दस्तावेज इत्यादि से संबंधित संशोधन कर इलेक्ट्रॉनिक दस्तावेजों एवं साक्ष्य को मान्यता प्रदान करने हेतु परिवर्तन एवं संशोधन है। इस एक्ट के माध्यम से संचार और सूचना के भंडारण के पेपर आधारित तरीकों के विकल्पों का उपयोग शामिल है।

बैंकों को वित्तीय नुकसान: जब किसी बैंक को डॉटा ब्रीच (breach) का सामना करना पड़ता है, यह ना केवल बैंक की प्रतिष्ठा को प्रभावित करता है, बल्कि बैंकों के वित्तीय नुकसान का भी कारण बन सकता है। यह

नुकसान बैंक या बैंक के किसी ग्राहक के खाते से धन की निकासी के रूप में प्रत्यक्ष वित्तीय हानि के रूप में या फिर बैंकों पर कमजोर सुरक्षा प्रणाली हेतु नियामक द्वारा वित्तीय दंड के प्रावधान के रूप में भी हो सकता है।

ग्राहकों को वित्तीय नुकसान: बैंक एवं ग्राहकों से संबंधित किसी भी जानकारी का चोरी या समझौता होना, ग्राहकों हेतु वित्तीय नुकसान के रूप में परिवर्तित हो सकता है। ग्राहकों द्वारा गलती या किसी व्यक्ति द्वारा धोखे से संवेदनशील जानकारी का आदान-प्रदान ग्राहकों हेतु एक बड़े वित्तीय नुकसान में परिवर्तित हो सकता है। बैंकों द्वारा साइबर सुरक्षा में एक छोटी सी चूक एक बड़े घातक नुकसान में परिवर्तित हो सकती है।

डेटा चोरी या उल्लंघन से बैंक की प्रतिष्ठा प्रभावित हो सकती है

डेटा चोरी या समझौता बैंकों के लिए एक महत्वपूर्ण एवं संवेदनशील विषय है। क्योंकि इससे ग्राहकों का डेटा और विश्वास दोनों की हानि होती है। ग्राहकों के डेटा के साथ कोई समझौता या चोरी बैंक के साइबर सुरक्षा पर एक प्रश्न चिन्ह के समान है। बैंक के ग्राहक डेटा से संबंधित जानकारी का चोरी या समझौता होना, किसी समाचार द्वारा प्रसारित होने पर बैंकों के लिए अति अपमानजनक एवं दीर्घकालीन प्रतिष्ठा में हानि का स्रोत बन सकता है।

बैंकों में साइबर अपराध रोकने के नवोन्मेषी सुरक्षात्मक उपाय एवं प्रबंधन को सुनिश्चित करने हेतु, निम्न चार आधार स्तम्भों का सशक्तिकरण एवं सुव्यवस्थित करना अति महत्वपूर्ण है:-

1. **बैंक की आंतरिक प्रणाली प्रबंधन**
2. **परिधीय (वाह्य) प्रणाली प्रबंधन**
3. **आंकड़ों की अनुकूलतम उपलब्धता एवं ज्ञान की उपयोगिता**
4. **नवोन्मेषी तकनीकी विकास, कार्यान्वयन, प्रशिक्षण एवं प्रबंधन**

प्रथम आधार स्तम्भ: - बैंक की आंतरिक प्रणाली प्रबंधन

एक आवश्यक कदम यह है कि साइबर अपराध से संबंधित मामलों को **नवीनतम तकनीकि से सूचीबद्ध कर बैंक के अन्य सभी कर्मचारियों को इस से अवगत एवं उपलब्ध** कराया जाए, इससे भविष्य में इसी तरह की अन्य घटनाओं की रोकथाम की जा सकती है तथा ऐसा करने पर नकारात्मक परिणाम या कार्यवाही का भय भी बना रहता है। यह भी ध्यान देने योग्य है कि कर्मचारियों के मध्य यह भाव स्थापित करना अति आवश्यक है कि **नकारात्मक परिणाम या कार्यवाही कार्यों के बेहतर प्रबंधन के लिए उठाया गया आवश्यक कदम है ना कि डर संचारित करने जैसा कोई ठोस कदम।**

द्वितिय आधार स्तम्भ: - परिधीय (वाह्य) प्रणाली प्रबंधन

बैंकों के विभिन्न कार्यकलापों में कई अन्य वाह्य संस्थाओं (सरकारी या निजी, बैंकिंग या गैर बैंकिंग) का भी महत्वपूर्ण हस्तक्षेप होता है।

उदाहरण के लिए प्रॉपर्टी या गृह ऋण हेतु स्थानीय प्राधिकरण से संबंध, कृषि ऋण (केसीसी इत्यादि) के लिए तहसील इत्यादि से संबंध, बैंक के कार्यालयों की बिजली, टेलीफोन इत्यादि विभागों से संबंध। यहां यह सुनिश्चित करना अति आवश्यक है कि इन सभी विभागों से प्राप्त सूचना या सेवाओं का बैंकों के नियमानुसार उपयोग एवं डॉक्यूमेंटेशन हो रहा है कि नहीं। पुनः ऐसे मामलों में **ऑनलाइन सत्यापन या लेखा परीक्षण द्वारा प्रामाणिकता सत्यापन** अति अनिवार्य है।

तृतीय आधार स्तम्भ: आंकड़ों की अनुकूलतम उपलब्धता एवं ज्ञान की उपयोगिता

साइबर अपराध रोकने के सुरक्षात्मक उपायों का तीसरा एवं एक महत्वपूर्ण आधार स्तम्भ '**आकडों अनुकूलतम उपलब्धता तथा ज्ञान की उपयोगिता**' है। इसका एक आवश्यक पहलू **सूचना की गोपनीयता** भी है।

बैंक, ग्राहक से संबंधित सूचना के आधार पर ना केवल उन्हें अच्छी सुविधा प्रदान करता है बल्कि अपने अन्य उत्पादों की बिक्री एवं मार्केटिंग के लिए भी उपयोग करता है।

साइबर अपराध रोकने के लिए यह अति आवश्यक है कि **आंकडें व सूचनाओं की गुणवत्ता को शीर्ष प्राथमिकता देकर उन्हें प्रारंभिक स्तर से ही अनुशासित, सुव्यवस्थित व गोपनीय** रखा जाए। उन से छेड़छाड़ करना या उन्हें अनधिकृत रूप से बदलना संभव ना हो। **आंकड़ों को अधिकृत रुप से ही बदला जा सके**।

चतुर्थ आधार स्तम्भ: नवोन्मेषी तकनीकी कार्यान्वयन, प्रशिक्षण एवं प्रबंधन

बैंक में वर्तमान में उपयोग की जाने वाली तकनीकी जैसे कि **ई-केवाईसी, सीबिल (CIBIL), CKYCR, बायोमेट्रिक, ऑनलाइन पैन/ आधार कार्ड सत्यापन** इत्यादि साइबर अपराध के महत्वपूर्ण उपाय हैं। खातों को आधार से लिंक कर तथा खातों के संचालन को पारदर्शी करना भी **नवोन्मेषी साइबर अपराध प्रबंधन** की एक पहल है, जिस से भविष्य में बैंकों में होने वाली साइबर अपराध की घटनाओं में कमी आएगी।

इसी प्रकार **CIBIL, CERSAEI, भू-लेख के उपयोग** से किसी ग्राहक की क्रेडिट रेटिंग, पहले लिए गए ऋण, बंधक प्रॉपर्टी , या जमीन के बारे में जानकारी प्राप्त हो जाती है, जिससे ऋण की संस्तुति या अनुमोदन करने में कोई कठिनाई नहीं होती है। इस प्रकार **सुरक्षात्मक उपाय व तकनीकी के उपयोग से बैंकों में साइबर अपराध रोकने के उद्देश्य** को महत्वपूर्ण आधार स्तम्भ मिल रहा है।

आईटी एक्ट 2000 के माध्यम से बैंकिंग में साइबर सुरक्षा का व्यवस्थित एवं स्वरूप लाने हेतु निम्नलिखित प्रावधान मुख्य रूप से आईटी एक्ट 2000 में परिभाषित किया गए हैं:

इलेक्ट्रॉनिक रिकॉर्ड की मान्यता: कानून के अनुसार किसी जानकारी या मामले का लिखित रूप में मुद्रित होना अति आवश्यक है। आईटी एक्ट 2000 इलेक्ट्रॉनिक रूप में प्रदान उपलब्ध कराए गए दस्तावेजों को एवं इलेक्ट्रॉनिक रिकॉर्ड को कानूनी मान्यता प्रदान करता है तथा यह सुनिश्चित करता है कि वह रिकॉर्ड जानकारी बाद के संदर्भ के लिए भी प्रयोग योग्य एवं मान्य हो।

इलेक्ट्रॉनिक हस्ताक्षरों के कानूनी मान्यता। कानून के अनुसार किसी जानकारी या मामले को प्रमाणित करने हेतु हस्ताक्षर की आवश्यकता होती है, इसी प्रकार आईटी एक्ट 2000 के माध्यम से इलेक्ट्रॉनिक हस्ताक्षर द्वारा किसी जानकारियां मामले को प्रमाणित किए जाने को पूर्णत: मान्य रूप में निर्धारित किया जाता है।

इस नियमावली के अनुसार साइबर सुरक्षा के तहत इलेक्ट्रॉनिक रिकॉर्ड को एक निश्चित या विशिष्ट अवैध के लिए रखा जाना उसी प्रकार से आवश्यक माना जाएगा जैसे अन्य सामान दस्तावेज रखे जाते हैं। बैंकिंग डेटाबेस एक जटिल एवं वृहद संरचना है, आईटी एक्ट 2000 के माध्यम से साइबर सुरक्षा प्रदान कर बैंकों की इस समस्या का भी समाधान किया गया। **बैंकिंग में साइबर सुरक्षा हेतु आईटी एक्ट 2000 के प्रावधानों के अनुसार ही**

नियंत्रक एवं विभिन्न अधिकारियों की नियुक्ति बैंकिंग व्यवस्था में साइबर सुरक्षा को और भी सुदृढ़ एवं सुनियोजित करती है।

साइबर कानून एवं सूचना प्रौद्योगिकी एक्ट के माध्यम से बैंकिंग में साइबर अपराध में दंड का प्रावधान इन घटनाओं को रोकने में प्रभावशाली है। किंतु इसके साथ-साथ प्रत्येक ग्राहक एवं व्यक्ति को बैंकिंग व्यवस्था में साइबर सुरक्षा के प्रति जागरूक होना एवं विभिन्न कार्यों के निष्पादन हेतु सुरक्षित प्रणाली का उपयोग एवं सतर्क रहना सिखाना, बैंकिंग में साइबर अपराधों से सुरक्षात्मक उपायों का एक महत्वपूर्ण अंग है।

भविष्य में बैंकिग में साइबर अपराधों का और जटिलतम स्वरूप देखने को मिल सकता है, जिसका प्रमुख कारण न्वोन्मेषी उत्पाद, जैसे कि नये-नये मोबाइल एप, डिजिटल मुद्रा का प्रचलन इत्यादि। इन अपराधों को पूर्णत: नियंत्रित करने हेतु यह अति आवश्यक है कि सुरक्षात्मक उपायों से समृद्ध प्रणाली का समुचित क्रियांवयन सुनिश्चित किया जाये।

*****

फणीष मणि त्रिपाठी

पदनाम:- प्रबंधक
संस्था का नाम:- इण्डियन ओवरसीज़ बैंक
मोबाइल नं. :- 9176888427
ई-मेल:- fanishmani@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

राम होने में या रावण में है अंतर इतना,
एक दुनिया को खुशी, दूसरा गम देता है!
हमने रावण को बरस दर बरस जलाया है,
कौन है वो जो इसे फिर से जनम देता है!

कहते हैं राम और रावण दोनों हमारे भीतर हैं। वे जो अपनी इंद्रियों पर काबू कर ले राम हैं, जिन्हें कुबुद्धि घेर ले वे रावण। त्रेता युग में राम ने रावण पर विजय हासिल की। पर युद्ध वहीं समाप्त नहीं हुआ। ये संघर्ष द्वापर में भी चला और कलियुग में भी जारी है। फर्क इतना है कि तब सिर्फ परमात्मा की बनाई दुनिया में ही राम संघर्षरत थे जबकि राम और रावण का ये द्वंद्व आज वास्तविक दुनिया के साथ मनुष्य की बनाई आभासी दुनिया में भी चल रहा है। हम बात कर रहे हैं साइबर संसार की जिसमें प्रतिपल राम की राह में चुनौती बन कर रावण खड़ा है। मायावी रावण बस इस ताक में बैठा है कि राम ज़रा सी गलती करें, थोड़ी भी लक्ष्मण रेखा लांघें, मृग-मारीच के मोह में आएं तो वो अपने मनसूबे पूरे कर लें।

इंटरनेट यूज़र्स बढ़ने से खिले साइबर क्रिमिनल्स के चेहरे

साइबर अपराधियों का दिन-ब-दिन बढ़ता वर्चस्व बैंकिंग जगत के लिए चुनौती बन गया है। इंटरनेट की दुनिया जैसे-जैसे बड़ी हो रही है साइबर खतरे भी बढ़ रहे हैं। साइबर क्राइम यानी एक ऐसा अपराध जिसको अंजाम देने में कंप्यूटर और इंटरनेट की मदद ली जाती है। आज इंटरनेट का संसार तेजी से पैर पसार रहा है। एक अनुमान के अनुसार कोविड महामारी की दस्तक के बाद भारत में करीब 80 करोड़ लोग इंटरनेट का इस्तेमाल कर रहे हैं। देश के 61 प्रतिशत घरों में इंटरनेट पहुंच चुका है। आभासी दुनिया में लोग इस कदर रम गए हैं कि कपड़ों की शॉपिंग, रेस्त्रां के ऑर्डर, दवाईयां मंगाना और बैंकिंग लेन-देन समेत सभी ज़रूरतें कमोबेश इंटरनेट से पूरी हो रही हैं। साइबर अपराधियों की नज़र ऐसे ही लोगों पर टिकी रहती है जो एटीएम, इंटरनेट और मोबाइल से बैंकिंग लेन-देन करते हैं।

अपराधियों के निशाने पर क्यों हैं बैंक

बैंक इसलिए साइबर अपराधियों के निशाने पर होते हैं क्योंकि उनके पास उपभोक्ताओं और नकदी का एक बड़ा भंडार होता है। देश के बैंकों में 150 ट्रिलियन जमा हैं। डिजिटल लेन-देन और लॉकडाउन जैसी स्थितियों के पनपने से ई-कॉमर्स का बाज़ार भी बढ़कर 70-80 बिलियन डॉलर का हो गया है। खरबों रुपए के इन्हीं खजानों पर गिद्धों की नज़रें टिकी हैं। साइबर हमले से सुरक्षित रहना और उन्हें रोकना बैंकों की सबसे बड़ी प्राथमिकता में है। इससे बैंकों को वित्तीय हानि होती है, रेगुलेटर की कार्रवाई झेलनी पड़ती है और सबसे बड़ा नुकसान कि

साख पर बट्टा लगता है। बैंकिंग की दुनिया आज दो प्रकार के साइबर हमले का शिकार हो रही है। एक साइबर हमला है जो संस्थागत स्तर पर होता है। इसमें पूरी बैंकिंग व्यवस्था, डेटाबेस को निशाना बनाया जाता है। बैंकिंग नेटवर्क को या तो पंगु कर दिया जाता है या बैंक ग्राहकों की सूचनाएं चुरा ली जाती हैं। दूसरे प्रकार के साइबर अपराध में सीधे बैंक ग्राहकों को शिकार बनाया जाता है। जिसमें मोबाइल संदेशों, ई-मेल, फर्जी वेबसाइट, लिंक आदि का सहारा लेकर बैंक ग्राहक के खाते में सेंध लगाई जाती है। साइबर फ्रॉड में एटीएम और ऑनलाइन बैंकिंग धोखाधड़ी के मामले देश में सबसे अधिक हैं। अभेद्य सुरक्षा कवच के जरिए बैंक अपने ग्राहकों को साइबर अपराधियों से बचाने की कोशिश कर रहे हैं लेकिन अपराधी भी नए-नए तरीकों से बैंक ग्राहकों को ठगी का शिकार बना ले रहे हैं। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो से प्राप्त आंकड़ों के अनुसार वर्ष 2020 में, साइबर फ्रॉड के कुल 50,035 मामलों में सबसे ज्यादा ऑनलाइन बैंकिंग धोखाधड़ी से सम्बन्धित थे। जबकि ओटीपी आधारित, क्रेडिट/ डेबिट कार्ड फ्रॉड, एटीएम फ्रॉड की घटनाएं एक से दो हजार के बीच रहीं।

बेलगाम बढ़ते साइबर अपराध	
वर्ष	**देश में साइबर अपराधों की संख्या**
2017	21796
2018	27248
2019	44735
2020	50,035

(स्रोत: राष्ट्रीय अपराध रिकॉर्ड ब्यूरो)

2020 में साइबर फ्रॉड की घटनाएं	
फ्रॉड का प्रकार	**घटनाओं की संख्या**
ऑनलाइन बैंकिंग	4047
ओटीपी	1093
क्रेडिट/ डेबिट	1194
एटीएम सम्बन्धित	2160

(स्रोत: राष्ट्रीय अपराध रिकॉर्ड ब्यूरो)

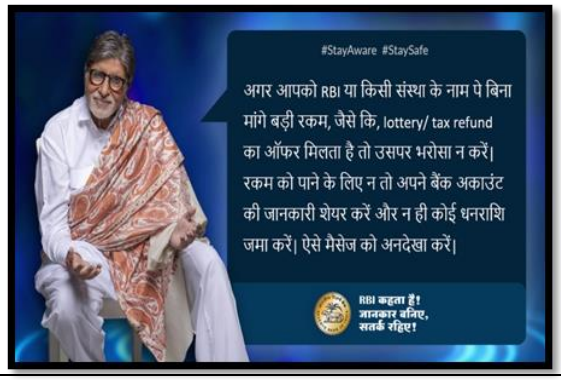
साइबर फ्रॉड के खिलाफ जागरूकता अभियान

साइबर ठगों और बैंकों के बीच ठना यह युद्ध निराला है। यहां न गोलियां चलती हैं, न खून बहता है। पर घाव गहरे होते हैं। इतने कि व्यक्ति छनछना जाए। पर हाथ मलने के अलावा कुछ हासिल नहीं होता।

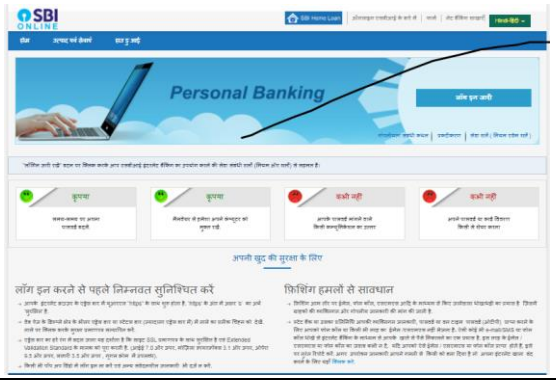
माया महा ठगनी हम जानी
तिरगुन फाँसि लिए कर डोलै बोलै मधुरी बानी

कबीर की ये पंक्तियां साइबर अपराधियों का मूल मंत्र है। उनकी मॉडस आपरेंडी इसी पर आधारित है। मीठा बोलो और सामने वाले शिकार को फाँस लो। फोन या ई-मेल के जरिए बैंक खाते का विवरण, डेबिट/ क्रेडिट कार्ड का विवरण लो और कर लो अपने वार-न्यारे। ये मायाजाल इतना सेकुलर और ओपेन माइंडेड होता है कि हिन्दू-मुस्लिम, पढ़े-अनपढ़ में फर्क नहीं करता। बस एकमेव लक्ष्य है, लोगों को अपना शिकार बनाना। इतना तगड़ा मायाजाल बुना जाता है कि लोग झांसे में आकर अपना एटीएम पिन, मोबाइल पर आए ओटीपी, कार्ड के सीवीवी तक साझा कर बैठते हैं। एक पल को भी ये ध्यान में नहीं आता कि हम अपने क्रेडेंशियल्स शेयर करके साइबर अपराधियों को खुद लूट का निमंत्रण दे रहे हैं। भारतीय रिज़र्व बैंक तमाम मीडिया मंचों से अपने विज्ञापनों के जरिए बार-बार हमें सचेत करता है कि 'जानकार बनिए, सतर्क रहिए'। सदी के महानायक तक हमसे अपील कर रहे हैं। फिर भी हम हैं कि धोखे खाते जा रहे हैं।

साइबर अपराध के खिलाफ RBI की जागरूकता मुहिम



SBI के इंटरनेट बैंकिंग लॉग-इन पेज पर चेतावनियां



यहां तक कि बैंक भी अपने ई-मेल संदेशों में अपनी वेबसाइट पर, मोबाइल संदेशों के जरिए आपको हमेशा सतर्क करते रहते हैं कि आप फिशिंग हमलों से सावधान रहें। बैंक की ओर से बार-बार ये चेतावनियां भेजी जाती हैं कि बैंक के नाम से आने वाले फर्जी ई-मेल से सावधान रहें, बैंक की वेबसाइट सुरक्षित है या नहीं ये जांच लें, बैंक कभी आपसे आपके बैंक खाते का विवरण नहीं माँगता। हम फिर भी शिकार हो जाते हैं।

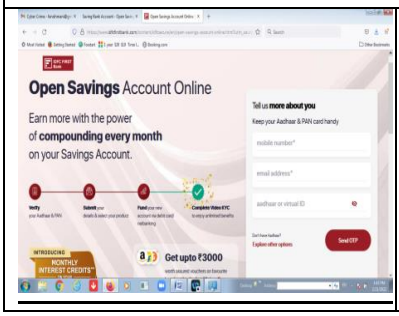
आखिर ये मायाजाल इतना मजबूत क्यों है कि तमाम अपीलों, चेतावनियों और जागरूकता अभियानों के बावजूद आम लोग आसानी से इसमें फंस जाते हैं और अपना नुकसान कर बैठते हैं। ये समझने के लिए हमें उन तरीकों को जानना होगा जिसका आजकल साइबर धोखाधड़ी में इस्तेमाल हो रहा है।

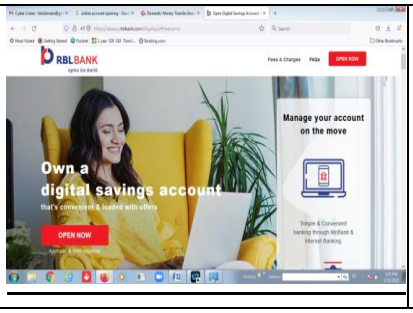
बैंकिंग में साइबर अपराध के तरीके और समाधान

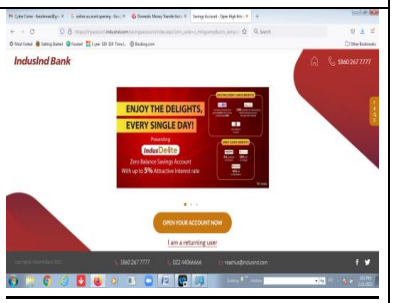
एक ज़माने में **फिशिंग** और **विशिंग** साइबर धोखाधड़ी के बेहद आम तरीके थे। फिशिंग के तहत धोखेबाज़, नामी कंपनियों व संस्थानों के नाम से फर्जी ई-मेल भेजते और बड़े इनाम का लालच देकर लोगों को निजी जानकारियां जैसे पासवर्ड, क्रेडिट कार्ड नंबर बताने के लिए मजबूर करते थे। ऐसे ही **विशिंग** के जरिए किसी को फोन करके, उसे मुश्किल में फंसा कर, उसकी निजी और बैंक खाते की जानकारियां हासिल की जाती थीं। इसके अलावा एटीएम में कार्ड रीडर लगाकर डेबिट / क्रेडिट कार्ड की जानकारियां हासिल कर ली जाती थीं। कार्ड क्लोनिंग के जरिए भी ग्राहकों को ठगा जाता था। हालांकि भारतीय रिज़र्व बैंक और बैंकों की जागरूकता की मुहिम की वजह से आम लोग इनके प्रति सचेत हो गए। यह भी सच है कि पिछले कुछ सालों में, विशेषतौर पर कोरोना के बाद बैंकिंग लेन-देन के तरीके बदलाव प्रक्रिया से गुजरे हैं। डिटिजल और ऑनलाइन लेन-देन का दायरा बढ़ा है। लिहाजा साइबर क्रिमिनल्स भी लोगों की बैंकिंग लेन-देन की आदतों और चलन के अनुसार अपनी मॉडस ऑपरेंडी में नित नए बदलाव कर रहे हैं। ठगी के इन नए तरीकों के बारे में जानना ज़रूरी है।

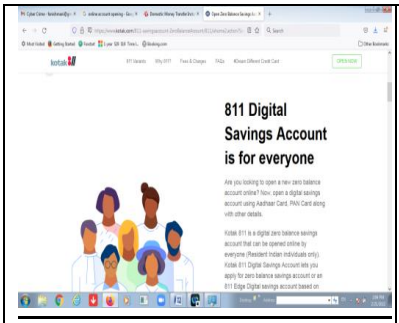
ऑनलाइन अकाउंट ओपनिंग फ्रॉड

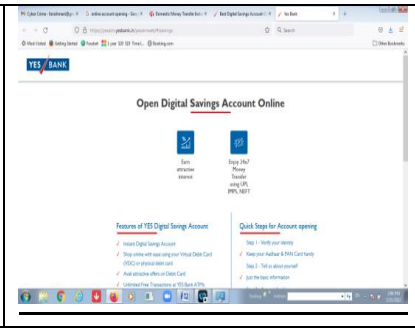
आधार + पैन कार्ड +आधार एनेबल्ड OTP माँगते हैं साइबर अपराधी

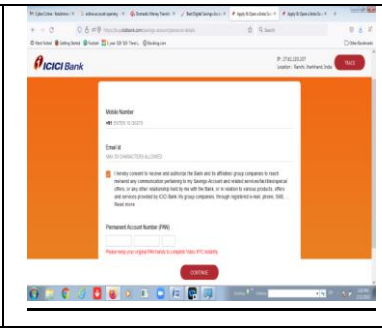












क्या है तरीका

आजकल कई बैंक घर बैठे बैंक खाता खोलने की सुविधा दे रहे हैं। कोरोना काल के दौरान ऑनलाइन बैंक अकाउंट खोलने का चलन और बढ़ा है। ऊपर विभिन्न बैंकों के ऑनलाइन अकाउंट ओपनिंग पेज का स्क्रीन शॉट है जिसमें देखा जा सकता है कि ऑनलाइन खाता खोलने के लिए मुख्य तौर पर आधार, PAN और आधार बेस्ड OTP की ज़रूरत पड़ती है। अब साइबर अपराधियों ने ऑनलाइन खाता खोलने की सुविधा में अपना फायदा ढूंढ़ लिया है। वे बैंक वाले बनकर आपको कॉल करते हैं और आपको बातों में फंसाकर आपसे आपका आधार और पैन हासिल कर लेते हैं। फिर ऑनलाइन बैंक खाते के लिए अप्लाई करते हैं जिसमें वो आपका नाम, आपका PAN और आपका आधार नंबर डालते हैं। ऑनलाइन वेरिफिकेशन के दौरान आधार बेस्ड ओटीपी मांगी जाती है। साइबर अपराधी आपसे ये ओटीपी भी हासिल कर लेते हैं। यानि पूरा खाता आपके नाम से और आपकी केवाईसी से ही खुलता है लेकिन खाता साइबर अपराधी का होता है। वे इस खाते में सिर्फ अपना मोबाइल नंबर डालते हैं ताकि वे बैंक खाते को अपने मोबाइल नंबर से ऑपरेट कर सकें। यानी नाम आपका और खाता फ्रॉड करने वाले का। साइबर अपराधी अलग-अलग लोगों को फोन करके, उनकी जानकारियां लेकर, ऐसे कई बैंक खाते खोलते हैं। अब अपराधी इन खातों को म्यूल यानि शिकार के तौर पर इस्तेमाल करते हैं। साइबर अपराध का पैसा वे इन्हीं खातों के जरिए ट्रांसफर करते हैं। पुलिस जब इन खातों के बारे में छानबीन करती है तो विक्टिम से पता चलता है कि उन्होंने कभी ऐसा खाता खोला ही नहीं है।

समाधान

* बैंकों को चाहिए कि वे वीडियो केवाईसी करते हुए ग्राहक को आधार पंजीकृत मोबाइल नंबर का ही उपयोग करने को कहें।
* राह चलते कभी भी अपना आधार और पैन किसी को नहीं दे दें।
* जब कभी भी टेलीकॉम कंपनी, बैंक में आधार या पैन की प्रति जमा कराएं तब उस पर यह ज़रूर लिखें कि आप किस इस्तेमाल के लिए दे रहे हैं और नीचे अपने हस्ताक्षर करें।

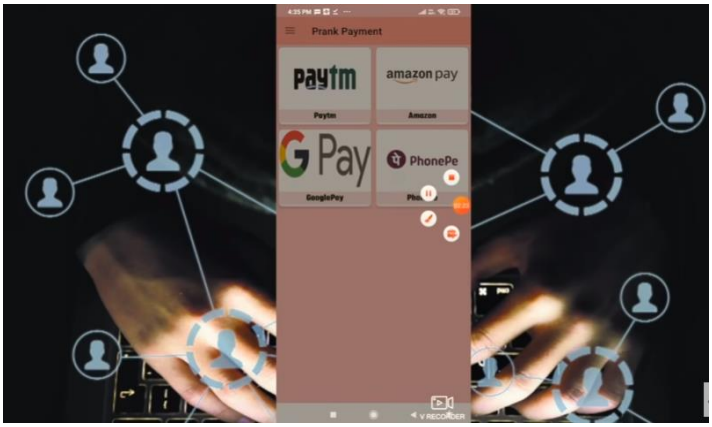
बैंक के नकली कस्टमर केयर नंबर के जरिए फ्रॉड

किसी भी बैंकिंग लेन-देन में फंसने पर अथवा बैंक से जुड़ी परेशानी का निजात पाने के लिए अक्सर लोग बैंकों के कस्टमर केयर नंबर की मदद लेते हैं। हड़बड़ी में और त्वरित समाधान के लिए आप गूगल करते हैं क्योंकि वहां से किसी भी बैंक के ग्राहक सेवा केंद्र का टोल फ्री नंबर आसानी से मिल जाता है। लेकिन आप ये नहीं जानते कि बैंकों के टोल फ्री नंबर की तरह ही साइबर आपराधियों ने अपने कस्टमाइज़्ड नंबर रखे हुए हैं। आप गलती से फ्रॉडस्टर के ही नंबर को टोल फ्री नंबर समझकर कॉल कर देते हैं और जाल में फंस जाते हैं।

समाधान

टोल फ्री नंबर के लिए कभी गूगल पर सर्च नहीं करें। टोल फ्री नंबर बैंक अधिकृत ऐप में मौजूद होता है। इसके अलावा आप बैंक के डबिट कार्ड के पीछे भी देख सकते हैं जहां बैंक का टोल फ्री नंबर स्पष्ट लिखा होता है।

SPOOF APP फ्रॉड



क्या है तरीका

UPI APP जैसे PAYTM/GOOGLEPAY/AMAZONPAY/PHONEPAY के SPOOF APP यानी फेक ऐप के जरिए फ्रॉड किया जा रहा है। स्पूफ ऐप एक नकली ऐप होता है जिसके जरिए धोखेबाज़ आपको धोखे का शिकार बनाते हैं। ये दरअसल फेक ऐप नहीं बल्कि APK फाइल होते हैं और बिल्कुल असली पेमेंट ऐप जैसे गूगल पे और पेटीएम से मेल खाता है। लेकिन इस एपीके फाइल को जब आप डाउनलोड करते हैं तो इससे आपके मोबाइल के सेंसिटिव डेटा चोरी हो सकते हैं। इसके अलावा इस फेक ऐप से नकली ट्रांजैक्शन दिखाकर भी कोई आपको धोखा दे सकता है। मान लीजिए कि कोई आपकी दुकान पर आता है और आपसे सामान खरीदकर आपको इस फेक ऐप से पेमेंट करता है। आपको दिखाता है कि उसने आपको पेमेंट कर दिया है। लेकिन हकीकत में फेक पेमेंट ऐप से किया गया ट्रांजैक्शन नकली है। ये ट्रांजैक्शन दिखता तो है लेकिन पैसा आपके खाते में नहीं जाता है और आप मान लेते हैं कि पैसा आपके खाते में आ गया है। इस तरह आप धोखाधड़ी के शिकार हो जाते हैं। डिजिटल लेन-देन करने वाले ग्राहक सावधान रहें। कैश बैक के नाम पर ठगी के झांसें में नहीं आएं। धोखेबाज़ आपको ये बोलकर फोन करते हैं कि PhonePe से आपको कैश बैक आया है, क्या आप उसे रिसीव करना चाहते हैं। यदि आपने लालच में आकर 'हां' कह दिया तो फिर आपको

PAYPAUL ऐप का लिंक भेजकर और उसमें राशि डालने के लिए कहा जाता है। आप समझते हैं कि आपकी डाली गई राशि आपको कैश बैक के रूप में मिलेगी जबकि धोखाधड़ी करने वाला PAYPAUL ऐप से आपके पैसे से अपना मोबाइल रीचार्ज करा लेता है या कैश निकाल लेता है।

समाधान

* एपीके फाइल्स को सोच-समझकर ही डाउनलोड करें
* कैश बैक के झांसे में नहीं आएं
* यदि कैश बैक आएगा भी तो कंपनी के ऐप में मौजूद आपके अकाउंट में आएगा।

'Any Desk' से फोन की हैकिंग या SCREEN MIRRORING FRAUD

क्या है तरीका

Any Desk App एक रिमोटली कंट्रोल्ड ऐप होता है। जो एक फोन से दूसरे फोन को कनेक्ट करता है। इससे आपके फोन में मौजूद सभी क्रेडेंशियल्स को जाना जा सकता है। आपके फोन की स्क्रीन को फ्रॉडस्टर अपने मोबाइल पर देख सकता है और आपके फोन को ऑपरेट कर सकता है। भारतीय रिज़र्व बैंक के आईटी सेल ने Any Desk App को डाउनलोड नहीं करने के बारे में चेतावनी भी जारी की है।

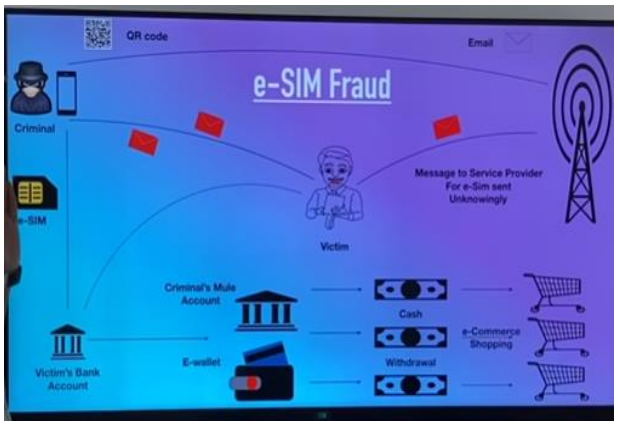
दरअसल, जब ऑनलाइन लेन-देन करते हुए पैसा फंस जाता है या फिर आपसे कोई गलती हो जाती है तो आप मदद के लिए कस्टमर केयर का नंबर गूगल पर सर्च करते हैं। आपको बैंक के कस्टमर केयर का नंबर मिलने की बजाय साइबर फ्रॉड का नंबर मिल जाता है और आप उस नंबर को कस्टमर केयर का नंबर समझकर कॉल कर देते हैं। फ्रॉडस्टर आपको Play Store में जाकर Any Desk App डाउनलोड करने के लिए कहता है। ये 6MB का ऐप होता है। इस ऐप को डाउनलोड करने के साथ ही 9 अंकों का एक कोड मिलता है जिसे आपसे शेयर करने के लिए कहा जाता है। आप ये नंबर शेयर कर देते हैं। फिर आपसे एक्सेस देने के लिए कहा जाता है। आप ये भी कर देते हैं और तब साइबर आपराधी आपके मोबाइल की स्क्रीन को अपने मोबाइल पर आसानी से देख पाता है। इसके बाद वो आपको समाधान बतलाता है जिसमें वो आपके कार्ड का नंबर, सीवीवी इत्यादि सब देख लेता है और आप धोखाधड़ी के शिकार हो जाते हैं।

समाधान

* कभी गूगल से कस्टमर केयर का नंबर नहीं सर्च करें।
* बैंक के ऐप में नंबर होता है उस पर कॉल करें।
* धोखाधड़ी का शिकार होने या इसकी आशंका होने पर सीधे बैंक के कर्मचारी को कॉल करें
* नजदीकी पुलिस स्टेशन में शिकायत करें।

* Any Desk, Team Viewer, Airdroid जैसे ऐप को डाउनलोड नहीं करें
* बैट्री या नेटवर्क कमज़ोर हो तब UPI का इस्तेमाल नहीं करें।

ई-सिम से धोखाधड़ी



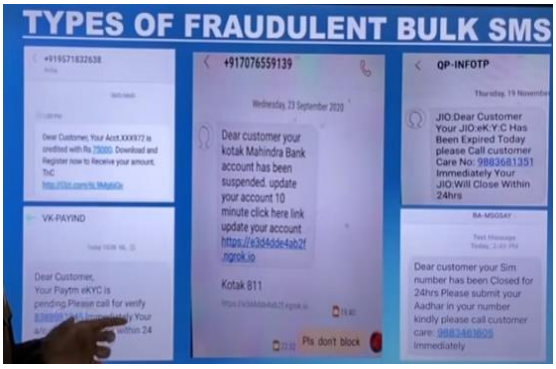
क्या है तरीका

मोबाइल में फिजिकल सिम की जगह वर्चुअल सिम का इस्तेमाल होता है। इसका इस्तेमाल हायर वर्शन के फोन में होता है। जब भी आप ई-सिम को एक्टिवेट /अपग्रेड/इंस्टाल करने जाते हैं, अपने फोन में सेट करने जाते हैं तब आपको क्यूआर कोड और अपने ई-मेल की आवश्यकता होती है। अपने फोन में ई-सिम डालने के बाद आपको अपनी ई-मेल आईडी टेलीकॉम सर्विस प्रोवाइडर को भेजनी होती है। यहीं साइबर फ्रॉड की एंट्री होती है और वे आपकी ई-मेल आइडी की जगह अपनी ई-मेल आईडी आपसे डालने के लिए कहते हैं। ये ऐसी यूनीक ई-मेल आईडी होती है जिस पर आप आसानी से यकीन कर लेते हैं क्योंकि इसमें कंपनी, सर्विस प्रोवाइडर का नाम होता है, जैसे AIRTEL1234@GMAIL.COM

साइबर फ्रॉडस्टर आपको कॉल करते हैं और ई-सिम एक्टिवेट करने की प्रक्रिया बताते हैं। वे आपसे कहते हैं कि सर्विस प्रोवाइडर को आप उनकी बताई ई-मेल आईडी भेजें। जैसे ही आप ई-मेल आईडी भेजते हैं साइबर फ्रॉडस्टर का ई-सिम एक्टिव हो जाता है। इसके बाद सर्विस प्रोवाइडर ग्राहक से प्राप्त ई-मेल पर क्यूआर कोड भेजता है। चूंकि ई-मेल क्रिमिनल का होता है इसलिए मिलने वाला क्यूआर कोड भी फ्रॉडस्टर को मिलता है। वो क्यूआर कोड डाउनलोड कर लेता है और ई-सिम से जुड़े आपके सभी बैंकिंग लेन-देन को वो कर सकता है क्योंकि आपके ई-सिम का ओटीपी भी उसे मिल रहा है। ये मल्टीपल चैनल के जरिए, आपके ई-वॉलेट से पैसे निकाल लेते हैं या फिर ऑनलाइन खरीदारी करते हैं और आपका बैंक अकाउंट खाली कर देते हैं।

समाधान

* आप ई-सिम एक्टिवेशन के झांसे में आकर ई-मेल आइडी नहीं बदलें।
* यदि आपके पास हायर वर्शन का फोन नहीं है तो वो ई-सिम इनेबल्ड फोन नहीं है। इसके बावजूद यदि कॉल आते हैं और आपको अपग्रेड करने के लिए कहा जाता है तो समझ लीजिए कि ये क्रिमिनल की कॉल है।
* यदि धोखेबाज़ आपको फोन सेवा बंद होने की धमकी भी देता है तो उसे नज़रअंदाज करें, उसके बहकावे में नहीं आएं।
* ई-सिम अपग्रेड कराते हुए बेहद सावधानी बरतें, सीधे सर्विस प्रोवाइडर के नंबर पर ही कॉल करें।
* कोई भी सर्विस प्रोवाइडर आपको सिम कार्ड ब्लॉक करने की चेतावनी नहीं देते हैं।
* सिम अपग्रेडेशन के नाम पर कभी भी सिम कार्ड ब्लॉक नहीं हो सकता है।



बल्क SMS फ्रॉड

साइबर अपराधी किसी के भी नाम पर बैंक खाता खोलते हैं। फिर टेलीकॉम सर्विस प्रोवाइडर से बल्क एसएमएस की सर्विस मांगते हैं। महज 3-4 हजार रुपए खर्च करके वे 50-60 हज़ार लोगों को बल्क एसएमएस भेज देते हैं। इस बल्क एसएमएस में क्या लिखा होता है टेलीकॉम सर्विस प्रोवाइडर को इसकी जानकारी नहीं होती है। जबकि धोखाधड़ी करने वाले बल्क एसएमएस में फर्जी रूप से खाते में क्रेडिट, लॉटरी जीतने का संदेश, सिम ब्लॉक और केवाईसी अपडेट लिंक इत्यादि जैसे संदेश भेजते हैं। जिन 50-60 नंबरों पर ये बल्क मैसेज जाता है उसमें से अधिकतर फर्जी होते हैं या वहां से कोई रेस्पॉन्स नहीं आता। लेकिन इनमें से 8-10 मोबाइल नंबरों से भी यदि वापस कॉल आ जाती है तो फॉड करने वाले के वारे न्यारे हो जाते हैं।

साइबर अपराध से बचने का मूलमंत्र

* आप किसी भी परिस्थिति में फंसे हों अपने धैर्य को खोकर अपराधियों के झांसे में आकर अपना बैंक विवरण अथवा ओटीपी किसी के साथ साझा नहीं करें।
* लॉटरी जीतने का कितना भी भरोसेमंद ई-मेल, SMS या लिंक आए, उसे अनदेखा करें।
* अपने कार्ड का पिन हर हफ्ते बदल दिया करें।
* कैश बैक के लालच में फंस कर अपना पैसा दूसरों के खाते में डालने की बेवकूफ़ी नहीं करें।
* कभी भी कोई टेलीकॉम सर्विस प्रोवाइडर आपका सिम कार्ड ब्लॉक नहीं करता है।
* कभी भी कोई बैंक या उसका स्टाफ आपसे आपके खाते का विवरण नहीं माँगता।
* यदि कोई केवाईसी अपडेट करने के नाम पर ब्लैकमेल कर रहा है तो उसकी बातों में नहीं फंसें।
* बैंक जाकर या टेलीकॉम कंपनी के दफ्तर जाकर सीधे बात करें और असलियत का पता लगाएं।
* कभी भी फोन पर बैंक से ये आग्रह नहीं करें कि वे आपके बैंक खाते में ई-मेल या मोबाइल नंबर डाल दें।
* समय-समय पर अपने इंटरनेट बैंकिंग पासवर्ड, मोबाइल पासवर्ड इत्यादि को बदलते रहें।
* मजबूत पासवर्ड रखें जिसमें अल्फा-न्यूमेरिक, स्पेशल कैरेक्टर्स हों।
* अपना पासवर्ड, ओटीपी, बैंक डेबिट/ क्रेडिट कार्ड किसी को नहीं दें, चाहे वो आपका रिश्तेदार ही क्यों न हो।
* कोई भी साइट सुरक्षित है या नहीं इसका पता यूआरएल से चल जाता है। सुरक्षित साइट के URL में https लिखा होता है। 'S' सिक्योर के लिए इस्तेमाल होता है।
* साइबर अपराध का शिकार होने पर बैंक के पंजीकृत टोल फ्री नंबर पर शिकायत करें।
* साइबर अपराध की शिकायत 1930 पर कॉल करके भी की जा सकती है।
* साइबर क्राइम की रिपोर्टिंग के लिए सरकार ने विशेषतौर पर पोर्टल लॉन्च किया है जिसका पता है cybercrime.gov.in

निष्कर्ष

समझदारी यही है कि धोखा कोई खाए और सबक हम और आप ले लें। आप जितने सतर्क रहेंगे, ठगी के नए-नए तरीकों के प्रति जागरूक रहेंगे। कभी-कभी बैंक ग्राहक इस बात से परेशान हो जाते हैं कि बैंक वाले फोन पर उनके खाते में ई-मेल अपडेट नहीं कर रहे हैं। फोन पर आग्रह करने के बावजूद बैंक उनका मोबाइल नंबर नहीं बदल रहा है। बैंक ऐसे अनुरोधों को यदि फोन पर नहीं स्वीकार कर रहे हैं तो ये आपके लिए ही अच्छा है। मोबाइल नंबर और ई-मेल आपको अपनी बैंक शाखा में जाकर ही अपडेट कराना चाहिए। मान लीजिए कि आपके नाम से कोई और ई-मेल और मोबाइल नंबर बदलने या अपडेट करने के लिए कहे और बैंक ऐसा कर दें तो आपको कितना बड़ा नुकसान हो सकता है।

साइबर ठगी से बचने के लिए दो मूलमंत्र है-कभी लालच में नहीं पड़ें। याद रखें कि साइबर अपराधी आप जैसे सैकड़ों ग्राहकों को ठगने की कोशिश करते हैं लेकिन उनके जाल में कुछ ही लोग फंसते हैं। फंसने वाले या तो नासमझ होते हैं या वे लालच में पड़ जाते हैं। दोनों ही आपके लिए नुकसानदेह है। आप नए साइबर खतरों और हमलों के प्रति हमेशा जागरूक रहें। खुद भी सचेत रहें और दूसरों को भी सचेत करें। अपने केवाईसी, पासवर्ड तथा बैंक विवरण को हमेशा गुप्त रखें। ऐसा करके, हम स्वस्थ डिजिटल बैंकिंग वातावरण तैयार कर सकते हैं।

*****

मंजुला वाधवा

पदनाम:- उप महाप्रबंधक
संस्था का नाम:- राष्ट्रीय कृषि और ग्रामीण विकास बैंक
मोबाइल नं. :- 6284315644
ई-मेल:- m.wadhwa@nabard.org

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

वैश्वीकरण के आधुनिक दौर में डिजिटल प्रौद्योगिकी ने संसार की अर्थव्यवस्थाओं, संस्कृतियों और आम जन को आपस में जोड़ दिया हैं, लिहाजा वैश्विक अर्थव्यवस्था और समाज का सशक्तिकरण हो रहा है। जहां भारत में 2020 में 74.5 करोड़ इंटरनेट उपयोगकर्ता थे, 2021 की अंतिम तिमाही तक इनकी संख्या 82.5 करोड़ हो गई है। इलैक्ट्रॉनिक लेनदेनों में हुई अभूतपूर्व वृद्धि और तेज़ी से विकसित हो रही डिजिटल अर्थव्यवस्था के चलते साइबर हमले अंतर्राष्ट्रीय स्तर पर गंभीर चिंता का विषय बन गए हैं। 2017 में साइबर अपराधों के 21796* मामले दर्ज हुए थे जो 2022 आते-आते 50000* के आंकड़े पार कर चुके हैं। ऐसे हमलावरों में 'हैक्टिविस्ट्स', साइबर अपराधी और आतंकवादी शामिल हैं जो राजनीतिक और वित्तीय अस्थिरता पैदा करने तथा वित्तीय अवसरंचना को बाधित करने के लिए वित्तीय प्रलोभनों से प्रेरित होते हैं। फेडरल ब्यूरो ऑफ इन्वेस्टिगेशन के इंटरनेट क्राइम कम्प्लेंट सेंटर (आईसी3) की नवीनतम रिपोर्ट के अनुसार कोरोनाकाल में डिजिटल बैंकिंग पर बढ़ती निर्भरता के कारण साइबर हमले 65% बढ़ गए हैं** और साइबर अपराधों के मामले में भारत यूके और कनाडा के बाद तीसरे स्थान पर हैं। नैशनल क्राइम रिकार्ड ब्यूरो*** के आंकड़े दर्शाते हैं कि 2020 में हुए साइबर अपराधों में से एक तिहाई से भी ज्यादा संचार माध्यमों से की गई बैंकिंग और वित्तीय धोखाधड़ी के थे। निम्न तालिका स्थिति को स्पष्ट करती है:-

संचार माध्यमों से किए गए आईपीसी अपराध

वर्ष	डेबिट कार्ड/क्रेडिट कार्ड	एटीएम	ऑनलाइन बैंकिंग फ्रॉड	ओटीपी
2017	395	1534	798	329
2018	309	1280	965	319
2019	365	2066	2091	549
2020	1193	2160	4028	1091

स्रोत ***: राष्ट्रीय अपराध रिकार्ड ब्यूरो ncrb.gov.in***

वस्तुत: साइबर स्पेस को भूमि, समुद्र, वायु और अंतरिक्ष के बाद युद्ध के 5वें आयाम के रूप में घोषित किया गया है। सबसे पहले इस अवधारणा को समझ लेते हैं- साइबर सुरक्षा से तात्पर्य साइबर स्पेस को हमले, क्षति, दुरुपयोग और आर्थिक जासूसी (economic espionage) से सुरक्षित करना है। साइबर स्पेस सूचना परिवेश के भीतर एक वैश्विक डोमेन है जिसमें परस्पर निर्भर आईटी अवसंरचना जैसे इंटरनेट, टेलीकॉम नेटवर्क, कंप्यूटर सिस्टम इत्यादि शामिल होते हैं। बैंकिंग जगत में आज साइबर अपराधों के नित्य नये स्वरूप व प्रकार सामने आ रहे हैं जैसे स्पैम ई-मेल, हैकिंग, वायरस फैलाना, सॉफ्टवेयर पायरेसी, फर्जी बैंक कॉल, सोशल नेटवर्किंग साइटों

पर अफवाह फैलाना और साइबर बुलिंग यानी इंटरनेट पर अशोभनीय टिप्पणियां करना, मज़ाक बनाना या धमकियां देना आदि।

वैश्विक बैंकिंग जगत पर दृष्टिपात करें तो अंतर्राष्ट्रीय मुद्रा कोष की साइबर हमलों पर प्रकाशित 2020 की रिपोर्ट**** में वित्तीय स्थिरता बोर्ड ने चेतावनी दी है कि यदि हम समय पर ना चेते तो अगला साइबर हमला पूरी दुनिया के वित्तीय तंत्र और आधारभूत सरंचना को हिला सकता है। जाहिर है, आज के सूचना तकनीक युग में साइबर सुरक्षा बहुत ज़रूरी है और प्रति पल मंडराते खतरों के मद्देनज़र सुरक्षा उपायों की ओर ध्यान देकर उन्हें सुनिश्चित करना नितांत आवश्यक है। नकदी भंडार और विशाल ग्राहक डेटाबेस होने के कारण हमलावरों के निशाने पर बैंक सर्वाधिक हैं। साइबर सुरक्षा की प्रमुख चुनौतियां हैं:-*जागरूकता की कमी *अपर्याप्त बजट और प्रबंधतंत्र से सहयोग न मिलना *खराब पहचान और पहुंच व्यवस्था *रैन्समवेयर में बढ़ोत्तरी, *मोबाइल डिवाइसिज़ व एप्प *ऑनलाइन सर्वर/वेबसाइट को बाधित कर देना *सोशल मीडिया आदि।

क्यों बढ़ रहे हैं साइबर अपराध:-

क्या आईटी पर लगातार बढ़ती हमारी निर्भरता एकमात्र कारण है? मेरे विचार में, सामाजिक-सांस्कृतिक कारण भी उतने ही जिम्मेदार हैं-बढ़ती मंहगाई, बेरोजगार युवा पीढ़ी के खाली दिमागों की जल्दी और आसानी से पैसा बनाने की फितरत। अन्य कारण है-वर्क फ्रॉम होम की बढ़ती संस्कृति-कार्यालय में डेस्कटॉप/लैपटॉप इस्तेमाल करने पर साइबर सुरक्षा के पुख्ता पेशेवराना इंतजाम होते हैं जो घर के माहौल में संभव नहीं हो पाते। डिजिटल थकान भी अहम कारण है फलत: डिजिटल लेनदेन करते समय उच्च पदस्थ अधिकारी भी लापरवाही बरतने लगते हैं।

साइबर सुरक्षा जरूरी क्यों:-

- **भारतीय रिज़र्व बैंक व भारत सरकार द्वारा डिजिटल बैंकिंग को प्रोत्साहन**: आधार, गवर्नमेंट ई-मार्केट, डिजीलॉकर, भारतनेट जैसे विभिन्न कार्यक्रमों से बड़ी संख्या में नागरिकों, कंपनियों और सरकारी एजेंसियों को ऑनलाइन बैंकिंग कारोबार करने के लिए प्रेरित करना।
- **स्टार्ट-अप डिजिटल को बढ़ावा देना**: भारत प्रौद्योगिकी संचालित स्टार्ट-अप्स के लिए अमेरिका और चीन के बाद तीसरा सबसे बड़ा केंद्र है, अनुमानत: इसका आईसीटी क्षेत्र 2022 तक 235 बिलियन डॉलर तक पहुंच जाएगा।
- **बढ़ती संवेदनशीलता:** साइबर सुरक्षा उल्लंघनों के मामले में भारत विश्व का पांचवां सबसे संवेदनशील देश है। भारत में 2017-2019 के बीच ऑनलाइन बैंकिंग फ्रॉड 162% बढ़ गए और कोविड19 ने अपराधियों के हौंसले और बुलंद कर दिए।
- **बढ़ती लागत:** 2021 में वैश्विक रैन्समवेयर हमले 151% बढ़ गए और भारत में साइबर हमलों से होने वाली अनुमानित हानि लगभग रू. 02 लाख करोड़ तक पहुंच गई और आगे भी 5जी नेटवर्क, स्मार्ट-सिटी परियोजना आदि के कारण इसके और बढ़ने की संभावना है।
- **इंटरनेट उपयोगकर्ताओं की बढ़ती संख्या**: उपयोगकर्ताओं की संख्या के मामले में भी भारत यूएसए और चीन के बाद तीसरे स्थान पर है। 2017 में जहां भारत में 622 मिलियन सक्रिय इंटरनेट उपयोगकर्ता थे, 2025 तक इनके बढ़कर 900 मिलियन हो जाने का अनुमान है।
- **ऑनलाइन कारोबार बढ़ना:** आंकड़ों की जुबानी, 2021 में बैंकिंग और बीमा क्षेत्र में डिजिटल लेनदेन 109 प्रतिशत बढ़ गए।

बैंकिंग में साइबर सुरक्षा संबंधी चुनौतियां:-

- ❖ वित्तीय व डिजिटल निरक्षरता:- आजादी का अमृत महोत्सव नजदीक आ जाने के बावजूद भारत में लगभग 77% नागरिक ही साक्षर हैं और महज 24% लोग वित्तीय और डिजिटल दृष्टि से साक्षर हैं, लिहाजा, साइबर अपराधियों को हमारा देश हमलों के लिए उर्वर भूमि नजर आता है।
- ❖ लाइसेंस रहित सॉफ्टवेयरों और अंडरपेड लाइसेंसों का व्यापक उपयोग।
- ❖ बैंकिंग आधारभूत सरंचना आज भी मजबूत नहीं हैं, नतीजतन, कुल क्रेडिट व डेबिट कार्ड में से लगभग 75% मेग्निटिक-स्ट्रिप आधारित हैं जिनका प्रतिरूपण(cloning) आसान होता है।
- ❖ मानकों के प्रयोग के कारण एकरूप सुरक्षा प्रोटोकॉल उपलब्ध करवाने में समस्या आती है। आयात पर निर्भरता भी भारत को असुरक्षित स्थिति में डालती है।
- ❖ देश में फिलहाल सुरक्षा संबंधी पदों पर रिक्तियां लगभग 3.5 मिलियन हैं यानी कुशल व प्रशिक्षित कार्मिकों की मांग आपूर्ति से काफी अधिक है।
- ❖ 90%+ साइबर क्राइम्स की रिपोर्ट ही नहीं की जाती, साइबर सुरक्षा एजेंसियों के बीच आपसी तालमेल की भी कमी है।

आइए, अब नजर डालते हैं साइबर सुरक्षा हेतु **रिज़र्व बैंक द्वारा उठाए गए कदमों पर** 2 जून 2016 को रिज़र्व बैंक ने सभी बैंकों को साइबर सुरक्षा संबंधी निम्न निर्देश जारी किए:-

- साइबर सुरक्षा जोखिमों के संबंध में ग्राहकों को जागरूक और शिक्षित करना।
- तृतीय पक्ष विक्रेता के साथ अपने लॉगिन क्रिडेंशियल्स/पासवर्ड साझा करने के नकारात्मक जोखिमों और उनके परिणामों के बारे में ग्राहकों को शिक्षित करना।

भारतीय रिज़र्व बैंक ने 21 जनवरी, 2018 को एटीएम सुरक्षा सुदृढ़ करने हेतु बैंकों और व्हाइट-लेबल एटीएम ऑपरेटरों को विभिन्न सुधारात्मक उपाय की सलाह दी जैसे बीआईओएस पासवर्ड को सक्षम करना, यूएसबी पोर्ट को अक्षम करना, ऑटो-रन की सुविधा अक्षम करना, ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर्स के नवीनतम पैच को लागू करना, टर्मिनल सुरक्षा समाधान, समय आधारित एडमिन-पहुंच, एंटी स्क्रीमिंग और व्हाइट लिस्टिंग समाधान लागू करना, ऑपरेटिंग सिस्टम के समर्थित संस्करणों के लिए एटीएम अपग्रेड करना आदि। कार्ड लेनदेन की सुरक्षा बढ़ाने हेतु बैंकों, कार्ड पेमेंट नेटवर्क और गैर-बैंक पीपीआई जारीकर्ताओं को भी निम्नानुसार निदेश दिए गए हैं:-

- सभी कार्ड (भौतिक/वर्चुअल) जारी/नवीकरण करते समय केवल भारत में उपयोग के संपर्क आधारित बिंदुओं पर इस्तेमाल करने के लिए सक्षम किए जाएं।
- पीओएस, एटीएम, ऑनलाइन लेनदेन/संपर्क रहित लेनदेन के लिए लेनदेन सीमा को 24x7 आरंभ/बंद करने और संशोधित करने की सुविधा।
- कार्ड की स्थिति में परिवर्तन होने पर एसएमएस/ई-मेल के जरिए अलर्ट आदि।

सुरक्षा समाधानों की दिशा में निरंतर सजगता अपनाते हुए भारतीय रिज़र्व बैंक ने फरवरी 2021 में कुछ नये दिशानिर्देश जारी किए:-

- डिजिटल पेमेंट ऐप में उपयोगकर्ताओं के लिए सुरक्षित और जिम्मेदाराना प्रयोग निदेश और प्रशिक्षण सामग्री शामिल करना।
- इन्हीं ऐप में उपभोक्ता शिकायतें दर्ज करने की प्रक्रिया का स्पष्ट उल्लेख करना।

- बैंक अनधिकृत लेनदेन या कार्ड के चोरी हो जाने की रिपोर्टिंग के लिए विभिन्न चैनल जैसे वेबसाइट, फोन बैंकिंग, एसएमएस, ई-मेल, आईवीआर, टॉल-फ्री हेल्पलाइन, होम ब्रांच को रिपोर्ट करना आदि सभी माध्यम उपलब्ध करवाएं।

बैंक धोखाधड़ी के मामलों की जांच करने और उन्हें कानून-प्रवर्तन एजेंसियों को रिपोर्ट करने, कर्मचारियों की जवाबदेही की जांच करने, फ्रॉड में शामिल राशि को पुन:प्राप्त करने के लिए कदम उठाने, यथा लागू बीमा का दावा करने और ऐसी घटनाओं के दोहराव से बचने हेतु अपनी प्रणालियां और प्रक्रियाएं प्रवाही बनाएं।

'भारतीय रिज़र्व बैंक कहता है' बैनर तले चलाए जा रहे जागरूकता अभियान में शामिल बिंदुओं पर भी यहां चर्चा करना समीचीन है:-

- एसएमएस से प्राप्त पिन/ओटीपी/पासवर्ड साझा न करें
- अनधिकृत लेनदेन पर प्राप्त एलर्ट पर शीघ्र प्रतिक्रिया दें
- मोबाइल में महत्वपूर्ण बैंकिंग डेटा न रखें
- केवल सत्यापित और विश्वसनीय वेबसाइटों का इस्तेमाल करें
- मुक्त नेटवर्क पर बैंकिंग लेनदेन से बचें
- नियमित रूप से पिन बदलें
- खोने/चोरी होने पर तुरंत एटीएम/क्रेडिट/प्रीपेड कार्ड को ब्लॉक करवाएं

इसके अतिरिक्त भारतीय रिज़र्व बैंक कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-IN) के सहयोग से समय-समय पर साइबर ड्रिल भी आयोजित करता है। अब तक ऐसी 50 ड्रिल संचालित की गई हैं जिनमें विभिन्न राज्यों और क्षेत्रों जैसे वित्त, रक्षा, बिजली, दूरसंचार, परिवहन, ऊर्जा, आईटी, अंतरिक्ष आदि से 450 संगठनों ने भाग लिया। इनमें से 12 ड्रिल वित्तीय क्षेत्र के संगठनों के लिए भारतीय रिज़र्व बैंक और द इंस्टीट्यूट फॉर डेवल्पमेंट एंड रिसर्च इन बैंकिंग टेक्नॉलिजी(IDRBT) के साथ समन्वय करके किए गए है। प्रौद्योगिकी में लगातार बढ़ रहे खतरों की समीक्षा हेतु सुरक्षा मानदंड/प्रोटोकॉल अपनाने संबंधी अध्ययन हेतु सभी हितधारकों के साथ मिलजुल कर साइबर सुरक्षा इंटर-डिस्पिलनरी समिति भी गठित की गई है जिसकी नियमित बैठकें होती है और उसकी सिफारिशों के अनुरूप गहन जांच-योग्य कुछ प्रमुख क्षेत्रों के लिए उप-समूह बनाए जाते हैं। भारतीय रिज़र्व बैंक में सूचना प्रौद्योगिकी प्र. लि. नामक एक आनुषंगिक आईटी निकाय भी स्थापित किया गया है जो भारतीय रिज़र्व बैंक और उसके द्वारा विनियमित सभी बैंकों की साइबर सुरक्षा पर ध्यान केंद्रित करता है। नियामक बैंक प्रमुख बैंकों के साइबर जोखिम लचीलेपन और प्रतिक्रिया का आकलन करने के लिए उनकी विस्तृत जांच और उनके द्वारा की गई सुधारात्मक कार्रवाई की निगरानी भी करता है।

भारतीय रिज़र्व बैंक ने शहरी सहकारी बैंकों के आकार, कार्यक्षेत्र, वित्तीय स्थिति, डिजिटल कामकाज असमान होने के कारण उन पर वाणिज्य बैंकों वाले सुरक्षा मानदंड लागू करना उचित नहीं समझा, अतः 24 सितम्बर, 2020 को शहरी सहकारी बैंकों के लिए **'विजन फॉर साइबर सिक्योरिटी 2020-23'** जारी किया और इसके तहत् टियर-वाइज अप्रोच अपनाते हुए निदेश दिया, कि जो यूसीबी वाणिज्य बैंकों की भांति आईटी समर्थित डिजिटल भुगतान सेवाएं उपलब्ध करा रहे हैं, उन्हें साइबर सुरक्षा मानदंडों का भी पालन करना होगा लेकिन इसकी लागत का कुछ हिस्सा वे ग्राहकों से वसूलेंगे। विजन के 5 स्तम्भ है:- सतत व गहन निगरानी, आईटी तकनीकों में अधिक निवेश, समुचित विनियमन व पर्यवेक्षण, अन्य बैंकों के साथ सतत-गहन संपर्क, साइबर सुरक्षा कौशल विकसित करना। साथ ही, उन्हें मुख्य सूचना सुरक्षा अधिकारी नियुक्त करने और आईटी कार्यनीति समिति, आईटी निगरानी समिति आदि भी गठित करने के अनुदेश दिए गए।

अब **भारत सरकार की पहलकदमियों** का भी जायजा लें :- दिनांक 2 जुलाई 2013 को जारी राष्ट्रीय सुरक्षा नीति का उद्देश्य संस्थागत सरंचनाओं, लोगो-प्रक्रिया, प्रौद्योगिकी और सहयोग के संयोजन द्वारा साइबरस्पेस में सूचना अवसरंचना की सुरक्षा करना, वलनरेबिलिटी घटाना, साइबर अपराधों को रोकने हेतु क्षमता निर्माण तथा ऐसे हादसों से होने वाले नुकसान को न्यूनतम करना है । सरकार स्वच्छ केन्द्र (botnet cleaning and malware Analysis entre) का भी संचालन कर रही है। केन्द्र द्वारा मैलिशियस प्रोग्राम्स का पता लगाने और इन्हें हटाने हेतु मुफ्त उपकरण प्रदान किए जा रहे हैं । देश में प्रीपेड भुगतान इंस्ट्रूमेंट जारीकर्ता प्राधिकृत संस्थाओं/बैंकों को सीईआरटी-आईएन द्वारा आरबीआई के माध्यम से सूचीबद्ध लेखापरीक्षकों द्वारा विशेष लेखापरीक्षा करने और उसके निष्कर्षो की अनुपालना और सुरक्षा के सर्वोत्तम अभ्यासों का कार्यान्वयन सुनिश्चित करने के लिए तत्काल कदम उठाने की सलाह दी गई है।

अंतत: बहु-आयामी सार्वजनिक-निजी सुरक्षा व्यवस्था, कानून प्रवर्तन एजेंसियों, आईटी उद्योग, सूचना सुरक्षा संस्थानों, इंटरनेट कंपनियों, वित्तीय संस्थाओं आदि के साथ तालमेल बिठाते हुए तकनीकी रूप से सुदृढ़ नेटवर्क का निर्माण करना हमारी सर्वोच्च प्राथमिकता होनी चाहिए और इसके लिए पेशेवर साइबर सुरक्षा-प्रदाता की सेवाएं लेना कारगर हो सकता है। इस संदर्भ में हमारे वर्तमान प्रधानमंत्री, श्री मोदी के निम्नलिखित शब्द सटीक प्रतीत होते हैं:-

''मेरा सपना है ऐसा डिजिटल इंडिया जहां साइबर सुरक्षा राष्ट्रीय सुरक्षा का अभिन्न अंग हो''

संदर्भ सामग्री:-

- *www.statista lcom*
- *https://www.ic3.gov-PDF-Annual Report*
- *नैशनल क्राइम रिकार्ड ब्यूरो, इंडिया की साइबर क्राइम रिपोर्ट 2020*
- *Outlookindia.com-banking frauds*

*****

मीरा

पदनाम:- सहायक प्रबंधक
संस्था का नाम:- सेंट्रल बैंक ऑफ़ इंडिया
मोबाइल नं. :- 9223420920

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

प्रस्तावना

ऐसे दिन बहुत पीछे छूट गए जब हम अपने परिजनों को अपना संदेश भेजने के लिए कबूतरों की राह देखा करते थे। हमें पता भी ना चला कब इन कबूतरों की जगह डाकिया और कब डाकिया की जगह ई मेल ने ले ली। आज का युग है बटन टेक्नोलॉजी का अर्थात् क्लिक क्लिक क्लिक... । सूचना प्रौद्योगिकी में आए क्रान्तिकारी परिवर्तनों के कारण बैंकिंग जगत में भारी बदलाव आया है और आधुनिक बैंकिंग "वन स्टॉप शॉप" बन गयी है।

सूचना प्रौद्योगिकी और इलेक्ट्रॉनिक बैंकिंग के विकास के मद्देनजर आधुनिक कंप्यूटर, एटीएम, इंटरनेट बैंकिंग, टेली-बैंकिग, डेबिट-क्रेडिट कार्ड, स्मार्ट कार्ड आदि का उपयोग अनिवार्य हो गया है। नोटबंदी के बाद डिजिटल बैंकिंग की तरफ बढ़ते कदमों ने कोरोना महामारी आपदा के दौरान तेज रफ्तार पकड़ी है। सूचना तकनीकी और प्रतिस्पर्धात्मक वातावरण में विकास से नए आयाम खुले हैं तो दूसरी ओर धोखाधड़ी/ जालसाजी/ कपट/ गबन जैसे विभिन्न प्रकार के अपराधों में भी बढ़ोतरी हुई है। विकास के साथ-साथ विध्वंसक प्रवृतियां भी जन्म लेने लगती है, वास्तव में साइबर अपराध इसी की देन है। आज-कल अखबारों एवं समाचारों में हम साइबर अपराधों के बारे में पढ़ते, सुनते व देखते रहते है। सूचना प्रौद्योगिकी से संबंधित धोखाधड़ी में साइबर अपराध के नए-नए मामले सामने आ रहे है। चिंता की बात यह है कि दिन-ब-दिन साइबर अपराध के मामले अत्यन्त क्लिष्ट और उलझे हुए नजर आ रहे है। आज बैंकिंग पर साइबर खतरों के काले बादलों की तरह मंडरा रहे हैं और इन साइबर खतरों से अपने ग्राहकों को सुरक्षा प्रदान करना बैंकों के लिए एक अनिवार्य दायित्व हो गया है।

साइबर की ऐतिहासिक पृष्ठभूमि

वर्ष 1966 में अमरीकी रक्षा विभाग के एडवांस्ड रिसर्च प्रोजेक्ट ने सबसे पहले सूचनाओं को एक दूसरे तक पहुँचाने के लिए नेटवर्क अर्पानेट तैयार किया था तथा 1969 में इस पर चार प्रोग्राम प्रोवाइडर कंप्यूटरों को जोड़ा गया था। शुरू में इनका उपयोग रक्षा अनुसंधान से जुड़े कार्यक्रम हेतु किया गया। 1989 में सरन वैज्ञानिक टीम **बरनरस ली** ने **वर्ल्ड वाइड वेब** (डब्ल्यू डब्ल्यू डब्ल्यू) स्थापित किया जो इंफॉर्मेशन टैफिक (संग्रहण तथा संप्रेषण) का मूल आधार बना। इसके बाद तो आधुनिकता और गति का ऐसा समागम बना कि नित नई कार्यप्रणालीयों ने दुनिया को आश्चर्यचकित कर दिया। ब्राडबैंड, ऑप्टिकल फाइबर एवं उपग्रह प्रणाली ने सूचनाओं के आदान-प्रदान ने गति को तीव्र से तीव्रतम करके आधुनिक युग को सूचना क्रांति में परिवर्तित किया जिसका सर्वाधिक फायदा बैंकिंग जगत को ई- बैंकिंग के रूप में प्राप्त हुआ।

साइबर अपराध - परिभाषा

कोई भी ऐसा कार्य जो कंप्यूटर, इंटरनेट पर अवैधानिक तरीके से किया गया हो एवं जिसमें बैंक, संस्था अथवा ग्राहक की राशि का कपटपूर्ण आहरण, दुरूपयोग अथवा हानि शामिल हो, साइबर अपराध कहलाता है।

साइबर विकास के साथ जिन विध्वंसक प्रवृत्तियों का जन्म हुआ उन्हें हम साइबर अपराध कहते है। इसमें निम्नलिखित शामिल हैं:

- सूचना व संचार तंत्र, कंप्यूटर प्रोग्राम, डेटा तथा आंकड़ों को बाधित करना।
- कंप्यूटरों में वायरस के माध्यम से सूचना व संचार प्रणाली पर आक्रमण करके आंकड़ों को बाधित एवं नष्ट करना।
- कंप्यूटर नेटवर्क को हैक करना।
- कंप्यूटर नेटवर्क के माध्यम से आंकड़ों की चोरी करना।
- कंप्यूटर का उपयोग हथियार के रूप में कर किसी का खाता या क्रेडिट कार्ड लेकर वित्तीय धोखाधड़ी करना या सूचनाओं से छेड़छाड़ करना।

बैंकिंग में साइबर अपराधों के स्वरूप

मानव मस्तिष्क की थाह पाना सर्वथा दुष्कर कार्य है। कौन, कब, कैसे, क्या आचरण कर बैठे इसका अंदाजा लगाना सहज नहीं होता है। अपराध को हमेशा दो नज़रिए से देख सकते हैं। भूख के लिए अपराध करना और अपराध की भूख होना ये दोनों विभिन्न पहलू हैं। एक साधारण व्यक्ति द्वारा भूख मिटाने हेतु की गई चोरी और बैंकिंग व्यवसाय में होने वाली सफेदपोश साइबर हेराफेरी दोनों अपराध एक जैसे होते हुए भी उन्हें अलग नज़रिए से देखना अत्यंत आवश्यक है।

बैंकिंग में साइबर अपराधों के कारण निम्नलिखित हैं:

- ✓ अशिक्षा - शिक्षा के अभाव के कारण गोपनीय सूचनाओं जैसे जन्मतिथि, पिन नंबर आदि को अंजान व्यक्तियों के साथ साझा करने के कारण ग्राहक अपराध का शिकार हो जाते है।
- ✓ असावधानी - एटीएम से आहरण के बाद खाताधारक कार्ड या पर्ची वहीं छोड़ जाते हैं जिसका अपराधी दुरूपयोग करते हैं।
- ✓ सुनियोजित ढंग से साइबर अपराधों का कार्यान्वयन - स्वयं को बैंक का अधिकारी दर्शाते हुए खाताधारक से कार्ड संबंधी सूचना मांगी जाती है और सूचना न देने पर खाता या कार्ड को ब्लॉक हो जाने की बात कर भोले-भाले ग्राहकों को अपने जाल में फँसाया जाता है। अपराधी फोन पर बड़े ही नियोजित तरीके से भ्रमित कर ठगते है। अल्पशिक्षित और अशिक्षित तो क्या शिक्षित लोग जैसे प्रशासनिक अधिकारी, पुलिस अधिकारी, न्यायिक अधिकारी, बैंक अधिकारी भी उनके झांसे में आ जाते है।
- ✓ लालच - श्रीमद्भगवत गीता में श्रीकृष्ण भगवान ने लालच को "नरक का द्वार" संबोधित कर यह सिद्ध किया है कि धोखाधड़ी/ कपट/ जालसाजी का मुख्य कारण लालच है न कि जरूरत। सफेदपोश साइबर अपराधों का मुख्य कारण बिना कुछ किए सबकुछ पाने का लालच ही है।

बैंकिंग जगत में साइबर अपराध

जैसे-जैसे हम बैंकिंग जगत में आधुनिक एवं उच्च प्रौद्योगिकी की तरफ बढ़ रहें हैं तथा बैंकिंग को सुविधाजनक बनाते जा रहे हैं, वैसे-वैसे हमें इन सफेदपोश साइबर अपराधों के खतरों का अधिक सामना करना पड़ रहा है। पिछले पाँच वर्षों के आंकड़े बताते हैं कि धोखाधड़ी के कुल मामलों का लगभग 65 प्रतिशत प्रौद्योगिकी विशेषकर इंटरनेट बैंकिंग, एटीएम, क्रेडिट कार्ड आदि से संबंधित रहे हैं। वर्ष 2013-14 में ₹10170 करोड़ की राशि के मामले सामने आए जबकि मात्र एक वर्ष के अंदर धोखाधड़ी की यह राशि लगभग 100 प्रतिशत बढ़कर ₹19361 करोड़ का आंकड़ा छू गई। पिछले दो वर्षों में साइबर अपराध के मामले अत्यधिक तेजी से बढ़ती ही जा रही है, जिनमें निम्नलिखित प्रमुख कारण हैं:

- ✓ कार्ड की चोरी - क्रेडिट कार्ड को चुराकर अधिकांश अपराध किए जाते है जिनमें परिवार के सदस्य तथा मित्र भी शामिल होते हैं।
- ✓ सूचनाओं की चोरी (स्किमिंग) - कभी कभी दुकानदारों के नौकर, हैकरों की गिरोह से मिलीभगत कर कार्ड का डेटा चुरा लेते है और डुप्लिकेट कार्ड बनाकर अपराध को अंजाम देते है।
- ✓ व्यक्तिगत सूचनाओं से धोखाधड़ी - अपराधी ग्राहक से संबंधित सूचनाएं जैसे जन्मतिथि, पता प्राप्त कर बैंक से पता बदलने का अनुरोध करते है। फिर कार्ड गुम होने की रिपोर्ट करते है और नया कार्ड प्राप्त कर अपराधिक गतिविधि करते है।
- ✓ ग्राहक के नाम से कार्ड प्राप्त करना – धोखाधड़ीकर्ताओं का सबसे अधिक लक्ष्य ग्राहक के विवरण जानने का होता है क्योंकि इससे उन्हें "खजाने की चाबी" प्राप्त हो जाती है। केवायसी के लिए नकली दस्तावेज प्रस्तुत करके पूरी प्लानिंग के साथ नया खाता खोलकर बैंक से कार्ड लेकर धोखाधड़ी को अंजाम दिया जाता है।
- ✓ एटीएम का प्रयोग - एटीएम का प्रयोग करते हुए लेन-देन को अधूरा छोड़ देने की स्थिती में अधिकतर अपराध का शिकार होते है।

बैंकिंग में साइबर अपराधों से रक्षा हेतु सुरक्षात्मक उपाय

बिल गेट्स का कहना है, "कारोबार में उपयोग की जानेवाली किसी प्रौद्योगिकी का पहला नियम है कि किसी कुशल परिचालन में स्वचालकता लागू कर दी जाए तो उसकी कुशलता में काफी इजाफा होता है। दूसरा नियम है कि किसी अकुशल परिचालन में स्वचालकता लागू कर दी जाए तो उसकी अकुशलता में काफी इजाफा होता है।" भारतीय रिज़र्व बैंक ने 2 जून, 2016 को बैंकों में साइबर सुरक्षा संरचना के संबंध में जारी अनुदेशों के तहत बैंकों को अपने बोर्ड द्वारा अनुमोदित सुरक्षा नीति लागू करने के निर्देश दिए ताकि साइबर संकट प्रबंधन योजना बनाई जा सके, निरंतर चौकसी की व्यवस्था की जा सकें, हार्डवेयर, साफ्टवेयर, नेटवर्क डिवॉइस आदि खरीदते/ कनेक्ट करते समय सुरक्षा पहलुओं का आकलन कर उपभोक्ता सूचना की रक्षा की जा सके।

साइबर अपराधों की रोकथाम हेतु निवारणात्मक उपाय

अंग्रेजी में एक प्रसिद्ध कहावत है, "प्रिवेंशन इज़ बेटर दैन क्युर" अर्थात् परहेज इलाज से बेहतर है। निवारक सतर्कता वह अवधारणा है जिसके तहत अपराधिक गतिविधियों को घटने/ रोकने के सुरक्षात्मक उपायों से हम रूबरू होते है जैसे –

- ग्राहक को जागरूक बनाने की आवश्यकता - ग्राहकों को साइबर अपराध से बचाव हेतु जागरूक बनाने के लिए बैंकों में प्रचार सामग्री का वितरण, शाखाओं में विडियो के माध्यम से जानकारी, डाक्यूमेंट्री का प्रदर्शन, टेलीविजन, पत्र-पत्रिकाओं के माध्यम से विज्ञापन देना जरूरी है।
- ग्राहक के द्वारा सावधानी बरतना - जैसे आईडी और पासवर्ड आदि गोपनीय सूचना को गुप्त रखना तथा इंटरनेट बैंकिंग सिर्फ अपने कंप्यूटर से करना ना कि साइबर कैफे, इंटरनेट बैंकिंग इस्तेमाल करने के बाद उसे लॉग-आउट करना, मोबाइल नंबर को खाते में अपडेट कराना ताकि खाते के लेन-देन की जानकारी प्राप्त हो सकें।
- एटीएम में प्रभावी कैमरा - इससे अपराधी द्वारा राशि आहरण की स्थिती में उसकी पहचान सुनिश्चित होगी।
- मोबाइल द्वारा स्थानीय भाषा में जानकारी - ग्राहकों को स्थानीय अथवा सरल भाषा में लगातार संदेश देने से वे लॉटरी, नौकरी या अन्य प्रलोभन से बच सकते है।

साइबर अपराध की रोकथाम हेतु दंडात्मक उपाय

साइबर अपराध एक दंडनीय अपराध है और इसकी रिपोर्टिंग तुरंत ही की जानी चाहिए। स्थानीय पुलिस स्टेशन या मुख्य नियंत्रण कक्ष (नंबर 100) को पीड़ित व्यक्ति या अपराध की जानकारी रखनेवाला अन्य व्यक्ति भी ऑनलाइन रिपोर्टिंग कर सकता है।

उपसंहार

एक ओर कोरोना वायरस ने दुनिया को तहस-नहस कर दिया तो दूसरी ओर साइबर अपराधों ने बैंकिंग जगत को अपने चपेट में ले लिया है। सूचना प्रौद्योगिकी और डिजिटलीकरण के दौर में विशेषकर साइबर अपराध एक गंभीर चुनौती के रूप में उभरने लगे हैं। ऐसा होना स्वाभाविक भी है क्योंकि पैसा अब न केवल मूर्त रूप में बल्कि ज्यादातर इलेक्ट्रानिक माध्यम से अंतरण हो रहा है। जालसाजों के लिए सूचना के माध्यम से पैसे उड़ाना उनके बाएं हाथ का खेल बन गया है। साइबर सुरक्षा का अर्थ है सूचना को सुरक्षित रखना एवं सूचना प्रणालियों को अनधिकृत पहुँच से बचाना तथा उनके दुरूपयोग, प्रकटीकरण, विघटन, संशोधन, अवलोकन, निरीक्षण, रिकॉर्डिंग अथवा उनको नष्ट होने से सुरक्षित रखना।

बैंक अर्थव्यवस्था के वास्तविक सेक्टरों से संबद्धता के कारण डिपॉजिटरी संस्थान के रूप में सार्वजनिक धनराशि के कस्टोडियन या संरक्षक है। यदि बैंकों को ग्राहकों का विश्वास बरकरार रखना है तो आवश्यक है कि वे अपना कॉर्पोरेट गवर्नेन्स सुधारें, सुदृढ़ आईटी सिस्टम लगाएं, प्रभावी नीतियां और कार्यपद्धतियां बनाएं, मानदंडों का कड़ाई से अनुपालन करें, अपितु साइबर अपराधियों के खिलाफ कठोर कार्रवाई करने में कोताही ना बरतें।

बैंकों के प्रति ग्राहकों का विश्वास बदस्तूर रहें, उनके लेन-देन सुरक्षित रहें, उनमें गोपनीयता रहें और उनकी सूचनाओं का सत्यापन हो सके इसके लिए बैंकों को केवल कार्यालय या शाखा स्तर पर ही नहीं, बल्कि प्रत्येक कर्मचारी स्तर पर सजग एवं सतर्क रहना होगा।

*****

राजीव कुमार

पदनाम:- प्रबंधक
संस्था का नाम:- बैंक ऑफ इंडिया
मोबाइल नं. :- 8171666165
ई-मेल:- rajeev.Kumar2@bankofindia.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

आज का युग सूचना प्रौद्योगिकी का युग है। आज जीवन के प्रत्येक क्षेत्र में प्रौद्योगिकी ने अपनी विशिष्ट पहचान बनाई है। यह प्रौद्योगिकी की ही देन है कि हम हजारों किलोमीटर दूर बैठे व्यक्ति से फोन या मोबाइल इत्यादि के माध्यम से ऑडियो या वीडियो कॉल से बात करते हैं। भारत सहित पूरे विश्व में कोविड-19 (कोरोना महामारी) ने पिछले 2 वर्षों में जान और माल दोनों की काफी क्षति की है। इस स्थिति में केवल प्रौद्योगिकी ही एकमात्र सहारा बनकर सामने आयी है जिससे हमारे देश सहित दुनिया की अर्थव्यवस्था भले ही धीमी गति से चली, किंतु चलती रही है। आज स्कूल, कॉलेज, निजी एवं सरकारी कार्यालयों इत्यादि में सभी प्रकार की पढ़ाई या कामकाज आदि ऑनलाइन माध्यम से ही किए जा रहे हैं। आज ऑनलाइन क्लास लेने के लिए घरों में छोटे-छोटे बच्चों के हाथ में उनके माता-पिता ने ही स्मार्ट मोबाइल फोन दे दिया है। आजकल लगभग बैंकिंग से सभी सेवाओं एवं उत्पादों में सूचना प्रौद्योगिकी का काफी उपयोग किया जा रहा है। यहां तक कि कोरोना महामारी के बाद से तो इंटरनेट उपयोगकर्ताओं की संख्या में बहुत अधिक वृद्धि हुई है। इंटरनेट उपयोगकर्ताओं की जो संख्या मार्च 2020 में 55 प्रतिशत थी वह दिसम्बर 2021 में बढ़कर लगभग 80 प्रतिशत हो गयी है।

भारत में बैंकिंग व्यवस्था:

भारत इस वर्ष अपनी स्वतंत्रता का 75वां अमृत महोत्सव मना रहा है। हमारे देश में आजादी से पूर्व बैंकिंग व्यवस्था अत्यंत सीमित थी। देश के कुछ गिने चुने लोगों के पास ही बैंकिंग सुविधा उपलब्ध थी।

बैंकिंग और बैंकिंग में साइबर अपराध को समझने से पूर्व भारत में बैंकों के इतिहास के बारे में जानना भी समीचीन होगा। **बैंकों को किसी भी देश की अर्थव्यवस्था का मेरुदंड माना जाता है।** हमारे देश में **प्रथम बैंक** 1770 **में 'बैंक ऑफ़ हिन्दुस्तान'** के नाम से स्थापित हुआ था फिर **1806 में 'बैंक ऑफ़ बंगाल'**, **1840 में 'बैंक ऑफ बाम्बे'** तथा **1843 में 'बैंक ऑफ मद्रास'** की स्थापना की गई। उक्त तीनों बैंकों का विलय कर बाद में इसका नाम **'इंपीरियल बैंक ऑफ़ इंडिया' भारतीय रिज़र्व बैंक अधिनियम, 1934** के अनुसार **01 मार्च 1935 को भारतीय रिज़र्व बैंक** की स्थापना की गई जो कि पूरी तरह से भारत सरकार का बैंक है। 01 **जुलाई, 1955 को इंपीरियल बैंक ऑफ़ इंडिया का राष्ट्रीयकरण** किया गया तथा इसका नाम बदलकर **भारतीय स्टेट बैंक (स्टेट बैंक ऑफ़ इंडिया)** कर दिया गया। हमारे देश में सन् 1969 में तत्कालीन भारत सरकार ने **19 जुलाई 1969 को 14 बड़े वाणिज्यिक बैंकों का राष्ट्रीयकरण** किया। इसके बाद, 15 अप्रैल, **1980 को 6 अन्य वाणिज्यिक बैंकों का राष्ट्रीयकरण** किया गया। अभी तक किए गए बैंकों के विलय के बाद आज सार्वजनिक क्षेत्र के बैंकों की कुल संख्या 12 रह गई हैं जिसमें भारतीय स्टेट बैंक शामिल है।

बैंकिंग में साइबर अपराध:

जिस प्रकार सूचना प्रौद्योगिकी ने जीवन के सभी क्षेत्रों को प्रभावित किया है, उसी प्रकार, बैंकिंग भी आज पूरी तरह से प्रौद्योगिकी-युक्त बन चुकी है आज बैंकिंग में अधिकांश कामकाज ऑनलाइन या प्रौद्योगिकी की सहायता से कर सकते हैं। हालांकि, कुछ कार्यों जैसे ऋण मंजूरी के समय साक्ष्यों या व्यक्ति की पहचान करने के लिए ग्राहक की शाखा में उपस्थिति अनिवार्य मानी जाती है। लेकिन जहां प्रौद्योगिकी ने बैंकिंग को फर्श से अर्श पर पहुंचाने का कार्य किया है, वहीं बैंकिंग में होने वाली भौतिक धोखाधड़ी संबंधी मामलों की अपेक्षा साइबर अपराधों में बेतहाशा वृद्धि हुई है। हालांकि, हम सब आज साइबर अपराध के बारे में भली भांति जानते हैं।

वास्तव में साइबर अपराध वह अपराध होता है जिसमें किसी न किसी रूप में इलेक्ट्रानिक उपकरणों या सूचना प्रौद्योगिकी का उपयोग किया जाता है। संयुक्त राष्ट्र संघ (यूएनओ) के अनुसार –''साइबर अपराध वर्तमान में अपराधों में सबसे जघन्य अपराध है, जो विश्व समुदाय और मानवता के लिए एक खतरा है।'' आजकल बैंकिंग में प्रौद्योगिकी के बढ़ते उपयोग के कारण, आपराधिक प्रवृत्ति के लोग आम ग्राहकों के साथ बैंकिंग में साइबर अपराध कर रहे हैं। इसलिए, किसी ने बिल्कुल सही कहा है कि **''सावधानी हटी, दुर्घटना घटी''**, विभिन्न प्रकार के अपराधों को करने वाले हमारी किसी भी छोटी से छोटी चूक का लाभ उठाते हैं और असावधानी बरतने वालों के साथ धोखाधड़ी करते हैं। साइबर अपराधों को बैंकिंग के परिप्रेक्ष्य में इस प्रकार समझा जा सकता है:

1. **साइबर स्टॉलिंग:** किसी व्यक्ति द्वारा इलेक्ट्रानिक संचार माध्यमों का उपयोग करना जिससे वह किसी व्यक्ति से बार-बार संपर्क करता है और उसकी व्यक्तिगत या निजी जानकारी प्राप्त करने का प्रयास करता है।
2. **विशिंग:** यह एक ऐसा प्रयास है जिसमें ग्राहक की आईडी, नेट बैंकिंग पासवर्ड, एटीएम पिन, ओटीपी, कार्ड समाप्ति की तारीख, सीवीवी इत्यादि को फोन के माध्यम से प्राप्त किया जाता है।
3. **साइबर बिलिंग:** इलेक्ट्रानिक अथवा संचार माध्यमों के उपयोग अर्थात् कंप्यूटर, मोबाइल, लैपटॉप इत्यादि के माध्यम से किया जाने वाला ऐसा शोषण है जिससे ग्राहक को काफी मानसिक परेशानी होती है।
4. **स्मिशिंग:** स्मिशिंग एक ऐसी धोखाधड़ी है जिसमें धोखेबाज व्यक्ति फर्जी फोन के माध्यम से पीड़ित को कॉलबैक करता है जिसमें फर्जी वेबसाइट या फोन के माध्यम से फर्जी विषय सामग्री दिखाई जाती है।
5. **डेबिट कार्ड या क्रेडिट कार्ड संबंधी धोखाधड़ी:** किसी दूसरे व्यक्ति के एटीएम कार्ड या क्रेडिट कार्ड के माध्यम से अनधिकृत रूप से खरीदारी करने या पैसा निकालने के लिए इस प्रकार की धोखाधड़ी का उपयोग किया जाता है।
6. **व्यक्तिगत पहचान की चोरी करना:** किसी अन्य व्यक्ति के इलेक्ट्रानिक हस्ताक्षर, पासवर्ड या अन्य किसी विशिष्ट पहचान का उपयोग करके इस प्रकार की धोखाधड़ी की जाती है।
7. **फिशिंग:** यह एक ऐसी धोखाधड़ी है जिसमें ग्राहक आईडी, पिन, क्रेडिट/ डेबिट कार्ड नंबर, कार्ड समाप्ति की तारीख, सीवीवी नं. इत्यादि को ई-मेल के माध्यम से मांगने का प्रयास किया जाता है।
8. **स्मैसिंग:** जब किसी व्यक्ति को ई-मेल, एसएमएस एवं ऐसे ही किसी अन्य माध्यम से कोई अनधिकृत वाणिज्यिक मेल प्राप्त होता है उसे स्मैसिंग कहते हैं।
9. **रैनसमवेयर:** यह एक कंप्यूटर वायरस है जो डेस्कटॉप, लैपटॉप, मोबाइल फोन इत्यादि जैसे संचार माध्यमों में स्टोर की गई फाइलों इत्यादि को नुकसान पहुंचाता है, जिससे वह डेटा या आंकड़े होल्ड हो जाते हैं।

पीड़ित व्यक्ति को उसकी फाइल वापस करने या उसकी डिवाइस को सही स्थिति में पाने के लिए पैसा मांगा जाता है। इसमें अपराधी जल्दी से पकड़ में नहीं आता है और उनका पता लगाना भी बहुत कठिन होता है।

10. **वायरस, वार्म्स एवं टॉजन होर्स:** कंप्यूटर वायरस एक प्रोग्राम है जिससे कंप्यूटर की फाइल को नुकसान पहुंचता है या उसमें बदलाव आ जाता है। वार्मस: एक ऐसा मैलेसियस प्रोग्राम है जो कि स्थानीय डिवाइस, नेटवर्क शेयर इत्यादि पर बार-बार उसकी कॉपी करता है। ट्रोजन: कोई वायरस नहीं है। यह एक त्रुटिपूर्ण प्रोग्राम है जो कि दिखने में सही प्रतीत होता है। इसके माध्यम से व्यक्तिगत एवं गोपनीय जानकारी चुराने का प्रयास किया जाता है।
11. **ई-मेल स्पूफिंग:** अक्सर आपके इनबॉक्स या स्पैम बॉक्स में कई तरह के इनाम देने वाले या बिजनेस पार्टनर बनाने वाले या फिर लॉटरी निकलने वाले मेल आते हैं। ये सभी मेल किसी दूसरे शख्स के -ई-मेल या फर्जी ई-मेल आईडी के जरिए किए जाते हैं। किसी दूसरे के ई-मेल पते का इस्तेमाल करते हुए गलत मकसद से दूसरों को ई-मेल भेजना इसी अपराध की श्रेणी में आता है। हैकिंग, फिशिंग, स्पैम और वायरस, स्पाईवेयर फैलाने के लिए इस तरह के फर्जी ई-मेल का अधिक उपयोग किया जाता है।
12. **हैकिंग:** किसी कंप्यूटर, डिवाइस, इंफॉर्मेशन सिस्टम या नेटवर्क में अनधिकृत रूप से घुसपैठ करना और डेटा से छेड़छाड़ करना 'हैंकिंग' कहलाता है। यह 'हैकिंग' उस सिस्टम की फिजिकल एक्सेस और रिमोट एक्सेस के जरिए भी हो सकती है। जरूरी नहीं कि ऐसी 'हैकिंग' के दौरान उस सिस्टम को नुकसान पहुंचा ही हो। अगर कोई नुकसान नहीं भी हुआ है तो भी घुसपैठ करना साइबर अपराध के तहत आता है जिसके लिए सजा का प्रावधान है।
13. **स्पाईवेयर फैलाना:** अक्सर कंप्यूटर में आए वायरस और स्पाईवेयर को हटाने पर लोग ध्यान नहीं देते हैं। उनके सिस्टम से होते हुए ये वायरस दूसरों तक पहुंच जाते हैं। हैकिंग, डाउनलोड, कंपनियों के गोपनीय नेटवर्क, वाईफाई कनेक्शन और असुरक्षित फ्लैश ड्राइव, सीडी के जरिए भी वायरस फैल जाते है। वायरस बनाने वाले अपराधियों की पूरी एक इंडस्ट्री है जिनके खिलाफ वक्त बेवक्त कड़ी कार्रवाई होती रहती है।

साइबर अपराध को लेकर सख्त कानून:

भारत में साइबर अपराधों में तेजी से इजाफा हो रहा है। सरकार ऐसे मामलों को लेकर बहुत गंभीर है। भारत में साइबर अपराध के मामलों में सूचना तकनीक अधिनियम, 2000 और सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 लागू हैं, मगर इसी श्रेणी के कई मामलों में भारतीय दंड संहिता (आईपीसी), कॉपीराइट कानून, 1957, कंपनी कानून, सरकारी गोपनीयता कानून और यहां तक कि आतंकवाद निरोधक कानून के तहत भी कार्रवाई की जा सकती है। साइबर अपराध के कुछ मामलों में सूचना प्रौद्योगिकी विभाग की ओर से जारी किए गए आई.टी. नियम 2011 के तहत भी कार्रवाई की जाती है। इस कानून के तहत निर्दोष लोगों को साजिश से बचाने के लिए भी प्रावधान हैं, लेकिन कंप्यूटर, इंटरनेट और दूरसंचार इस्तेमाल करने वालों को हमेशा सतर्क रहना चाहिए।

उपर्युक्त विभिन्न प्रकार के साइबर अपराधों के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 77 बी, सूचना प्रौद्योगिकी (संशोधन) अधिनियम 2008 की धारा 42(ए), धारा 66, 66 डी, आईपीसी की धारा 268 379, 405, 406, 417, 419, 420 और 465 के तहत अपराध साबित होने पर 3 वर्ष की जेल या 5 लाख रुपये तक जुर्माना हो सकता है। देश की सुरक्षा को खतरा पहुंचाने के लिए फैलाए गए वायरस पर आतंकवाद से जुड़ी धारा 66 (एफ) भी लगाई जाती है। आईपीसी की धारा लगाए जाने का प्रावधान भी है। दोष साबित होने पर 3 वर्ष तक की जेल या जुर्माना हो सकता है।

इसके अतिरिक्त विभिन्न फर्जी वेबसाइट के माध्यम से खरीदारी करवाने हेतु इंटरनेट बैंकिंग या एटीएम डेबिट/क्रेडिट कार्ड आदि का उपयोग किया जाता है जिससे ग्राहकों के साथ धोखाधड़ी होती है। साइबर अपराधों की संख्या दिन-प्रतिदिन बढ़ती जा रही है और इसके शिकार वे लोग या वे ग्राहक होते हैं जिन्हें तकनीकी का कम ज्ञान है या जिनमें सतर्कता एवं सूचना प्रौद्योगिकी संबंधी नियमों, कानूनों की जानकारी कम होती है। किसी भी ग्राहक को प्रौद्योगिकी के इस युग में अधिक सतर्क एवं सजग रहने की आवश्यकता है अन्यथा उन्हें भारी नुकसान उठाना पड़ सकता है।

आजकल अधिकांश लेन-देन ऑनलाइन हो रहे हैं। बैंकिंग के इस बदलते स्वरूप से बैंकिंग धोखाधड़ियों की संख्या भी काफी बढ़ गई है। बैंकों में लगातार बढ़ते अपराधों में साइबर अपराध सर्वाधिक हैं। साइबर अपराधों को रोकने के लिए आवश्यक सुरक्षात्मक उपाय इस प्रकार हैं:

1. बैंक खातों की जानकारी किसी अन्य व्यक्ति को न दें।
2. एटीएम कम डेबिट या क्रेडिट कार्ड की जानकारी किसी अन्य व्यक्ति को न दें।
3. केवाईसी संबंधी जानकारी किसी के साथ साझा न करें।
4. इंटरनेट का सुरक्षित उपयोग करें।
5. मोबाइल या अपने कंप्यूटर में पिन, खाता संबंधी जानकारी न रखें।
6. किसी भी व्यक्ति से अपनी व्यक्तिगत जानकारी साझा न करें।
7. एटीएम से पैसा लेते समय किसी भी अनजान व्यक्ति से सहायता न लें।
8. साइबर कैफे में कभी भी इंटरनेट बैंकिंग संबंधी लेन-देन न करें।
9. लॉटरी निकलने संबंधी मेल या फोन कॉल का जवाब न दें।
10. विभिन्न अनजान ई-मेल आदि को न खोलें।
11. असुरक्षित पाथ से कभी भी कुछ डाउनलोड न करें।
12. नि:शुल्क एंटीवायरस को अपने कंप्यूटर में सक्रिय न करें।
13. ग्राहक ऑनलाइन लेन-देन संबंधी जानकारी तुरंत अपनी शाखा को दें।
14. शाखाओं को ऑनलाइन लेन-देन संबंधी धोखाधड़ी की सूचना तत्काल नियंत्रक कार्यालय को देनी चाहिए।
15. आम जनता हेतु एटीएम मशीनों तथा शाखा परिसरों में साइबर अपराधों के बारे में जागरूकता संबंधी सूचनाएं प्रदर्शित की जानी चाहिए।
16. विभिन्न अखबारों, टीवी, रेडियो, सिनेमा हॉल, सार्वजनिक बस अड्डे, स्टेशन, एयरपोर्ट एवं सोशल मीडिया पर साइबर अपराध संबंधी जागरूकता फैलाएं।
17. 'इलाज से बचाव बेहतर': साइबर अपराध से बचाव हेतु सतर्कता ही मुख्य साधन है। इस नियम का पालन करें एवं करवाएं।
18. साइबर अपराधों के विवेचकों को निरंतर तकनीकी ज्ञान प्रदान करते रहें।

निष्कर्ष: प्रौद्योगिकी ने जहां मनुष्य को त्वरित बैंकिंग सेवाएं उपलब्ध कराई हैं, वहीं ऑनलाइन लेन-देनों में जोखिम भी ज्यादा बढ़ा है। साइबर अपराधों से बचने के लिए सावधानी बेहद जरूरी है। थोड़ी सी लापरवाही आपके खाते को पूरी तरह से खाली करा सकती है। उदाहरण के लिए नागपुर शहर के झिंगाबाई टाकली कॉलोनी के रहने वाले श्री मोहन रमन गेडाम (बदला हुआ नाम) का बाजार में शॉपिंग करते समय किसी व्यक्ति ने स्मार्ट मोबाइल फोन चुरा लिया। उस फोन में उनके अलग-अलग बैंकों के बैंक खातों के इंटरनेट बैंकिंग यूजरआईडी एवं पासवर्ड, ट्रांजेक्शन पासवर्ड आदि भी स्टोर थे। मोबाइल चुराने वाले ने उसी रात्रि में उनके

विभिन्न बैंकों के बैंक खातों से लगभग 3 लाख रुपए इंटरनेट बैंकिंग का उपयोग करते हुए निकाल लिया। पुलिस में एफआईआर भी दर्ज हो गई लेकिन न मोबाइल फोन मिला और न ही अभी तक उनका पैसा वापस मिला है। आपने देखा कि उनके द्वारा बैंकिंग की संपूर्ण जानकारी अपने मोबाइल फोन में रखी गई थी जिसका फायदा मोबाइल चुराने वाले व्यक्ति ने उठाया।

इस प्रकार, कहा जा सकता है कि साइबर अपराध से बचने के लिए संबंधित बैंकों को पूरी सतर्कता के साथ अपनी इंटरनेट बैंकिंग को सुरक्षित करना चाहिए तथा समय-समय पर इसकी समीक्षा भी करते रहना चाहिए ताकि उसमें निरंतर सुधार किया जाता रहे। इसके साथ ही, बैंक ग्राहकों को भी ऊपर बताई गई विभिन्न अपेक्षित सावधानियों को बरतना चाहिए ताकि उनका पैसा सुरक्षित रहे। अंत में, हम तो यही कहेंगे कि–

बैंकिंग लेन-देन करते समय, सदैव रहें सतर्क और सावधान।
न साझा करें किसी से खाते की जानकारी, वरना हो सकता है नुकसान।।

संदर्भ सामग्री:

1. **राष्ट्रीय अपराध रिकार्ड ब्यूरो की वेबसाइट।**
2. **पुलिस अनुसंधन एवं विकास ब्यूरो, नई दिल्ली की वेबसाइट।**

*****

विजय रामदास

पदनाम:- प्रबंधक
संस्था का नाम:- यूनियन बैंक ऑफ़ इंडिया
मोबाइल नं. :- +94 7674027611
ई-मेल:- vijju20071988@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

साइबर अपराध कंप्यूटर अथवा इंटरनेट के माध्यम से किसी भी आपराधिक गतिविधि से संबंध रखता है। अन्य शब्दों में, किसी भी कंप्यूटर अथवा इलेक्ट्रॉनिक उपकरण और इंटरनेट के जरिये अपराधी द्वारा किये गए अनधिकृत धन स्थानांतरण एवं धनाहरण जैसे कई अवैध कार्यों को डिजिटल अनाचार या साइबर अपराध के नाम से निर्दिष्ट किया जा सकता है।

21वीं शताब्दी में साइबर क्राइम अधिकतम घातक व प्रतिशोधी अस्त्र के रूप में उभरा है जिसे कोई भी व्यक्ति किसी को धमकाने या धोखा देने के लिए इस्तेमाल कर सकता है।

आज की इस विश्वव्यापी दुनिया को रुचिकर बनाने के लिए बैंकिंग क्षेत्र अपने उपभोगताओं को ऑनलाइन बैंकिंग और क्रेडिट कार्ड सेवाएं जैसे अनेक सेवाएं प्रदान करता है। ऑनलाइन विकल्प के माध्यम से ग्राहकों को बैंक की सभी सुविधाएं किसी भी समय उपलब्ध होने की सम्भावना है।

हालाकि यह बोधगम्य है कि कंप्यूटर जिंदगी का अनिवार्य अंग बन गए हैं लेकिन इन उपकरणों से ऐसा परिमंडल विकसित हुई है जिससे साइबर अपराधों को सहायता मिलती है। तेजी से बदलते परिवेश और सूचना प्रौद्योगिकी क्षेत्र के अहम योगदान की सहायता से आज साइबर अपराध प्रमुख चुनौती प्रस्तुत करते हैं।

कंप्यूटर हैकर ऑनलाइन बैंकिंग प्रणाली का अनुचित लाभ उठाते हुए बैंक वेबसाइट और ग्राहकों के बैंक खातों को सेंधकर उपभोक्ता के खातों में अव्यवस्था और धन की चोरी करते हैं।

देश के विकास और वृद्धि को तय करने वाले आधार स्तंभों में से अर्थव्यवस्था एक है। बैंकिंग क्षेत्र को अर्थव्यवस्था के अहम अंग के रूप में माना जाता है। नित्य व्यापर के परिचालन में नकद, चेक और डिमांड ड्राफ्ट की तुलना में आज डेबिट कार्ड, क्रेडिट कार्ड, इंटरनेट बैंकिंग, मोबाइल बैंकिंग इत्यादि जैसे ऑनलाइन बैंकिंग प्रणाली का अधिक इस्तेमाल होता है।

बैंकिंग क्षेत्र का उद्देश्य अपनी सेवाओं का विस्तार कर नवीनीकरण के माध्यम से उत्तम ग्राहक सेवा उपलब्ध कराना है। फिर भी साइबर अपराध एक घोर समस्या के रूप में बाधा उत्पन्न करता है। इंटरनेट पर जो कुछ भी जानकारी उपलब्ध है उसे साइबर अपराधी आसानी से हासिल कर सकते हैं।

इंटरनेट, एटीएम, मोबाइल बैंकिंग इत्यादि जैसे अनेक विकल्पों के जरिये परिवर्धित ऑनलाइन मान्यता के कारण भारत देश में डेबिट कार्ड व क्रेडिट कार्ड की मात्रा में वृद्धि देखी गई है।

साइबर अपराधों के कारण:

- **आंकड़ों की सरल उपलब्धता:** एक बार जब साइबर आक्रामक किसी भी कंप्यूटर प्रणाली में प्रवेश प्राप्त करता है, तो वह संभवतः ग्राहकों के गोपनीय वित्तीय दस्तावेज सहित निजी विवरणों को हासिल करने की क्षमता रखता है जिसका अनुकरण अथवा छोटे निराकरणीय उपकरण में अंतरित किया जा सकता है।
- लम्बे समय तक यंत्रो के उपयोग के कारण डिजिटल थकान, घर बैठे कार्यचालन करना इत्यादि से ऑनलाइन वित्तीय गबन में वृद्धि देखी गयी है।
- कुछ विशेषज्ञों के अनुसार प्रचंड महंगाई, बेरोजगारी, अल्प परिमाण में नौकरी के अवसर इत्यादि जैसे सामाजिक परिस्थितियां देश में बढ़ते साइबर अपराधों के प्रमुख कारक हैं।
- कम्पूटरों में संचित गोपनीय आंकड़ो और जानकारी को सुरक्षित रखने हेतु कंप्यूटर प्रणाली का इस्तेमाल करने वाले सभी अधिकारियों को अत्यंत सावधान व सतर्क रहना चाहिए। कोई भी लापरवाही साइबर अपराधियों को खास उपकरणों व अभिलेखों तक पहुंचने में सरल बनाता है।
- कोविड19 के प्रकोप ने लोगों को डिजिटल जिंदगी की ओर रुख करने पर मजबूर किया है। समाचार पढ़ने, भोजन आर्डर करना इत्यादि से लेकर चीजों के खरीदने तक, बुज़ुर्ग हो या नौजवान, सभी नागरिको को ऑनलाइन प्रणाली सीखनी ही थी। जब जन समूह घर बैठे ऑनलाइन लेन-देन से आराम की अनुभूति कर रहे थे, वही साइबर अपराधी लोगों के प्रौद्योगिकी पर आश्रय होने का गलत फायदा उठाते हुए एक से एक ऑनलाइन अपराध की ओर बढ़ते गए।
- कार्यालय व्यवस्था में उच्च स्तरीय सुरक्षा प्रणाली के अस्तित्व में होने के कारण कर्मचारी अधिक सुरक्षा के साथ लैपटॉप व कम्प्यूटरो पर कार्य कर सकते हैं लेकिन जब लोग घर बैठे कार्यरत होते हैं तो घरों में डिजिटल व गोपनीय उपाय न होने के कारण लापरवाही से डिजिटल प्रमाण छोड़ने की अधिक सम्भावना है जिसका अवैध लाभ उठाया जा सकता है।

बैंकिंग क्षेत्र से संबंधित साइबर अपराध: साइबर अपराधों को चार श्रेणियों में वर्गीकृत किया जा सकता है, जो कुछ इस प्रकार है:

- साइबर छल।
- साइबर हिंसा।
- साइबर अश्लीलता।
- साइबर अतिक्रमण।

ऑनलाइन बैंकिंग क्षेत्र से संबंधित साइबर अपराध साइबर छल के अंतर्गत समाविष्ट होते है।

- **एटीएम स्किम्मिंग और पॉइंट ऑफ़ सेल (POS) अपराध:** एटीएम मशीन एवं पीओएस प्रणाली को जोखिम में डालने के लिए यह एक ऐसी युक्ति है जहां मशीन कुंजीपटल के ऊपर स्किम्मिंग उपकरण को स्थित किया जाता है अथवा यंत्र को कार्ड रीडर से जोड़ दिया जाता है जिससे लोग उसे वास्तविक कुंजीपटल या मशीन का अंग मान सकें।
- **क्रेडिट/डेबिट कार्ड कपट:** जब कोई ग्राहक किसी ऑनलाइन भुगतान के लिए अपने क्रेडिट कार्ड अथवा डेबिट कार्ड का इस्तेमाल करता है तब कोई अन्य व्यक्ति दुर्भावपूर्ण इरादों से उस ग्राहक के कार्ड की जानकारी व पासवर्ड को हैक कर उसका दुरूपयोग करने की क्षमता रखता है।
- **डीएनएस कैश विषाक्तीकरण:** कंपनी के संजाल में पहले प्राप्त सवालों के परिणाम को पकड़कर डीएनएस सर्वर संकल्प प्रतिक्रिया समय को बढ़ाने की चेष्टा करते हैं। डीएनएस सॉफ्टवेयर में कमजोरी

को शोषित कर डीएनएस सर्वर पर विषाक्तीकरण आक्रमण निष्पादित किए जाते हैं । इसके परिणामस्वरूप सर्वर भूल से डीएनएस प्रतिक्रियाओं को अभिषृष्ट करते है जिससे वह आधिकारिक स्त्रोत को सुनिश्चित करता है। जो उपभोक्ताएं समान निवेदन करते है उन सभी को अशुद्ध प्रविष्टियां दी जाती हैं।

- **हैकिंग (Hacking):** हैकिंग एक ऐसा साइबर अपराध है जिसमें कोई व्यक्ति अवैध रूप से ग्राहक के खातों अथवा बैंक वेबसाइट में प्रवेश हासिल कर सुरक्षा प्रक्रिया को बिगाड़ने की चेष्टा करता है।
- **की लॉगिंग (Key Logging):** यह गुप्त रूप से कुंजीपटल पर दबाए गए कुंजी को अभिलेकन करने की प्रक्रिया है। इस कारण वह उपभोक्ता इस बात से अनजान है कि उसकी प्रत्येक गतिविधि पर नजर रखी जा रही है।
- **मैलवेयर आधारित आक्रमण:** यह ऑनलाइन बैंकिंग सेवाओं के अधिकतम खतरनाक व तेजी से बढ़ते आतंको में से एक है। ऐसे हमलो में एक दुर्भावनापूर्ण कूट तैयार किया जाता है। उदाहरण के लिए ज़ीउस मैलवेयर आधारित आक्रमण का एक नमूना है।
- **फार्मिंग (Pharming):** इसका अनुकरण इंटरनेट के माध्यम से होता है। जब ग्राहक बैंक के वेबसाइट में प्रवेश करता है तब आक्रामक बैंक वेबसाइट का ऐसे तरीके से अपहरण करते हैं जिससे उस ग्राहक को, उसके जाने बगैर, नकली वेबसाइट पर ले जाया जाता है एवं यह वेबसाइट बैंक के मूल वेबसाइट के समरूप जान पड़ता है।
- **फिशिंग (Phishing):** यह जालसाजी का ऐसा प्रकार है जहां वास्तविक स्त्रोत से प्रतीत होने वाले ई-मेल से डेबिट/ क्रेडिट कार्ड संख्या, ग्राहक आईडी, पिन संख्या, सीवीवी संख्या, कार्ड समाप्ति दिनांक इत्यादि जैसे व्यक्तिगत जानकारी को चुराया जाता है।
- आजकल फिशिंग करने वाले अपराधि **एसएमएस (Smishing)** और **मोबाइल (Voice Phishing)** का भी इस्तेमाल करते हैं।
- **स्पाईवेर (Spyware):** यह कपटपूर्ण उद्देश्यों के उपयोग हेतु ऑनलाइन बैंकिंग प्रत्यय को चुराने की अति साधारण पद्धति है। स्पाईवेर कम्प्यूटरों और वेबसाइटों के बीच जानकारी को प्राप्त अथवा प्रसार कर प्रचलित होता है।
- **वायरस:** यह स्व-प्रतिलिपिकारी प्रोग्राम का एक प्रकार है जो साध्य कूटों अथवा दस्तावेजों में स्वयं को भीतर डालते हुए प्रदूषित करने की क्षमता रखता है। यह प्रोग्राम साध्य फाइलों पर बुरा असर करते हैं जिससे संक्रमित फाइल असाधारण रूप से आचरण करती है। यह प्रोग्राम फाइल व परिचालन प्रणाली से संयोजन के जरिये फैलता है।
- **वाटरिंग होल आक्रमण (Watering Hole):** वाटरिंग होल साइबर कपट को फिशिंग से उत्पन्न एक शाखा के रूप में सुविचारित किया जाता है। यह एक ऐसी योजना है जहां आक्रामक अनुमान करते हुए यह देखता है कि संस्थाए/ बैंक अक्सर किन वेबसाइटों का उपयोग करती है और इन वेबसाइटों को मैलवेयर से संक्रमित करने की चेष्टा करता है।

भारत देश में बैंक पर साइबर आक्रमण के उदाहरण:

कॉसमॉस बैंक पर साइबर आक्रमण: वर्ष 2018 में पुणे शहर में स्थित कॉसमॉस बैंक पर साइबर आक्रमण हुआ था। जब हैकरों ने पुणे में स्थित कॉसमॉस सहकारी बैंक लि. से रुपये 14.42 करोड़ चुराए थे तब भारत देश में सम्पूर्ण बैंकिंग क्षेत्र व्याकुल हो उठा।

साइबर अपराधों का बैंकों पर प्रभाव: साइबर अपराध के आतंक से बैंको पर संभवतः दीर्घावधिक और भयानक परिणाम हो सकते हैं।

साइबर अपराधों के कारण बैंकों पर कुछ नतीजे निम्नानुसार हैं:

- वित्तीय नुकसान।
- गोपनीय जानकारी का उल्लंघन।
- कानूनी परिणाम।
- प्रतिष्ठा एवं परिचालन संबंधित जोखिम इत्यादि।

भूराजनीतिक और सार्वभौमिक बृहत् अर्थशास्त्र संबंधी हालातों के कारण पूरे विश्व में बैंकिंग उद्योग को कठिन परिस्थिति का सामना करना पड़ रहा है जो कि विचारोत्तेजक है।

साइबर अपराधों पर प्रतिबंध लगाने के तरीके: बैंकिंग क्षेत्र में साइबर अपराध खतरनाक ढंग से बढ़ गए है जिससे महत्वपूर्ण आर्थिक नुक्सान हुए हैं।

साइबर सुरक्षा नीति से संबंधित तमाम मामलो के प्रभावकारी कार्यान्वयन हेतु सरकार ने राष्ट्रीय सुरक्षा परिषद के साथ अंतर-विभागीय सूचना सुरक्षा कर्मी दल (ISTF) को केन्द्रक अभिकरण के रूप में स्थापना किया है।
साइबर अपराध के रोकथाम के प्रमुख उपाय निम्नलिखित हैं :

- साइबर अपराध को पहचान कर उसका निरीक्षण प्रत्येक व्यक्ति द्वारा करना चाहिए। तभी हम सब साइबर अपराध को जड़ से निकालने में सफल रहेंगे।
- साइबर सुरक्षा को संबोधित करने वाले नीतियों को सूत्रित करना चाहिए। प्रत्येक कर्मचारी को नीति के अनुसार हर तीन महीने में पासवर्ड अनिवार्य रूप से बदलना चाहिए।
- ग्राहकों से संबंधित आंकड़ों को नियमित रूप से सुरक्षित रखते हुए उनका प्रतिलिपि अथवा बैक-अप रखना चाहिए।
- प्रशासकों को कर्मचारियों द्वारा अनधिकृत सॉफ्टवेयर का अधोभारण तथा पदासीन करने पर प्रतिबन्ध लगाना चाहिए।
- बैंक नीतियों द्वारा उचित अनुमोदन संबंधी प्रोटोकॉल को समय-समय पर निर्धारित करना चाहिए।
- सूचना प्रौद्योगिकी अधिनियम को संशोधित कर साइबर अपराध की परिभाषा के अतिरिक्त अधिनियम के क्षेत्रातित अधिकार होने वाले सूचियों को भी शामिल करना चाहिए।
- **बैंक कर्मचारियों का प्रशिक्षण**: सभी कर्मचारियों व ग्राहकों को साइबर अपराध के जोखिम और अज्ञात सूत्रों से ई-मेल संलग्नक को खोलने अथवा अपलोड करने के खतरों से अवगत कराना चाहिए।
- कर्मचारियों को बैंक से संबंधित गोपनीय जानकारी को जाहिर करने से वर्जित करना चाहिए।
- बैंक के कॉल सेंटर में कार्यरत कर्मचारियों को ग्राहक के परिचय की जांच करनी चाहिए जिससे किसी अन्य ग्राहक की जानकारी जाहिर न हो और साथ ही ग्राहक की असलियत का पता लग सके।
- **उपकरण अथवा मशीनों का नियमित रूप से दृढीकरण:** बैंक के सूचना प्रौद्योगिकी विभाग को यह सुनिश्चित करना चाहिए कि बैंक में प्रत्येक कार्यस्थल और इंटरनेट से जुड़े हर उपकरण फायरवॉल के साथ सक्षम हो। फायरवॉल अप्राधिकृत स्त्रोत से आये सभी संचार व्यवस्था को अवरुद्ध करने की क्षमता रखता है।
- बैंक के आईटी विभाग को यह सुनिश्चित करना चाहिए कि बैंक के सभी परिचालन प्रणालियों का नियमित रूप से सुरक्षा अद्यतनीकरण किया जाए।
- सभी प्रणालियों में स्पाईवेयर व वायरस विरोधक सॉफ्टवेयर संस्थापित करना चाहिए जिससे बैंक के संजाल में द्वेषपूर्ण सॉफ्टवेयर का पता लग सके।

- जहां संभव हो, बैंको को दो-कारक प्रमाणीकरण (2FA) ऐप अथवा भौतिक सुरक्षा कुंजियों का इस्तेमाल कर तमाम ऑनलाइन खातों में (2FA) सक्षम बनाना चाहिए।

उपसंहार: प्रत्येक बैंक अपने दैनिक गतिविधियों के लिए विविध प्रकार की परिचालन प्रणालियों का इस्तेमाल करता है। अतः बैंको को यह सुनिश्चित करना चाहिए कि आतंरिक सूचना प्रौद्योगिकी संबंधित लेखापरीक्षा प्रणालियां व नियंत्रक निरंतर रूप से कार्यान्वित रहें।

बैंकिंग क्षेत्र किसी भी देश के अर्थव्यवस्था का अति महत्वपूर्ण आधार स्तंभ है। अतः न केवल बैंक के आईटी विभाग बल्कि विश्व व्यापी स्तर पर सभी बैंक कर्मचारियों और ग्राहकों को एकजुट होकर साइबर अपराध को जड़ से नामोनिशान मिटाना चाहिए।

अंत में "संपूर्ण साइबर सुरक्षा ही बैंक की असली सुरक्षा है।"

*****

विधि चंद्रकांत जटनिया

पदनाम:- अधिकारी
संस्था का नाम:- केनरा बैंक
मोबाइल नं. :- 9428058126
ई-मेल:- vidhijataniya@canarabank.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

सूचना प्रौद्योगिकी की क्रांति के बाद पूरी वैश्विक अर्थव्यवस्था के साथ-साथ हमारे बैंकिंग जगत में भी नयी क्रांति आ गयी। आज बैंकिंग क्षेत्र में सूचना प्रौद्योगिकी की वैकल्पिक डिलीवरी चैनलों के माध्यम से बैंकिंग में विभिन्न सुविधापूर्वक बदलाव आया है। बैंकिंग जगत में ग्राहकों को अपना काम करवाने जहां घंटों कतारों में खड़ा रहना पड़ता था, आज वह जैसे बीते दिनों की बात हो गयी है। आज कंप्यूटर, सूचना तथा संचार प्रौद्योगिकी तथा नयी तकनीकों ने बैंकिंग क्षेत्र को 24*7 घंटो तक असीमित विस्तृत किया है। आधुनिक बैंकिंग का स्वरूप 'कहीं भी' और 'कभी भी' बैंकिंग का एक नया ही अवतार लेकर ग्राहकों की सुविधा के लिए खड़ा है।

साइबर का इतिहास :

सूचनाओं के आदान-प्रदान के लिए सन 1966 में अमरीकी रक्षा विभाग के एडवांस रिसर्च प्रोजेक्ट्स ने सबसे पहले इलेक्ट्रोनिक विधियों को कंप्यूटर के माध्यम से एक दूसरों से जोड़कर एक नेटवर्क अर्पानेट (ARPANET) तैयार किया। इस नेटवर्क पर सन 1969 में चार विभिन्न प्रोग्राम प्रदान करने वाले कम्प्यूटरों को जोड़ा गया था। शुरुआत में रक्षा अनुसंधान से जुड़े कार्यक्रम के लिए इस नेटवर्क का उपयोग किया गया। सन 1989 में सारण की वैज्ञानिक टीम बरनस ली, आजकल जो पूरे विश्व में प्रसिद्ध है, ने वो वर्ल्ड वाइड वेब (www) को स्थापित किया था। यह वर्ल्ड वाइड वेब संग्रहण तथा संप्रेषण का मूल आधार बना। तब से लेकर आज तक वर्ल्ड वाइड वेब में कई नयी नयी उपलब्धि तथा सुविधा आती रही और आधुनिकता से सभर www सबको सुविधाएं पिरोसता रहा। उपग्रह प्रणाली, ब्रॉड बैंड, ऑप्टिकल फाइबर ने सूचनाओं के आदान-प्रदान को त्वरित कर दिया और इन सबसे ही हमारा आधुनिक युग सूचना प्रौद्योगिकी का युग बन गया। आज इन्हीं सब उपलब्धियों का फायदा हमारे बैंकिंग क्षेत्र को भी भरपूर हुआ है। आज के ग्राहक की संतुष्टि ही जैसे वैकल्पिक डिलीवरी चैनलों – मोबाइल बैंकिंग, नेट बैंकिंग आदि से हो गई है। कह सकते हैं –

"जी हां, कर ली दुनिया मुट्ठी में।"

साइबर अपराध का अर्थ :

कहते हैं हर आविष्कार व विकास के साथ-साथ उनके ध्वंस का भी आविष्कार हो जाता है। नए आविष्कार का ध्वंस ही साइबर अपराध की देन है। आज नयी-नयी तकनीकी के रूप में उपलब्ध सूचना प्रौद्योगिकी के नए-नए आयाम के साथ साइबर अपराध यानी धोखाधड़ी भी उतनी ही बढ़ती जा रही है। यह एक चिंता का विषय है। हमारा बैंकिंग क्षेत्र अर्थव्यवस्था से जुड़ा है, अर्थ यानी धन और जहां धन की बात हो वहां अपराध, नुकसान एवं खतरे की बात है।

हर सिक्के के दो पहलू होते हैं। सुविधाओं की बढ़ती पैठ के साथ एक खतरा भी जुड़ा है। यह सब कार्य इंटरनेट के माध्यम से संभव होने के कारण साइबर अपराध का एक खतरा भी साथ में संभावित है।

साइबर अपराध की स्थितियां:

अब प्रश्न आता है कि क्या है ये साइबर अपराध और ये होता कैसे है? आइए साइबर अपराध की मुख्य स्थिति पर द्रष्टिपात करते हैं –

- कंप्यूटर नेटवर्क को हैक करना
- कंप्यूटर नेटवर्क से आंकड़ो की चोरी करना
- पासवर्ड व विवरण की चोरी करना
- कंप्यूटर प्रोग्राम, डेटा तथा गोपनीय आंकड़ो को बाधित करना
- वाइरस के माध्यम से जानकारी को बदलना या नष्ट करना
- सेवा में व्यवधान डालना
- ई- मेल और सूचना की चोरी

साइबर अपराध का वर्गीकरण :

साइबर अपराध आज हमारे लिए एक गंभीर समस्या बन गई है, इसने बैंकिंग क्षेत्र व ग्राहकों के लिए एक बहुत बड़ा खतरा खड़ा किया है। साइबर अपराध को हम इस तरह से वर्गीकृत कर सकते हैं –

- एक कंप्यूटर को निशाना बनाकर हैकिंग, वाइरस या अन्य रूप से कई तरीकों से उस कंप्यूटर में साइबर अपराध करना।
- एटीएम, क्रेडिट कार्ड आदि के पासवर्ड की जानकारी लेकर धोखाधड़ी
- महत्वपूर्ण डेटा व सूचनाओं में परिवर्तन करना आदि।

साइबर अपराध के स्वरूप :

साइबर अपराध एक ऐसा दुष्कार्य है जिसमें कंप्यूटर, इंटरनेट या तकनीक के माध्यम से बैंक, संस्थाएं व ग्राहकों की राशि का दुरुपयोग व हानि पहुंचाकर राशि हासिल करने का प्रयास किया जाता है।

साइबर अपराध विभिन्न प्रकार से किए जाते हैं, आइए साइबर अपराध के स्वरूप पर द्रष्टिपात करें –

हैकिंग:

वर्तमान समय में हैकिंग बहुत ही आम हो गई है। बैंकिंग क्षेत्र में हैकर ग्राहक के फोन नंबर एवं ई मेल ट्रेस कर सकता है, जिसके द्वारा वह उनके पासवर्ड का अधिकृत उपयोग करके खाते से राशि का आहरण करता है। साइबर स्पेस के माध्यम से आज हैकर ग्राहक के खातों पर भी नजर रखकर उनकी जानकारी व राशि का दुरुपयोग करता है।

पासवर्ड की चोरी:

पासवर्ड की चोरी अनेक रूप से की जाती है

- अनुमान के द्वारा
- बृटफोर्स हमला
- डिफ़ाल्ट पासवर्ड
- शब्दकोश आधारित हमले

पासवर्ड क्रेकिंग का सबसे सरल तरीका अनुमान से पासवर्ड लगाना है। यह प्रक्रिया धीमीगति से चलती है इसलिए कई बार हैकर शब्दकोश के विभिन्न शब्दों द्वारा पासवर्ड की कोशिश करता है। बृटफोर्स हमले में

स्वचालित सॉफ्टवेर द्वारा अलग-अलग पासवर्ड को प्रयोग कर हैकिंग की कोशिश की जाती है। सामान्यत: कई बार पासवर्ड डिफ़ाल्ट रूप में दिये जाते हैं, इनका न बदलना भी एक बड़ा खतरा है।

फिशिंग :

कंप्यूटर सुरक्षा के क्षेत्र में, फिशिंग एक धोखाधड़ी की प्रक्रिया है जिसके द्वारा नकली पहचान बनाकर ग्राहकों की संवेदशील जानकारी जैसे पासवर्ड, राशि, क्रेडिट कार्ड के विवरण आदि की चोरी का प्रयास किया जाता है। फिशिंग के प्रकार –

- भ्रामक फिशिंग
- मेलवेयर आधारित फिशिंग

आइए इन पर विस्तृत चर्चा करें।

भ्रामक फिशिंग:

भ्रामक फिशिंग के जरिए फिशिंग करनेवाला व्यक्ति एक लिंक भेजता है जिस पर क्लिक करने के लिए प्राप्तकर्ता को बार-बार आग्रह किया जाता है। लिंक पर क्लिक करते ही व्यक्ति किसी नकली वेबसाइट पर पहुंच जाता है और वहां पर दी गई सभी जानकारियां गलत हाथों में पहुंच जाती हैं। कई बार फिशिंग करने वाले उन जानकारियों का उपयोग नहीं करते किन्तु बाजार में किसी और को यह जानकारी प्रदान करके नुकसान पहुंचाते हैं।

मेलवेयर आधारित फिशिंग:

मेलवेयर आधारित फिशिंग में शिकार व्यक्ति के कंप्यूटर पर डाउनलोड के माध्यम से क्षति करने वाला सॉफ्टवेर चला दिया जाता है। यह मेलवेयर कई प्रकार के नुकसान पहुंचा सकते हैं। सामान्य तौर पर ये डाउनलोड किए सॉफ्टवेर के माध्यम से आते हैं। उनके रूप देखें तो वे हैं–

स्क्रीन लागर, स्पाइ वेयर, की लागर आदि।

ई- मेल और सूचनाओं की चोरी:

- कई बार उपयोगकर्ता नाम और पासवर्ड ई-मेल द्वारा सादे शब्दों में भेजते हैं, जिसकी चोरी कर हमलावर इसका दुरुपयोग कर सकते हैं।
- कई हैकरो द्वारा ई-मेल का दुरुपयोग कर महत्वपूर्ण जानकारी की चोरी की जा सकती है।
- अगर 'सेव पासवर्ड' के विकल्प का प्रयोग किया जाए, तो पासवर्ड का पता किया जा सकता है।
- लगभग 60 प्रतिशत ई मेल स्पैम होते हैं।
- ई मेल के आम खतरे में जाली ई मेल और स्पैम शामिल हैं।

स्निफर :

स्निफर मूलत: रिकॉर्डिंग सॉफ्टवेर हैं जो की नेटवर्क पर भेजे जा रहे डेटा पैकेट को रिकॉर्ड और स्टोर करता है। मूलत: इसका विकास नेटवर्क के रखरखाव करने हेतु इसको विकसित किया गया था।

उदाहरण के तौर पर किसी हवाई जहाज का ब्लेक बॉक्स भी इसी तरह का होता है।

स्निफर का प्रयोग करके नेटवर्क पर भेजी जा रही सूचनाओं की चोरी की जा सकती है और बाद में उनका दुरुपयोग होता है।

इंटरनेट पायरसी:

किसी भी कॉपीराइट फ़ाइल को गैरकानूनी तरीके से चोरी करने के लिए इंटरनेट का प्रयोग करने का मतलब है **इंटरनेट पायरसी ।** आज का युग प्रतिस्पर्धात्मक युग है, हर जगह प्रतिस्पर्धा है । इसके तहत अपनी कंपनी या संस्था को आगे लाने के लिए दूसरी कंपनी या संस्था की जानकारी तथा गोपनीय दस्तावेज़ इंटरनेट पायरसी से चुरा लिए जाते हैं ।

सेवा रोकने वाले हमले:

वेबसाइट पर सामान्य गतिविधियों को रोकने के इरादे से किए जाने वाले हमले सेवा रोकने वाले हमले होते हैं । इस प्रकार के हमले में कंप्यूटर संबंधित संसाधनों जैसे मेमरी, नेटवर्क, सीपीयू आदि को बाधित कर दिया जाता है, जिससे सामान्य गतिविधियां रुक जाती हैं । इन सेवाओं के रुकने से ग्राहकों का संपर्क वास्तविक साइट से नहीं हो पाता ।

उदाहरण के तौर पर स्पर्धा और सीन हमले सेवा रोकने वाले हमले हैं ।

वित्तीय क्षेत्र में हुए कुछ साइबर अपराधों के किस्से :

सबसे पहला साइबर अपराध सन 1983 में 'मॉरिस वर्म' नाम के वाइरस से हुआ था । हाल में 2019 में हैक करके मुंबई के को-ओपरेटिव इंडियन बैंक में साइबर अपराध हुआ था । 2020 में कोविड महामारी की वजह से फरवरी 2020 से अप्रैल 2020 में करीब 238% साइबर अपराध बैंक और वित्तीय क्षेत्र में बढ़ गए हैं । हाल ही 2022 में अभी रशिया और यूक्रेन के बीच चल रहे टकराव में सबसे पहले यूक्रेन पर जो हमला किया गया है, वह है साइबर हमला । इससे हम जान सकते हैं कि साइबर सुरक्षा की आज के दिन में कितनी आवश्यकता है । यूक्रेन पर किए गए साइबर हमले में सबसे ज्यादा यूक्रेन के रक्षा विभाग को प्रभावित किया गया है ।

कहा जाता है –

पत्थरों की वो चट्टान
जो कमजोर आदमियों की राह में रोड़ा होती है,
वो ही शक्तिशालियों की
सफलता की सीढ़ी बन जाती है ।

अगर साइबर अपराध है तो उसके सुरक्षा के लिए कवच भी होना आवश्यक है ।

साइबर अपराध के रोकथाम के सुरक्षात्मक उपाय:

वर्तमान समय की पहली मांग साइबर अपराध के खतरों को रोकना है । उपर्युक्त साइबर अपराध की उपलब्ध जानकारी से हम अनुमान लगा सकते हैं कि अपनी सूचनाओं को सुरक्षित रखना हमारे लिए कितना आवश्यक है, विशेषकर तब जब ये सूचनाएं धन व वित्त से संबंधित हों ।

साइबर अपराध को खत्म करने के लिए निम्नलिखित उपाय कारगर हो सकते हैं:-

जागरूकता:

साइबर अपराध से बचने के लिए सभी उपभोक्ताओं को शिक्षित एवं जागरूक बनाना चाहिए । बैंकों को ग्राहकों को पेम्प्लेट का वितरण करना चाहिए । शाखा में ग्राहकों की बैठक के दौरान वीडियो के माध्यम से जानकारी देनी चाहिए । बैंकों के मुख्य कार्यालय द्वारा हर एक ग्राहक को एसएमएस के माध्यम से हर माह एक मैसेज भेजना चाहिए । अखबार में लेख तथा टेलिविजन में विज्ञापन के द्वारा जागरूकता लानी चाहिए ।

उदाहरण के तौर पर दूरदर्शन पर आने वाला कार्यक्रम 'जागो ग्राहक जागो' । विशेष रूप से एसे कार्यक्रम बार-बार प्रदर्शित करने चाहिए।

गोपनीयता:

यूजर्स को अपने आईडी और पासवर्ड को गोपनीय रखकर, किसी को भी नहीं दिखाना चाहिए और न ही साझा करना चाहिए। ऐसे पासवर्ड कभी मोबाइल या डायरी में अपने पास लिखकर नहीं रखने चाहिए।

सुरक्षा निर्देश :

ऑनलाइन बैंकिंग करते समय दिये गए सभी सुरक्षा निर्देशों का पालन अवश्य ही करना चाहिए।

पासवर्ड :

उपभोक्ताओं को पासवर्ड बनाते समय मिश्र कैरेक्टरों से बनाना चाहिए ताकि अन्य व्यक्ति इसे आसानी से खोज न सकें।

फायरवाल :

फायरवाल एक सिक्योरिटी गार्ड का काम करती है और नेटवर्क में अनचाहे यूजर्स की कोशिशों से हमें बचाती है । विंडोज ऑपरेटिंग सिस्टम में फायरवाल 'ऑन' ही रहना चाहिए, ताकि हम कंप्यूटर को सुरक्षित रखकर साइबर अपराध से बच सकें।

सॉफ्टवेयर:

बैंकिंग सेक्टर के सभी कंप्यूटरों में केवल मान्यता प्राप्त सॉफ्टवेयर का ही उपयोग किया जाना चाहिए।

- अपने पासवर्ड, आईडी, पिन कभी भी किसी के साथ साझा न करें।
- कभी भी आकर्षक विज्ञापन पर अपने केवाईसी दाखिल न करें।
- जब आप पैसे प्राप्त करना चाहते हों कभी भी स्केन या क्यूआर कोड या एमपिन दाखिल न करें।

साइबर अपराध होते ही तुरंत भारत सरकार की साइट cybercrime.gov.in एवं 1930 नंबर पर जानकारी देनी चाहिए।

साइबर अपराध आज की एक बड़ी चुनौती है तथा दिन-प्रतिदिन गंभीर समस्या बन गई है, इसने बैंकिंग क्षेत्र तथा बैंकिंग ग्राहकों को चिंतित कर दिया है । साइबर अपराधियों की सक्रियता बढ़ी हुई है इसलिए हमें साइबर अपराधों के बारे में सतर्क और जागरूक रहने की आवश्यकता है । इस क्रम में बैंकिंग संस्थाओं को उपर्युक्त उपायों से साइबर अपराधों को रोकना चाहिए, साथ ही अभी जो कदम उठाए जा रहे हैं वह भी तारीफ के काबिल हैं। जनहित की रक्षा यानी उनकी धन की रक्षा बैंकिंग की जिम्मेवारी है, साइबर अपराध को रोककर सुरक्षित रहें और समाज में खुशहाली लाएं।

आइए करें सुरक्षा की पहल, साइबर सुरक्षा से करें लोगों की समस्या हल।

संक्षिप्त में इतना ही कहूंगी,

"श्रम की स्याही लेकर कर दिए हैं हस्ताक्षर,
नई योजनाओं, नई उपलब्धि और नए दृष्टिकोण पर।"

जय हिन्द * जय हिन्दी * जय भारत

*****

विनय कुमार पाठक

पदनाम:- मुख्य प्रबन्धक (संकाय)
संस्था का नाम:- भारतीय स्टेट बैंक
मोबाइल नं. :- 9001895412
ई-मेल:- binay.pathak@sbi.o.ion

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

बैंकिंग आज के युग में अत्यंत महत्वपूर्ण व्यवसाय है। आज की बैंकिंग डिजिटलीकरण की ओर तेजी से बढ़ रही है। सूचना प्रौद्योगिकी और आर्टिफ़िशियल इंटेलिजेंस का प्रभाव बैंकिंग व्यवसाय पर पड़ रहा है। यही कारण है कि अब कहीं भी बैंकिंग और कभी भी बैंकिंग की अवधारणा मूर्त रूप ले चुकी है। आज हर व्यक्ति के लैपटॉप/ कंप्यूटर में तथा जेब में मोबाइल फोन के जरिए बैंकिंग सुविधा उपलब्ध है। परंतु अपराधियों ने किसी भी क्षेत्र को निरापद नहीं रहने दिया है। बैंकिंग भी अपराधियों के निशाने पर हमेशा रहा है। यही कारण है कि सूचना प्रौद्योगिकी और आर्टिफ़िशियल इंटेलिजेंस के प्रयोग के वावजूद अपराधी बैंकिंग जगत को अपना शिकार बनाते रहे हैं। अब वे कंप्यूटर और नेटवर्क का प्रयोग कर अपराध कर रहे हैं। साइबर अपराध द्वारा बैंकों और बैंक के ग्राहकों को निशाना बनाया जा रहा है।

साइबर अपराध

साइबर अपराध क्या है

वस्तुतः कोई भी अपराध जिसमें कंप्यूटर या नेटवर्क या हार्डवेयर का प्रयोग किया जाए वह साइबर अपराध है। साइबर अपराध कई प्रकार के होते हैं। जैसे- कंप्यूटर के डेटा में हेरफेर करना, कंप्यूटर सिस्टम में अनधिकार एक्सेस करना चाहिए। हैकिंग एवं वायरस अटैक इसके अंतर्गत आते हैं। जिसमें पारंपरिक अपराध जो कंप्यूटर के माध्यम से की जाती है वह भी साइबर अपराध माना जा सकता है।

कुछ प्रमुख साइबर अपराध जिनका प्रयोग कर बैंकों या बैंक के ग्राहकों को नुकसान पहुंचाया गया है। इसके अतिरिक्त हजारों घटनाएं हैं। साइबर अपराध सिर्फ़ बैंकिंग तक सीमित नहीं है, जीवन के हर क्षेत्र में इसका दुष्प्रभाव है।

साइबर अपराध के स्वरूप

साइबर अपराध के कुछ स्वरूप निम्नानुसार है:

फिशिंग - किसी अपराधी द्वारा अधिकृत व्यक्ति के छद्मवेश में इलेक्ट्रॉनिक तरीके से यूजरनेम, पासवर्ड आदि संवेदनशील जानकारी प्राप्त करना फिशिंग कहलाता है।

विशिंग- फिशिंग का ही यह एक स्वरूप है। इसके अंतर्गत कॉल कर अर्थात् टेलीफ़ोन अथवा मोबाइल से कॉल कर फिशिंग कार्य को अंजाम दिया जाता है।

स्मिशिंग- इसमें एसएमएस द्वारा अपराधी संवेदनशील सूचना प्राप्त करता है या लिंक प्रदान कर प्राप्तकर्ता से उनके बैंक/ कार्ड के बारे में जानकारी मांगी जाती है।

स्पीयर फिशिंग- इसमें विशेष संगठन के व्यक्तियों को लक्ष्य कर फिशिंग किया जाता है। अपराधी इसमें सोशल नेटवर्किंग साइट का प्रयोग करता है। फेशबुक, ट्विटर, इन्स्टाग्राम, गूगल, पिंटरेस्ट, यूट्यूब जैसे सोशल साइट से अपने शिकार से संबंधित जानकारी एकत्र कर वह अपने कुकृत्य को अंजाम देता है।

सोशल इंजीनीयरिंग- इसके अंतर्गत तकनीकी हैकिंग की अपेक्षा लोगों के बारे में जानकारी लेकर धोखाधड़ी की जाती है।

स्पूफिंग- इसका प्रयोग कर सुरक्षित सिस्टम में अवैध तरीके से प्रवेश किया जाता है। इसके अंतर्गत यह दर्शाया जाता है कि आधिकारिक श्रोत से यथा पीड़ित के बैंक, डॉक्टर, सरकारी विभाग आदि से उन्हें लिंक भेजा जा रहा है।

फ़ार्मिंग- यह एक प्रकार का साइबर अटैक है जिसका उद्देश्य वेबसाइट को नकली वेबसाइट पर रिडायरेक्ट करना होता है ताकि व्यक्तिगत सूचना प्राप्त की जा सके।

मालवर्टाइजिंग- इसके अंतर्गत ऑनलाइन विज्ञापन का प्रयोग कर मालवेयर का प्रसार किया जाता है। कहने का तात्पर्य यह है कि विज्ञापन दूषित मालवेयर से युक्त होता है।

ऐडवेयर- यह दूषित प्रोग्राम का एक रूप होता है जो सिस्टम में छुपा हुआ होता है और उपयोगकर्ता को विज्ञापन के साथ भेजा जाता है।

क्रॉस साइट स्क्रिप्टिंग अटैक- इसमें विश्वस्त परंतु भेद्य वेबसाइट का लिंक भेजा जाता है। जब लिंक को खोला जाता है तब उपयोगकर्ता को दूषित वेबसाइट पर रिडायरेक्ट कर दिया जाता है।

स्टेगनोग्राफी- किसी फ़ाइल के अंदर किसी फाइल संदेश, चित्र या वीडियो को छिपाना इसके अंतर्गत आता है।

व्हेलिंग- यह एक प्रकार का फ़िशिग अटैक है जिसमें किसी कंपनी के सर्वोच्च प्रबंधन को लक्ष्य बनाया जाता है। इसका उद्देश्य किसी संगठन के संवेदनशील सूचना को चुराना होता है। सामान्यतौर पर बिजनेस ई-मेल धोखाधड़ी के लिए इसका प्रयोग किया जाता है।

रैनसमवेयर- इसके अंतर्गत दूषित सॉफ्टवेयर द्वारा उपयोगकर्ता या किसी संस्थान पर अटैक करके उनके कंप्यूटर पर फाइलों के एक्सेस को रोक देता है अर्थात फाइलों को एन्क्रिप्ट कर देता है। जब अपराधी द्वारा मांगी गई फिरौती की रकम दी जाती है तभी उसे वापस उपयोग लायक बनाया जाता है।

की लॉगर – इसके अंतर्गत दूषित प्रोग्राम द्वारा कीबोर्ड पर की गई गतिविधि से यूजरनेम और पासवर्ड आदि जैसी संवेदनशील सूचना एकत्र की जाती है।

स्केअरवेयर – इसमें इस प्रकार का मालवेयर डाल दिया जाता है जो उपयोगकर्त्ता को भयभीत कर देता है। उदाहरण के लिए यदि उपयोगकर्ता के स्क्रीन पर यह मैसेज आए कि उसका कंप्यूटर कल से काम करना बंद कर देगा, इससे बचने के लिए दिए गए लिंक पर जानकारी दें। उपयोगकर्ता यह सोच कर कि यह उसके सहायता के लिए है, इस प्रकार के लिंक को क्लिक कर देता है और उसे उसका खामियाजा उसे भुगतना पड़ जाता है।

जूस जैकिंग- इसके अंतर्गत अपराधी के द्वारा चार्जिंग पोर्ट या केबल का प्रयोग कर डिवाइस से डेटा चुराया या उसे मालवेयर से संक्रमित किया जाता है।

सिम क्लोनिंग और सिम स्वैपिंग- विगत में अनेक घटनाएं हुई हैं जिनमें सिम को क्लोन कर या सिम को बदलकर ग्राहक के खाते से धोखाधड़ी से रकम निकाल लेता है। इसमें ग्राहक के मोबाइल के सिम के स्थान पर नया सिम ले लिया जाता है। इससे पुराने सिम पर संदेश आना बंद हो जाता है और नए सिम पर संदेश आने लगते है। इस कारण से खाताधारक के खाते से अपराधी लेनदेन करता रहता है और खाताधारक को इसकी भनक भी नहीं लगती है खाताधारक जब पासबुक अद्यतन करवाता है या स्टेटमेंट का अध्ययन करता है तभी उसे धोखाधड़ी की जानकारी मिलती है। इनके अतिरिक्त और भी अनेक प्रकार के साइबर अपराध हैं और साइबर अपराधी नित नए हथकंडे अपना रहे हैं।

सुरक्षात्मक उपाय

साइबर सुरक्षा से तात्पर्य है डेटा, इससे संबंधित तकनीक एवं डेटा के संग्रहण को किसी प्रकार के खतरे से बचाना। यदि बैंक के साइबर सुरक्षा में किसी प्रकार की कमजोरी है तो अपराधी इसका लाभ उठाकर बैंक को नुकसान पहुंचाएंगे। उपर्युक्त वर्णित उदाहरणों के माध्यम से पता चला हैं कि किस प्रकार संस्थाओं को साइबर अपराधियों द्वारा नुकसान पहुंचाया गया है। बैंकों में डिजिटल सिस्टम यथा क्रेडिट कार्ड, डेबिट कार्ड, एनईएफटी आदि के द्वारा ट्रांजेक्शन में अत्यधिक वृद्धि हुई है। इसके साथ ही साइबर धोखाधड़ी में भी काफी वृद्धि हुई है।

सुरक्षा के उपाय

कैसे साइबर अपराध से सुरक्षित रहा जाए ! इसका एक मात्र उपाय है जागरूक रहना। यदि बैंक के कर्मचारी जारूक होंगे, ग्राहक जागरूक रहेंगे, यदि वे धोखाधड़ी के तरीकों से अवगत रहेंगे तो बैंक और स्वयं को अपराधियों के शिकार होने से बचा पाएंगे। सबसे पहले यह सुनिश्चित करने की आवश्यकता है कि संदेश भेजने वाला वही व्यक्ति है या नहीं जो कि वह दावा कर रहा है अर्थात् कहीं किसी अधिकृत व्यक्ति के स्थान पर कोई अपराधी संदेश भेजकर ठगी को अंजाम तो नहीं दे रहा है। कहीं ऐसा तो नहीं कि बैंक का प्रतिनिधि बनकर कोई अपराधी संदेश भेज रहा है। अपराधी अपने शिकार को बहुत कम समय देते हैं जवाब देने के लिए उनका उद्देश्य होता है शिकार को सोचने का मौका दिए बिना उनसे मनचाहा कार्य करवा लें। वे अपने शिकार को कड़ी कार्रवाई की धमकी भी देते हैं। कई बार बड़ा प्रस्ताव खोने की बात कह तुरंत कार्य करने के लिए प्रेरित करते हैं।

उपकरण की सुरक्षा

लेनदेन करने के लिए कंप्यूटर, टैब, लैपटॉप, मोबाइल आदि का प्रयोग किया जाता है। इन उपकरणों को सुरक्षित रखना काफी जरूरी है। सबसे पहले इन्हें लावारिश नहीं छोड़ना चाहिए। इन्हें हमेशा लॉक/ पासवर्ड युक्त रखना चाहिए। ऑटो लॉक सुविधा का प्रयोग करने से कुछ देर के लिए उपकरण पर काम नहीं करने से वह लॉक हो जाता है। ऐसी व्यवस्था करनी चाहिए कि वह सिर्फ़ पिन या पैटर्न से ही ओपन हो। मोबाइल के आईएमईआई नंबर को लिख कर रख लेना चाहिए। मोबाइल के सिम को लॉक रखना तथा मोबाइल एवं सिम के लिए अलग-अलग पिन रखना ही समझदारी है। जब आवश्यक न हो तो नेटवर्क को बंद रखना चाहिए। नेटवर्क से किसी उपकरण को जोड़ने के लिए पासवर्ड रखना चाहिए ताकि कोई बाहरी व्यक्ति उस नेटवर्क से जुड़ न सके।

पासवर्ड सुरक्षा से संबंधित कुछ जरूरी बातें

पासवर्ड ही वह माध्यम है जिसके द्वारा हम किसी उपकरण में अपनी पहुंच बना सकते है और दूसरों को उपकरण का प्रयोग करने से रोक सकते हैं। अतः पासवर्ड बनाते समय कुछ विशेष बातों पर ध्यान रखना चाहिए। सर्वप्रथम यह ध्यान रखना चाहिए कि याद रखने की सहूलियत के कारण पासवर्ड को आसान नहीं बनाना चाहिए। यह याद रखने योग्य परंतु जटिल होना चाहिए जिसमें अक्षर, अंक एवं विशेष चिह्न से युक्त हो। एक ही पासवर्ड सभी उपकरण या सेवा के लिए नहीं रखना चाहिए। इसे समय-समय पर बदलते रहना चाहिए।

आहरण रकम की सीमा तय करना

अब यह सुविधा उपलब्ध है कि किसी भी लेनदेन के लिए आहरण या लेनदेन की सीमा तय की जा सकती है। उदाहरण के लिए एटीएम से नकद निकासी या अन्य लेनदेन, पॉइंट ऑफ सेल से निकासी या अन्य लेनदेन, कांटैक्टलेस लेनदेन की सीमा, अंतर्राष्ट्रीय लेनदेन की सीमा को ऑन या ऑफ किया जा सकता है या रकम की सीमा तय की जा सकती है।

एंटिवायरस सॉफ्टवेयर

एंटिवायरस सॉफ्टवेयर बहुत बड़ा सुरक्षाकवच है। इससे डेटा वायरस, वर्म, ट्रोजन, स्पाइवेयर, की-लोगर्स, आदि से बचा रहता है। कई बार यह सोचकर कि एंटिवायरस से कंप्यूटर की गति धीमी होती है, लोग एंटिवायरस को निष्क्रिय कर देते हैं या डिलीट कर देते हैं। ऐसा बिलकुल भी नहीं किया जाना चाहिए। किसी भी डोक्यूमेंट को डाउनलोड करने से पहले स्कैन किया जाना चाहिए। एंटिवायरस सॉफ्टवेयर को समय-समय पर अद्यतन भी किया जाना चाहिए। आज के युग में अधिकांश कार्य मोबाइल से होते हैं अतः मोबाइल पर भी एंटिवायरस सॉफ्टवेयर इन्स्टाल किया जाना चाहिए।

किसी अजनबी द्वारा भेजे गए लिंक को क्लिक नहीं करना

अपराधी विभिन्न प्रकार के प्रलोभन देकर या एटीएम कार्ड/ खाता के निष्क्रिय होने का भय दिखलाकर कोई लिंक एसएमएस, ई-मेल, व्हाट्सऐप आदि से भेजते हैं। इस प्रकार के लिंक को कभी भी क्लिक नहीं करना चाहिए। इस प्रकार से फिशिंग, स्मिशिंग, स्पूफिंग आदि से बचा जा सकता है।

व्यक्तिगत जानकारी को किसी से साझा नहीं करना चाहिए

अपराधी अक्सर ऐसा दर्शाते हैं कि वे बैंक के प्राधिकृत अधिकारी हैं और ग्राहक की सुविधा के लिए उनसे उनकी व्यक्तिगत जानकारी मांग रहे हैं इस तरह के झांसे में कभी भी न आए। इससे विशिंग से बचा जा सकता है।

आधिकारिक पोर्टल पर शिकायत दर्ज करना

यदि कोई व्यक्ति धोखाधड़ी का शिकार हो जाता है तो उसे शीघ्र ही आधिकारिक वेबसाइट पर इसकी सूचना देनी चाहिए। सभी ऑनलाइन शॉपिंग साइट धोखाधड़ी की सूचना देने के लिए हेल्पलाइन नंबर, ई-मेल पता उपलब्ध करवाते हैं। तत्क्षण उस नंबर पर कॉल कर या ई-मेल पते पर इसकी जानकारी पूर्ण विवरण के साथ दी जानी चाहिए। साथ ही पुलिस में भी शिकायत दर्ज करवानी चाहिए। भारत सरकार ने एक पोर्टल प्रारंभ किया है जो **नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल** के नाम से जाना जाता है। इस पर साइबर अपराध की शिकायत ऑनलाइन दर्ज की जा सकती है।

निष्कर्ष

निष्कर्ष के तौर पर हम कह सकते हैं कि साइबर अपराधी विभिन्न तकनीक अपनाकर अपने कुत्सित इरादे को अंजाम देने में लगे रहते हैं, अतः साइबर सुरक्षात्मक उपाय का अत्यंत महत्व है और इसके लिए जागरूकता बढ़ाना, स्वयं एवं समाज को शिक्षित करना ही एक मात्र उपाय है। अतः हम सभी सुरक्षात्मक उपाय के महत्व को समझें, लोगों को जागरूक करें एवं बैंक तथा बैंक के ग्राहकों को साइबर अपराध से सुरक्षित रखें और यदि अपराधी कामयाब हो गया हो तो यथाशीघ्र उसकी रिपोर्ट कर उसे दंड दिलाने में सहयोग करें।

*****

विलास वैष्णव

पदनाम:- मुख्य प्रबन्धक (संकाय)
संस्था का नाम:- भारतीय स्टेट बैंक
मोबाइल नं. :- 7600037646
ई-मेल:- vilas.vaishnav@sbi.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

मैं अपने प्रमोशन के बाद नयी शाखा में शाखा प्रबन्धक का चार्ज लेने के लिए बहुत उत्साहित था। इतनी कम उम्र में शाखा प्रबन्धक बनने की खुशी मेरे चेहरे पर साफ-साफ नजर आ रही थी। मैंने महीने के दूसरे सप्ताह में जब अपनी शाखा में कदम रखा तो देखा कि शाखा में बहुत ज्यादा भीड़ है। 10 तारीख के बाद भी इस किस्म की भीड़ को देखकर मैं सोच में पड़ गया। जब मैंने गौर से देखा तो पाया कि सभी स्टाफ नीचे सर झुकाये सभी काउंटर पर काम में लगे हुए हैं। इतनी तल्लीनता से काम करते हुए कोई भी स्टाफ ग्राहक से ज्यादा बात नहीं कर रहे हैं और न ही ग्राहक को एटीएम या जीआरसी जैसे डिजिटल मोड को इस्तेमाल करने की बात कर रहे हैं।

मुझे शाखा की स्थिति देखकर ये तो समझ आ गया था कि इस शाखा में काम करना इतना आसान नहीं होगा और मुझे कुछ महत्वपूर्ण बदलाव यहां लाने होंगे। शाम को कैश काउंटर बंद होने के बाद मैंने स्टाफ सदस्यों की मीटिंग बुलवाई। सबसे पहले अपनी शाखा के सभी सदस्यों के साथ परिचय किया और फिर शाखा की इस 'भीड़ वाले' मुद्दे पर चर्चा करने लगा। मैंने सभी स्टाफ सदस्यों को बताया कि हमारी शाखा में ग्राहक उन कामों के लिए ज्यादा आते हैं, जो काम आसानी से डिजिटल चैनलों पर किये जा सकते हैं। इस पर शाखा के ग्राहक मित्र श्री राजन ने जवाब दिया, "सर इस शाखा में डिजिटल बैंकिंग तो बिलकुल नहीं चलने वाली, यहां पर ग्राहक और स्टाफ दोनों ही पहले से डरे हुए हैं। बाकी जहां तक ग्राहक सेवा की बात है, तो हम सब लोग बहुत मन लगाकर हमारे ग्राहकों का काम करते हैं"।

श्री राजन की ये बातें सुनकर मैंने पूछा, "राजन जी मैंने आज सभी स्टाफ सदस्यों की काम में तल्लीनता देखी। पर आप ऐसा क्यूं कह रहे हैं कि ग्राहक और स्टाफ दोनों डिजिटल बैंकिंग से डरे हुए हैं"? श्री राजन ने धीरे से जवाब दिया, "सर यहां नजदीक की ही एक शाखा में कुछ ग्राहकों के खाते में ऑनलाइन प्लैटफ़ार्म पर धोखाधड़ी हुई है और ये बात अब सभी ग्राहक जानते हैं। यही कारण है कि ग्राहक डिजिटल बैंकिंग से दूर रहना चाहते हैं। ऐसे माहौल में हम भी आखिर ग्राहक को डिजिटल बैंकिंग कैसे समझाएं?"

मैं स्थिती को समझ तो गया था परंतु डिजिटल बैंकिंग ग्राहकों के लिए कितनी महत्वपूर्ण है, ये भी मैं जानता था। स्टाफ मित्रों से और थोड़ी चर्चा से मुझे ये समझ आया कि डिजिटल प्रोडक्टस की हमारे स्टाफ को ज्यादा जानकारी नहीं है। खासतौर पर डिजिटल प्रोडक्टस को सुरक्षित तरीके से कैसे इस्तेमाल किया जाए, इस जानकारी का अभाव मुझे स्टाफ में नजर आया। मैंने डिजिटल प्रोडक्टस के बारे में बात करने का मन बनाया और चर्चा के रुख को उस तरफ मोड़ दिया। स्टाफ सदस्यों का विश्वास जीतने के लिए मैंने सबसे पहले कुछ डिजिटल धोखाधड़ी के किस्से साझा करना शुरू किया:

केस-1

श्रीमान स्मार्ट अपने पुराने मोबाइल फोन को ओएलएक्स (olx) साइट पर ₹15000/- में बेचने के लिए रखते हैं। विज्ञापन को देखने के बाद कुछ लोगों ने उन्हे संपर्क किया। दो दिन बाद ही उन्हें नटवरलाल नामक एक व्यक्ति का मोबाइल खरीदने के लिए फोन आया। थोड़े मोल-भाव के बाद, फोन का सौदा ₹13500/- में तय हुआ। नटवरलाल ने फोन खरीदने की जल्दी दिखाई और अग्रिम राशि ₹10000/- उनके अकाउंट में गूगल-पे के जरिये ट्रान्सफर करने की बात कही। इस पर श्रीमान स्मार्ट बहुत खुश हुए, उन्हें अग्रिम राशि इतनी जल्दी जो मिल रही थी। श्रीमान स्मार्ट ने तुरंत अपना गूगल-पे आईडी नटवरलाल को बताया।

नटवरलाल ने श्रीमान स्मार्ट को फोन पर बाते करते हुए कहा कि अग्रिम राशि उनके खाते में ट्रान्सफर हो रही है। नटवरलाल ने श्रीमान स्मार्ट को पैसा अपने खाते में लेने का अनुरोध स्वीकार करने को कहा, उन्होने तुरंत उसे स्वीकार कर लिया। कुछ देर फोन को होल्ड करने के बाद नटवरलाल ने कहा कि कुछ टेक्निकल परेशानी की वजह से लेन-देन पूरा नहीं हुआ है और दो-तीन बार प्रयास करने पर भी लेन-देन नहीं हो पा रहा। ऐसा करते हुए 10 मिनट बाद उन्होने कहा की लेन-देन हो गया है। नटवरलाल ने श्रीमान स्मार्ट का घर का पता नोट किया और दूसरे दिन मोबाइल घर से लेने की बात कही। कुछ देर बाद जब श्रीमान स्मार्ट ने अपने गूगल-पे खाते को चेक किया तो वे भोचन्क्के रह गए। उनके गूगल-पे खाते से तीन बार ₹10000/- डेबिट हो गये थे। बाद में श्रीमान स्मार्ट को जानकारी मिली कि यूपीआई से व्यवहार करते समय जब खाते में कोई राशि जमा हो रही हो, तो हमें यूपीआई पिन डालने की जरूरत नहीं है। पिन की आवश्यकता अपने खाते से पैसे निकासी (डेबिट) करने के समय ही होती है।

केस -2

रवींद्र अपने काम से मुंबई गया हुआ था, सफर के दौरान उसने मोबाइल की बैटरी चार्ज करने के लिए सार्वजनिक स्थल पर लगे चार्जिंग पोर्ट से अपने फोन को चार्ज कर लिया। रवींद्र की इस छोटी सी भूल से उसने अपने खाते से ₹25000/- गंवा दिए। हैकर्स, जूस जेकिंग के तरीके से सार्वजनिक चार्जिंग पोर्ट पर फाइल रीडर या कार्ड रीडर चिप का प्रयोग करके, चिप चार्जिंग पोर्ट पर लगने वाले स्मार्टफोन का सारा निजी डेटा कॉपी कर लेते हैं और साथ ही फोन में वायरस डाल देते हैं।

दोनों ही केस सभी स्टाफ बड़े ही ध्यान से सुन रहे थे। मैंने बताया कि ये कुछ नए तरीके हैं जो धोखाधड़ी करने के लिए अपनाए जा रहे हैं। हमें इन तरीकों को समझने की जरूरत हैं, ना की घबराने की।

बैंकों का मूल उदेश्य नयी पीढ़ी को असाधारण सेवाएं प्रदान करना होना चाहिए। आज भारत अभूतपूर्व तरीके से डिजिटल हो रहा है, जहां लगभग सब कुछ बस एक क्लिक पर उपलब्ध है– चाहे वह लोन हो, इन्शुरेंस हो, क्रेडिट कार्ड, बैंकिंग, खरीदारी, या फिर रेल या बस का टिकिट खरीदना।
चलिए अब डिजिटल धोखाधड़ी के कुछ नए तरीकों को समझते हैं:

स्मिशिंग

हैकर्स यहां पर ऑनलाइन शॉपिंग करने वाले ग्राहकों को निशाना बनाते हैं, ग्राहकों को डिस्काउंट या कैश बैक का लालच देकर ग्राहक की निजी जानकारी जैसे डेबिट या क्रेडिट कार्ड का डेटा ले लेते हैं। इसके बाद ग्राहक के खाते से लेनदेन करके उनके खाते की राशि निकाल लेते हैं।

रिमोट ऐसिसटेंस

इस धोखाधड़ी मे हैकर्स हमें क्विक सपोर्ट और एनीडेस्क जैसे एप्स डाउनलोड करने को कहते हैं और इसके बाद ये ऐप्स आपके फोन का पूरा एक्सेस हैकर्स को दे देते हैं। इससे आपकी पूरी निजी जानकारी दूर बैठे हैकर्स तक पहुंच जाती है और वह आपके फोन को कंट्रोल कर लेता है।

फिसिंग

इस फ्रॉड के तहत हैकर्स हमें वायरस वाले लिंक या एसएमएस भेजते हैं और इसके बाद निजी जानकारी साझा करने को कहते हैं। जानकारी साझा करने के कुछ ही देर में हैकर्स हमारे खाते से रुपये निकाल लेते हैं।

ऑनलाइन ट्रांजेक्शन

हैकर्स इस तरीके के तहत ई-कॉमर्स प्लेटफॉर्म से हमें कॉल करने का दावा करते हैं। इसके बाद ग्राहक को रिफंड का लालच देकर उसकी निजी जानकारी चुरा लेते हैं। जानकारी हाथ लगते ही हैकर्स कुछ देर में ग्राहक के खाते से लाखों रुपये निकाल लेते हैं।

इन सब तरीकों को जानने के बाद हमें यह समझना होगा कि जिस तरह बैंक में सुरक्षा का ख्याल रखा जाता है, हमे अपने डिजिटल व्यवहार एवं मोबाईल को भी उसी तरह से सुरक्षित रखना होगा।

तो आइये अब हम जानें कि हम अपने डिजिटल व्यवहारों को किस तरह से सुरक्षित रख सकते हैं:

एटीएम कार्ड:

अपने एटीएम कार्ड को निश्चित समय के लिए लॉक या अनलॉक किया जा सकता है। जैसे, यदि आप ऑनलाइन ख़रीदारी या अंतरराष्ट्रीय लेन-देन रोज नहीं करते, तो आप इन सुविधाओं को बंद कर सकते हैं। इससे हम विभिन्न प्रकार की धोखाधड़ी से बच सकते हैं। यदि हमें ये सारी सुविधाएं पुनः शुरू करनी हैं तो हमें उसे फिर से सक्रिय करने मे सिर्फ एक मिनट का समय लगेगा।

एटीएम कार्ड स्किमिंग से बचने के लिए योनो केश से एटीएम कार्ड के बिना भी एटीएम मशीन से नगदी निकासी कर सकते हैं। इसके द्वारा एटीएम में होने वाली धोखाधड़ी से बचा जा सकता है।

यूपीआई लेन-देन

1. SMS/email के द्वारा मिली किसी भी लिंक पर यूपीआई पिन प्रविष्ट न करें।
2. किसी भी अनजान व्यक्ति के साथ फोन पर ओटीपी/ डेबिट कार्ड की जानकारी साझा न करें।
3. फोन पर आए हुए एसएमएस को किसी तीसरे व्यक्ति के कहने पर, किसी और व्यक्ति के साथ साझा न करें।
4. अपने यूपीआई पिन को यूपीआई ऐप के अलावा कहीं और प्रविष्ट न करें।
5. किसी अनजान व्यक्ति से प्राप्त collect request को स्वीकार न करें।
6. कस्टमर केयर के नंबर को ऑनलाइन सर्च न करें, इसके बजाय कंपनी की अधिकारिक वेबसाइट से नंबर प्राप्त करें।
7. अपनी व्यक्तिगत जानकारी को सोशल मीडिया पर साझा न करें।
8. स्पेम ई-मेल को न तो खोलें और न ही किसी को फॉरवर्ड करें।
9. अपने विवादित डिजिटल लेन-देन को सोशल मीडिया पर साझा न करें। धोखेबाज आपको संपर्क करके, आपको समाधान देने के लालच में आपके खाते की राशि निकाल लेते हैं।
10. हमेशा URL टाइप करते समय सुनिश्चित कर लें कि https:// में 'S' है और padlock साइन ग्रीन हुआ है या नहीं। यदि नहीं, तो अपने आईडी एवं पासवर्ड प्रविष्ठ न करें। 'S' मतलब secure सुरक्षित।

ऑनलाइन बैंकिंग

1. किसी भी अनजान व्यक्ति के द्वारा मिले किसी भी ई-मेल/ एसएमएस या कॉल का उत्तर न दें।
2. SMS/email के द्वारा आई किसी भी लिंक पर क्लिक न करें।
3. हमेशा ऑनलाइन बैंकिंग साइट का एड्रेस स्वयं टाइप करें एवं सुनिश्चित कर लें कि पेडलॉक साइन ग्रीन हुआ है या नहीं। यदि नहीं, तो अपने आईडी एवं पासवर्ड प्रविष्ठ न करें।
4. यदि कोई आपको बैंक कर्मचारी या शासकीय कार्यालय का कर्मचारी बनकर आपसे बात करें, तो फोन पर उनसे अपने बैंक खाते की जानकारी साझा न करें।
5. यदि कोई एसएमएस या ई-मेल से आपको प्रलोभन दे, जैसे कॉनर्सट की टिकिट, मूवी टिकिट या किसी बीमारी का इलाज तो ऐसे SMS/email का जवाब न दें।

अपने मोबाइल लैपटाप कंप्यूटर को निम्न लिखित सुरक्षा जरूर प्रदान करें :

फिजिकल सुरक्षा	वायरलेस सुरक्षा	डेटा सुरक्षा	ऐप्लिकेशन सुरक्षा
अपने फोन को अपने से दूर न रखें/ छोड़ें	उपयोग में नहीं होने पर अपना 3G/4G डेटा कनैक्शन बंद रखें	अपने डेटा का बैकअप नियमित रूप से करें	अपने डिवाइस को अनाधिकृत पहुंच से दूर रखें
ऑटो-लॉक का उपयोग करें	मोबाइल ब्लूटूथ का प्रबंधन सही तरह से करें	अपने मोबाइल या कम्प्युटर में संवेदनशील जानकारी जैसे आईडी/ पासवर्ड कभी न रखें	लोकेशन ट्रैकिंग सेवा के बारे में जागरूक रहें
खोए हुए या चोरी किए गए उपकरणों की रिपोर्ट करें	अन्य उपकरणों के साथ जोड़ते समय पासवर्ड का उपयोग करें	कंप्यूटर से मोबाइल पर डेटा स्थानांतरित करने से पहले वायरस से बचने के लिए स्कैन जरूर करें	ऑपरेटिंग सिस्टम को नियमित रूप से अपडेट करें
यूनिक आईएमईआई नंबर रिकॉर्ड में रखें	सार्वजनिक नेटवर्क के बारे में सावधान रहें जैसे: Wi-Fi/Juice jacking	"Factory Reset" सेटिंग्स के बारे में जानकारी रखें	हमेशा विश्वसनीय स्रोतों से ऐप्लिकेशन डाउनलोड करें
	केवल विश्वसनीय नेटवर्क से कनेक्ट करें		एंटिवाइरस नियमित रूप से अपडेट करें

इस सब जानकारी के बाद मुझे अपने स्टाफ सदस्यों में डिजिटल बैंकिंग के लिए कुछ विश्वास दिखा। सभी ने ग्राहक को डिजिटल बैंकिंग प्लैटफ़ार्म पर ले जाने का मन बना लिया था। कुछ ही देर में हम लोग इस काम कि कैसे शुरुआत कि जाए, उसकी तैयारी कर रहे थे। मैं मन ही मन प्रसन्न हो रहा था कि अब हम अपने ग्राहकों को डिजिटल बैंकिंग की ओर आकर्षित कर पाएंगे, जिससे बैंक और ग्राहक दोनों को फाइदा होगा।

*****

विवेक चंद्रकांत जटनिया

पदनाम:- सहायक
संस्था का नाम:- न्यू इंडिया एशुरेंस
मोबाइल नं. :- 7990429539
ई-मेल:- vivekjataniya008@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

आज का युग कंप्यूटर और इंटरनेट का युग है। आज जब हर जगह कंप्यूटर और इंटरनेट का आधिपत्य है तो हमारा वित्तीय क्षेत्र भला इससे अछूता कैसे रह सकता है? हर क्षेत्र की तरह आज हमारे वित्तीय क्षेत्र में भी कंप्यूटर का दबदबा है और यह भी कह सकते हैं कि सूचना प्रौद्योगिकी एवं वैकल्पिक डिलिवरी चैनलों का ही आज ज्यादा प्रभाव है। जहां पहले ग्राहकों को बैंकिंग सेवाओं के लिए घंटों लंबी कतार में खड़े रहना पड़ता था, आज एक क्लिक मात्र से 24*7 कहीं भी कभी भी बैंकिंग सेवाएं हमारे लिए उपलब्ध हैं। ये सेवाएं ग्राहकों को अभूतपूर्व एवं महत्वपूर्ण सेवाएं प्रदान कर रही है। कह सकते हैं -

"विज्ञान के अद्भुत चमत्कार ने कर दिया चकित जहान,
घर-घर उल्लास उर्मिया जागी, मुश्किलें हुई आसान."

परंतु इस तस्वीर का दूसरा पक्ष भी है। इन तकनीकी सेवाओं की वजह से अपराधियों द्वारा ग्राहकों से अक्सर ही ओटीपी, ई-मेल आदि जैसी गोपनीय जानकारियां हासिल की जाती हैं और फिर उनके खातों से विभिन्न तरीकों से रकम निकाल ली जाती है। ग्राहक को पता भी नहीं होता और उनके साथ इंटरनेट के माध्यम से सेंध लगायी जाती है। इस तरह की जालसाजी घटना को साइबर अपराध कहते हैं।

साइबर अपराध:
कंप्यूटर और इंटरनेट की मदद से किया जाने वाला अपराध साइबर अपराध है।

वर्तमान में साइबर अपराध में तेजी से वृद्धि हुई है जो चिंता का विषय है। साइबर अपराध के कुछ स्वरूप इस प्रकार हैं-

- **साइबर अपराध के विविध स्वरूप**:
- **वैश्विक महामारी कोविड-19**

  तकनीक आधारित ऑनलाइन बैंकिंग की बढ़ती लोकप्रियता में वैश्विक महामारी कोविड-19 का महत्वपूर्ण स्थान है। ऐसे ग्राहक जो पहले केवल ऑफलाइन बैंकिंग करना पसंद करते थे, उन्हें भी कोविड-19 महामारी में सुरक्षा एवं सलामती के लिए ऑनलाइन बैंकिंग की तरफ अपने कदम रखने पड़े। इस तरह बहुत सारे ऑनलाइन लेन-देन की वजह से भी साइबर अपराध बढ़ने लगे।
- **प्रमाणभूत वेबसाइट पर खतरा**:

  जो वेबसाइट प्रमाणभूत हो वहां पर साइबर अपराध का खतरा अब बढ़ने लगा है, उदाहरण के तौर पर इनकम टैक्स की साइट अपनी माहिती उस साइट पर डालेंगे और हैकर आपकी सारी माहिती ले लेंगे। ऐसी साइट पर ज्यादातर साइबर अटैक अब बढ़ने लगे हैं।

❖ **कंप्यूटर वायरस** :

कंप्यूटर वायरस या वर्म्स ऑडियो, वर्ड या किसी अन्य रूप में हो सकता है। डेटा का स्थानांतरण करते समय या इंटरनेट के माध्यम से कोई फ़ाइल डाउनलोड करते समय ये वायरस कंप्यूटर में आ जाते हैं और तब तक अपनी प्रतिलिपियां बनाते रहते हैं, जब तक कि कंप्यूटर की मेमोरी पूरी तरह से नहीं भर जाती है और इस तरह से ये कंप्यूटर सिस्टम की कार्यशील क्षमता को पूरी तरह से नष्ट कर देते हैं।

इन वायरस या वर्म्स से कंप्यूटर की सुरक्षा को बड़ा खतरा होता है। बैंकिंग क्षेत्र में ये बहुत हानिकारक हो सकते हैं क्योंकि यहां से जमा राशि, ऋण विभाग आदि से संबंधित सभी महत्वपूर्ण जानकारियां कंप्यूटर में ही रहती है।

उदाहरण के तौर पर सन् 2000 में "**लव बग**" नामक वायरस ने अमेरिका को 200 बिलियन डॉलर की हानि पहुंचाई थी।

- **क्रॉस साइट स्क्रिप्टिंग**:

क्रॉस साइट स्क्रिप्टिंग ऐप्लिकेशन में आ रही एक प्रकार की कमजोरी है। इसके माध्यम से हमलावर पहुंच नियंत्रण यानि Access Controls को बाईपास करने में सक्षम हो सकता है। क्रॉस साइट स्क्रिप्टिंग से कई प्रकार का नुकसान हो सकता है।

- **हैकिंग:**

हैकिंग भी साइबर अपराध का एक मुख्य स्वरूप है जिससे कंप्यूटर या अन्य डिवाइस हैक किए जाते हैं।

- **डेटा डिडलिंग**:

डेटा डिडलिंग के कंप्यूटर सिस्टम में संग्रहीत डेटा में अनधिकृत संशोधन करता है। इसके माध्यम से कंप्यूटर में इनपुट से पहले या इनपुट के दौरान डेटा बदलना और फिर प्रोसेसिंग पूरा होने पर इसे वापस बदलना है। इसमें कई प्रकार की चोरी जैसे राशि अंतरित करना, खाते का विवरण प्राप्त करना या फिर ग्राहक की जानकारी प्राप्त करना भी हो सकता है।

- **लॉजिक बम**:

यह एक ऐसा प्रोग्राम होता है जो किसी निश्चित दिन या समय पर सक्रिय हो जाता है। यह सक्रिय होते ही कंप्यूटर के मुख्य प्रोग्राम में कोई भी कार्य करने में बाधा उत्पन्न करता है तथा उस प्रोग्राम को भ्रमित करने की कोशिश करता है। उदाहरण के तौर पर अत्यधिक संख्या में ई-मेल भेजकर किसी ई-मेल अकाउंट को या फिर वहां के किसी सर्वर को नष्ट कर देना। आज की बैंकिंग पूरी तरह से सर्वर पर ही निर्भर है तो इस मामले में बैंकिंग क्षेत्र को भी सतर्क रहना अति आवश्यक है।

- **डीएनएस आधारित फिशिंग**:

डीएनएस आधारित फिशिंग में डोमेन नामक सर्वर के साथ छेड़खानी की जाती है। इस प्रकार के फिशिंग में वास्तविक साइट की जगह फर्जी साइटों पर पहुंचा दिया जाता है और वहां यूजर आई डी या पासवर्ड दर्ज करते ही अपराधियों द्वारा उन जानकारी पर कब्जा करके नुकसान किया जाता है।

- **सुरक्षात्मक उपाय:**

सिस्को के भूतपूर्व सीईओ जॉन चैंबर्स ने उद्यमों में साइबर जोखिम के महत्व को रेखांकित करते हुए कहा है, "केवल दो प्रकार के संगठन है, एक वे जो हैक कर लिए गए है और दूसरे वे जो यह नहीं जानते कि उन्हें कर लिया गया है."

बैंकों में साइबर सुरक्षा के दो प्रमुख आयाम हैं:

1. आंतरिक सूचना प्रौद्योगिकी सुरक्षा

2. नेटवर्क की कमजोरियां

जैसे-जैसे इंटरनेट का इस्तेमाल बढ़ता गया वैसे-वैसे बैंकिंग उत्पादों एवं सेवाओं की डिलीवरी के लिए इंटरनेट का चैनलों के रूप में उपयोग बढ़ गया।

बैंकिंग प्रौद्योगिकी में हुए नवोन्मेषिता की लंबी श्रंखला में सबसे आधुनिक यूनिफाइड पेमेंट इंटरफ़ेस (यूपीआई) है, जिसने विप्रेषण की सीमाओं को बढ़ा दिया है। इस लंबी कहानी को यदि संक्षेप में कहें तो प्रौद्योगिकी का इस्तेमाल कई गुना बढ़ गया है और आज कोई भी बैंक तीव्र प्रौद्योगिकी ग्राहक, ग्राहक-मैत्रीय डिजिटल उत्पाद, बाधारहित उपयोक्ता अनुभव तथा सतत् नवीनीकरण के बिना जीवित नहीं रह सकता है। ऐसे में आइन्स्टाइन का यह कथन सटीक प्रतीत होता है-

"हर कठिनाई में अवसर निहित है, केवल उसे तलाशना मात्र होता है."

साइबर अपराध को खत्म करने के लिए सुरक्षात्मक उपाय करना बहुत जरूरी है।

→ **रियल टाइम डिटेक्शन** :

हमें एक नया सॉफ्टवेयर real time detection बनाना चाहिए जिसके अंतर्गत जब भी कोई ट्रांजैक्शन हो उसी समय अगर वह संदिग्ध लगे तो उसे रोक दिया जाए। ग्राहकों के पैसे को सुरक्षित रखने के लिए ऐसा सॉफ्टवेयर सबसे ज्यादा उपयुक्त होगा। कहा जाता है, **सावधानी हटी, दुर्घटना घटी**.

यदि लेन-देन करते समय ही सावधानी रखी जाएगी तो अवश्य ही हम दुर्घटना यानी किसी भी नुकसान को होने से रोक पाएंगे।

→ **धोखाधड़ी का पहले से पता लगाना:**

धोखाधड़ी से बचने के लिए कई विभिन्न सुरक्षात्मक कदम लिए जा सकते हैं जिसमें दो शब्द काफी महत्वपूर्ण है-

प्रोएक्टिव और रिएक्टिव

प्रोएक्टिव यानी कि पहले ही योजना बना लेना
रिएक्टिव यानी कि किसी घटना के बाद उस पर कार्रवाई करना.

हमें भी साइबर अपराध से सुरक्षात्मक कदम के लिए proactive बनना पड़ेगा और कठिन सुरक्षा व जागरूकता के साथ साइबर अपराध से बचना होगा।

→ **कैप्चा (CAPTCHA)** :

कैप्चा यानी Completed Automated Public Turing test to tell computers and Human Apart इसके प्रयोग से साइबर क्राइम के स्वचालित हमलों से बचा जा सकता है। इसमें उपयोगकर्ता एक तस्वीर में दिखाये गए शब्द को पहचान कर वेबपेज में उपलब्ध जगह पर दर्ज करे तभी आगे बढ़ने की अनुमति मिलती है। इससे साइबर क्राइम को हम रोक सकते हैं।

→ **प्रशिक्षण से जागरूकता**:

साइबर अपराध और उनसे सुरक्षा उपायों पर जागरूकता लाने के लिए सभी बैंक कर्मचारियों को प्रशिक्षण देना आवश्यक है। साइबर सलामती के लिए प्रशिक्षण एक महत्वपूर्ण उपाय है।

→ **सलामती**:

कंप्यूटरों पर जब भी वर्चुअल की-बोर्ड का उपयोग किया जाए तब ये ध्यान रखा जाए कि कोई व्यक्ति आपकी 'की' को देख तो नहीं रहा या फिर यह वहां 'सेव' तो नहीं हो रहा है।

→ **सुरक्षा निर्देश** :

ऑनलाइन बैंकिंग करते समय दिये गए सभी सुरक्षा निर्देशों का पालन सभी को अवश्य ही करना चाहिए। सुरक्षा निर्देशों से हमें सुरक्षा मिलती है।

→ **सॉफ्टवेयर**:

बैंकिंग सेक्टर के सभी कंप्यूटरों में केवल मान्यता प्राप्त सॉफ्टवेयर का उपयोग किया जाना चाहिए।

→ **पेनड्राइव का प्रयोग**:

बैंक को कोई भी अनजान व्यक्ति की पेन ड्राइव या सीडी अपने सिस्टम में नहीं लगानी चाहिए। इसके प्रयोग से सिस्टम में वायरस आ सकते हैं। अगर प्रयोग करना आवश्यक हो तो प्रयोग करने के पहले उन्हें एंटीवायरस द्वारा स्कैन किया जाना चाहिए।

→ **फायरवाल** :

साइबर सिक्योरिटी में 'फायरवॉल' की महत्वपूर्ण भूमिका होती है। ई-बैंकिंग के किसी भी उत्पाद में फायरवॉल का बहुत महत्व है। ज्यादातर सरकारी दफ्तरों, बैंकों तथा निजी संस्थाओं में अपना ही एक पर्सनल कंप्यूटर नेटवर्क होता है जिसे 'इंट्रानेट' कहते हैं। इससे संस्था की कोई भी जानकारी बाहर ना जाए इसलिए उसमें 'फायरवॉल' का उपयोग किया जाता है। फायरवॉल एक सिक्योरिटी गार्ड का काम करती है।

रिज़र्व बैंक ने श्री गोपालकृष्ण के अधीन एक बड़ी पहल यह की है कि सूचना सुरक्षा, इलेक्ट्रॉनिक बैंकिंग के संबंध में प्रौद्योगिकी जोखिम प्रबंधन और साइबर धोखाधड़ी पर एक कार्य समूह का गठन किया है। इस समूह ने 9 बड़े क्षेत्रों के बारे में सिफारिशें की है जैसे कि आईटी अभिशासन, सूचना सुरक्षा, आईएस ऑडिट, आईटी परिचालन, आईटी सेवाओं की आउटसोर्सिंग, साइबर धोखाधड़ी, कारोबार निरंतरता योजना, ग्राहक जागरूकता कार्यक्रम और कानूनी पहलू। भारतीय रिज़र्व बैंक द्वारा दिए गए दिशानिर्देश अनुसार इन सिफारिशों का कार्यान्वयन जोखिम आधारित हो और प्रत्येक बैंक की गतिविधियों के स्वरूप एवं दायरे तथा प्रौद्योगिकी पर उनके कारोबार प्रक्रिया की निर्भरता के अनुरूप हो। ये भी साइबर सुरक्षा में बहुत महत्वपूर्ण है।

बैंकों मैं बोर्ड स्तरीय समितियों को यह आदेश दिया गया है कि इन दिशानिर्देशों को लागू करने की स्थिति पर निगरानी रखें। आज बैंकों में जिस प्रकार से प्रौद्योगिकी ने अपना प्रमुख स्थान बना लिया है उसे देखते हुए इसे मात्र अनुपालन कर लिए जाने का मामला नहीं समझा जाना चाहिए बल्कि इसे अपने कारोबार का प्रमुख अंग मानना चाहिए।

ग्राहकों को शिक्षित करें:

बैंकों में सुरक्षा संस्कृति में बेहतर बदलाव लाने की आवश्यकता है। एक पक्के मकान में शाखा के होने पर यदि तिजोरी के लिए अच्छा ताला लगाने का सिस्टम नहीं है, या दीवारों में दरारें पड़ी हुई हैं, छत टपक रही है, क्या बैंकों ने इस पर ध्यान दिया है। डिजिटल जगत में क्या यह जरूरी नहीं है कि इस प्रकार से छत के टपकने, दरारों को तथा प्रभावित होने की संभावना के लिए उचित कार्यवाही की जाए? ग्राहकों पर फिशिंग के आक्रमण बढ़ रहे हैं। क्या यह बैंकों की जिम्मेदारी नहीं है कि वह अपने ग्राहकों को शिक्षित करें?

साइबर सुरक्षा पूरे विश्व में खास तौर से वित्तीय क्षेत्र में एक महत्वपूर्ण क्षेत्र के रूप में उभरा है जिस पर ध्यान देने की आवश्यकता है। साइबर की घटनाएं अधिकांशतः अंतिम उपयोक्ता को निशाना बनाने के बजाए वित्तीय संस्थाओं को लक्ष्य करने की ओर बढ़ती जा रही है।

डिजिटल संसार बड़ी ही तेजी से आगे बढ़ रहा है और इसीलिए सूचना प्रौद्योगिकी का बहुत ही सावधानीपूर्वक प्रयोग करना अपेक्षित नहीं बल्कि अनिवार्य भी है। बैंकों को अपने स्टाफ सदस्यों के साथ ग्राहकों को भी जागरूक करना होगा । ग्राहकों को साइबर अपराध के लिए उपलब्ध भारत सरकार की साइट cybercrime.gov.in एवं नंबर1930 की जानकारी जनता में साझा करानी होगी।

"इधर कुछ नई संभावनाएं,
उधर कुछ परंपरागत मान्यताएं,
और प्रौद्यौगिकी की हर नई चुनौतियों को स्वीकारते,
आइए! करें साइबर अपराध से बचने की सुरक्षाएं".

*****

शिल्पी बरुआ

पदनाम:- प्रबंधक
संस्था का नाम:- पंजाब नेशनल बैंक
मोबाइल नं. :- 7896941173

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

अर्थव्यवस्था उन स्तंभों में से एक है जो किसी राष्ट्र की प्रगति और विकास को परिभाषित करता है। बैंकिंग क्षेत्र को अर्थव्यवस्था की रीढ़ माना जाता है। बैंक कम्प्यूटरीकरण के क्षेत्र में पहली पहल कम्प्यूटरीकरण (रंगराजन समिति) पर लगातार दो समितियों से हुई थी। पहली समिति का गठन 1984 में किया गया था जिसने बैंकिंग उद्योग में मशीनीकरण और कम्प्यूटरीकरण का ढाचा तैयार किया था। दूसरी समिति का गठन 1989 में किया गया था, जिसने बैंकिंग कार्यों में पूरी तरह से तकनीकी सफलताओं को लागू करने के लिए दूरसंचार और कंप्यूटर के एकीकृत उपयोग का मार्ग प्रशस्त किया। 1990 के दशक के मध्य तक, दुनिया के अधिकांश हिस्सों में बैंकिंग क्षेत्र सरल और विश्वसनीय था; हालांकि, प्रौद्योगिकी के आगमन के बाद से, बैंकिंग क्षेत्र ने इस परिघटना में एक आदर्श बदलाव देखा। वित्तीय प्रणाली समिति (नरसिम्हम समिति) 1991-1998 की सिफारिश पर बैंकिंग क्षेत्र में सूचना और प्रौद्योगिकी का उपयोग किया गया था। डिजिटल तकनीक ने विश्व अर्थव्यवस्थाओं को आपस में जोड़ा है। बैंकों ने अपने ग्राहक आधार को बढ़ाने के लिए कई प्लेटफॉर्म पेश किए जिसके माध्यम से बिना अधिक प्रयास के लेनदेन किया जा सकता है। इन तकनीकों ने ग्राहक को एटीएम और ऑनलाइन बैंकिंग प्रक्रियाओं के माध्यम से 24*7 और साल भर अपने बैंक वित्त तक पहुंचने में सक्षम बनाया।

एक ओर जहां प्रौद्योगिकी ने बैंकों और वित्तीय संस्थानों के लिए लाभ पैदा किया है, वहीं दूसरी ओर, इसमें जोखिम भी शामिल हैं। तकनीकी जोखिमों का न केवल बैंक पर परिचालन जोखिम के रूप में सीधा प्रभाव पड़ता है बल्कि क्रेडिट जोखिम और बाजार जोखिम जैसे अन्य जोखिमों को भी बढ़ा सकता है।

प्रौद्योगिकी ने बैंकिंग सेवाओं, उत्पादों, संचालन के तरीकों और बैंकों के कार्य करने के तरीके में भारी बदलाव किया है। इसने बैंक को ग्राहकों को प्रसन्न करने, परिचालन दक्षता बढ़ाने, बैंकिंग सेवाओं के परिचालन खर्च को कम करने आदि के लिए अधिक उत्पाद लाने में मदद की है, लेकिन यह भी उतना ही सच है कि प्रौद्योगिकी के आगमन ने बैंक को साइबर हमले के प्रति संवेदनशील बना दिया है। आजकल सुरक्षा उल्लंघन, संवेदनशील आईटी संपत्तियों से समझौता और संवेदनशील जानकारी बैंक के लिए एक वास्तविक बड़ी चुनौती है। बढ़ते साइबर खतरों का मुकाबला करने और साइबर जोखिमों को दूर करने के लिए बैंकिंग प्रणाली के लचीलेपन को बढ़ाने के लिए, आरबीआई ने अपने परिपत्र सं. आरबीआई/2015-16/418 दिनांक 2 जून, 2016 ने बैंकों को निम्नानुसार निर्देशित किया:

"व्यापार की जटिलता के स्तर और उनके बोर्ड द्वारा विधिवत अनुमोदित जोखिम के स्वीकार्य स्तरों को देखते हुए एक उपयुक्त दृष्टिकोण वाली रणनीति को स्पष्ट करने वाली साइबर सुरक्षा नीति को लागू करने के लिए।"

बैंकिंग क्षेत्र से संबंधित साइबर अपराध

हैकिंग

एक अपराध है, जिसका अर्थ है किसी व्यक्ति द्वारा सिस्टम को क्रैक करने के लिए अनधिकृत पहुंच या ग्राहकों के बैंकिंग साइटों या खातों को हैक करके सुरक्षा तंत्र को बायपास करने का प्रयास। धारा 43 (ए) के तहत सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 की धारा 66 के साथ और भारतीय दंड संहिता, 1860 की धारा 379 और 406 के तहत एक हैकर को दंडित किया जा सकता है।

कार्ड धोखाधड़ी

ऑनलाइन कार्ड धोखाधड़ी तब होती है जब ग्राहक किसी ऑनलाइन भुगतान के लिए अपने क्रेडिट कार्ड या डेबिट कार्ड का उपयोग करते हैं और कोई अन्य व्यक्ति, दुर्भावनापूर्ण इरादे से, ऐसे कार्ड विवरण और पासवर्ड का उपयोग हैक करके और ग्राहकों द्वारा हैक किए गए कार्ड विवरण या कार्रवाई का उपयोग करके ऑनलाइन खरीदारी के लिए इसका दुरुपयोग करता है।

कीस्ट्रोक लॉगिंग या कीलॉगिंग

कीलॉगिंग एक ऐसी विधि है जिसके द्वारा धोखेबाज वास्तविक कीस्ट्रोक्स और माउस क्लिक को रिकॉर्ड करते हैं। कीलॉगिंग "ट्रोजन" सॉफ़्टवेयर प्रोग्राम हैं जो कंप्यूटर के ऑपरेटिंग सिस्टम को लक्षित करते हैं और वायरस के माध्यम से "इंस्टॉल" होते हैं। ये विशेष रूप से खतरनाक हो सकते हैं क्योंकि जालसाज यूजर आईडी और पासवर्ड, अकाउंट नंबर और टाइप की गई किसी भी चीज को पकड़ लेता है।

वायरस

वायरस एक प्रोग्राम है जो एक निष्पादन योग्य फाइल को संक्रमित करता है और इसे संक्रमित करने के बाद फाइल को असामान्य तरीके से कार्य करने का कारण बनाता है। यह स्वयं को एप्लिकेशन प्रोग्राम और ऑपरेटिंग सिस्टम जैसी निष्पादन योग्य फाइलों से जोड़कर खुद को प्रचारित करता है। निष्पादन योग्य फाइल चलाने से वायरस की नई प्रतिलिपियां बन सकती हैं।

स्पाइवेयर

स्पाइवेयर नंबर एक तरीका है जिससे ऑनलाइन बैंकिंग क्रेडेंशियल चोरी हो जाते हैं और धोखाधड़ी गतिविधियों के लिए उपयोग किए जाते हैं। स्पाइवेयर या तो कंप्यूटर पर जानकारी कैप्चर करके काम करता है या जब यह कंप्यूटर और वेबसाइटों के बीच प्रसारित होता है।

मैलवेयर आधारित हमले

मैलवेयर आधारित हमले इलेक्ट्रॉनिक बैंकिंग सेवाओं से संबंधित सबसे खतरनाक साइबर खतरों में से एक हैं। ऐसे हमलों में, एक दुर्भावनापूर्ण कोड डिज़ाइन किया गया है। आजकल बैंकिंग सेक्टर में मालवेयर अटैक की संख्या बढ़ती जा रही है। कुछ कुख्यात बैंकिंग मैलवेयर Carbep, Tinba, Spyeye, Zeus और KINS हैं। Zeus इन मैलवेयर में सबसे पुराना है। यह जुलाई 2007 में पता चला था जब संयुक्त राज्य अमेरिका के परिवहन विभाग से जानकारी खो गई थी और चोरी हो गई थी।

डिस्ट्रीब्यूटेड डिनायल-ऑफ-सर्विस (DDoS) अटैक

एक दुर्भावनापूर्ण प्रयास है जो लक्षित सर्वर, सेवा या नेटवर्क के सामान्य ट्रैफ़िक को बाधित करने के लिए इंटरनेट ट्रैफ़िक की बाढ़ के साथ लक्ष्य या उसके आस-पास के बुनियादी ढांचे को प्रभावित करता है।

Man in the Middle Attack (MIDM)

हमला साइबर हमले का एक रूप है जहां एक उपयोगकर्ता को दो पक्षों के बीच किसी दुर्भावनापूर्ण व्यक्ति द्वारा किसी प्रकार की बैठक के साथ पेश किया जाता है, दोनों पक्षों में हेरफेर करता है और उस डेटा तक पहुंच प्राप्त करता है जिसे दो लोग एक-दूसरे तक पहुंचाने का प्रयास कर रहे थे।

एसक्यूएल इंजेक्शन (SQLI)

SQL इंजेक्शन एक सामान्य हमला है जो तब होता है जब साइबर अपराधी संवेदनशील जानकारी तक पहुंचने के लिए बैकएंड डेटाबेस हेरफेर के लिए दुर्भावनापूर्ण 501 स्क्रिप्ट का उपयोग करते हैं। एक बार हमला सफल हो जाने पर, SQL डेटाबेस में संग्रहीत संवेदनशील कंपनी डेटा, उपयोगकर्ता सूचियों या निजी ग्राहक विवरणों को देख, बदल या हटा सकता है।

ब्रूट फोर्स अटैक

एक क्रिप्टोग्राफिक हैक है जो सही जानकारी की खोज होने तक सभी संभावित संयोजनों का अनुमान लगाने के लिए एक परीक्षण-और-ब्रुटि पद्धति का उपयोग करता है।

डोमेन नेम सिस्टम (DNS) अटैक

DNS हमला एक प्रकार का साइबर हमला है जिसमें साइबर अपराधी साइट उपयोगकर्ताओं को दुर्भावनापूर्ण वेबसाइटों (DNS अपहरण) पर पुनर्निर्देशित करने और प्रभावित कंप्यूटरों से डेटा चोरी करने के लिए डोमेन नाम प्रणाली की खामियों का फायदा उठाते हैं। यह एक गंभीर साइबर सुरक्षा जोखिम है क्योंकि DNS सिस्टम इंटरनेट इन्फ्रास्ट्रक्चर का एक अनिवार्य तत्व है।

साइबर सुरक्षा का उद्देश्य

इंटरनेट से जुड़े सिस्टम जैसे कंप्यूटर, सर्वर, मोबाइल डिवाइस, इलेक्ट्रॉनिक सिस्टम, नेटवर्क और डेटा को दुर्भावनापूर्ण हमलों से बचाने की तकनीक को साइबर सुरक्षा के रूप में जाना जाता है। सुरक्षा समुदाय डेटा को साइबर हमलों से बचाने के लिए तीन संबंधित सिद्धांतों का एक त्रिकोण प्रदान करता है। इस सिद्धांत को CIA ट्रायड कहा जाता है।

हम CIA मॉडल को तीन भागों में विभाजित कर सकते हैं: गोपनीयता, अखंडता और उपलब्धता।

साइबर सुरक्षा के प्रति बैंक का दृष्टिकोण निम्नलिखित सिद्धांतों पर आधारित है;

ग्राहक की गोपनीय जानकारी, सिस्टम और नेटवर्क की सुरक्षा और उनकी गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने के लिए बैंक की एक महत्वपूर्ण जिम्मेदारी है। इसलिए, बैंक नवीन और नई तकनीकों को बनाने और अपनाने के दौरान साइबर सुरक्षा आवश्यकताओं को लागू करने के एक उदाहरण का नेतृत्व करता है

साइबर सुरक्षा उद्देश्य के खिलाफ प्रगति के लिए पहल

i) साइबर सुरक्षा प्रशिक्षण और जागरूकता का संचालन करना।
ii) सॉफ्टवेयर और ऑपरेटिंग सिस्टम का अद्यतनीकरण।
iii) एंटी-वायरस सॉफ़्टवेयर का उपयोग।
iv) समय-समय पर सुरक्षा समीक्षा करना।
v) मजबूत पासवर्ड का इस्तेमाल।

vi) अज्ञात प्रेषकों के ई-मेल अटैचमेंट नहीं खोलना।
vii) सार्वजनिक स्थानों पर असुरक्षित वाई-फाई नेटवर्क का उपयोग करने से बचें।

साइबर सुरक्षा उपायों को स्पष्ट करने के लिए, लिखित मानदंडों की आवश्यकता होती है। इन मानदंडों को साइबर सुरक्षा मानकों के रूप में जाना जाता है: कुछ उपायों के आदर्श निष्पादन के लिए नुस्खे के सामान्य सेट।

सुरक्षा मानक आम तौर पर सभी संगठनों के लिए प्रदान किए जाते हैं, चाहे उनका आकार कुछ भी हो या जिस उद्योग और क्षेत्र में वे काम करते हैं। इस खंड में प्रत्येक मानक के बारे में जानकारी शामिल है जिसे आमतौर पर किसी भी साइबर सुरक्षा रणनीति के एक आवश्यक घटक के रूप में मान्यता प्राप्त है।

i. ISO

ISO का मतलब अंतर्राष्ट्रीय मानकीकरण संगठन है। अंतर्राष्ट्रीय मानक काम करने के लिए चीजें बनाते हैं। ये मानक गुणवत्ता, सुरक्षा और दक्षता सुनिश्चित करने के लिए उत्पादों, सेवाओं और कंप्यूटरों के लिए विश्व स्तरीय विनिर्देश प्रदान करते हैं। वे अंतर्राष्ट्रीय व्यापार को सुविधाजनक बनाने में महत्वपूर्ण भूमिका निभाते हैं।

ii. IT अधिनियम

सूचना प्रौद्योगिकी अधिनियम को आईटीए-2000 के रूप में भी जाना जाता है या आईटी अधिनियम का मुख्य उद्देश्य भारत में कानूनी बुनियादी ढांचा प्रदान करना है जो साइबर अपराध और ई-कॉमर्स से निपटता है।

iii. कॉपीराइट अधिनियम

कॉपीराइट अधिनियम 1957, कॉपीराइट संशोधन अधिनियम 2012 द्वारा संशोधित, भारत में कॉपीराइट कानून के विषय को नियंत्रित करता है। यह अधिनियम 21 जनवरी, 1958 से लागू है।

साइबर सुरक्षा उपकरण

i) फ़ायरवॉल:

फ़ायरवॉल एक प्रोग्राम या हार्डवेयर डिवाइस है जो आने वाले और बाहर जाने वाले नेटवर्क ट्रैफ़िक का विश्लेषण करता है और पूर्व निर्धारित नियमों के आधार पर वायरस और हमलावरों को ब्लॉक करने में बाधा उत्पन्न करता है। अगर कोई भी आने वाली जानकारी फ़िल्टर द्वारा फ़्लैग की जाती है, तो उसे ब्लॉक कर दिया जाता है।

ii) एंटीवायरस सॉफ्टवेयर

एंटीवायरस सॉफ़्टवेयर एक प्रोग्राम है जिसे व्यक्तिगत कंप्यूटर, नेटवर्क और आईटी सिस्टम पर वायरस और अन्य मैलवेयर हमलों को रोकने, पता लगाने और हटाने के लिए डिज़ाइन किया गया है।

iii) PKI सेवाएं

PKI का मतलब पब्लिक की इंफ्रास्ट्रक्चर है। यह उपकरण सार्वजनिक एमन्क्रिप्शन कुंजियों के वितरण और पहचान का समर्थन करता है। यह उपयोगकर्ताओं और कंप्यूटर सिस्टम को इंटरनेट पर सुरक्षित रूप से डेटा का आदान-प्रदान करने और दूसरे पक्ष की पहचान सत्यापित करने में सक्षम बनाता है।

iv) मैनेज्ड डिटेक्शन एंड रिस्पांस सर्विस (MDR)

आज के साइबर अपराधियों और हैकर्स ने संगठन की सुरक्षा को भंग करने के लिए अधिक उन्नत तकनीकों और

सॉफ़्टवेयर का उपयोग किया है, इसलिए प्रत्येक व्यवसाय के लिए साइबर सुरक्षा के अधिक शक्तिशाली रूपों का उपयोग करने की आवश्यकता है । यह एक उन्नत सुरक्षा सेवा है जो खतरे के शिकार, खतरे की खुफिया जानकारी, सुरक्षा निगरानी, घटना विश्लेषण और घटना प्रतिक्रिया प्रदान करती है।

v) पेनेट्रेशन टेस्टिंग

पेनेट्रेशन टेस्टिंग, कमजोरियों का सुरक्षित रूप से फायदा उठाने की कोशिश करके व्यावसायिक सुरक्षा प्रणालियों और आईटी बुनियादी ढांचे की सुरक्षा का मूल्यांकन करने का एक महत्वपूर्ण तरीका है।

vi) Vulnerability Testing

यह सूचना प्रणाली में सुरक्षा कमजोरियों की एक व्यवस्थित समीक्षा है। यह मूल्यांकन करता है कि क्या सिस्टम किसी भी ज्ञात कमजोरियों के लिए अतिसंवेदनशील है, उन कमजोरियों के लिए गंभीरता के स्तर प्रदान करता है और जब भी आवश्यक हो, उपचार की सिफारिश करता है।

vii) हनीपोट

हनीपोट एक सुरक्षा तंत्र है जो हमलावरों को लुभाने के लिए एक आभासी जाल बनाता है। एक जानबूझकर समझौता किया गया कंप्यूटर सिस्टम हमलावरों को कमजोरियों का फायदा उठाने की अनुमति देता है ताकि बैंक अपनी सुरक्षा नीतियों को बेहतर बनाने के लिए उनका अध्ययन कर सकें।

viii) कर्मचारियों के प्रशिक्षण

स्टाफ प्रशिक्षण एक 'साइबर सुरक्षा उपकरण' नहीं है, लेकिन जानकार कर्मचारी जो साइबर सुरक्षा को समझते हैं, वो साइबर हमलों के खिलाफ रक्षा के सबसे मजबूत रूप हो सकते हैं ।

साइबर हमलों से बचाव के लिए बैंकों को सभी चैनलों और ग्राहकों के व्यवहार पर व्यापक दृष्टिकोण रखना चाहिए। संदिग्ध लेनदेन का पता लगाने में सुधार के लिए मशीन लर्निंग (ML), आर्टिफिशियल इंटेलिजेंस (AI) और बिग डेटा सहित तकनीकों का तेजी से उपयोग किया जा सकता है। #. और |/॥ के साथ मजबूत पहचान और प्रमाणीकरण विधियों को जोड़कर, बैंक वास्तविक समय में बड़ी मात्रा में डेट की छानबीन कर सकते हैं और संदिग्ध लेनदेन की पहचान कर सकते हैं। बिग डेटा संदिग्ध आईपी पते और फ़िशिंग हमलों के बीच लिंक स्थापित करने में सक्षम बनाता है, बैंक को उस पते से लेनदेन के लिए सचेत करता है। |॥. के साथ बिग डेटा को मिलाकर, साइबर सुरक्षा आगे बढ़ने वाली विसंगतियों का पता लगाने के लिए 'सीख' सकती है। ग्राहक के सामान्य व्यवहार के साथ असंगत लेनदेन से भी अलर्ट उत्पन्न हो सकते हैं। साइबर हमलों की जटिल प्रकृति के लिए बैंकों को लेनदेन को अधिक सक्रिय रूप से ट्रैक और पता लगाने की आवश्यकता है।

*****

शिव कुमार

पदनाम:- प्रबंधक
संस्था का नाम:- आईएफसीआई लिमिटेड
मोबाइल नं. :- 9560021905
ई-मेल:- shiv.kumar@ifciltd.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

परिचय:

प्रौद्योगिकी में प्रगति के साथ बैंकिंग क्षेत्र पारंपरिक बैंकिंग से ई-बैंकिंग में तेजी से परिवर्तित हो गया है, एटीएम (स्वचालित टेलर मशीन), इंटरनेट बैंकिंग और मोबाइल बैंकिंग जैसे विभिन्न तरीकों के माध्यम से 24x7 बैंकिंग सुविधा प्रदान करता है, जिसने बैंक और ग्राहक के बीच की खाई को कम कर दिया है।

विकास के आह्वान ने इस इकाई को अनेकों अवसर दिए हैं और इसलिए, बैंक वर्तमान में आईटी के सबसे बड़े ग्राहकों में से एक हैं। यूपीआई, नेफ्ट (नेशनल इलेक्ट्रॉनिक स्टोर एक्सचेंज), आरटीजीएस, ईसीएस (इलेक्ट्रॉनिक क्लियरिंग एडमिनिस्ट्रेशन) और पोर्टेबल एक्सचेंज जैसे प्रगति पर बढ़ते ऑनलाइन एक्सचेंजों पर इनकी गहन नज़र है। जैसा कि यह जग जाहिर है कि एक सिक्के के दो पहलू होते हैं। यदि इतनी सुविधाएं हैं तो साथ में खतरे भी, उपलब्धियां हैं तो कठिनाइयां भी साथ होती हैं। परिणामस्वरूप, पीसी और वेब नवाचार के त्वरित विकास के साथ, नए प्रकार के समग्र अपराध जिन्हें 'डिजिटल रांगड्यूगिंस' के रूप में जाना जाता है, वे भी काफी मात्रा में बढ़े हैं। कुछ अपरिभाषित समय में, साइबर अपराध की घटनाओं की रूपरेखा, प्रकृति और उदाहरण उत्तरोत्तर आधुनिक और जटिल हो गए हैं। हाल के एक दशक में बैंक और धन से संबंधित फाउंडेशन डिजिटल अपराधियों का बेरोकटोक फोकस बना हुआ है।

साइबर क्राइम क्या है?

ऐसा कोई भी अपराध, जिसमें कंप्यूटर और नेटवर्क शामिल हैं। कुछ मामलों में, कंप्यूटर का उपयोग अपराध करने के लिए किया गया हो सकता है और अन्य मामलों में कंप्यूटर अपराध का लक्ष्य हो सकता है। साइबर अपराध को आम तौर पर एक आपराधिक गतिविधि के रूप में परिभाषित किया जा सकता है जिसमें सूचना प्रौद्योगिकी प्रणाली अपराध को अंजाम देने के लिए उपयोग किए जाने वाले साधन हैं।

2016 में, जुनिपर एक्सप्लोरेशन की एक जांच ने मूल्यांकन किया कि 2019 तक साइबर अपराध का दुनिया भर में खर्च 2.1 ट्रिलियन तक हो सकता है। वैसे भी, यह मूल्यांकन केवल आंके गए हैं और बिना रिपोर्ट किए गए नुकसान सहित साइबर अपराध का वास्तविक खर्च अतुलनीय है। दि हिंदू समाचार-पत्र द्वारा प्रकाशित रिपोर्ट के अनुसार, भारत में 2020 में साइबर अपराधों में 11.8% की वृद्धि दर्ज की गई।

बैंकिंग क्षेत्र से संबंधित साइबर अपराध: बैंकिंग क्षेत्र से संबंधित साइबर अपराध कुछ सामान्य साइबर अपराधों की व्याख्या नीचे की गई है:

(1) हैकिंग : हैकिंग एक अपराध है, जिसका अर्थ है किसी व्यक्ति द्वारा सिस्टम को क्रैक करने के लिए अनधिकृत पहुंच या ग्राहकों के बैंकिंग साइटों या खातों को हैक करके सुरक्षा तंत्र को बायपास करने का प्रयास।

निवारक उपाय:

1) अपने सिस्टम/डिवाइस (डेस्कटॉप, लैपटॉप, मोबाइल) को हमेशा नवीनतम पैच के साथ अपडेट रखें और नवीनतम संस्करण के साथ एंटी-वायरस जैसे सुरक्षा सॉफ्टवेयर के माध्यम से सिस्टम/डिवाइस को सुरक्षित रखें।
2) हमेशा ज्ञात विश्वसनीय स्रोतों से ही सॉफ्टवेयर या ऐप्लिकेशन डाउनलोड करें। अपने सिस्टम/डिवाइस पर कभी भी पायरेटेड सॉफ्टवेयर का उपयोग न करें।
3) सुनिश्चित करें कि सभी डिवाइस/खाते एक मजबूत पिन या पास कोड द्वारा सुरक्षित हैं। पिन या पासवर्ड कभी भी किसी के साथ साझा न करें।
4) कंप्यूटर/लैपटॉप एक फायरवॉल और एंटीवायरस स्थापित, सक्षम और नवीनतम संस्करणों के साथ अद्यतन होना चाहिए।
5) अपने कंप्यूटर, लैपटॉप या हाथ से पकड़े जाने वाले उपकरणों पर कभी भी पायरेटेड सॉफ्टवेयर, ऐप्लिकेशन आदि को डाउनलोड या इंस्टॉल न करें।
6) कंप्यूटर से कनेक्ट करते समय हमेशा बाहरी उपकरणों को वायरस के लिए स्कैन करें।

(2) फिशिंग या पहचान की चोरी:

फिशिंग एक ऐसा घोटाला है जहां इंटरनेट धोखेबाज ऑनलाइन उपयोगकर्ताओं से व्यक्तिगत जानकारी का अनुरोध करते हैं। ये अनुरोध आमतौर पर किसी संगठन के ई-मेल के रूप में होते हैं जिसके साथ कोई व्यवसाय कर सकता है या नहीं भी कर सकता है। कई मामलों में, ई-मेल को ठीक उसी तरह बनाया गया है जैसे किसी वैध संगठन का ई-मेल कंपनी के लोगो और अन्य ठोस जानकारी के साथ पूर्ण दिखाई देगा। ई-मेल में आमतौर पर सभी उपयोगकर्ता को उस साइट के लिंक पर क्लिक करने के लिए कहा जाता है जो बिल्कुल वास्तविक चीज़ की तरह दिखती है कि बैंक को व्यक्तिगत जानकारी अपडेट करने की आवश्यकता है या खाता निष्क्रिय होने वाला है। फिशिंग वित्तीय संस्थानों के ग्राहकों द्वारा स्वतःस्फूर्त संदेशों की प्राप्ति का संकेत देता है, उनसे किसी कारण से अपने खाते तक पहुंचने के लिए अपना उपयोगकर्ता नाम, पासवर्ड या अन्य व्यक्तिगत डेटा दर्ज करने के लिए कहता है। इसके बाद जालसाज को ग्राहक से प्राप्त विवरण का धोखे से दुरुपयोग करके बैंक खाते में उपलब्ध ग्राहक के ऑनलाइन वित्तीय शेष और उस खाते में निहित धनराशि में प्रवेश मिलता है।

22 सितंबर, 2021 को शोधकर्ताओं ने बताया कि भारत में एंड्रॉइड फोन बैंकिंग ग्राहकों को ड्रिनिक बैंकिंग ट्रोजन मैलवेयर को लक्षित किया जा रहा था। मैलवेयर ने फिशिंग तकनीकों का उपयोग करके उपयोगकर्ताओं का व्यक्तिगत डेटा और धन चुरा लिया।

निवारक उपाय:

सुनिश्चित करें कि सभी डिवाइस/खाते एक मजबूत पिन या पास कोड द्वारा सुरक्षित हैं। कभी भी अपना पिन या पासवर्ड किसी के साथ साझा न करें।

अपना नेट-बैंकिंग पासवर्ड, वन टाइम पासवर्ड (ओटीपी), एटीएम या फोन बैंकिंग पिन, सीवीवी नंबर आदि किसी भी व्यक्ति के साथ साझा न करें, भले ही वह बैंक का कर्मचारी या प्रतिनिधि होने का दावा करता हो और ऐसी घटनाओं को तुरंत बैंक में रिपोर्ट करें।

(3) विशिंग: मौद्रिक पुरस्कारों के साथ निजी व्यक्तिगत डेटा तक पहुंचने के लिए फोन ढांचे के माध्यम से सामाजिक डिजाइनिंग का उपयोग करना, यह आपराधिक दिनचर्या है। इस प्रकार के अपराध में आपको धोखाधड़ी वाले कॉल प्राप्त हो सकते हैं जहां कॉलर बैंक प्रतिनिधि के रूप में पेश होता है और आपके खाते की जानकारी मांगता है।

निवारक उपाय:

अपना नेट-बैंकिंग पासवर्ड, वन टाइम पासवर्ड (ओटीपी), एटीएम या फोन बैंकिंग पिन, सीवीवी नंबर आदि किसी भी व्यक्ति के साथ साझा न करें, भले ही वह बैंक का कर्मचारी या प्रतिनिधि होने का दावा करता हो और और ऐसी घटनाओं को तुरंत बैंक में रिपोर्ट करें।

(4) क्रेडिट कार्ड पुनर्निर्देशन और फार्मिंग: फार्मिंग शब्द 'खेती' और 'फिशिंग' से जुड़ा हुआ है। फार्मिंग में एक बैंक के यूआरएल को अपराधियों द्वारा इस तरह से हाईजैक कर लिया जाता है कि जब कोई ग्राहक बैंक की वेबसाइट पर लॉग इन करता है तो उन्हें दूसरी वेबसाइट पर भेज दिया जाता है जो नकली है लेकिन बैंक की मूल वेबसाइट की तरह दिखती है।

निवारक उपाय:

1. असुरक्षित लिंक पर कभी भी क्लिक न करें
2. बैंक के यूआरएल को ठीक से जांचें और यूआरएल बार में केवल एचटीपीएस और पैडलॉक आइकन वाली प्रामाणिक वेबसाइट का उपयोग करें
3. एक अच्छे एंटीवायरस का उपयोग करें जो संपूर्ण इंटरनेट सुरक्षा प्रदान करता हो

(5) एटीएम स्किमिंग: एटीएम स्किमिंग एक प्रकार से आपके कार्ड की डुप्लीकेट प्रति बना कर धोखाधड़ी करना है। यह छिपे हुए रिकॉर्डिंग उपकरणों के साथ मशीनों में हेराफेरी करके क्रेडिट कार्ड और डेबिट कार्ड से पिन और अन्य जानकारी चुराने का एक तरीका है।

निवारक उपाय:

एटीएम का उपयोग करने से पहले स्किमर्स या पिन देखने वाले लोगों के लिए परिवेश का निरीक्षण करें और पिन दर्ज करते समय कीपैड को कवर करें।

अपने बैंक और क्रेडिट कार्ड स्टेटमेंट की अक्सर जांच करें

1. पिन को छिपाने के लिए उचित सावधानी बरतते हुए स्वयं पिन दर्ज करें
2. यह सुनिश्चित करने के लिए कीपैड को भौतिक रूप से जांचें कि उसमें ओवरले डिवाइस तो नहीं है।
3. एटीएम/डेबिट कार्ड/क्रेडिट कार्ड से लेन-देन करते समय किसी को भी अपने पास या पीछे खड़े न होने दें।
4. ऐसा पिन न रखें जिसका अंदाजा आसानी से लगाया जा सके। पिन बदलते रहें।
5. सुनिश्चित करें कि आपको लेन-देन की रसीद या पुष्टिकरण एसएमएस के माध्यम से प्राप्त हो।
6. सुनिश्चित करें कि एटीएम मशीन का कोई भी हिस्सा खुला या ढीला जुड़ा न हो।

(6) मैलवेयर आधारित हमले: मैलवेयर आधारित हमले इलेक्ट्रॉनिक बैंकिंग सेवाओं से संबंधित सबसे खतरनाक साइबर अपराधों में से एक है। मैलवेयर हमला एक सामान्य साइबर हमला है जहां मैलवेयर (सामान्यतः दुर्भावनापूर्ण सॉफ्टवेयर) पीड़ित के सिस्टम पर अनधिकृत कार्रवाइयां निष्पादित करता है। इस सॉफ्टवेयर में कई विशिष्ट प्रकार के हमले शामिल हैं जैसे रैंसमवेयर, स्पाईवेयर, कमांड और नियंत्रण, और बहुत कुछ।

सुरक्षा पत्रिका के अनुसार, बैंकिंग उद्योग ने 2021 में रैंसमवेयर हमलों में 1318% की वृद्धि देखी है।

निवारक उपाय:

- **अच्छे एंटी-मैलवेयर सॉफ़्टवेयर का उपयोग करें**
- **सार्वजनिक वाई-फाई नेटवर्क पर वीपीएन सेवाओं का उपयोग करें**
- **अपने प्रोग्राम और ऑपरेटिंग सिस्टम को अपडेट रखें**
- **संदिग्ध ई-मेल अटैचमेंट न खोलें**
- **ऑफलाइन बैकअप**

(8) **गुगल पे/फोनपे/पेटीएम पर पैसे मांगने के लिए क्यूआर कोड/लिंक से धोखाधड़ी**: साइबर धोखेबाज पीड़ितों को गुगल पे/फोनपे/पेटीएम के माध्यम से उनके बैंक खातों में पैसे स्कैन करने और प्राप्त करने के लिए डेबिट लिंक या क्यूआर कोड भेजते हैं। लेकिन धन प्राप्त करने के बजाय, यह ग्राहक के खाते से डेबिट हो जाता है क्योंकि अपराधी एक अनुरोध धन क्यूआर कोड / लिंक भेजते हैं।

निवारक उपाय:

- किसी भी लिंक को कभी भी स्वीकार/क्लिक न करें या असत्यापित स्रोतों से किसी भी क्यूआर कोड को स्कैन न करें क्योंकि वह लिंक आपको कोई अपराधी भी भेज सकते हैं।
- पैसे प्राप्त करने के लिए, एमपिन या यूपीआई पिन दर्ज करने की आवश्यकता नहीं है।

साइबर अपराध रोकने के सामान्य उपाय :

बैंकिंग क्षेत्र हमारी अर्थव्यवस्था की रीढ़ है। साइबर अपराध के मामलों की बढ़ती संख्या के कारण हमारी अर्थव्यवस्था को भारी नुकसान हुआ है। उपयुक्त कानून सुनिश्चित करके साइबर हमलों को रोका जाना चाहिए जिसे प्रभावी ढंग से लागू किया गया है। बैंकों और ग्राहक दोनों को इसमें शामिल करके जोखिम और सुरक्षा उपायों के बारे में जागरूक किया जाना चाहिए। साइबर अपराध का मुकाबला करने के लिए विभिन्न हितधारकों के बीच सहयोग की आवश्यकता है। भारत सरकार ने अपनी साइबर सुरक्षा रणनीति के प्रभावी कार्यान्वयन से संबंधित सभी मामलों के समन्वय के लिए नोडल एजेंसी के रूप में राष्ट्रीय सुरक्षा परिषद के साथ एक अंतर विभागीय सूचना सुरक्षा कार्य बल (आईएसटीएफ) की स्थापना की है।

ग्राहक को शिक्षा:

ग्राहक को विभिन्न बैंक धोखाधड़ी के बारे में शिक्षित और जागरूक किया जाना चाहिए और उन्हें सुरक्षा तंत्र के उपायों के बारे में सूचित किया जाना चाहिए ताकि वे साइबर अपराध के शिकार न हों। यदि कोई ग्राहक जागरूक है और साइबर अपराध की सूचना देता है, तो प्रारंभिक चरण में भी साइबर अपराध की घटनाओं को कम किया जा सकता है। एक ग्राहक को ई-बैंकिंग से संबंधित क्या करें और क्या न करें के बारे में जागरूक किया जाना चाहिए। इसे बैंक की वेबसाइट पर प्रकाशित करके, समाचार पत्रों में प्रकाशित करके, विज्ञापनों

के माध्यम से, एसएमएस अलर्ट भेजकर, पोस्टर शिक्षा आदि के माध्यम से किया जा सकता है। यदि कोई बैंक आरबीआई के दिशानिर्देशों के अनुसार कोई नई नीति पेश करता है या कोई परिवर्तन करता है, जिसका पालन सभी बैंकों को करने की आवश्यकता होती है, तो बैंकों को ग्राहक को मेल के माध्यम से या टेलीफोन के माध्यम से सूचित करना चाहिए। कानून और आरबीआई दिशा-निर्देशों में बदलावों को ध्यान में रखते हुए जागरूकता सामग्री को समय पर अद्यतन किया जाना चाहिए।

बैंक कर्मचारियों को प्रशिक्षण

बैंकों द्वारा कर्मचारियों के लिए प्रशिक्षण और अभिविन्यास कार्यक्रम आयोजित किए जाने चाहिए। कर्मचारियों को धोखाधड़ी की रोकथाम के उपायों के बारे में जागरूक किया जाना चाहिए। यह समाचारपत्रों या पत्रिकाओं के माध्यम से किया जा सकता है जो वरिष्ठ अधिकारियों द्वारा बैंकों के धोखाधड़ी से संबंधित पहलुओं पर प्रकाश डालते हैं, कर्मचारियों के कार्यस्थल पर 'क्या करें और क्या न करें' डालें, कोर बैंकिंग में लॉग इन करते समय स्क्रीन पर सुरक्षा युक्तियों को प्रदर्शित करें। समाधान सॉफ्टवेयर, साइबर अपराध पैदा करने वाले कारकों पर चर्चा करें और उनसे निपटने के लिए आवश्यक कार्रवाई करें।

मजबूत एन्क्रिप्शन-डिक्रिप्शन विधियां:

ई-बैंकिंग गतिविधियों को सिक्योर सॉकेट लेयर (एसएसएल) का उपयोग करके निपटाया जाना चाहिए। यह एक वेब सर्वर और एक इंटरनेट ब्राउज़र के बीच डेटा का एन्क्रिप्शन लिंक प्रदान करता है। लिंक सुनिश्चित करता है कि डेटा गोपनीय और सुरक्षित रहे। सुरक्षा लेन-देन सुनिश्चित करने के लिए भुगतान प्रणाली जैसे आरटीजीएस, एनईएफटी, चेक ट्रंकेशन सिस्टम में सार्वजनिक कुंजी अवसंरचना का उपयोग किया जाना चाहिए। वायरलेस सुरक्षा समाधान भी शामिल किए जाने चाहिए। डेनियल ऑफ सर्विस अटैक के मामलों में, बैंकों को नेटवर्क सुरक्षा उपकरणों को स्थापित और कॉन्फ़िगर करना चाहिए।

शारीरिक और कार्मिक सुरक्षा:

बैंकों को खतरों के संबंध में और संस्थान की विशिष्ट भौगोलिक स्थिति और पड़ोसी संस्थाओं आदि के आधार पर उचित भौतिक और पारिस्थितिकी तंत्र नियंत्रण निष्पादित करना चाहिए। साथ ही, जब कोई नया कर्मचारी कार्यरत होता है तो आवेदक के सत्यापन की प्रक्रिया होनी चाहिए। सत्यापन का स्तर स्थिति और जॉब प्रोफाइल के आधार पर अलग-अलग हो सकती है।

एटीएम में हमेशा एक सुरक्षा गार्ड होना चाहिए जिसने उचित प्रशिक्षण प्राप्त किया हो। ऐसा इसलिए है क्योंकि कई घटनाएं होती हैं जहां एटीएम मशीनों को स्किम किया जाता है और एटीएम धोखाधड़ी होती है।

निष्कर्ष:

वर्तमान परिदृश्य में, भारतीय बैंकिंग क्षेत्र इलेक्ट्रॉनिक माध्यम से की जाने वाली बैंकिंग गतिविधियों से बच नहीं सकता है, लेकिन साइबर अपराध वास्तविक जीवन अपराधों की तुलना में अधिक गंभीर अपराध है, इस समस्या को दूर करने के लिए ग्राहकों को इन मामलों की सूचना निकटतम पुलिस स्टेशन और साइबर अपराध में देनी चाहिए। बैंकों में इन मुद्दों को रोकने के लिए, विधायिका को बैंकों की कार्य प्रणाली पर नजर रखनी चाहिए और इस तरह के गलत कामों की निगरानी के लिए कानून का कार्यान्वयन सख्त होना चाहिए और इसके अलावा बैंकों को ग्राहकों को अक्सर साइबर अपराधों के बारे में जागरूकता के बारे में शिक्षित करना चाहिए।

*****

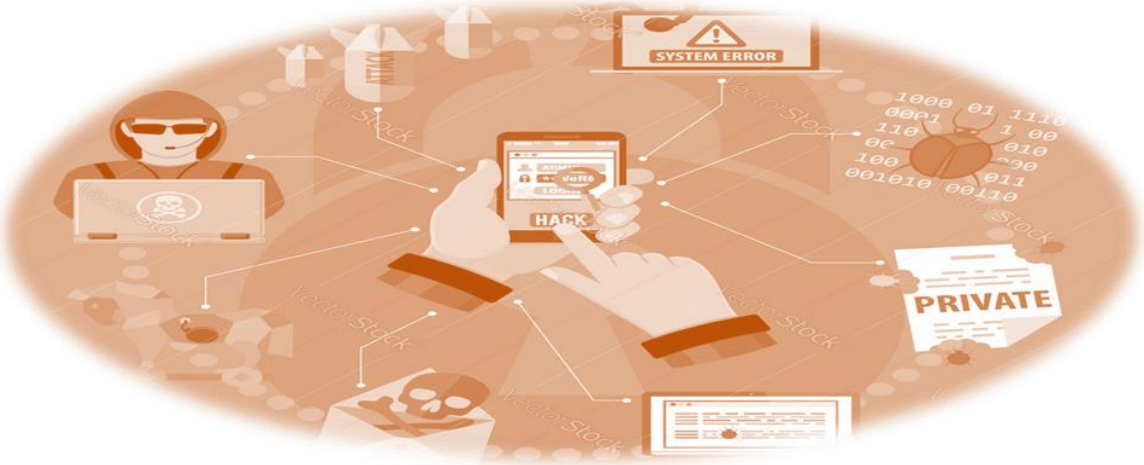
शेषांत कुमार

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 8604078698
ई-मेल:- sheshant.kumar@bankofbaroda.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

मनुष्य दिन प्रतिदिन प्रगति के पथ पर अग्रसर है। इस प्रगति में प्रौद्योगिकी एवं तकनीक का महत्वपूर्ण योगदान रहा है। इनकी अनुपस्थिति में इस अभूतपूर्व प्रगति की कल्पना भी नहीं की जा सकती। जीवन के हर क्षेत्र में तकनीक ने अपनी गहरी पैठ बना ली है। आज आप जो भी सोच सकते हैं उस तक इंटरनेट के माध्यम से पहुंच भी सकते हैं। विगत कुछ वर्षों में हमारे देश में आई इंटरनेट की सुगम एवं कम लागत में उपलब्धता ने इस आयाम को और व्यापक बना दिया है।

मार्च, 2020 में समस्त विश्व के समक्ष कोविड 19 के रूप में एक नयी चुनौती प्रकट हुई जिसके कारण समस्त व्यक्तिगत एवं व्यावसायिक गतिविधियां ठहर सी गईं। इस विशिष्ट परिस्थिति ने भी हम सभी को इंटरनेट एवं संबंधित तकनीकों के उपयोग की ओर अग्रसारित किया तथा भारत वस्तुतः डिजिटल भारत बनने की राह पर चल पड़ा।



विगत कुछ वर्षों में बैंकिंग प्रणाली ने भी लेन-देन एवं अन्य कार्यों के संपादन के लिए अपने पारंपरिक कलेवर से निकलकर वैकल्पिक माध्यमों को खुली बाँहों से अपनाया है। आज किसी भी प्रकार की बैंकिंग सेवा प्राप्त करने के लिए बैंक जाने की आवश्यकता नहीं है, इस संबंध में सभी बैंकिंग संस्थान "**बैंक आपके द्वार**" से आगे बढ़कर "**बैंकिंग आपकी उँगलियों पर**" के तर्ज पर सेवाएं उपलब्ध करा रहे हैं।

इस नयी परिस्थिति ने साइबर अपराधों को भी बढ़ावा दिया है तथा इन अपराधियों ने अपराध और तकनीक के समन्वय से इस नयी कार्यप्रणाली को अंगीकार कर नयी चुनौती पेश कर दी है। दिन-प्रतिदिन हम अपने आस-पास हो रही इन साइबर धोखाधड़ियों के बारे में सुनते एवं देखते रहते हैं। आइए, साइबर अपराध की गंभीरता को प्रदर्शित करते आंकड़े पर एक नजर डालते हैं:

वर्ष	संख्या
2017-18	1,59,761
2018-19	2,46,514
2019-20	2,90,445

(स्रोत: भारतीय कंप्यूटर आपात प्रतिक्रिया दल - सीईआरटी)

सन् 2001 में अंतर्राष्ट्रीय स्तर पर राष्ट्रों के पारस्परिक सहयोग से साइबर अपराध की रोकथाम हेतु संधि की गई जिसे बुडापेस्ट कन्वेंशन के नाम से जाना जाता है एवं दिसंबर, 2020 तक इसके अंतर्गत कुल -65 - राष्ट्र आ चुके हैं। अंतर्राष्ट्रीय परिदृश्य में साइबर सुरक्षा पर अक्तूबर, 2016 में जी-7 देशों की बैठक में वित्तीय क्षेत्र के लिए साइबर सुरक्षा के मूल तत्वों को परिभाषित एवं क्रियान्वयित किए जाने की दिशा में बात की गई थी जिसमे निम्नांकित मूलभूत बिंदु शामिल थे:

- कार्यनीति एवं क्रियान्वयन का ढांचा
- जोखिम का आंकलन
- निगरानी एवं नियंत्रण
- सूचना साझा किया जाना
- अभिशासन

बैंकों पर एक बड़े साइबर हमले की आशंका तब से बढ़ गई है जब हैकर्स ने फरवरी 2016 में बांग्लादेश के केंद्रीय बैंक से लगभग 100 मिलियन अमरीकी डॉलर की सफलतापूर्वक चोरी कर ली। यूनियन बैंक ऑफ़ इंडिया भी जुलाई 2016 में एक हमले का शिकार हुआ। साइबर चोरों ने उसके नोस्ट्रो खाते से लगभग 171 मिलियन अमरीकी डॉलर की चोरी की। कथित तौर पर हमलावरों ने नकली आरबीआई आईडी का उपयोग करके स्पीयरफिशिंग का उपयोग करके प्रवेश किया। इन घटनाओं के आलोक में भारत के केंद्रीय बैंक रिज़र्व बैंक ऑफ़ इंडिया ने भी अपने 2016 के परिपत्र के माध्यम से बैंकों के लिए साइबर खतरे से निपटने हेतु आवश्यक तंत्र विकसित करने के आदेश दिए हैं। इस संबंध में बैंकों की तैयारियों की निगरानी करने हेतु विशेष प्रकोष्ठ का भी गठन किया गया है जिसके माध्यम से इन दिशानिर्देशों के अनुपालन की स्थिति का मूल्यांकन किया जाता है।

साइबर अपराध क्या हैं ?

सभी आपराधिक गतिविधियां जिनमें किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी को अनधिकृत रूप से प्राप्त करने या किसी डिवाइस को अक्षम करने के लिए किया जाता है तब उसे साइबर अपराध की संज्ञा दी जा सकती है।

मुख्य तौर पर इन अपराधों को दो वर्गों में बांटा जा सकता है:

- ऐसे अपराध जहां कंप्यूटर पर हमला कर जानकारी चुराने/ अक्षम करने का प्रयास किया जाता है।
- ऐसे अपराध जहां कंप्यूटर का प्रयोग एक हथियार/ साधन के तौर पर किया जाता है।

बैंकिंग से संबंधित साइबर अपराध

आइए! अब कुछ साइबर धोखाधड़ी/ अपराध जो दैनंदिन रूप से घटित हो रहे हैं उनके कार्य प्रणाली एवं निवारक सतर्कता के बारे में जानते हैं:

क) पहचान की चोरी: अनधिकृत रूप से किसी की भी व्यक्तिगत जानकारी जैसे नाम, फ़ोन नंबर, पता, बैंक खाता संख्या, आधार नंबर या क्रेडिट/ डेबिट कार्ड नंबर आदि प्राप्त करना इसके अंतर्गत आता है। इसके कई प्रतिकूल प्रभाव हो सकते हैं जैसे कि बैंक खातों का अनधिकृत इस्तेमाल, केवाईसी दस्तावेजों का अनधिकृत प्रयोग आदि।

निवारक सतर्कता: इस प्रकार की धोखाधड़ी की रोकथाम हेतु निम्नांकित उपाय कारगर हो सकते हैं:

- कभी भी लॉगआउट किए बगैर ब्राउज़र विंडो को बंद न करें।
- अपना लॉगिन आईडी एवं पासवर्ड ब्राउज़र में सुरक्षित न करें।
- सोशल मीडिया खाते के साथ अपना मोबाइल नंबर लिंक करें ताकि किसी भी अनधिकृत लॉगिन की सूचना प्राप्त हो सके।
- साइबर कैफ़े में यदि कोई दस्तावेज डाउनलोड किया है तो तुरंत उनकी प्रतियां डिलीट कर देनी चाहिए।
- किसी को भी अपने केवाईसी दस्तावेजों की प्रति देते समय उसपर स्पष्ट रूप से उद्देश्य का उल्लेख किया जाना चाहिए।
- किसी भी सार्वजनिक प्लेटफॉर्म (सोशल मीडिया) आदि पर अपनी व्यक्तिगत संवेदनशील जानकारी साझा न करें।

ख) मानवीय व्यवहार से संबंधित मनोवैज्ञानिक चालें : इस प्रकार की धोखाधड़ियों में अपराधियों द्वारा अपने शिकार की मानसिक परिस्थिति का अपने हित में इस्तेमाल किया जाता है। जैसे कि फिशिंग/ विशिंग/ स्मिशिंग/ लुभावने वादे/ आकर्षक उपहार आदि के द्वारा व्यक्ति की संवेदनशील जानकारी चुराई जाती है।

फिशिंग वह कार्यप्रणाली है जिसके अंतर्गत ई-मेल के माध्यम से लोगों को ठगी का शिकार बनाया जाता है। इस प्रकार की ई-मेल फ़र्ज़ी होती हैं पर यह वैध मालूम पड़ती हैं। यदि इस प्रकार की ई-मेल में मौजूद किसी लिंक/ अटैचमेंट को डाउनलोड/ क्लिक किया जाता है तो इसमें उपस्थित सॉफ्टवेयर/ वायरस के माध्यम से उपयोगकर्ता की जानकारी अपराधी तक पहुँच जाती है।

इसी कड़ी में यदि फ़ोन कॉल के जरिए प्रयोगकर्ताओं को निशाना बनाया जाता है तो इसे **विशिंग** एवं एसएमएस माध्यम का उपयोग होने पर **स्मिशिंग** की संज्ञा दी जाती है।

इस प्रकार के हमलों के दौरान साइबर अपराधियों द्वारा पीड़ित को यह बताया जाता है कि उसने **आकर्षक लॉटरी** जीत ली है। इस इनाम को प्राप्त करने हेतु उसे कुछ जानकारी प्रदान करनी होगी तथा उसके पश्चात रकम उसके बैंक खाते में जमा कर दी जाएगी। इस रकम को प्राप्त करने के लिए पीड़ित से टोकन राशि भेजने का अनुरोध किया जाता है तथा उसके पश्चात उसकी व्यक्तिगत जानकारी मांगी जाती है। इसी प्रकार **कार्ड ब्लॉक होने का डर** दिखाकर एवं **नौकरी का लालच** देकर भी जानकारी जुटाई जाती है जिसके माध्यम से यह अपराधी अपना हितसाधन करते हैं।

निवारक सतर्कता: इस प्रकार की धोखाधड़ी की रोकथाम हेतु निम्नलिखित उपाय कारगर हो सकते हैं:

- अज्ञात स्रोत से प्राप्त किसी भी फ़ोन कॉल/ एसएमएस/ ई-मेल संदेशों का जवाब न दें।
- किसी भी प्रकार के संदेहास्पद लिंक अथवा अटैचमेंट को न खोलें।
- किसी भी संदेश पर कार्य करने से पहले उसकी सत्यता परख लें।
- अपना पिन/ ओटीपी/ सीवीवी किसी के साथ साझा न करें, यह याद रखें कि बैंक कभी भी आपसे यह जानकारी नहीं मांगता है।
- किसी भी प्रकार से अनधिकृत लेन-देन की आशंका होने पर अपने बैंक को तुरंत सूचित करें।
- यदि ई-मेल संदेश में किसी भी प्रकार की वर्तनी संबंधी अशुद्धि है तो सावधान हो जाएं यह एक फिशिंग मेल हो सकती है।
- यदि कोई जानकारी अत्यधिक लुभावनी, आकर्षक अथवा भय उत्पन्न करने वाली है तो उस पर कार्यवाही करने से पहले सावधानी से उसके सत्यता की जांच करें।

घ) मोबाइल अनुप्रयोगों द्वारा धोखाधड़ी: आज स्मार्टफोन एवं इंटरनेट के उपयोगकर्ताओं की संख्या में बढ़ोत्तरी के साथ साथ इनकी सुरक्षा से संबंधित जोखिम भी बढ़ गए हैं। इसका प्रयोग न सिर्फ मनोरंजन बल्कि प्रतिदिन के कार्यों जैसे बिल भुगतान/ शॉपिंग/ बैंकिंग लेन-देन आदि के लिए भी किया जाता है। अतएव, इनके माध्यम से होने वाले साइबर अपराध काफी सामान्य हैं।

अधिकतर मोबाइल ऐप्लिकेशन उपयोगकर्ता से उसके मोबाइल के कैमरे/ माइक्रोफोन/ एसएमएस आदि में प्रवेश का अधिकार मांगते हैं तथा समान्यतः यह अधिकार प्रदान कर दिए जाते हैं। इसी प्रकार **स्क्रीन शेयरिंग ऐप्लिकेशन** के माध्यम से भी साइबर अपराधों को अंजाम दिया जाता है।

ये ऐप्लिकेशन साइबर अपराधियों के मुख्य हथियार के तौर पर कार्य करते हैं, यदि एसएमएस तक उनकी पहुँच है तो वह आसानी से ओटीपी प्राप्त कर आपके खाते से राशि ट्रांसफर कर सकते हैं।

निवारक सतर्कता: इस प्रकार की धोखाधड़ी की रोकथाम हेतु निम्नांकित उपाय कारगर हो सकते हैं:

- हमेशा आधिकारिक ऐप्लिकेशन स्टोर से ही मोबाइल ऐप्लिकेशन डाउनलोड करें।
- किसी भी प्रकार की मुफ्त ऐप्लिकेशन डाउनलोड करने से पहले उसकी सत्यता की जांच कर लें।
- सभी अनुमति अनुरोधों को विशेष जांच करने के बाद ही स्वीकार करें।
- मोबाइल के सॉफ्टवेयर को नियमित रूप से अद्यतन करें ताकि नवीनतम सुरक्षा उपायों को कार्य में लिया जा सके।

ङ) ऑनलाइन बैंकिंग से संबंधित धोखाधड़ी: आज अधिकांश बैंकिंग सेवाएं डिजिटल माध्यम से उपलब्ध हैं। मोबाइल बैंकिंग/ यूपीआई/ इंटरनेट बैंकिंग आदि के प्रयोग ने बैंकिंग को सुगम बना दिया है। साइबर अपराधी भी इसका दोहन अपने हितसाधन के लिए कर रहे हैं तथा लोगों की गाढ़ी कमाई लेकर चम्पत हो रहे हैं।

बैंकिंग ऐप्लिकेशन की मजबूत सुरक्षा उसी प्रकार आवश्यक है जिस प्रकार हम अपने कीमती सामान को ताला लगाकर सुरक्षित रखते हैं। साइबर अपराधी अपने शिकार को विश्वास में लेकर उसके खाते की जानकारी ले लेते हैं तथा उसे उपयोग करके अपना कार्यनिष्पादन करते हैं।

निवारक सतर्कता: इस प्रकार की धोखाधड़ी की रोकथाम हेतु निम्नांकित उपाय कारगर हो सकते हैं:

- बैंक के साथ अपना ई-मेल एवं फ़ोन नंबर रजिस्टर करें ताकि किसी भी प्रकार के संदिग्ध अंतरण की समय रहते सूचना दी जा सके।
- कभी भी अपने बैंक खाते की जानकारी/ कार्ड की जानकारी किसी के साथ साझा न करें।
- हमेशा पासवर्ड बनाते समय ध्यान रखें कि व्यक्तिगत जानकारी का उपयोग न किया गया हो।
- द्विचरणीय सत्यापन द्वारा अपने बैंक खाते को सुरक्षित रखें।

च) शोल्डर सर्फिंग : इस तकनीक में साइबर अपराधी लक्ष्य के आस-पास मौजूद रहकर उसके लॉगिन आईडी एवं पासवर्ड की जानकारी हासिल कर लेते हैं तथा उसके दुरुपयोग से हानि पहुंचाते हैं।

छ) अपदेश: इस प्रकार की धोखाधड़ी में साइबर अपराधी लक्षित व्यक्ति के सामने एक काल्पनिक परिदृश्य उत्पन्न करते हैं जिसमें वे खुद को बैंक/ सेवा प्रदाता के प्रतिनिधि के तौर पर प्रस्तुत करते हैं एवं संवेदनशील जानकारी जुटाते हैं।

ज) कार्ड स्किमिंग: इसमें अपराधी एटीएम मशीन पर एक छोटा उपकरण स्थापित कर देता है एवं उसके माध्यम से आपके कार्ड की मैग्नेटिक पट्टी पर दर्ज सारी संवेदनशील जानकारी चुराकर अपना हितसाधन करता है। इसी

प्रकार कार्ड स्वाइप मशीन को भी स्किमिंग उपकरण से बदल कर कार्ड की जानकारी अनधिकृत रूप से चुरा ली जाती है।

निवारक सतर्कता: इस प्रकार की धोखाधड़ी की रोकथाम हेतु निम्नांकित उपाय कारगर हो सकते हैं:

- ऐसे व्यक्ति जो कर्मचारियों या अन्य आंतरिक जानकारी के विषय में पूछ रहे हों उनसे सतर्क रहें। यदि कोई अज्ञात व्यक्ति एक वैध संगठन से होने का दावा करे, उसकी पहचान सीधे कंपनी के साथ सत्यापित करने का प्रयास करें।
- निजी अथवा अपने संगठन की जानकारी तब तक न दें जब तक आपको उस व्यक्ति की विश्वसनीयता के विषय में कुछ निश्चित न हो।
- किसी भी प्रकार की संदिग्ध गतिविधियों को अपने कार्यालय के सुरक्षा प्रभारी को सूचित करें।
- ऑनलाइन भुगतान करते समय अथवा किसी भी एटीएम मशीन का प्रयोग करते समय सावधान रहें ताकि आपके कार्ड की जानकारी सुरक्षित रहे।

अंत में यही कहना चाहूंगा की साइबर धोखाधड़ी के नियंत्रण हेतु जागरूकता एवं जानकारी का साझा किया जाना सबसे कारगर कदम है। हिंदी में एक कहावत है कि **"उपचार से सावधानी भली"**, यह साइबर अपराध की रोकथाम में भी पूर्णतया लागू होती है। सामान्य साक्षरता के अंतर्गत साइबर जानकारी को शामिल किया जाना आवश्यक है। आज जबकि हमारा देश एक डिजिटल अर्थव्यवस्था बनने की राह पर अग्रसर है, जिसकी सफलता काफी हद तक साइबर अपराधों के प्रभावी सुरक्षात्मक उपायों पर निर्भर है। आइए! यह संकल्प लें कि हम सभी साइबर जागरूक बनेंगे तथा अन्य लोगों को भी जागरूक बनाएंगे।

*****

संजय कुमार

पदनाम:- प्रबंधक
संस्था का नाम:- भारतीय रिज़र्व बैंक
मोबाइल नं. :- 8840193383
ई-मेल:- sanjaikumar@rbi.org.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

अर्थ मनुष्य के लिए हमेशा से महत्वपूर्ण रहा है, क्योंकि अर्थ से ही उसकी समस्त क्रियाएं संचालित होती हैं। अर्थ की इसी महत्ता को देखते हुए राजा भर्तृहरि ने कहा था- "सर्वे गुणा: काञ्चनमाश्रयन्ति'। अर्थ का इतिहास जितना पुराना है, उतना ही पुराना अर्थ और अपराध का संबंध भी है। पुरातन काल में जब विनिमय का माध्यम अनाज या जानवर हुआ करते थे, उस समय इन चीज़ों की चोरी होती थी। जब सोने-चांदी और बहुमूल्य रत्नों का दौर आया तो अधिकतर लूटपाट इन बहुमूल्य धातुओं और उनसे बने आभूषणों, बर्तनों आदि को हथियाने को लेकर होती थीं। मुग़लकाल में बादशाहों ने जब सोने-चांदी के सिक्के चलाए तो लोगों ने उनसे मिलते-जुलते नकली सिक्के चलाने शुरू कर दिए। जब कागज़ी मुद्रा का चलन शुरू हुआ तो धोखेबाजों ने जाली मुद्रा चलानी शुरू कर दी। कहने का आशय यह है कि धन-दौलत को अनुचित तरीके से हड़पने का सिलसिला उतना ही पुराना है जितनी की मानव सभ्यता। हालांकि अब तक के सफर में जो खास बात थी वह यह थी कि धन-दौलत हड़पने के लिए लुटेरे को धन तक भौतिक पहुंच बनानी पड़ती थी, किन्तु जबसे डिजिटल लेनदेन का दौर शुरू हुआ, अपराधियों को मौके पर जाने की ज़रूरत भी न रही। वे दुनिया के किसी भी कोने से घटना को अंजाम देने में सक्षम हो गए। साइबर अपराधों की इसी गंभीरता को देखते हुए सिस्को के भूतपूर्व सीईओ जान चेंबर्स कहते हैं - "केवल दो प्रकार के संगठन हैं, एक वे जो हैक कर लिए गए हैं और दूसरे वे जो यह नहीं जानते कि उन्हें हैक कर लिया गया है"। चूंकि बैंक विशुद्ध रूप से अर्थ से जुड़ा कारोबार करते हैं, अतएव, उनका और उनके ग्राहकों का साइबर अपराधियों के निशाने पर होना लाज़मी है। बैंकों में होने वाले साइबर अपराधों के स्वरूप पर विस्तार से चर्चा करने के पहले साइबर अपराध का आशय समझ लेना प्रासंगिक होगा।

साइबर अपराध:

'साइबर' शब्द की उत्पत्ति 'साइबरनेटिक्स' से हुई है, जो मूलत: जीवित प्राणियों और मशीनों के बीच संचार और नियंत्रण प्रणालियों के अध्ययन की एक शाखा थी। समय के साथ-साथ 'साइबर' की संकल्पना में बदलाव आया और अब इसका आशय 'सूचना प्रौद्योगिकी' से है। वर्तमान समय में कोई भी चीज़ जो कम्प्यूटिंग और इंटरनेट से संबंधित है, साइबर की श्रेणी में रखी जा सकती है। वहीं, साइबर अपराध का आशय ऐसे गैर-कानूनी कृत्यों से है जो सूचना प्रौद्योगिकी का इस्तेमाल कर अंजाम दिए जाते हैं। इसमें कम्प्यूटर या कम्प्यूटर नेटवर्क, अपराध करने का उपकरण या लक्ष्य दोनों हो सकता है।

आरंभ में साइबर अपराध शरारती तत्वों द्वारा शौकिया तौर पर किए जाते थे, पर आजकल ये उद्दण्ड राष्ट्रों द्वारा प्रायोजित भी होते हैं और इन अपराधों का प्रमुख उद्देश्य धन हड़पना, किसी प्रणाली को ध्वस्त कर देना, सिस्टम को हैक कर लेना और फिरौती मांगना, बदनाम करना, काबिलियत साबित करना, शोहरत पाना आदि होता है। बैंकिंग जगत में ये अपराध मुख्यत: धन हड़पने की लालसा से किए जाते हैं। अकेले वर्ष 2020 में साइबर

अपराध के 50,035 मामले सामने आए जिनमें सबसे अधिक 60.20% मामले वित्तीय धोखाधड़ी से संबंधित थे।

बैंकों में साइबर अपराधों का स्वरूप और सुरक्षात्मक उपाय :

प्रौद्योगिकी ने जहां एक ओर "कभी भी, कहीं भी बैंकिंग" का सपना साकार किया है तो वहीं जोखिम की संभावना भी हर समय और हर जगह से पैदा की है। यदि बैंकों में साइबर अपराधों के स्वरूप की बात की जाए तो इसके कितने स्वरूप हो सकते हैं यह निश्चित तौर पर नहीं कहा जा सकता, क्योंकि प्रत्येक नई घटना एक नए स्वरूप को उजागर करती है। तथापि ज्ञात मामलों के आधार पर साइबर अपराधों की प्रकृति का एक सामान्य खाका अवश्य खींचा जा सकता है।

1. ग्राहकों को लक्षित कर किए जाने वाले साइबर अपराध: ग्राहकों के साथ होने वाले साइबर अपराधों से हमारा आशय ग्राहकों के साथ होने वाली साइबर धोखाधड़ी से है, जो प्राय: निम्नलिखित रूप से की जाती है:

फ़र्ज़ी फोन कॉल द्वारा: इस प्रकार की धोखाधड़ी को साइबर की भाषा में **'विशिंग'** कहते हैं। आम ग्राहक सबसे अधिक शिकार इसी धोखाधड़ी के होते हैं। इसमें साइबर अपराधी बैंक अधिकारी बनकर ग्राहक को फोन करते हैं और उसे उसके डेबिट/ क्रेडिट कार्ड के बंद/ निष्क्रिय हो जाने की जानकारी देते हैं तथा कार्ड चालू रखने हेतु कार्ड संख्या, सीवीवी, पिन और ओटीपी जैसे विवरण उपलब्ध कराने को कहते हैं। इंटरनेट बैंकिंग का इस्तेमाल करने वाले ग्राहकों से सिस्टम आदि के अपडेट होने का बहाना बनाया जाता है और सुविधा जारी रखने के लिए लॉगिन ऑईडी, पासवर्ड जैसे विवरण मांगे जाते हैं। विवरण मिलते ही ग्राहक का खाता खाली कर दिया जाता है। इस श्रृंखला में एक नया ट्रेंड केवाईसी अपडेशन का है। केवाईसी अपडेशन के नाम पर धोखेबाज़ पहले ग्राहक को एक मेसेज भेजते हैं *"KYC updation in your account is pending, failing which your account will be freezed "*. फिर इस हेतु फोन लगाकर ग्राहक से आधार, पैन, आयु, पता आदि का विवरण पूछने के साथ-साथ कार्ड और नेट बैंकिंग की गोपनीय सूचना भी पूछ लेते हैं। पुन: एक मेसेज भेजा जाता है *"Your KYC is being updated, you will receive an OTP. Pl share it with your Bank Officer for successful completion of KYC"*. इन संदेशों से ग्राहक के मन में रही सही शंका भी दूर हो जाती है और वह ओटीपी आते ही तुरंत शेयर कर बैठता है। ओटीपी किसलिए आया है; इसको पढ़ने की ज़ुर्रत तक नहीं करता।

सुरक्षात्मक उपाय:

- अपने बैंक खाते की गोपनीय जानकारी किसी के भी साथ साझा न करें।
- अपने बैंक के मेसेज कोड (जैसे-एसबीआई के मामले में BP-SBIINB, AD-SBIINB आदि) को पहचानें और मेसेज को पूरी तरह पढ़कर ही प्रतिक्रिया दें।
- विभिन्न प्रयोजनों हेतु कार्ड/ नेट बैंकिंग की दैनिक लिमिट सेट कर लें।
- फोन को लॉक रखें ताकि आपकी अनुपस्थिति में कोई अन्य सदस्य फोन पर आए ओटीपी को साझा न कर बैठे।
- बैंकों को भी इस तरह के मेसेज प्रारूप *"<OTP is 2986 for a transaction of Rs ....> "* से बचना चाहिए क्योंकि इस मेसेज में ओटीपी शुरू में होने के कारण मोबाइल का स्क्रीन लॉक खोले बिना ही दिख जाता है। इसके बजाए *"For transaction of Rs ... your OTP is....."* जैसा प्रारूप उचित होगा।

एसएमएस द्वारा: इस प्रकार की धोखाधड़ी को साइबर की भाषा में **स्मिशिंग** (एसएमएस+ फिशिंग) कहते हैं। इसमें ग्राहक के फोन पर एक के बाद एक कई टेक्स्ट मेसेज भेजकर पहले तो उसे विश्वास में लिया जाता है, फिर

बड़ी चालाकी से उससे बैंक विवरण, पासवर्ड जैसी गोपनीय सूचनाएं हासिल की जाती हैं अथवा दिए गए लिंक पर क्लिक करने हेतु प्रेरित किया जाता है। स्मिशर के पास गोपनीय सूचनाएं पहुंचते ही, वह चपत लगा देता है।

सुरक्षात्मक उपाय:

- अपरिचित स्रोतों से आए संदेशों पर प्रतिक्रिया करने से बचें।
- किसी भी टेक्स्ट मेसेज में दिए गए लिंक से किसी ऐप को इंस्टाल न करें। यदि कोई ऐप इंस्टाल करना ही है तो आधिकारिक ऐप स्टोर से करें।

ई-मेल के द्वारा : इस प्रकार की धोखाधड़ी को साइबर की भाषा में **'फिशिंग'** कहते हैं। इसमें ग्राहक को ई-मेल भेजे जाते हैं जो देखने में अधिकृत संस्था/ बैंक द्वारा भेजे गए लगते हैं। इन मेल्स में यूज़र को दिए गए लिंक, जो आधिकारिक वेबसाइट/ बैंक का प्रतीत होता है, पर क्लिक करने के लिए प्रेरित किया जाता है। जैसे ही यूज़र उस पर लॉगिन करता है अथवा अपनी व्यक्तिगत पहचान का विवरण भरता है, उसकी सारी सूचनाओं की ऑनलाइन चोरी हो जाती है और वह धोखाधड़ी का शिकार हो जाता है।

सुरक्षात्मक उपाय:

- बैंकिंग लेनदेन हेतु बैंक के URL को ब्राउज़र के एड्रेस बार में टाइप करें। किसी लिंक अथवा गूगल जैसे सर्च इंजन से एक्सेस न करें।
- लॉगिन आईडी और पासवर्ड डालने के पूर्व यह सुनिश्चित कर लें कि साइट 'https://' से शुरू होती है और उसमें पैडलॉक दिखता है।
- लॉगिन आईडी, पासवर्ड जैसे विवरण कंप्यूटर/ मोबाइल पर सेव न करें।
- अपने ब्राउज़र से 'आटो कम्पलीट' विकल्प निष्क्रिय कर दें।
- जिस पीसी/लैपटोप/मोबाइल से लेनदेन करते हों, उसमें 'स्क्रीन शेयर' जैसे ऐप डाउनलोड न करें।
- साइबर कैफे/सार्वजनिक वाई-फाई से नेट बैंकिंग ऐक्सेस न करें।

वायरस के द्वारा: वायरस के द्वारा भी बैंकिंग धोखाधड़ी को अंजाम दिया जाता है। वायरस के डिलीवरी चैनल अलग-अलग हो सकते हैं ताकि वे फायरवाल से बचकर ग्राहक के सिस्टम में दाखिल हो सकें। वे किसी ई-मेल के अटैचमेंट, सॉफ्टवेयर, पेनड्राइव अथवा किसी छद्म वेबसाइट पर क्लिक करने और कुछ इस तरह के सुरक्षा संदेशों कि "आपके कंम्प्यूटर में वायरस है और आपको नया सॉफ्टवेयर डाउनलोड करने की आवश्यकता है", के जरिए भेजे जाते हैं। जैसे ही ग्राहक इन पर क्लिक करता है, वह वास्तविक वायरस डाउनलोड कर लेता है। आज टार्जन हॉर्स, लॉजिक हॉर्स, वर्म जैसे कई प्रोग्राम हैं, जो की-स्ट्रॉक्स को कैप्चर कर लेते हैं और उसे बाहरी साइटों पर प्रेषित कर देते हैं।

सुरक्षात्मक उपाय:

- हमेशा ब्रांडेड कंपनी का लाइसेंस वाला एंटी वायरस डालें।
- अपने वेब ब्राउज़र में 'pop-up blocker' सक्रिय कर लें।
- किसी भी अपरिचित लिंक/ अटैचमेंट को न खोलें।
- कंप्यूटर पर पाइरेटेड सॉफ्ट्वेयर न डालें।
- कंप्यूटर के आप्रेटिंग सिस्टम को निरंतर अपडेट रखें।

फर्ज़ी प्रलोभन के द्वारा: साइबर ठगों द्वारा लोगों को ई-मेल, टेक्स्ट मेसेज भेजकर लॉटरी निकलने, इनाम जीतने, किसी संपत्ति का लकी वारिस चुने जाने की खबरें दी जाती हैं और ऐसी इनामी राशि को क्रेडिट करने के

लिए उनसे खाता विवरण एवं अन्य गोपनीय सूचनाएं जुटा ली जाती हैं। जो लोग लोभ में आ जाते हैं, वे अपनी पूंजी गवां बैठते हैं।

सुरक्षात्मक उपाय:

- अपने लालच को नियंत्रित करें और भाग्य से अधिक कर्म पर विश्वास करें।
- इस चीज़ में प्रबल विश्वास रखें कि खैरात में कुछ भी नहीं मिलता।

2. बैंक, ग्राहक और अन्य मध्यस्थों की संयुक्त विफलता से जुड़े साइबर अपराध

बैंकिंग में साइबर अपराध के कुछ मामले एक से अधिक पक्षों की लापरवाही के कारण घटित होते हैं। इस संबंध कुछ कार्य-पद्धतियां दृष्टव्य हैं:

फ़र्ज़ी कस्टमर केयर नम्बर के द्वारा धोखाधड़ी: हाल ही में साइबर धोखाधड़ी का एक ऐसा मामला सामने आया जिसमें नेट बैंकिंग का इस्तेमाल करने वाले एक ग्राहक ने अपनी एफडी तुड़वाने की प्रक्रिया समझने के लिए गूगल पर एक बैंक का कस्टमर केयर नंबर सर्च किया। साइबर अपराधियों ने सर्च इंजन ऑप्टीमाइन (SEO) के द्वारा इस नंबर को सर्च हिस्ट्री में सबसे ऊपर कर रखा था। इस नंबर पर फोन करने पर हिंदी के लिए '1' दबाएं, अंग्रेजी के लिए 2 दबाएं... । से गुज़रता हुआ जब ग्राहक फोन बैंकिंग ऑफिसर तक पहुंचा तो छद्म फोन बैंकिंग ऑफिसर ने कहा कि वेबसाइट पर फिलहाल एफडी तोड़ने का विकल्प नहीं है, इसके लिए मैं आपको एक लिंक भेजता हूं, उसमें दिए गए फार्म में आप अपनी एफडी आदि का विवरण भरकर सबमिट कर दीजिए। इस फार्म में अन्य के साथ-साथ यूज़र आईडी और पासवर्ड आदि का विवरण भी भरना था। जैसे ही ग्राहक ने उक्त फार्म सबमिट किया, धोखेबाज़ ने फिक्स जमाएं तोड़ी, ग्राहक के खाते में दर्ज मोबाइल नंबर बदला और खाते की राशि विभिन्न खातों में ट्रांसफर कर दी। इस घटना में जहां ग्राहक ने यूज़र आईडी, पासवर्ड उजागर करने की लापरवाही की, तो सर्च इंजन ने गैर-सत्यापित टोल-फ्री नंबर प्रदर्शित करने की। सबसे बड़ी प्रणालीगत चूक बैंक के स्तर पर हुई जिसने नेट बैंकिंग द्वारा खाते में मोबाइल नंबर बदलने की इज़ाजत दी। फर्ज़ी कस्टमर केयर नंबर पर शिकायत के एक अन्य मामले में साइबर अपराधी ने शिकायतकर्ता से उसके कार्ड का पूरा विवरण लिया और कहा कि आपकी शिकायत दर्ज़ हो गई है, शिकायत नंबर प्राप्त करने के लिए आप भेजे गए लिंक से ऐप डाउनलोड कर लें। ऐप डाउनलोड करते ही पीड़ित के पास जो ओटीपी आता था वह अपराधियों को दिखाई देता था और वे उसका खाता खाली कर देते थे।

सुरक्षात्मक उपाय:

- किसी भी बैंक का कस्टमर केयर नंबर केवल बैंक की आधिकारिक वेबसाइट से प्राप्त करें और इसे हमेशा अपने मोबाइल में सेव रखें ताकि समय रहते सूचना देकर नुकसान को कम कर सकें।
- सर्च इंजनों और प्रिंट व इलेक्ट्रॉनिक मीडिया को भी गैर-सत्यापित नंबर प्रकाशित नहीं करने चाहिए।
- बैंक-खाते में मोबाइल नंबर या ई-मेल जैसी संवेदनशील सूचनाएं कम से कम दो स्तरों के अधिप्रमाणन के बाद ही बदली जानी चाहिए।

एटीएम स्किमिंग/ कार्ड क्लोनिंग: स्किमिंग/ कार्ड क्लोनिंग एक हाईटेक तरीका है जिसमें आपराधिक तत्व एटीएम/ पीओएस पर एक स्किमिंग डिवाइस लगा देते हैं जो कार्ड की चुम्बकीय पट्टी की सारी सूचनाएं कॉपी कर लेता है। फिर इन सूचनाओं को नए कार्ड की चुम्बकीय पट्टी में ट्रांसफर कर दिया जाता है और डुप्लीकेट कार्ड तैयार करके पैसा निकाल लिया जाता है।

सुरक्षात्मक उपाय:

- यदि आपको एटीएम के कार्ड स्लॉट में कुछ अनजान हरकत दिखे तो कार्ड स्वाइप न करें।

- कम रोशनी वाले और बिना सुरक्षा-गार्ड वाले एटीएम का प्रयोग करने से बचें।
- यदि लेनदेन सफल होने की सूचना के बाद रुपए न निकलें तो सतर्क हो जाएं और कैश स्लॉट सहित आस-पास की संरचना पर भी नज़र दौड़ाएं।
- भुगतान हेतु कार्ड को अपने सामने स्वाइप कराएं और देखें कि कार्ड पीओएस टर्मिनल के सिवाय कहीं अन्यत्र तो स्वाइप नहीं किया जा रहा है।
- पिन हमेशा छिपाकर डालें।
- बैंकों को अपने एटीएम पर यथासंभव सुरक्षा गार्ड लगाने चाहिए और एटीएम में किसी भी प्रकार की छेड़छाड़ हेतु एक अलार्म सिस्टम विकसित करना चाहिए। कैश रिफिल करने वाले वेंडरों को एटीएम के इंटरफेस की नियमित जांच का दायित्व भी सौंपा जा सकता है।

ई-कामर्स साइटों और बिल भुगतान पोर्टलों के जरिए साइबर धोखाधड़ी : वर्तमान समय में जनोपयोगी सुविधाओं और ऑनलाइन शॉपिंग हेतु डिजिटल भुगतान एक लोकप्रिय विकल्प है। पर कुछ ऐसे मामले भी प्रकाश में आए हैं जहां तथाकथित सुविधा प्रदाताओं की वेबसाइटों/ई-कामर्स साइटों पर बिल के भुगतान के लिए जब ग्राहक ने 'Pay Now' पर क्लिक किया तो वे गलत लिंक पर पहुंच गए और पैसा कहीं और दे बैठे। यही नहीं, 'ट्रांज़ेक्शन फेल्ड' का मेसेज आया और वे पुन: भुगतान कर बैठे।

सुरक्षात्मक उपाय:

- वेबसाइट पर प्रदर्शित लिंक के माध्यम से भुगतान प्राप्त करने वाले विभागों/ ई-कामर्स कंपनियों को अपनी भुगतान प्रणाली का नियमित फोरेंसिक ऑडिट कराना चाहिए।
- ऑनलाइन भुगतान करते समय प्रत्येक चरण को बारीकी से जांचते हुए आगे बढ़ना चाहिए।

3. बैंक को निशाना बनाकर किए जाने वाले साइबर अपराध: बैंकों को निशाना बनाकर किए जाने वाले अपराधों में प्रमुख हैं:

हैकिंग/ रैनसमवेयर:

रैनसमवेयर एक ऐसा साइबर अपराध है जिसमें मैलवेयर के जरिए टारगेट कंप्यूटर/ सिस्टम को या तो लॉक कर दिया जाता है अथवा उनकी फाइलों को इंक्रिप्ट कर दिया जाता है। फिर उन्हें अनलॉक/ डिक्रिप्ट करने के एवज़ में एक मोटी धनराशि की मांग की जाती है। यह एक तरह से अपहरण और फिरौती की मांग जैसा है। रैनसमवेयर आज दुनिया के सामने एक बड़ा खतरा बनकर उभरा है। इसकी भयावहता का अंदाजा इसी बात से लगाया जा सकता है कि वर्ष 2014 में जे ।पी। मार्गन डेटा ब्रीच मामले में मालवेयर व सोशल इंजीनियरिंग के जरिए तकरीबन 83 मिलियन ग्राहकों की गोपनीय सूचनाएं हैक कर ली गई थीं। फरवरी 2016 में साइबर अपराधियों ने ड्राइडेक्स मैलवेयर के जरिए बंग्लादेश बैंक के स्विफ्ट नेटवर्क पर अनुदेश भेजकर 81 मिलियन डालर अमेरिकी फेडरल रिज़र्व में अंतरित कर लिए थे। 12 मई, 2017 को 'WannaCry' और 'Notpetya' नामक रैंसमवेयर हमले में बैंकों, एटीएम नेटवर्क और कार्ड भुगतान प्रणालियों को प्रभावित करते हुए लगभग 10 बिलियन डॉलर की चपत लगाई गई। वर्ष 2018 में पुणे स्थित कॉसमॉस को-ऑपरेटिव बैंक पर हुए मैलवेयर हमले में हैकरों ने बैंक के एटीएम सर्वर को हैक करके वीज़ा और रुपे कार्डधारकों का विवरण निकालकर कार्ड क्लोनिंग के द्वारा रु. 94.42 करोड़ पार कर दिए थे।

सुरक्षात्मक उपाय:

- डेटा के कम से कम दो बैक-अप रखने चाहिए और अपने नेटवर्क संचार, डेटा सेंटर, क्लाउड सुरक्षा संरचना की नियमित समीक्षा करनी चाहिए।

- आपरेटिंग सिस्टम और सॉफ्टवेयर निरंतर अपडेट रखें।
- बैंक की आईएस पॉलिसी और एक्सेस मैनेजमेंट पॉलिसी का कड़ाई से अनुपालन सुनिश्चित करें।
- कर्मचारियों को साइबर अपराधों के प्रति जागरुक करें और उन्हें उचित प्रशिक्षण दें।
- प्रणाली की भेद्यता(vulnerability) परखने के लिए एथिकल हैकर्स की सेवाएं ली जा सकती हैं।
- मुकम्मल डिज़ास्टर रिकवरी प्लान भी तैयार रखें ताकि कम से कम समय में वैकल्पिक माध्यमों से परिचालन शुरू किया जा सके।

डीडीओज़ अटैक (Distributed Denial of service)

इस प्रकार के साइबर अपराध में किसी कंप्यूटर या नेटवर्क पर कई स्रोतों/ स्थलों, विशेषकर बाट्नेट्स (संक्रमित कंप्यूटरों का एक बड़ा नेटवर्क) से हमला किया जाता है। चूंकि इनकमिंग ट्रैफिक हज़ारों जगह से आ रहा होता है, अतएव, कंप्यूटर सिस्टम के लिए किसी खास आईपी एड्रेस को ब्लॉक करना मुश्किल होता है और इसी क्रम में हमलावर ट्रोजन जैसे खतरनाक वायरसों को प्रवेश कराने में सक्षम हो जाते हैं। दूसरे, इतने अधिक ट्रैफिक के कारण बैंडविड्थ खत्म हो जाती है, जिसके कारण ऑनलाइन बैंकिंग सेवाएं या तो धराशायी हो जाती हैं अथवा बेहद मंद पड़ जाती हैं।

सुरक्षात्मक उपाय:

- नेटवर्क की बैंडविड्थ पर्याप्त रखनी चाहिए।
- बॉटनेट्स रिमूवल टूल्स की भी मदद ली जा सकती है ताकि वे बॉटनेट्स की पहचान कर उन्हें रिमूव कर सकें।

अंत में, सारांश के तौर पर कहा जा सकता है कि डिजिटल बैंकिंग समय की मांग है। इसके कारण बैंकों और ग्राहकों के समय, श्रम और संसाधनों की बचत हो रही है। चूंकि बैंकिंग से जुड़े साइबर अपराधों में अपराधियों को सीधे तौर पर वित्तीय लाभ पहुंचता है, अतएव यहां अपराधों की संभावना काफी प्रबल है। इसलिए प्रौद्योगिकी आधारित बैंकिंग को सतत महफ़ूज़ रखने के लिए बैंकों को साइबर सुरक्षा पर अच्छी-खासी राशि खर्च करने की ज़रूरत होगी। बैंकों का यह खर्च एक तरह का निवेश होगा, जो उन्हें भावी हानियों से बचाने का काम करेगा। साइबर अपराधों की रोकथाम के लिए घटनाओं की समय से रिपोर्टिंग भी महत्वपूर्ण है क्योंकि इससे जहां इंस्टीट्यूशनल मेमोरी तैयार होती है, वहीं नियामक की ओर से दण्ड से भी बचा जा सकता है। समय से रिपोर्टिंग अपराधियों तक पहुंचने और फंड की वसूली में भी मददगार हो सकती है। जागरुकता हर समस्या के निवारण की दिशा में सबसे कारगर औज़ार होता है। अतएव, डिजिटल लेनदेन की सावधानियों तथा साइबर अपराधों की प्रकृति के बारे में ग्राहकों, कर्मचारियों, हितधारियों को जितना अधिक जागरूक किया जाएगा, वे उतने ही सावधान रहेंगे और उतनी ही कम घटनाएं होंगी। बैंकिंग में साइबर अपराध की घटनाएं रोकने में उन पक्षों की भी अहम भूमिका है, जो प्रत्यक्ष या परोक्ष रूप से बैंकिंग गतिविधि को सहारा दे रहे हैं। उदाहरण के लिए यदि पैन, वोटर कार्ड, मनरेगा कार्ड जैसी आईडी जारी करने वाले विभाग पहचान का विधिवत सत्यापन किए बिना इन्हें जारी कर दें और इन फर्ज़ी आईडी पर खाते खुल जाएं अथवा कोई टेलीकॉम कंपनी केवाईसी का समुचित सत्यापन किए बिना सिम जारी कर दे या किसी को किसी अन्य का डुप्लीकेट सिम जारी कर दें तो साइबर ठगी भी होगी और अपराधियों तक पहुंचना भी मुश्किल होगा। ध्यान रहे कि साइबर ठगी का पैसा विविध खातों, वालेट्स, ई-कामर्स साइटों से होता हुआ ही अंतिम पड़ाव तक पहुंचता है और यदि श्रृंखला से जुड़े सभी पक्षकार अपनी ज़िम्मेदारी का निष्ठा और ईमानदारी से निर्वहन करें तो साइबर अपराध की घटनाएं काफी हद तक कम हो सकती हैं।

*****

संजीव ठाकुर

पदनाम:- मुख्य प्रबंधक
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 8879620499
ई-मेल:- security.mgz@bankofbaroda.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

मनुष्यता के इतिहास के साथ अपराध भी जुड़े रहे हैं। समय के साथ समाज में बदलाव हुआ है और ऐसे ही समाज में होने वाले अपराधों में भी समय और परिस्थितियों के अनुसार परिवर्तन होता रहा है। इन अपराधों की व्यापक वृद्धि वैश्विक चिंता का विषय बन गई है तथा साइबर अपराध एक नई चुनौती बन कर उभरी है। अपराधी शारीरिक रूप से बिना उपस्थित हुए गुमनाम रूप से पीड़ित से बहुत दूर रहकर भी अपराध को अंजाम दे देता है। यह साइबर अपराधी पकड़े जाने के भय के बिना दूर से ही किसी अपराध को अंजाम दे देते हैं।

विश्व के लगभग सभी देशों ने साइबर अपराध से निपटने हेतु कानून बनाए हैं लेकिन इस से साइबर क्राइम में कोई कमी आती हुई दिखाई नहीं दे रही। हालांकि कानून अपना काम करता है इसलिए कानून के महत्व को कम नहीं आंका जा सकता।

इन अपराधों में पैसों की चोरी, ठगी, साइबर स्टेकिंग, पहचान की चोरी, हैकिंग, सॉफ्टवेयर पायरेसी, कॉपीराइट उल्लंघन आदि अपराध शामिल हैं। इस आलेख में हम बैंकिंग से संबंधित साइबर क्राइम और उनकी रोकथाम पर चर्चा करेंगे।

बैंकिंग संबंधित साइबर क्राइम में अपराधी का मुख्य उद्देश्य सामने वाले का पैसा लेना होता है इसके लिए अपराधी जो हथकंडे अपनाता है वो इस प्रकार हैं :

विशिंग (Vishing):

विशिंग में अपराधी फोन कॉल के जरिए गोपनीय जानकारी को हासिल करने की कोशिश करते हैं. वे यूजर आईडी, लॉगिन और ट्रांजेक्शन पासवर्ड, ओटीपी (वन टाइम पासवर्ड), यूआरएन (यूनिक रजिस्ट्रेशन नंबर), कार्ड पिन, ग्रिड कार्ड वैल्यू, सीवीवी या निजी जानकारी जैसे जन्म की तारीख, माता का नाम आदि जैसे डिजिटल हासिल कर लेते हैं. अपराधी बैंक की ओर से होने का दावा करते हैं और ग्राहकों को झांसे में फंसाकर फोन पर ही उनकी निजी और वित्तीय डिटेल्स को हासिल कर लेते हैं. इन डिटेल्स का इस्तेमाल फिर पीड़ित के अकाउंट के साथ बिना उसकी इजाजत के धोखाधड़ी करने के लिए होता है. इससे पीड़ित को वित्तीय नुकसान पहुंच सकता है।

विशिंग हमलों के विशिष्ट उदाहरण :

- **ओटीपी/सीवीवी धोखाधड़ी** - अपराधी बैंक ग्राहकों को ठगने के लिए ओटीपी/ सीवीवी पूछकर या ग्राहक को क्विक सपोर्ट, एनी डेस्क, टीम व्यूयर आदि जैसे रिमोट एक्सेस ऐप डाउनलोड करने के लिए प्रेरित करके स्मार्टफोन तक पहुंच बनाकर ओटीपी/ सीवीवी को पढ़ लेते हैं।

- **लॉटरी धोखाधड़ी** - जालसाज कॉल करके कहते हैं कि आपने लॉटरी में बड़ी राशि जीती है। लॉटरी के पैसे प्राप्त करने के लिए आपको फर्जी वेबसाइट के एक लिंक पर क्लिक कर अपनी व्यक्तिगत जानकारी देने के लिए कहा जाता है। ऑफर स्वीकार करने के लिए टोकन के रूप में कुछ पैसे ट्रांसफर करने के लिए बताया जाता है। एक बार जब आप अपना विवरण भरकर उन वेबसाइटों के माध्यम से भुगतान करने की कोशिश करते हैं तो आपकी सभी व्यक्तिगत जानकारियां और वित्तीय विवरण चोरी कर लिए जाते हैं।
- **आयकर रिफंड धोखाधड़ी** - साइबर अपराधी फोन कॉल्स के जरिए आयकर रिफंड प्राप्त करने का लालच देकर बैंक ग्राहकों को निशाना बनाते हैं। इस तरह धोखे से ग्राहकों के संवेदनशील व्यक्तिगत जानकारी एकत्र किए जाते हैं।
- **केवाईसी धोखाधड़ी** - साइबर अपराधी ग्राहकों को अपने केवाईसी विवरण अपडेट करने के लिए लिंक पर क्लिक करने के लिए कहते हैं। इस तरह के कॉल इस धमकी के साथ किए जाते हैं कि अगर आप अभी अपना केवाईसी अपडेट नहीं करते हैं तो आपका खाता ब्लॉक हो जाएगा।

विशिंग से बचने के उपाय:

- हमेशा फोन करने वाले के पहचान की पुष्टि करें।
- अपने मोबाइल या कंप्यूटर पर कोई भी अनजान सॉफ्टवेयर इंस्टॉल न करें।
- अवांछित बिक्री, मार्केटिंग या अन्य संदेशों का जवाब न दें।
- फोन पर ओटीपी, एटीएम पिन, सीवीवी शेयर न करें।
- बैंक कभी भी आपके बैंक खाते, डेबिट/क्रेडिट कार्ड का विवरण, सीवीवी नंबर आदि की जानकारी नहीं मांगता।

फिशिंग (fishing)

फिशिंग कपटपूर्ण वह तकनीक है जिसमें किसी व्यक्ति का लॉगिन आईडी और पासवर्ड, डेबिट/क्रेडिट कार्ड विवरण, पिन, जन्म तिथि और मोबाइल नंबर आदि निजी जानकारी धोखे से प्राप्त की जाती है। आजकल होने वाले सोशल इंजीनियरिंग हमलों में सबसे ज्यादा मामले फिशिंग के होते हैं।

अधिकांश फिशिंग हमले निम्न उद्देश्य से किए जाते हैं:

- संक्षिप्त या भ्रामक लिंक का उपयोग करके व्यक्तिगत जानकारी जैसे नाम, पता, बैंक खाता विवरण, पैन, आधार आदि प्राप्त करना।
- उपयोगकर्ता को भय, लोभ तथा जल्दबाजी के लिए उकसा कर तुरंत कार्रवाई करने के लिए मजबूर करना।

फ़िशिंग के उदाहरण

- बैंक के ग्राहक को रैंडम नंबर से एक एसएमएस प्राप्त होता है, जिसमे उन्हें एक लिंक पर क्लिक करके केवाईसी अपडेट करने के लिए कहा जाता है अन्यथा, उनका क्रेडिट/ डेबिट कार्ड ब्लॉक कर दिया जाएगा। देखने पर वो लिंक बैंक का लगता है पर वास्तव में फर्जी होता है।
- उन्होंने तुरंत एसएमएस पर कार्रवाई की और अपने केवाईसी को अपडेट करने के लिए लिंक पर क्लिक किया।

- क्लिक करने पर जो वेबपेज दिखाई दिया वह बैंक की वेबसाइट के जैसा लग रहा था, हालांकि वह एक फर्जी वेबसाइट थी। ग्राहक ने फर्जी वेबसाइट के यूआरएल की त्रुटि पर ध्यान नहीं दिया और अपनी सारी गोपनीय जानकारी फर्जी वेबसाइट पर दर्ज कर दी।
- उस फर्जी वेबसाइट ने उन्हें अगले पेज पर रीडायरेक्ट कर दिया जहां ग्राहक ने अपना मोबाइल नंबर और ट्रांजेक्शन पासवर्ड भी साझा कर दिया।
- अब जालसाज को ग्राहक की पूरी संवेदनशील जानकारी ज्ञात हो गयी जिससे जालसाज उनके खाते में धोखाधड़ी लेनदेन करने में सक्षम हो जाएगा।

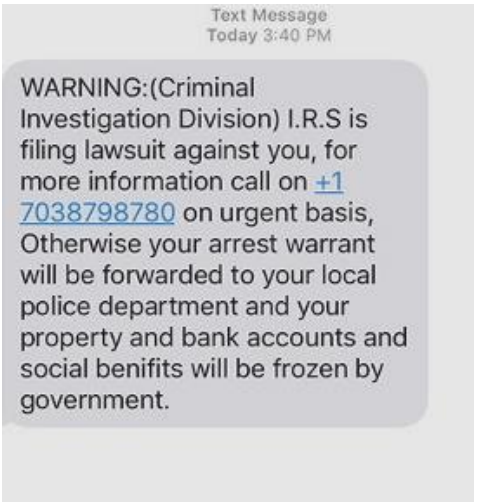
फ़िशिंग हमलों से बचने के तरीके:

- लुभावने ऑफरों से सावधान रहें।
- किसी भी अनजान हाइपरलिंक या मेल अटैचमेंट पर क्लिक न करें।
- भेजने वाले की पहचान या प्रामाणिकता की जांच करें।
- वैध वेबसाइट की पुष्टि के लिए यूआरएल की जांच अवश्य करें।
- मेल से प्राप्त सन्देश में टाइपिंग और व्याकरण की अशुद्धियों पर ध्यान दें।
- हमेशा याद रखें, बैंक कभी भी आपकी निजी जानकारी नहीं मांगता है।

स्मिशिंग (Smishing)

स्मिशिंग साइबर अपराधियों द्वारा इस्तेमाल की जाने वाली वो तकनीक है जिसमें वो किसी व्यक्ति को एसएमएस भेज कर उसे फसाने की कोशिश करते हैं। ऐसे संदेश आपके मोबाइल पर मैसेज संदेशों के रूप में भेजे जाते हैं जो वैध संस्थाओं से होने का दावा करते हैं। जालसाज एसएमएस में लुभावने ऑफर द्वारा या कानूनी कार्यवाही की धमकी द्वारा किसी लिंक पर क्लिक करने के लिए उकसाते हैं जो की वास्तव में फर्जी होता है।

स्मिशिंग हमलों के विशिष्ट उदाहरण



स्मिशिंग हमलों से बचने के तरीके:

- व्यक्तिगत या वित्तीय जानकारी मांगने वाले टेक्स्ट संदेशों से सावधान रहें।
- टेक्स्ट मैसेज पर कोई संवेदनशील जानकारी साझा न करें।
- एसएमएस से प्राप्त किसी भी लिंक पर क्लिक न करें।

- सहायता के लिए कृपया बैंक को कॉल करें या केवल आधिकारिक वेबसाइटों पर जानकारी का संदर्भ लें।

साइबर क्रिमिनल इनके अलावा किसी और तरीके से भी आपकी गोपनीय जानकारी हासिल कर के आपके अकाउंट से पैसे ट्रान्सफर करने की कोशिश कर सकते हैं या आपके क्रेडिट कार्ड की लिमिट का इस्तेमाल कर सकते हैं। इनसे बचने के लिए कुछ उपाय निम्नानुसार हैं:

बैंकिंग साइबर अपराध से बचनें के उपाय (Prevent Cyber Crime)

- अपने इंटरनेट बैकिंग और बैकिंग के लेन-देन का प्रयोग कभी भी किसी पब्लिक साइबर कैफे और ना ही किसी भीड़भाड़ वाले जगहों पर न करें जहां पर आपकी निजी जानकारी आसानी से चोरी हो सकती है।
- इंटरनेट बैकिंग के अंतर्गत किसी भी प्रकार का ट्रांजेक्शन किसी दूसरे व्यक्ति के कंप्यूटर से कदापि न करें और ट्रांजेक्शन करने के पश्चात ई-मेल अकाउंट को लॉगआउट करना न भूलें। इस प्रकार के ब्राउजिंग के डेटा को उसके हिस्ट्री में जाकर डिलीट कर दें।
- लॉगिन करने के बाद कंप्यूटर के द्वारा पूछे गये ऑप्शन जैसे 'कीप ओन लागिंग' या 'पासवर्ड रिमेम्बर' वाले लिंक पर क्लिक नहीं करें।
- आप अपने ई-मेल अकाउंट के इनबाक्स में आये किसी भी स्पैम मेल को न तो ओपन करें और ना ही किसी अटैचमेंट को डाउनलोड करें।
- अपने कंप्यूटर को एंटी-वायरस और एंटी-मैलवेयर साफ्टवेयर का उपयोग करें ताकि कंप्यूटर को वायरस अटैक से बचाया जा सके।
- आप अपने कंप्यूटर, ई-मेल अकाउंट और अन्य प्रकार के इन्टरनेट ट्रांजेक्शन के लिए स्ट्रोंग पासवर्ड का प्रयोग करें, जो कि शब्दों और नंबरों से मिलकर बना हो।

मोबाइल सुरक्षा

आजकल मोबाइल पर बैंकिंग लेनदेन करने के लिए स्मार्ट फोन और ऐप आधारित सेवाओं का उपयोग तेजी से बढ़ रहा है। यह बेहद सुविधाजनक है, लेकिन हमें अपने मोबाइल एप्लिकेशनों के उपयोग में विशेष रूप से वित्तीय लेनदेन करते समय अधिक सावधान रहने की जरूरत है।

मोबाइल फोन के सुरक्षित उपयोग के उपाय:

- अपने फोन पर मजबूत पासवर्ड का इस्तेमाल करें।
- मोबाइल डिवाइस गुम या चोरी होने पर सिम कार्ड को सर्विस प्रोवाइडर द्वारा तुरंत ब्लॉक करें।
- अपना बैंक खाता नंबर या पिन कभी भी मोबाइल फोन पर स्टोर न करें।
- अपने मोबाइल पर एंटी वायरस सॉफ्टवेयर इंस्टॉल करें और उसे अपडेट रखें।
- अपने मोबाइल में प्राधिकृत और सत्यापित ऐप ही इस्तेमाल करें और दी गई अनुमतियों की नियमित रूप से निगरानी करें।
- मोबाइल फोन को सार्वजनिक वायरलेस नेटवर्क से जोड़ने से बचें।
- मोबाइल फोन गुम हो जाने पर बैंक को रिपोर्ट करें ताकि पिन और मोबाइल बैंकिंग ऐप के माध्यम से बैंक खाते तक पहुंच को निष्क्रिय किया जा सके।

अगर सभी सावधानियों के बाद भी कोई साइबर क्राइम का शिकार हो जाता है तो उसे तुरंत संबंधित बैंक और लोकल पुलिस स्टेशन में उसकी शिकायत करनी चाहिए इसके अलावा वो चाहे तो ऑनलाइन भी इसकी शिकायत कर सकता है।

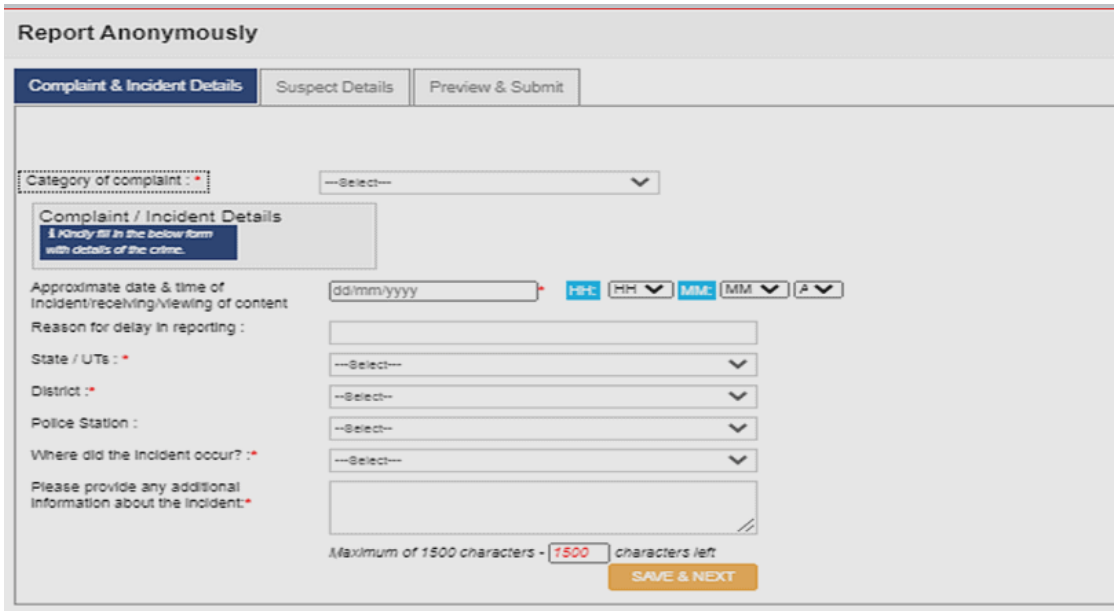
ऑनलाइन शिकायत करने का तरीका इस प्रकार है :

बढ़ते साइबर अपराध को देखते हुए सरकार ने लोगों की सुविधा हेतु ऑनलाइन वेबसाइट cybercrime.gov.in शुरू की है जिसके माध्यम से आप अपने घर बैठे शिकायत दर्ज कर सकते हैं। ऑनलाइन वेबसाइट पर साइबर अपराध की शिकायत दर्ज करने के बाद आप उसके स्टेटस की जानकारी भी प्राप्त कर सकेंगे। किसी भी अपराध की ऑनलाइन शिकायत करने के बाद गृह मंत्रालय से मामला जांच के लिए प्रदेश पुलिस को भेज दिया जाता है।

ऑनलाइन शिकायत करने की प्रक्रिया

- साइबर अपराध से संबंधित शिकायत करने के लिए राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल cybercrime.gov.in पर जाएं।

- अब आपके सामने एक नया पेज ओपन होगा, जिसमें File a Complaint पर क्लिक करना है।



- अब आपके सामने एक फार्म ओपन होगा जिसमें आपको सभी जानकारी दर्ज करने के साथ ही अपराध के बारे में विवरण देना होगा।
- सभी जानकारियां भरने के बाद आपको नेक्स्ट पर क्लिक कर बताये गये क्रम से आगे बढ़ते जाना है। इस प्रकार आपकी शिकयत दर्ज हो जाएगी, साथ ही आपको एक शिकायत नंबर मिलेगा। इस नंबर की सहायता से आप शिकायत का स्टेटस भी चेक कर सकते हैं।

साइबर अपराध प्रकृति में अंतराष्ट्रीय है और इसका दायरा दुनिया के विभिन्न हिस्सों पर अलग-अलग है। साइबर अपराध के खिलाफ लड़ने के लिए चुनौती से निपटने के लिए कई अंतराष्ट्रीय सम्मेलन आयोजित किए जाने के बावजूद भी कई बार वांछित सफलता नहीं मिलती है क्योंकि इन अपराधियों को पकड़ना अत्यंत कठिनाई भरा कार्य है। दुनिया भर में विशेष रूप से साइबर अपराध के लिए कानूनों की एकरूपता साइबर अपराधों और अपराधियों के खिलाफ लड़ने की सबसे बड़ी जरूरत है। फिर भी **हम सुरक्षा संबंधी छोटे-छोटे कदम उठा कर साइबर अपराध से बड़ी आसानी से बच सकते हैं।**

*****

सर्वेश कुमार

पदनाम:- अधिकारी
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 9651603402
ई-मेल:- skumar.smu11@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

सारांश

बैंकिंग क्षेत्र में डिजिटलीकरण की शुरुआत कोविड के कारण हुई। फ्रंट-एंड और बैक-एंड दोनों ऑपरेशन अब डिजिटल हो गए हैं। इस बढ़ती हुई तकनीक के साथ साइबर हमले लगातार बढ़ रहे हैं और हमलावर सक्रिय रूप से बैंकिंग एवं वित्तीय प्रणालियों के संवेदनशील डेटा पर दुर्भावनापूर्ण साइबर हमला कर रहे हैं। इस नए डिजिटल कार्यबल ने अधिकांश बैंकिंग क्षेत्रों को ऑनलाइन जाने के लिए प्रेरित किया है। ऑनलाइन प्रक्रिया में वीडियो कॉन्फ्रेंसिंग भी शामिल है जिसके कारण गोपनीयता भंग हो रही है और फ़िशिंग के प्रयास के साथ-साथ रैंसमवेयर हमले भी किए जा रहे हैं। चूंकि बैंकिंग क्षेत्र ऑनलाइन बैंकिंग पर निर्भर हैं, इसलिए मोबाइल और वेब दोनों सेवाओं में कमजोर सुरक्षा प्रणाली होती है, जिसके कारण साइबर सुरक्षा खतरे अधिक प्रमुख होते जा रहे हैं। अधिकतर, साइबर अपराधी ग्राहक और कर्मचारी की जानकारी प्राप्त करने के लिए बैंकिंग क्षेत्र को लक्षित करना पसंद करते हैं और उनका उपयोग बैंक डेटा और धन चोरी करने के लिए करते हैं।

साइबर खतरों के प्रकार

बड़े पैमाने पर एंटी-फ्रॉड बायपास: ऑनलाइन ट्रांजैक्शन में वृद्धि के साथ अपराधी एंटी-फ्रॉड सेफगार्ड्स को विफल करने के तरीकों की तलाश कर रहे हैं, वे असली फिंगरप्रिंट को किसी और के पीसी से चुराए गए मौजूदा लोगों के साथ दोहराने की कोशिश करते हैं।

- **एटीएम मैलवेयर:** यह मैलवेयर का एक दिलचस्प स्वरूप है, जो भारत में वित्तीय संस्थानों में पाया गया है और एटीएम को कैश आउट करने के लिए प्रोग्राम किया गया है।
- **खाता-केंद्रित धोखाधड़ी:** यह धोखाधड़ी के सामान्य प्रकारों में से एक है, ये धोखाधड़ी मुख्य रूप से खाता संख्या, पासवर्ड, ओटीपी, आदि जैसे संवेदनशील विवरणों को चुराने और हैक करने पर केंद्रित है।
- **फ़िशिंग:** फ़िशिंग धोखे से दुर्भावनापूर्ण लिंक खोलने का एक तरीका है, जिससे मैलवेयर इंस्टाल हो जाती है जो सिस्टम को फ़्रीज़ कर देता है। फ़िशिंग का उपयोग अक्सर उपयोगकर्ता के डेटा को चोरी करने के लिए किया जाता है, जिसमें लॉगिन क्रेडेंशियल आदि शामिल हैं।
- **पहचान की चोरी:** जब डेटा उल्लंघन होता है, तो ग्राहकों के डेटा को साइबर अपराधियों द्वारा उपयोग करने के लिए बेच दिया जाता है ताकि क्रेडिट जानकारी प्राप्त करने के लिए उनकी सहमति के बिना पैसे उधार लेने और खरीद उल्लंघन करने के लिए उपयोग किया जा सके।
- **कर्मचारियों से खतरा:** नाखुश या असंतुष्ट कर्मचारी कंपनी की नीतियों का उल्लंघन कर और संगठनों के लिए सुरक्षा खतरे पैदा करके बड़े पैमाने पर जोखिम में योगदान करते हैं।
- **रैंसमवेयर:** रैंसमवेयर हमले मुख्य रूप से छोटे बैंकों को प्रभावित करेंगे क्योंकि उनके पास आईटी संसाधनों, पुरानी सुरक्षा तकनीक और साइबर सुरक्षा पर प्रोटोकॉल की कमी है। इस रैंसमवेयर से बचाने के लिए बैंकों को अपने पूरे नेटवर्क में सुरक्षा परतों को अपनाना चाहिए जो दुर्भावनापूर्ण सॉफ़्टवेयर हमलों को रोकने में एक बाधा के रूप में कार्य करने में मदद करता है।

बैंकिंग में साइबर सुरक्षा क्यों महत्वपूर्ण है?

बैंकिंग क्षेत्र में साइबर सुरक्षा निम्नलिखित कारणों से अत्यंत महत्वपूर्ण हैं:

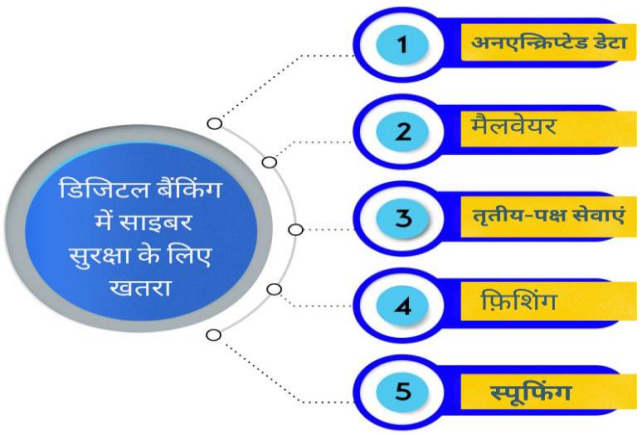
- डिजिटल इंडिया ने कैशलेस लेन-देन, डिजिटल मनी के उपयोग में वृद्धि की है। इस संदर्भ में डेटा और गोपनीयता की रक्षा के लिए सभी सुरक्षा उपाय करना महत्वपूर्ण है।
- बैंकिंग क्षेत्र में डेटा उल्लंघन एक गंभीर समस्या है। एक कमजोर साइबर सुरक्षा प्रणाली के कारण उनके ग्राहक आधार को साइबर सुरक्षा खतरों का सामना करना पड़ सकता है।
- जब कभी बैंक के डेटा का उल्लंघन होता है, तो इस डेटा उल्लंघन से उबरना समय लेने वाला और तनावपूर्ण हो सकता है। इसलिए बैंकिंग सुरक्षा प्रणाली को बढ़ाना बहुत जरूरी है!
- यदि आपने अपना कार्ड खो दिया है और उसके विरुद्ध शिकायत की है तथा कार्ड रद्द कर दिया गया है, फिर भी आपका डेटा संवेदनशील है।
- बैंकों को चौबीसों घंटे सावधान रहने की जरूरत है; यदि नहीं, तो बैंक के साथ आपके डेटा का उल्लंघन किया जा सकता है।

डिजिटल बैंकिंग में साइबर सुरक्षा की आवश्यकता

डिजिटल बैंकिंग में साइबर सुरक्षा का प्राथमिक उद्देश्य ग्राहक की संपत्ति की रक्षा करना है। लोग अपने डिजिटल पैसे जैसे क्रेडिट कार्ड और डेबिट कार्ड का उपयोग लेन-देन के लिए करते हैं जिन्हें साइबर सुरक्षा के तहत संरक्षित करने की आवश्यकता होती है। डिजिटल बैंकिंग में साइबर अपराध न केवल ग्राहक को प्रभावित करते हैं, बल्कि डेटा को पुनर्प्राप्त करने का प्रयास करते समय बैंकों को भी प्रभावित करते हैं। डेटा या जानकारी को पुनर्प्राप्त करने के लिए बैंकों को काफी राशि खर्च करने की आवश्यकता हो सकती है। बैंकों के लिए एक सुदृढ़ साइबर सुरक्षा जरूरी है क्योंकि डेटा उल्लंघनों से वित्तीय संस्थानों पर भरोसा करना मुश्किल हो सकता है। इससे

बैंकों को भारी परेशानी हो सकती है। डिजिटल बैंकिंग में साइबर सुरक्षा सुनिश्चित करती है कि आपका संवेदनशील डेटा सुरक्षित करती है जिसका खुलासा होने पर धोखाधड़ी जैसी कई समस्याएं हो सकती हैं। साइबर सुरक्षा के तहत सुरक्षित नहीं होने पर किसी के डेटा को आसानी से भंग किया जा सकता है। साइबर अपराध होने की स्थिति में यह किसी व्यक्ति को पर्याप्त वित्तीय नुकसान और मानसिक तनाव का कारण बन सकता है।

डिजिटल बैंकिंग में साइबर सुरक्षा के लिए खतरा



सुदृढ़ साइबर सुरक्षा उपाय के बिना आपका संवेदनशील डेटा खतरे में पड़ सकता है।

अनइन्क्रिप्टेड डेटा :- यह बैंकों के समक्ष आम खतरों में से एक है जहां डेटा को अनइन्क्रिप्टेड छोड़ दिया जाता है, और हैकर्स या साइबर अपराधी तुरंत डेटा का उपयोग करते हैं, जिससे वित्तीय संस्थान के लिए गंभीर समस्याएं पैदा होती हैं। वित्तीय संस्थानों में या ऑनलाइन कंप्यूटर पर संग्रहीत सभी डेटा पूरी तरह से इन्क्रिप्टेड होना चाहिए। यह सुनिश्चित करेगा कि भले ही आपका डेटा चोरी हो गया हो, साइबर अपराधी उनका उपयोग नहीं कर पाएंगे।

मैलवेयर :- कंप्यूटर और मोबाइल उपकरणों जैसे एंड-टू-एंड-यूज़र उपकरणों का उपयोग ज्यादातर डिजिटल लेन-देन करने के लिए किया जाता है, इसलिए, इसे सुरक्षित किया जाना चाहिए। यदि मैलवेयर के साथ समझौता किया जाता है, तो यह बैंक की साइबर सुरक्षा के लिए एक गंभीर जोखिम पैदा कर सकता है। संवेदनशील डेटा इस नेटवर्क से होकर गुजरता है और यदि उपयोगकर्ता डिवाइस में बिना किसी सुरक्षा के मैलवेयर इंस्टॉल हो गया है तो मैलवेयर आपके बैंक के नेटवर्क के लिए गंभीर खतरा पैदा कर सकता है।

तृतीय-पक्ष सेवाएं :- कई बैंक और वित्तीय संस्थान अपने ग्राहकों को बेहतर सेवा देने के लिए अन्य विक्रेताओं की तृतीय-पक्ष सेवाओं का उपयोग करते हैं। हालांकि, अगर इन विक्रेताओं के पास मजबूत साइबर सुरक्षा उपाय नहीं हैं तो जिस बैंक ने उन्हें नियुक्त किया है, उन्हें बहुत अधिक नुकसान होगा।

स्पूफिंग:- यह बैंकों के सामने आने वाले साइबर खतरों के नवीनतम रूपों में से एक है। साइबर अपराधी एक बैंकिंग वेबसाइट के यूआरएल को एक ऐसी वेबसाइट के साथ प्रतिरूपित करेंगे जो मूल वेबसाइट के समान है और उसी तरह कार्य करती है और जब उपयोगकर्ता अपने लॉगिन क्रेडेंशियल में प्रवेश करता है तो इन अपराधियों द्वारा लॉगिन क्रेडेंशियल चुरा लिए जाते हैं और बाद में इसका उपयोग करते हैं। यह साइबर खतरा अगले स्तर पर चला गया है जहां इन अपराधियों द्वारा नई स्पूफिंग तकनीकों का इस्तेमाल किया गया है। इसमें वे एक जैसे यूआरएल का इस्तेमाल करते हैं और सही यूआरएल पर जाने वाले यूजर्स को टारगेट करते हैं।

फ़िशिंग:- फ़िशिंग का अर्थ है इलेक्ट्रॉनिक संचार में ट्रस्टेड बॉडी के रूप में दुर्भावनापूर्ण गतिविधियों के लिए संवेदनशील जानकारी जैसे क्रेडिट कार्ड विवरण आदि प्राप्त करने का प्रयास। ऑनलाइन बैंकिंग फ़िशिंग घोटाले लगातार विकसित हुए हैं।

डिजिटल बैंकिंग में साइबर सुरक्षा से संबंधित चुनौतियां क्या हैं?

कुछ कारकों ने डिजिटल बैंकिंग में साइबर सुरक्षा को गंभीर चुनौती दी है। इनका उल्लेख नीचे किया गया है:

1. **जागरुकता की कमी :-** साइबर सुरक्षा के बारे में लोगों के बीच जागरूकता काफी कम रही है और बहुत सी कंपनियां लोगों के बीच समग्र साइबर सुरक्षा जागरूकता के प्रशिक्षण और सुधार में निवेश नहीं करती हैं।
2. **अपर्याप्त बजट और प्रबंधन की कमी :-** साइबर सुरक्षा को कम प्राथमिकता दी जाती है; इसलिए, वे ज्यादातर समय बजट में उपेक्षित होते हैं। शीर्ष प्रबंधन का ध्यान भी साइबर सुरक्षा पर कम रहता है और ऐसी परियोजनाओं के लिए समर्थन को कम प्राथमिकता दी जाती है। ऐसा इसलिए हो सकता है क्योंकि वे इन खतरों के प्रभाव को गलत समझते हैं।
3. **कमजोर पहचान और एक्सेस प्रबंधन :-** पहचान और एक्सेस प्रबंधन साइबर सुरक्षा का मूल तत्व रहा है और विशेष रूप से ऐसे समय में जब हैकर्स का दबदबा है। इसे एंटरप्राइज़ नेटवर्क में प्रवेश करने के लिए केवल हैक किए गए क्रेडेंशियल की आवश्यकता हो सकती है। इस संबंध में थोड़ा सुधार हुआ है, लेकिन अभी भी इस क्षेत्र में बहुत काम किया जाना बाकी है।
4. **रैंसमवेयर का उदय :-** मैलवेयर हमलों की हाल की घटनाओं ने हमारा ध्यान रैंसमवेयर के बढ़ते खतरे पर केंद्रित किया है। साइबर अपराधी उन तरीकों का उपयोग करना शुरू कर रहे हैं जो निष्पादन योग्य फ़ाइलों पर केंद्रित समापन बिंदु सुरक्षा कोड द्वारा उनका पता लगाने से बचते हैं।
5. **मोबाइल डिवाइस और ऐप्स :-** अधिकांश बैंकिंग संस्थानों ने व्यवसाय करने के लिए मोबाइल फोन को एक माध्यम के रूप में अपनाया है। जैसे-जैसे आधार हर दिन बढ़ता है, यह धोखाधड़ीकर्ताओं के लिए आदर्श विकल्प भी बन जाता है। मोबाइल फोन हैकर्स के लिए एक आकर्षक लक्ष्य बन गए हैं क्योंकि हम मोबाइल फोन लेन-देन में वृद्धि देख रहे हैं।
6. **सामाजिक मीडिया :-** सोशल मीडिया को अपनाने से हैकर्स ने और भी अधिक शोषण किया है।

डिजिटल बैंकिंग में साइबर सुरक्षा के खतरे का समाधान -

डिजिटल बैंकिंग में साइबर सुरक्षा के लिए खतरे को रोकने के लिए कुछ तरीकों का पालन किया जा सकता है।

मशीन लर्निंग और बिग डेटा एनालिटिक्स

साइबर फ़्लेक्सिबिलिटी का लाभ उठाने में एनालिटिक्स एक आवश्यक तत्व है। सुरक्षा विश्लेषण की एक नई पीढ़ी सामने आई है जो वास्तविक समय में बड़ी संख्या में सुरक्षा डेटा को संग्रहीत और मूल्यांकन कर सकती है।

सुरक्षा के महत्व को समझें

सुरक्षा खतरों के जोखिम और उसके प्रभाव का विश्लेषण किया जाना चाहिए तभी सुरक्षा के महत्व को सही मायने में समझा जा सकता है।

जानकारी को सुरक्षित रखें

आज डेटा विभिन्न उपकरणों और क्लाउड में संग्रहीत है, इसलिए संवेदनशील डेटा रखने वाले प्रत्येक सिस्टम को सुरक्षा के साथ संरक्षित किया जाना चाहिए।

उपभोक्ता जागरूकता

यह उन महत्वपूर्ण पहलुओं में से एक है जहां उपभोक्ता को अपनी बैंकिंग साख को किसी के सामने प्रकट न करने के बारे में जागरूक किया जाना चाहिए। उन्हें अपने लेन-देन में या अपने बैंक खाते में किसी भी संदिग्ध घटनाक्रम के मामले में जल्द से जल्द साइबर सुरक्षा सेल को रिपोर्ट करना चाहिए।

एंटी-वायरस और एंटी-मैलवेयर एप्लिकेशन

फ़ायरवॉल सुरक्षा बढ़ा सकता है, लेकिन यह तब तक हमला नहीं रोकेगा जब तक कि अद्यतन एंटी-वायरस और एंटी-मैलवेयर एप्लिकेशन का उपयोग नहीं किया जाता है। नवीनतम एप्लिकेशन को अपडेट करना आपके सिस्टम पर संभावित विनाशकारी हमलों को रोक सकता है।

निष्कर्ष

बैंकिंग क्षेत्र में प्रमुख साइबर अपराध एटीएम धोखाधड़ी, सेवा में बाधा, क्रेडिट कार्ड धोखाधड़ी, फ़िशिंग आदि हैं। वैश्विक स्तर पर तेजी से इलेक्ट्रॉनिक अपराध के विकास और इसकी जटिलता जांच के लिए साइबर नियामक प्रणाली की आवश्यकता है। वर्तमान में बैंक द्वारा किए गए उपाय पर्याप्त नहीं हैं और इसलिए दुनिया भर के बैंकों के बीच सहयोग बढ़ाना अनिवार्य है। डिजिटल बैंकिंग में साइबर सुरक्षा एक ऐसी चीज है जिससे समझौता नहीं किया जा सकता है। बैंकिंग उद्योग में डिजिटलीकरण के विकास के साथ यह साइबर अपराधियों के हमलों के प्रति अधिक संवेदनशील हो गया है। इसलिए एक फुलप्रूफ साइबर सुरक्षा होनी चाहिए जो ग्राहक और वित्तीय संस्थान के डेटा और धन की सुरक्षा से समझौता न करें।

*****

सिमरनजीत कौर

पदनाम:- अधिकारी
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 8054041347
ई-मेल:- bo0018@pnb.co.in

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

एक वित्तीय संस्थान के रूप में, बैंक लोगों को न केवल अपने धन को बचाने और विकसित करने में मदद करता है, बल्कि उन व्यवसायों को धन उधार देने में भी मदद करता है जो व्यवसाय विस्तार और निवेश करना चाहते हैं। बैंक की यह बुनियादी विशेषता अर्थव्यवस्था को बढ़ाने में मदद करती है। हालांकि, बैंकिंग तकनीक में डिजिटलीकरण के साथ बड़े पैमाने पर बदलाव देखा गया है जिससे कई चुनौतियां सामने आई हैं। साइबर सुरक्षा खतरा किसी के निजी डेटा को चुराकर किसी के डिजिटल जीवन को नुकसान पहुंचाने, चोरी करने या बाधित करने के लिए एक दुर्भावनापूर्ण कार्य है। साइबर सुरक्षा खतरे कंप्यूटर वायरस, डेटा में सेंध और यहां तक कि सेवाओं से इनकार के रूप में आ सकते हैं।

कुछ उदाहरणों के अनुसार एक साइबर सुरक्षा खतरा किसी कंप्यूटर को पूरी तरह से नुकसान पहुंचा सकता है और शायद ही कोई ऐसा व्यक्ति हो जिसे इससे चुनौती न मिली हो।

साइबर सुरक्षा क्या है?

साइबर सुरक्षा इलेक्ट्रॉनिक सिस्टम जैसे कंप्यूटर आदि और डेटा को दुर्भावनापूर्ण हमलों से बचाने का माध्यम है। इसे सूचना प्रौद्योगिकी सुरक्षा या इलेक्ट्रॉनिक सूचना सुरक्षा भी कहा जाता है।

डिजिटल बैंकिंग में साइबर सुरक्षा की क्या आवश्यकता है?

डिजिटल बैंकिंग में साइबर सुरक्षा का प्राथमिक उद्देश्य ग्राहक की संपत्ति की रक्षा करना है। जैसे-जैसे लोग कैशलेस होते जाते हैं, वैसे-वैसे अधिक से अधिक वित्तीय लेन-देन ऑनलाइन किए जाते हैं। लोग अपने डिजिटल पैसे जैसे क्रेडिट कार्ड और डेबिट कार्ड का उपयोग लेनदेन के लिए करते हैं जिन्हें साइबर सुरक्षा के तहत संरक्षित करने की आवश्यकता होती है।

डिजिटल बैंकिंग में साइबर अपराध न केवल ग्राहक को प्रभावित करते हैं, बल्कि डेटा को पुनर्प्राप्त करने का प्रयास करते समय बैंकों को भी प्रभावित करते हैं। डेटा या जानकारी को पुनर्प्राप्त करने के लिए बैंकों को काफी राशि खर्च करने की आवश्यकता हो सकती है।

बैंकों के लिए एक मजबूत साइबर सुरक्षा जरूरी है क्योंकि डेटा उल्लंघनों से वित्तीय संस्थानों पर भरोसा करना मुश्किल हो सकता है। इससे बैंकों को भारी परेशानी हो सकती है। डिजिटल बैंकिंग में साइबर सुरक्षा सुनिश्चित करती है कि आपका संवेदनशील डेटा सुरक्षित है जिसका खुलासा होने पर धोखाधड़ी जैसी कई समस्याएं हो सकती हैं।

साइबर सुरक्षा के तहत सुरक्षित नहीं होने पर किसी के डेटा का आसानी से दुरुपयोग किया जा सकता है। साइबर अपराध होने की स्थिति में यह किसी व्यक्ति को पर्याप्त वित्तीय नुकसान और मानसिक तनाव का कारण बन सकता है।

बैंकिंग नियामक अनुपालन

राजस्व और व्यवसाय वृद्धि बैंकों की वित्तीय स्थिति और प्रासंगिकता के लिए महत्वपूर्ण कारक हैं। बैंकिंग नियामक अनुपालन और खतरों की पहचान करना और उन पर कार्रवाई करना किसी भी वित्तीय संस्थान के लिए महत्वपूर्ण है। बढ़ते साइबर खतरों और धोखाधड़ी से निपटने के लिए, वित्तीय उद्योग को गति और बड़े पैमाने पर मुद्दों की पहचान करने तथा उन्हें हल करने के लिए एक समग्र, बहुस्तरीय साइबर सुरक्षा रुख के साथ-साथ एआई-संचालित नियामक अनुपालन और धोखाधड़ी का पता लगाने वाले उपकरणों की आवश्यकता है।

बैंकों द्वारा सामना किए जाने वाले साइबर सुरक्षा खतरे

सबसे पहले, मौजूदा साइबर सुरक्षा खतरों को समझना सबसे अच्छा है जो एक बैंक रोज ही सामना करता है। पिछले कुछ वर्षों में बैंकिंग की परिभाषा में बदलाव के साथ, बैंकिंग तकनीक कई चुनौतियां लेकर आई है जिसमें ज्यादातर साइबर सुरक्षा खतरे हैं। यहां बैंक साइबर सुरक्षा के बारे में कुछ गंभीर चिंताएं हैं जिनमें से कुछ निम्नानुसार हैं:-

मोबाइल ऐप से जोखिम

डिजिटलीकरण के उदय के साथ, मोबाइल ऐप्लिकेशन बैंकिंग का एक विकल्प बन गया है। ग्राहक सेवा को सुविधाजनक बनाने के लिए बैंक अधिक से अधिक आसान और समय बचाने वाले मोबाइल ऐप लेकर आए हैं। प्रत्येक बार ग्राहक द्वारा ऐप खोलने पर साइबर सुरक्षा खतरे का सामना करना पड़ता है। तकनीकी प्रगति के साथ, मोबाइल में पहले से मौजूद किसी भी दुर्भावनापूर्ण सॉफ़्टवेयर के माध्यम से या ऐप का उपयोग करते समय कड़ी सुरक्षा की कमी से भी कदाचार हो सकता है। इसलिए, साइबर सुरक्षा इंजीनियरों को डेटा लीकेज के डर के बिना एक निर्दोष उपयोगकर्ता अनुभव सुनिश्चित करने की आवश्यकता होती है।

तृतीय पक्ष के संगठन विशेष रूप से संवेदनशील लक्ष्य हैं:-

हम सभी ई-शॉपिंग करते हैं, यह उपयोग में आसान और बाधारहित होने के साथ-साथ बिना किसी गड़बड़ी के कभी भी कहीं से भी खरीदारी करने की सुविधा प्रदान करता है। कोविड-19 के प्रसार के साथ-साथ लेन-देन को डिजिटल बनाने की भारत सरकार की विभिन्न डिजिटल पहलों के साथ पेटीएम और जीपे जैसे डिजिटल भुगतान ऐप का उपयोग भी कई गुना बढ़ गया है।

बैंकिंग में साइबर सुरक्षा के खतरे

सोशल इंजीनियरिंग

सिस्टम की कमजोरियों का फायदा उठाने वाले पारंपरिक हमलों के विपरीत, सोशल इंजीनियरिंग के हमले मानवीय कमजोरियों को भुनाने का काम करते हैं। हैकर्स संवेदनशील क्रेडेंशियल्स का उपयोग महत्वपूर्ण डेटा चोरी करने या उपयोगकर्ताओं को उनके सिस्टम से बाहर करने के लिए डेटा एन्क्रिप्ट करने के लिए भी कर सकते हैं।

डेटा मैनिपुलेशन

कई साइबर अपराधी डेटा को सीधे चोरी करने के बजाय उसमें हेरफेर करते हैं। वे सिस्टम में संग्रहीत लेन-देन संबंधी डेटा में परिवर्तन करते हैं। चूंकि ये परिवर्तन वैध प्रतीत होते हैं, इसलिए उन्हें पहचानना लगभग असंभव

है। यहां तक कि छोटे, अनिर्धारित परिवर्तन लाइन के नीचे बड़े पैमाने पर मुद्दों में स्नोबॉल कर सकते हैं। डेटा हेरफेर से डेटा मानकों का गैर-अनुपालन भी हो सकता है जिसके परिणामस्वरूप पर्याप्त नियामक जुर्माना हो सकता है।

तृतीय-पक्ष सेवाएं

अधिकांश बैंक अपनी डिजिटल बैंकिंग जरूरतों को पूरा करने के लिए तीसरे पक्ष के सेवा प्रदाताओं पर भरोसा करते हैं। भले ही बैंक के पास अभेद्य सुरक्षा प्रणालियां हों, लेकिन तृतीय-पक्ष प्रणालियों में कमजोरियां बैंक को प्रभावित कर सकती हैं। इसलिए, बैंकों को यह सुनिश्चित करने की आवश्यकता है कि उनके सभी सेवा प्रदाता सुरक्षा प्रोटोकॉल में नवीनतम उद्योग मानकों के अनुरूप हों।

स्पूफिंग

स्पूफिंग वित्तीय संस्थानों के लिए चिंता का एक प्रमुख कारण बन गया है। हमले के इस तरीके में साइबर अपराधी फर्जी वेबसाइट बनाते हैं जो देखने में बैंक की असली वेबसाइट से काफी मिलती-जुलती हैं। उपयोगकर्ताओं को नकली वेबसाइट पर पुनर्निर्देशित किया जाता है, जहां उन्हें अपने लॉगिन क्रेडेंशियल दर्ज करने के लिए कहा जाता है। चूंकि वेबसाइट बैंक की असली वेबसाइट जैसी ही दिखती है, इसलिए अधिकांश उपयोगकर्ताओं को गड़बड़ी का संदेह नहीं भी होता है। एक बार जब उपयोगकर्ता अपनी साख भरते हैं, तो उन्हें मूल बैंक की वेबसाइट पर भेज दिया जाता है। इस तरह से उपयोगकर्ता के क्रेडेंशियल्स चोरी करने के बाद हैकर्स बड़े पैमाने पर मौद्रिक और प्रतिष्ठित क्षति का कारण बन सकते हैं। ऐसे बहुत सारी फर्जी वेबसाइट है जिसमें लोग आसानी से फंस जाते हैं और अपने धन की हानि करवा बैठते हैं।

अनएन्क्रिप्टेड डेटा

साइबर सुरक्षा में निवेश करने के लिए कम धन वाले छोटे क्षेत्रीय और सहकारी बैंकों पर हमलों के लिए डेटा को एन्क्रिप्ट नहीं करना विशेष रूप से जिम्मेदार हैं। अनएन्क्रिप्टेड डेटा को स्टोर करना हैकर्स के लिए इसका फायदा उठाना बहुत आसान बना सकता है। सभी संग्रहीत डेटा को एन्क्रिप्ट करना सुनिश्चित करता है कि हैकर्स एक्सेस प्राप्त करने के बाद भी चोरी की गई जानकारी का उपयोग नहीं कर पाएंगे।

फ़िशिंग

फ़िशिंग का अर्थ है इलेक्ट्रॉनिक संचार में एक भरोसेमंद इकाई के रूप में प्रच्छन्न रूप से दुर्भावनापूर्ण गतिविधियों के लिए संवेदनशील जानकारी जैसे क्रेडिट कार्ड विवरण आदि प्राप्त करने का प्रयास। ऑनलाइन बैंकिंग फ़िशिंग घोटाले लगातार विकसित हुए हैं। वे एकदम वास्तविक प्रतीत होते हैं, लेकिन वे लोगों को एक्सेस की जानकारी देने में ठगी का शिकार बनाते हैं।

बैंकिंग में साइबर सुरक्षा के लिए खतरे को रोकने के लिए कुछ तरीकों का पालन किया जा सकता है जैसे कि:

सुरक्षा के महत्व को समझें

सुरक्षा खतरों के जोखिम और उसके प्रभाव का विश्लेषण किया जाना चाहिए तभी सुरक्षा के महत्व को सही मायने में समझा जा सकता है। बैंकों और संस्थानों को ऐसी प्रौद्योगिकियों में निवेश करना चाहिए जो धोखाधड़ी में प्रयुक्त प्रथाओं और कार्यों को पहचान सकें और समाप्त कर सकें।

जानकारी को सुरक्षित रखें

आज डेटा विभिन्न उपकरणों और क्लाउड में संग्रहीत है, इसलिए संवेदनशील डेटा रखने वाले प्रत्येक सिस्टम को सुरक्षा के साथ संरक्षित किया जाना चाहिए।

उपभोक्ता जागरूकता

यह उन महत्वपूर्ण पहलुओं में से एक है जहां उपभोक्ता को अपनी बैंकिंग साख को किसी के सामने प्रकट न करने के बारे में जागरूक किया जाना चाहिए। उन्हें अपने लेन-देन में या अपने बैंक खाते में किसी भी संदिग्ध घटनाक्रम के मामले में जल्द से जल्द साइबर सुरक्षा प्रकोष्ठ को रिपोर्ट करना चाहिए।

एंटी-वायरस और एंटी-मैलवेयर ऐप्लिकेशन

फ़ायरवॉल सुरक्षा बढ़ा सकता है, लेकिन यह हमले को तब तक नहीं रोकेगा जब तक कि अपडेट किए गए एंटी-वायरस और एंटी-मैलवेयर ऐप्लिकेशन का उपयोग नहीं किया जाता है। नवीनतम ऐप्लिकेशन को अपडेट करना आपके सिस्टम पर संभावित विनाशकारी हमलों को रोक सकता है।

साइबर सुरक्षा के लिए कुछ आयामों का पालन कर साइबर हमलों से काफी हद तक बचा जा सकता है, जैसे:-

1. एक पूर्ण-सेवा सुरक्षा किट और एंटी वायरस का इस्तेमाल करना ताकि किसी भी फर्जी लिंक के खुलने से पहले आपको चेतावनी मिल सके।
2. अपने पासवर्ड को समय-समय पर बदलना और ऐसे पासवर्ड बनाए जो आसानी से निर्धारित न किए जा सकें जैसे- अपनी जन्म या एनिवर्सरी की तारीख अथवा अपना या अपने परिजनों के नाम कभी भी पासवर्ड के रूप में न रखे।
3. अपनी आईडी की चोरी से खुद को बचाने के उपाय करें। सार्वजनिक स्थलों पर वाईफ़ाई का उपयोग कर लेन-देन करने से बचें।

निष्कर्ष

डिजिटल बैंकिंग में साइबर सुरक्षा एक ऐसी चीज है जिससे समझौता नहीं किया जा सकता है। बैंकिंग उद्योग में डिजिटलीकरण के विकास के साथ, यह साइबर अपराधियों के हमलों के प्रति अधिक संवेदनशील हो गया है। इसलिए एक फुलप्रूफ साइबर सुरक्षा होनी चाहिए जो ग्राहक और वित्तीय संस्थान के डेटा और धन की सुरक्षा से समझौता न करें।

*****

स्नेहा ताकसांडे

पदनाम:- आई. टी. अधिकारी
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 9503157165
ई-मेल:- Sneha.taksande11@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

आज हम एक आधुनिक दौर में रह रहे हैं। रेलवे, एयरलाइन्स, बैंक, स्टॉक मार्केट, हॉस्पिटल के अलावा सामान्य जनजीवन से जुड़ी हुई सभी सेवाएं कंप्यूटर नेटवर्क के साथ जुड़ी हैं। इनमे से तो कई पूरी तरह से इंटरनेट पर ही आश्रित हैं। अब हर कोई अपने सभी काम इंटरनेट की मदद से करता है। आज भारत भी दुनिया के विभिन्न देशों के साथ कदम से कदम मिला कर चल रहे हैं। इंटरनेट के उपयोग में भारत आज तीसरे स्थान पर है। इस बात से हम समझ सकते हैं कि हमारा देश कितना आगे बढ़ चुका है। इसी के साथ कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर ही निर्भर करती है । बैंकों और उनके संघटकों द्वारा सूचना प्रौद्योगिकी का प्रयोग तेजी से बढ़ा है और यह अब बैंकों की परिचालन कार्यनीति का एक महत्वपूर्ण अंग है। गत समय में साइबर घटनाओं की संख्या और प्रभाव में काफी वृद्धि हुई है। विशेष रूप से बैंक सहित वित्तीय क्षेत्र के मामले, जो संकेत दे रहे हैं कि बैंकों में सुदृढ़ साइबर सुरक्षा तथा आघात सहनीयता की रुपरेखा को लागू करने की तत्काल आवश्यकता है। आसान होते साइबर हमले, इनका विकसित स्वरुप, स्तर और वेग में वृद्धि, बैंकिंग प्रणाली में साइबर खतरों की उपस्थिति को ध्यान में रखते हुए यह आवश्यक है कि साइबर जोखिमों से निपटने के लिए वर्तमान सुरक्षा में सुधार किया जाए।

आज कोरोना महामारी के दौर में लगातार डिजिटल बैंकिंग क्षेत्र का विस्तार देखा गया है और उसी मुकाबले साइबर खतरा लगातार बढ़ता जा रहा है। इसमें इंटरनेट के माध्यम से हैकिंग कर हमारे बैंक खाते और अन्य कई प्रकार के डेटा को चुरा लिया जाता है। उसका इस्तेमाल करके हमारे बैंक खाते से पैसे निकाले जाते हैं। इस समस्या से बचने के लिए इंटरनेट से जुड़े सभी प्रकार के कार्यों के लिए एक प्रकार की सुरक्षा की व्यवस्था की गई है, जिसे साइबर सुरक्षा कहा जाता है। साइबर अपराध या डेटा चोरी को रोकने के लिए साइबर सुरक्षा के अंतर्गत कई प्रकार के स्तर पर कार्य किये जाते हैं। इनमे डेटा सुरक्षा, जानकारी सुरक्षा, नेटवर्क सुरक्षा, एप्लिकेशन सुरक्षा, यूजर सुरक्षा इसके साथ क्लाउड सुरक्षा की भी व्यवस्था की गई है। समय के साथ तकनीकी में बड़े बदलाव हर किसी के लिए चुनौती है। लेकिन बदलते समय के साथ हमें अपनी सुरक्षा में भी बदलाव करना जरुरी है। जैसे-जैसे तकनीक में बदलाव हो रहे हैं, साइबर हमलों की प्रकृति भी बदल रही है। ऐसे ही कुछ घातक साइबर अपराधों के प्रकार नीचे वर्णित है।

मालवेयर :– किसी भी डिवाइस के डेटा को अपने नियंत्रण में लाने के लिए इसका इस्तेमाल किया जाता है। किसी भी नेटवर्क को हैक करने के लिए स्त्रोत में लिंक और ई-मेल अटैच होते हैं, जिसको क्लिक करने पर सॉफ्टवेयर रन हो जाता है और यूजर के डिवाइस का नियंत्रण हैकर के हाथों में चला जाता है। इसके अंतर्गत स्पायवेयर, वायरस, वार्म, रैंसमवेयर आदि आते हैं।

फिशिंग :- ये एक प्रकार की डिजिटल धोखाधड़ी करने की प्रक्रिया है। जिसमें किसी प्रतिष्ठित संस्था के नाम से किसी यूजर को ई-मेल किया जाता है और उनकी संवेदनशील जानकारी मांग ली जाती है, जैसे क्रेडिट कार्ड नंबर, डेबिट कार्ड नंबर, पासवर्ड और बैंक खाता विवरण प्रस्तुत करने का अनुरोध करते हैं। इस तरह उपभोक्ताओं की सारी जानकारी हासिल कर उनके बैंक खाते से पैसे निकाले जा सकते हैं।

मैन इन द मिडल अटैक :- इसमें हमलावर किसी भी दो पक्षों के बीच हुई बातचीत को हैक कर लेते हैं। हमलावर खुद को दो संस्थाओं में से एक के रूप में प्रस्तुत करता है, जिससे यह प्रतीत होता है की दोनों वैध पक्ष एक दूसरे के साथ संवाद कर रहे हैं। इस प्रकार दोनों पक्षों के बीच शेयर की गई सभी जानकारी का एक्सेस ले लिया जाता है। ऐसे हमलों का लक्ष्य पीड़ित से व्यक्तिगत और संवेदनशील जानकारी प्राप्त करना होता है जिसमे आम तौर पर बैंकिंग और वित्त संबंधी जानकारी शामिल होती है। इस तरह के हमलों से बचने के लिए हमेशा HTTPS वाली ही वेबसाइट का इस्तेमाल करना चाहिए।

स्मिशिंग :- यह साइबर हमले का एक एसएमएस संस्करण है। इसमें हैकर्स ई-मेल के बजाय एसएमएस का उपयोग करते हैं। ताकि ये उपयोगकर्ताओं को एक एसएमएस के उत्तर के माध्यम से उनकी संवेदनशील जानकारी जैसे बैंक खाता नंबर, क्रेडिट कार्ड नंबर, डेबिट कार्ड नंबर प्राप्त कर सके।

साइबर सुरक्षा की प्रमुख अवधारणा – संपूर्ण रूप से साइबर सुरक्षा एक बहुत व्यापक शब्द है। लेकिन ये तीन मूलभूत अवधारणाओं पर आधारित है। इसमें गोपनीयता, अखंडता और उपलब्धता शामिल हैं। इसे "CIA ट्रायड" मॉडल भी कहा जाता है। यह सूचना सुरक्षा के क्षेत्र में साइबर सुरक्षा की नीतियों के साथ संगठनों को मार्गदर्शन करने के लिए बनाया गया है।

गोपनीयता:- यह उन नियमों को परिभाषित करता है, जो जानकारी की पहुंच को सीमित करता है। साइबर हमलावरों द्वारा संवेदनशील जानकारी को एक्सेस करने से प्रतिबंधित करने के उपायों पर गोपनीयता बरती जाती है। बैंकिंग व्यवस्था में भी लोगों को एक विभाग में सही व्यक्तियों को अधिकृत करके अपनी श्रेणी के अनुसार जानकारी के उपयोग की अनुमति या खंडन किया जाता है। उन्हें जानकारी साझा करने और मजबूत पासवर्ड के साथ अपने खातों को सुरक्षित करने के बारे उचित प्रशिक्षण भी दिया जाता है। गोपनीयता सुनिश्चित करने के लिए दो कारक प्रमाणीकरण, डेटा एन्क्रिप्शन, डेटा वर्गीकरण, बायोमेट्रिक सत्यापन और सुरक्षा टोकन जैसे विभिन्न तरीके अपनाए जाते हैं।

अखंडता:- यह आश्वस्त करता है की डेटा अपनी समयावधि के अनुरूप सटीक और भरोसेमंद है। इसका अर्थ है की पारगमन के भीतर के डेटा को परिवर्तित या अवैध रूप से एक्सेस नहीं किया जाना चाहिए। इसकी सुरक्षा सुनिश्चित करने के लिए संगठन में उचित उपाय किए जाते हैं। डेटा उल्लंघन को नियंत्रित करने के लिए फाइल अनुमति और उपयोगकर्ता अभिगम नियंत्रण जैसे उपाय किए जाते हैं। साथ ही डेटा में किसी भी परिवर्तन या उल्लंघन का पता लगाने के लिए उपकरण और प्रौद्योगिकियां लागू होनी चाहिए। डेटा हानि आकस्मिक विलोपन या साइबर हमलों से निपटने के लिए नियमित बैकअप होना चाहिए। क्लाउड बैकअप अब इसके लिए भरोसेमंद समाधान है।

उपलब्धता:- हार्डवेयर, सॉफ्टवेयर, नेटवर्क और सुरक्षा उपकरण जैसे सभी आवश्यक घटकों की उपलब्धता सभी को बनाए रखना चाहिए और अपग्रेड किया जाना चाहिए। यह बिना किसी व्यवधान के सुचारु कामकाज और डेटा की पहुंच सुनिश्चित करेगा। इसमें किसी भी आपदा या अड़चनों के मामले में अतिरिक्त सुरक्षा उपकरणों का चयन शामिल है। फ़ायरवॉल, डिजास्टर रिकवरी प्लान, प्रॉक्सी सर्वर और उचित बैकअप समाधान जैसी उपयोगिताए भी इसमें शामिल हैं।

बैंकिंग में साइबर सुरक्षा- बैंकिंग एक ऐसी व्यवस्था है, जहां हर व्यक्ति बड़े विश्वास के साथ अपनी मेहनत की कमाई जमा रखता है। उनको पूरा विश्वास होता कि हमारे पैसे बैंक में सुरक्षित रहेंगे। लेकिन साइबर हमलों की बढ़ती संख्या लोगों के इस विश्वास को डगमगा रही है। ऐसे वक्त में हमारा कर्तव्य है कि हम उनका यह विश्वास बनाएं रखें। साइबर हमले ना हो इसके लिए बैंक स्तर पर कुछ उपाय योजना करे। ग्राहकों में साइबर हमलों को लेकर जागरूकता बढ़ाए, ताकि प्रत्यक्ष या अप्रत्यक्ष रूप में उनसे कोई भूल न हो और वो सतर्क रहे। साइबर हमलों से बचने के लिए हमें हर वो प्रयास करना चाहिए जिससे ग्राहकों के पैसे बैंक में सुरक्षित रहे।

इस कोरोना काल में डिजिटल ट्रांजेक्शन का इस्तेमाल काफी बढ़ा है। लोग सोशल डिस्टेंसिंग बनाए रखने के लिए अपने बैंक के जुड़े सभी काम घर से कर रहे हैं। अब लगभग सभी बैंकों ने अपने ग्राहकों को एनईएफ़टी, आरटीजीएस, आईएमपीएस और यूपीआई जैसी इ-बैंकिंग सुविधाएं दी हैं। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, यूपीआई और आईएमपीएस जैसे डिजिटल पेमेंट के जरिए लोग आसानी से अपने बिल का भुगतान बिना कैश के कर पाते हैं। सभी बैंकों ने अपने ग्राहको को ऑनलाइन बिल भुगतान का विकल्प दिया है। जिसमें बिजली, पानी, गैस, टेलीफोन, बीमा प्रीमियम आदि जैसी जरुरी सुविधाओं के लिए बिलों का भुगतान ऑनलाइन ही कर सकते हैं। इससे लोगों का समय तो बच ही रहा है तथा बिल भुगतान के लिए लाइन में खड़े होने से भी बच रहे हैं जो आज के समय की जरुरत है। इसी के साथ लोग कोरोना पीड़ितों के इलाज के लिए पैसों का लेन देन, दवाओं, हॉस्पिटलों के बिल का भुगतान भी ऑनलाइन ही कर रहे हैं। ऐसे में साइबर अपराधों का खतरा भी तेजी से बढ़ रहा है। बीते दस महीनो में इसमें करीब दो गुना बढ़ोतरी हुई है। इसके मद्देनज़र रिज़र्व बैंक ने शहरी सहकारी बैंको के लिए साइबर सुरक्षा विज़न की रुपरेखा जारी की है, जिसको "साइबर सुरक्षा के लिए प्रौद्योगिक विज़न 2020-2023 के नाम से प्रकाशित किया गया है। इसका उद्देश्य यह है कि बढ़ते साइबर हमलों से बचाव, पता लगाने, प्रतिक्रिया करने और पुनर्प्राप्ति के लिए बैंकों की सुरक्षा व्यवस्था को बढ़ाया जाए। इसमें निम्नलिखित पंच सूत्रीय उपाययोजना जारी की है।

शासन प्रणाली प्रबंध - इसमें बोर्ड प्रबंधन पर ध्यान केंद्रित किया जाएगा। निदेशक मंडल शहरी सहकारी बैंकों की सूचनाओं की सुरक्षा के लिए जिम्मेदार होगा तथा एक प्रभावी सूचना प्रौद्योगिकी और सूचना सुरक्षा को सुनिश्चित करने में सक्रिय भूमिका निभाएगा।

उपयोगी तकनीकी निवेश - साइबर सुरक्षा परियोजनाओं के कार्यान्वयन हेतु निधि का निर्माण किया जाएगा। तथा आईटी सम्पत्तियों की पूरी प्रक्रिया की उचित निगरानी करने के लिए हार्डवेयर और सॉफ्टवेयर दोनों क्षेत्रों में बैंक अपने उद्यम आईटी अवसंरचना के लिए निवेश करेंगे। बिज़नेस को सुचारु और सुरक्षित रूप से संचालित करने के लिए व्यवस्था और प्रक्रियाओं पर ध्यान केंद्रित किया जाएगा।

उपयुक्त विनियमन और पर्यवेक्षण - इसमें साइबर सुरक्षा दिशानिर्देशों के संबंध में शहरी सहकारी बैंकों की प्रभावी निगरानी के लिए एक प्रणाली स्थापित की जाएगी। इसके साथ ही सुरक्षित प्रक्रियाओं को लागू करने में उचित मार्गदर्शन किया जाएगा। जिसमें विशेषाधिकार प्राप्त प्रबंधन, नेटवर्क विभाजन, सुरक्षित व्यवस्था का प्रारूप और आकस्मिक मामलों में सुरक्षा जैसी विभिन्न सर्वोत्तम प्रणालियों को साझा करेगा।

मजबूत सहयोग - इसमें सर्वश्रेष्ठ प्रणालियों को साझा करने के लिए एक प्लेटफॉर्म स्थापित करने की संभावना तलाश कर सकते हैं। इसके अलावा उचित जोख़िमों का मूल्यांकन करने के बाद आईटी समाधान और साइबर सुरक्षा नियंत्रण करने के लिए लागत प्रभावी प्रौद्योगिकियों जैसे क्लाउड आधारित सेवाओं का उपयोग किया जा सकता है।

आईटी और साइबर सुरक्षा कौशल का विकास करना - साइबर सुरक्षा जोखिमों के प्रबंधन के लिए बैंककर्मियों को क्षेत्रीय भाषाओं में तकनिकी कौशल प्रदान करने के लिए लक्षित कौशल उन्मुख प्रशिक्षण और प्रमाणपत्र कार्यक्रम तैयार किए जाएंगे। इसका उद्देश्य साइबर सुरक्षा की बेहतर समझ के लिए स्थानीय भाषा में बैंकों को साइबर सुरक्षा चुनौतियां और विनियामक अपेक्षाओं को संप्रेषित करना है।

साइबर अपराध एक गैर क़ानूनी काम है और इसमें कुछ आपराधिक गतिविधियां भी शामिल हो सकती है। इनमें हैकिंग, डेटा चोरी, धोखाधड़ी के साथ अन्य कई कार्य भारतीय दंड संहिता के अंतर्गत आते हैं। इन गैर क़ानूनी कार्यों को रोकने के लिए भारत में भी साइबर सुरक्षा की जरुरत है। ऐसे साइबर अपराधों को संज्ञान में लेते हुए भारत सरकार द्वारा देश में कई कदम उठाए गए हैं। "सूचना प्रौद्योगिकी अधिनियम 2000 " पारित किया गया जिसमे साइबर हमलों को निपटाने के प्रबंध किए गए हैं। इसमें कई धाराएं बनाई गई है जो हैकिंग और साइबर अपराधों से संबंधित हैं। साइबर सुरक्षा के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय को नोडल एजेन्सी बनाया है। इसके साथ राष्ट्रीय प्रद्योगिकी अनुसंधान संगठन को भी नोडल एजेन्सी बनाया गया है। भारत सरकार द्वारा 2013 में राष्ट्रीय सुरक्षा नीति जारी की गई। इसके तहत राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre-NCIIPC) का भी गठन किया गया है। इसके अलावा कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-In) की भी स्थापना की गई जो साइबर सुरक्षा के लिए बनाया गया है।

साइबर हमलों से बचने के लिए हमें व्यक्तिगत स्तर पर भी सतर्क रहना बहुत जरुरी है। उसके लिए कुछ सुरक्षात्मक उपाय निचे वर्णित है।

- इंटरनेट या मोबाइल फोन से किसी भी तरह के संवेदनशील डेटा को चोरी, गलत इस्तेमाल या उसे मिटने/खो जाने से बचाने के लिए मोबाइल फोन और सभी एप्लीकेशन सुरक्षित रखना जरुरी है। किसी अज्ञात स्त्रोत से ऐप डाउनलोड न करें।
- सोशल मीडिया अकाउंट के जरिए किसी और ऐप में साइन इन करते हुए सतर्क रहे। कुछ ऐप सोशल मीडिया साइटों के साथ जुड़े होते है, ऐसे में वो ऐप अपने सोशल मीडिया अकाउंट से सूचनाएं ले सकते हैं।
- एसएमएस और ई-मेल पर आए लिंक पर क्लिक करने, अज्ञात स्त्रोत से आए अटैचमेंट खोलने से पहले ध्यान दे इसमें वायरस का खतरा हो सकता है।
- किसी भी बैंक के नाम से आने वाली फोन कॉल मैसेज या ई-मेल पर भरोसा ना करें और अपने खाते की जानकारी किसी से साझा न करें।
- किसी भी ऐप द्वारा पैसे ट्रांसफर या ऑनलाइन बिल का भुगतान करते समय सतर्क रहें।
- डेबिट कार्ड या क्रेडिट कार्ड से पेमेंट करते समय ध्यान दें।

आज के समय में साइबर सुरक्षा, दुनिया की सबसे बड़ी जरुरत है क्योंकि ये अपने संवेदनशील जानकारी से तो कभी ये बैंक में पैसों से संबंधित होते हैं। इसलिए ये न केवल सरकार की बल्कि हर एक व्यक्ति की जिम्मेदारी है कि वो ऐसे कामों में सावधानी बरते। अंत: हर एक व्यक्ति साइबर सुरक्षा को देश की सुरक्षा समझकर सतर्क रहे और अपना कर्त्तव्य निभाए, तो निश्चित रूप से साइबर हमलों पर रोक लगाकर विजय प्राप्त कर सकते हैं।

*****

हेमलता भाटिया

पदनाम:- प्रबंधक
संस्था का नाम:- यूनियन बैंक ऑफ इंडिया
मोबाइल नं. :- 8720008974
ई-मेल:- bhatiahemlata@gmail.com

बैंकिंग में साइबर अपराध - स्वरूप एवं सुरक्षात्मक उपाय

प्रस्तावना

अनेकसंशयोच्छेदि, परोक्षार्थस्य दर्शकम् ।
सर्वस्य लोचनं शास्त्रं, यस्य नास्त्यन्ध एव सः ॥

अर्थ-यह कई शंकाओं को दूर करता है, जो स्पष्ट नहीं है उसका पूर्वाभास करता है।
विज्ञान सबकी आंख है, जिसके पास नहीं है, वह नेत्रहीन के समान है।

आज विज्ञान तकनीक,टेक्नोलॉजी के रूप में सभी के पास है चाहे बड़े-बुजुर्ग हो,स्कूल जाते बच्चे या फिर गृहनियां। हर कोई तकनीक से जुड़ा हुआ है। हमें धन्यवाद कहना चाहिए मोबाइल फोन टेक्नोलॉजी को जो बड़े से बड़े शहर से लेकर गांव तक फैली हुई है एवं लोग उसका बहुत खूब इस्तेमाल कर रहें हैं।परन्तु जैसा की पुरानी मान्यता है कि हर अच्छाई के साथ कुछ बुराइयां जरूर आती हैं। वैसे ही नई तकनीक के साथ-साथ उसका गलत फायदा उठाने वाले व्यक्तियों की भी कमी नहीं है। जरूरी है तकनीक को इस्तेमाल करते समय हम अपनी आँखें हमेशा खुली रखें।

इंटरनेट के द्वारा हम अनगिनत कार्य करते हैं। इंटरनेट के द्वारा दफतर के कार्य, ऑनलाइन पढ़ाई, शॉपिंग, नौकरी खोजना, एक दूसरे से संपर्क साधना इस तरह के कार्य हम करते हैं। ऐसे में इंटरनेट का इस्तेमाल कुछ लोग गलत और अवैध कार्यो के लिए करते हैं।

क्राइम रिकार्ड्स ब्यूरो के मुताबिक़ साइबर अपराध दिन प्रतिदिन बढ़ रहे हैं। रिपोर्ट के अनुसार 2011 के बाद से साइबर क्राइम में बढ़ोतरी हुयी है। ऐसे लोग जो साइबर क्राइम कर रहे हैं, आंकड़ों के मुताबिक उनकी आयु तकरीबन 18 से 30 साल तक की है।

साइबर क्राइम से प्रभावित लोग अपने निजी डेटा को दुनिया के साथ साझा नहीं करना चाहते हैं। हैकर्स के कारण लोगों को बहुत नुकसान होता है। साइबर अपराध इंटरनेट की मदद से होता है। इसमें अपराधी किसी व्यक्ति के कंप्यूटर नेटवर्क को बेकार ट्रैफिक और मैसेज से भर देते हैं। साइबर अपराधी यह सारे अपराध जो करते हैं, उनके पीछे अलग-अलग उद्देश्य होते हैं। कोई किसी व्यक्ति को निजी तौर पर नुकसान पहुंचाना चाहता है, तो कोई पैसे के लालच में करता है।

साइबर अपराध के प्रकार

1. पहचान की चोरी

आये दिन इंटरनेट पर कई लोगों के निजी डेटा चोरी हो जाते हैं। कुछ लोगों के इंटरनेट के द्वारा बैंक संबंधित जानकारी चोरी हो जाती है, जिसकी वजह से लोगो को काफी नुकसान होता है।

2. हैकिंग की समस्या

हैकिंग में किसी के कंप्यूटर के डेटा को बिना अनुमति के गैरकानूनी ढंग से उपयोग किया जाता है। हैकर्स घुसपैठ के जरिए किसी के कंप्यूटर सिस्टम में घुसकर उसे हानि पहुंचाते हैं। यह एक प्रकार का अपराध है।

3. यौन शोषण

इंटरनेट पर बच्चों के साथ गलत व्यवहार होता है। ऐसे कई मामले आये हैं जिसमे अपराधी बच्चों को अश्लील चीज़ें भेजते है और उनका गलत फायदा उठाते है। अपराधी उनका भरोसा जीतकर उनका शोषण करते है। ऐसे गलत साइबर अपराधों को रोकना बेहद आवश्यक है।

4. स्टॉकिंग अपराध

इंटरनेट पर साइबर स्टॉकिंग एक दूसरी बड़ी समस्या है, जिसके शिकार बहुत मासूम लोग हो चुके है। अपराधी किसी इंसान जिसे वह मानसिक और शारीरिक रूप से नुकसान पहुंचाना चाहते है, उसका इंटरनेट के ज़रिये पीछा करते हैं। उसके बारे में गैरकानूनी ढंग से सब कुछ जान लेते हैं और इंटरनेट का उपयोग करके उन्हें बदनाम करने की कोशिश करते हैं।अपराधी उन्हें मैसेज या कॉल करके परेशान करते हैं। अपराधी का सिर्फ एक ही मकसद होता है, उन्हें शारीरिक और मानसिक तौर पर तोड़ना और निरंतर परेशान करके पीड़ित व्यक्ति को धमकाना। साइबर स्टॉकिंग करना अपराध है।

5. वेबसाइट का गलत तरीके से नियंत्रण

कभी कभी अपराधी किसी के वेबसाइट को गलत तरीके से नियंत्रित कर लेते हैं। वेबसाइट के मालिक अपने वेबसाइट का अधिकार खो बैठते हैं। वह अपने वेबसाइट संबंधित सारी जानकारी खो बैठते हैं। इसके कारण उन्हें काफी मुश्किलों का सामना करना पड़ सकता है।

6. वित्तीय अपराध

हैकिंग करके कुछ लोग उपयोगकर्ता या खाताधारकों के पैसे चुराते हैं। इस प्रकार वे कंपनियों का डेटा भी चुराते हैं। यह सब वित्तीय अपराध की श्रेणी में आते हैं। इसके फलस्वरूप लेनदेन में भारी जोखिम होता है। हर साल हैकर्स कारोबारियों और सरकार के लाखों-करोड़ों रुपये चुरा लेते हैं।

साइबर अपराधी बैंक कर्मचारी बनकर भी यह कर सकता है। वह हर व्यक्ति के बैंक अकाउंट से हर महीने पांच रूपए भी काट ले, तो वह किसी के नज़र में नहीं आएगा। हर महीने के आखिर में अपराधी के पास काफी रूपए इकट्ठा हो जायेंगे। यह एक सोचा समझा वित्तीय अपराध है।

7. वायरस द्वारा लोगों की जानकारी पर हमला

साइबर क्राइम में वायरस अटैक एक सबसे बड़ी समस्या मानी जाती है। यह एक ऐसा नुकसानदेह सॉफ्टवेयर होता है, जो कंप्यूटर में मौजूद जानकारी को तबाह कर देता है। वायरस अटैक से किसी व्यक्ति के सॉफ्टवेयर को दूसरे सॉफ्टवेयर के साथ जोड़ दिया जाता है। वायरस कंप्यूटर को इतने बुरे तरीके से प्रभावित करते है कि उसे और इस्तेमाल ही नहीं किया जा सकता है।

8. फिशिंग

साइबर अपराध में फिशिंग के ज़रिये किसी भी व्यक्ति की ज़रूरी जानकारी निकाल ली जाती है। इसमें झूठी वेबसाइट बनाकर या ई-मेल भेजकर व्यक्ति की निजी जानकारी चुरा ली जाती है।

ऐसे में लोगो को सावधान रहना चाहिए। किसी अनजान स्पैम मेल में किसी लिंक को क्लिक करने से जानकारी चोरी होने का खतरा हो सकता है। साइबर अपराधी ऐसे जानकारी निकालकर वह पीड़ित व्यक्ति को तकलीफ पहुंचाते हैं।

9. एटीएम की धोखाधड़ी

आजकल अपराधी एटीएम मशीन से पिन और नंबर निकालकर झूठे कार्ड तैयार कर लेते हैं। यह लोग इतने चालाक होते हैं कि लोगों को आसानी से लूट लेते हैं और उनके परिश्रम से कमाया हुआ पैसा चोरी कर लेते हैं। एटीएम धोखाधड़ी से बहुत सारे लोग अपने पैसे गवा देते हैं।

10. पायरेसी की समस्या

साइबर अपराध के दौरान कुछ अपराधी सरकारी वेबसाइट को हैक कर लेते हैं। इससे महत्वपूर्ण डेटा लीक हो जाता है। अपराधी पायरेटेड डेटा की डुप्लीकेट कॉपी बना लेते हैं, जिसके कारण सरकार को काफी नुकसान झेलना पड़ता है।

11. सिस्टम पर अटैक

साइबर अपराधी कंप्यूटर के सिस्टम को क्षति पहुंचाने के लिए एक सॉफ्टवेयर का इस्तेमाल करते हैं, जिसे मालवेयर कहा जाता है। यह कंप्यूटर सिस्टम को बुरे तरीके से नुकसान पहुंचाता है। इसका उद्देश्य कंप्यूटर में मौजूद विशेष जानकारी तक पहुंचना होता है। उसके बाद वह उस जानकारी का गलत उपयोग करते हैं।

साइबर अपराध से बचाव के उपाय

कंप्यूटर हैकर्स से कंप्यूटर को बचाने के लिए उसकी सुरक्षा ज़रूरी है। इसके लिए फ़ायरवॉल का उपयोग करना चाहिए। एंटी वायरस सॉफ्टवेयर का इस्तेमाल करने से कंप्यूटर और उसकी जानकारी सुरक्षित रहती है।

लोगों को अपने वित्तीय जानकारी कभी भी किसी से साझा नहीं करनी चाहिए। उपभोगकर्ताओं को सुरक्षित वेबसाइट पर ही शॉपिंग करनी चाहिए। क्रेडिट कार्ड की कोई जानकारी इंटरनेट पर हरगिज़ ना दे।

यूज़र्स को एक ठोस पासवर्ड का चयन करना चाहिए, जिससे हैकर्स किसी के वेबसाइट या मेल आईडी को हैक ना कर पाए। आजकल बच्चे भी इंटरनेट का उपयोग करते हैं। अभिभावकों को अपने बच्चों को सीमित मात्रा में ही इंटरनेट का इस्तेमाल करने देना चाहिए।

हमेशा सोशल मीडिया जैसे फेसबुक, ट्विटर, यूटूब और इंस्टाग्राम इत्यादि के पासवर्ड और सेटिंग्स को सही से रखें और हमेशा सतर्क रहें। सोशल मीडिया पर गोपनीयता को बनाये रखने के लिए सेटिंग्स की हमेशा नियमित जांच करे। इससे लोगो की निजी जानकारी सुरक्षित रहती है।

सार्वजनिक वाई-फाई का इस्तेमाल करते समय लोगों को वित्तीय लेन देन नहीं करना चाहिए। इससे निजी जानकारी चोरी होने का भय रहता है। लोगों को नाम, पता, फ़ोन नम्बर या किसी तरह की वित्तीय जानकारी देते समय सचेत रहना ज़रूरी है।

यह हमेशा पता कर लें की जिस वेबसाइट पर आप अपनी निजी जानकारी साझा कर रहे हैं वह सुरक्षित है या नहीं। किसी भी अज्ञात मेल के लिंक को ना खोले। सन्देश कहां से आया है उसकी जांच पड़ताल के बाद ही कोई प्रतिक्रिया जाहिर करें।

साइबर सेल

साइबर अपराधो को रोकने के लिए अंतराष्ट्रीय स्तर पर काफी कोशिशें की गयी हैं। देश में साइबर सेल की शुरुआत हो गयी है, जहां आप साइबर अपराध की शिकायत कर सकते हैं। साइबर सेल अपराधियों को सजा देते हैं।

पुलिस विभाग ने साइबर क्राइम के विरुद्ध कड़े कानून बनाये हैं, ताकि अपराधी गुनाह करने से पूर्व दस बार सोचे। साइबर सुरक्षा हमारे निजी और गोपनीय जानकारी को लीक होने से बचाती है। साइबर अपराधों पर अंकुश लगाने के लिए साइबर सेल अपना काम कर रहा है।

अगर किसी संगठन के अंदरूनी डेटा तक आपकी आधिकारिक पहुंच है, लेकिन अपनी जायज पहुंच का इस्तेमाल आप उस संगठन की इजाजत के बिना, उसके नाजायज दुरुपयोग की मंशा से करते हैं, तो वह भी इसके दायरे में आएगा। कॉल सेंटरों, दूसरों की जानकारी रखने वाले संगठनों आदि में भी लोगों के निजी डेटा की चोरी के मामले सामने आते रहे हैं।

साइबर क्राइम से जुड़े कानून:-

साइबर क्राइम के बढ़ते अपराधों को देखकर सरकार ने कई कानून बनाए हैं और समय-समय पर संशोधन भी किया गया है कुछ कानून निम्नलिखित हैं:-

- आईटी (संशोधन) कानून 2008 की धारा 43 (बी), धारा 66 (ई), 67 (सी)
- आईपीसी की धारा 379, 405, 420
- भारत में भी साइबर क्राइम मामलों में तेजी से इजाफा हो रहा है. सरकार ऐसे मामलों को लेकर बहुत गंभीर है.

भारत में साइबर क्राइम के मामलों में सूचना तकनीक कानून 2000 और सूचना तकनीक (संशोधन) कानून 2008 लागू होते हैं. मगर इसी श्रेणी के कई मामलों में भारतीय दंड संहिता (आईपीसी), कॉपीराइट कानून 1957, कंपनी कानून, सरकारी गोपनीयता कानून और यहां तक कि आतंकवाद निरोधक कानून के तहत भी कार्रवाई की जा सकती है।

हैकिंग: धाराएं और सजा

किसी कंप्यूटर, डिवाइस, इंफॉर्मेशन सिस्टम या नेटवर्क में अनधिकृत रूप से घुसपैठ करना और डेटा से छेड़छाड़ करना हैकिंग कहलाता है। यह हैकिंग उस सिस्टम की फिजिकल एक्सेस और रिमोट एक्सेस के जरिए भी हो सकती है। जरूरी नहीं कि ऐसी हैकिंग के दौरान उस सिस्टम को नुकसान पहुंचा ही हो। अगर कोई नुकसान नहीं भी हुआ है, तो भी घुसपैठ करना साइबर क्राइम के तहत आता है, जिसके लिए सजा का प्रावधान है। आईटी (संशोधन) एक्ट 2008 की धारा 43 (ए), धारा 66 - आईपीसी की धारा 379 और 406 के तहत अपराध साबित होने पर तीन साल तक की जेल या पांच लाख रुपये तक जुर्माना हो सकता है।

जानकारी या डेटा चोरी

किसी व्यक्ति, संस्थान या संगठन आदि के किसी सिस्टम से निजी या गोपनीय डेटा या सूचनाओं की चोरी करना भी साइबर क्राइम है। अगर किसी संस्थान या संगठन के अंदरूनी डेटा तक आपकी पहुंच है, लेकिन आप अपनी उस जायज पहुंच का इस्तेमाल संगठन की इजाजत के बिना, उसके नाजायज दुरुपयोग की मंशा से करते हैं, तो वह भी इसी अपराध के दायरे में आएगा। कॉल सेंटरस् या लोगों की जानकारी रखने वाले संगठनों में इस तरह की चोरी के मामले सामने आते रहे हैं। ऐसे मामलों में आईटी (संशोधन) कानून 2008 की धारा 43 (बी), धारा

66 (ई), 67 (सी), आईपीसी की धारा 379, 405, 420 और कॉपीराइट कानून के तहत दोष साबित होने पर अपराध की गंभीरता के हिसाब से तीन साल तक की जेल या दो लाख रुपये तक जुर्माना हो सकता है।

वायरस, स्पाईवेयर फैलाना

अक्सर कम्प्यूटर में आए वायरस और स्पाईवेयर को हटाने पर लोग ध्यान नहीं देते हैं। उनके सिस्टम से होते हुए ये वायरस दूसरों तक पहुंच जाते हैं। हैकिंग, डाउनलोड, कंपनियों के अंदरूनी नेटवर्क, वाई-फाई कनेक्शनों और असुरक्षित फ्लैश ड्राइव, सीडी के जरिए भी वायरस फैल जाते हैं। वायरस बनाने वाले अपराधियों की पूरी एक इंडस्ट्री है, जिनके खिलाफ वक्त बेवक्त कड़ी कार्रवाई होती रही है। लेकिन आम लोग भी कानून के दायरे में आ सकते हैं। अगर उनकी लापरवाही से किसी के सिस्टम में कोई खतरनाक वायरस पहुंच जाए और बड़ा नुकसान कर दे। इस तरह के केस में आईटी (संशोधन) एक्ट 2008 की धारा 43 (सी), धारा 66, आईपीसी की धारा 268 और देश की सुरक्षा को खतरा पहुंचाने के लिए फैलाए गए वायरस पर साइबर आतंकवाद से जुड़ी धारा 66 (एफ) भी लगाई जाती है। दोष सिद्ध होने पर साइबर-वॉर और साइबर आतंकवाद से जुड़े मामलों में उम्र कैद का प्रावधान है। जबकि अन्य मामलों में तीन साल तक की जेल या जुर्माना हो सकता है।

पहचान की चोरी

किसी दूसरे शख्स की पहचान से जुड़े डेटा, गुप्त सूचनाओं वगैरह का इस्तेमाल करना भी साइबर अपराध है। यदि कोई इंसान दूसरों के क्रेडिट कार्ड नंबर, पासपोर्ट नंबर, आधार नंबर, डिजिटल आईडी कार्ड, ई-कॉमर्स ट्रांजैक्शन पासवर्ड, इलेक्ट्रॉनिक सिग्नेचर वगैरह का इस्तेमाल करके शॉपिंग या धन की निकासी करता है तो वह इस अपराध में शामिल हो जाता है। जब आप किसी दूसरे शख्स के नाम पर या उसकी पहचान का आभास देते हुए कोई जुर्म करते हैं, या उसका नाजायज फायदा उठाते हैं, तो यह जुर्म आइडेंटिटी थेफ्ट के दायरे में आता है। ऐसा करने वाले पर आईटी (संशोधन) एक्ट 2008 की धारा 43, 66 (सी), आईपीसी की धारा 419 लगाए जाने का प्रावधान है। जिसमें दोष साबित होने पर तीन साल तक की जेल या एक लाख रुपये तक जुर्माना हो सकता है।

ई-मेल स्पूफिंग और फ्रॉड

अक्सर आपके इनबॉक्स या स्पैम बॉक्स में कई तरह के इनाम देने वाले या बिजनेस पार्टनर बनाने वाले या फिर लॉटरी निकलने वाले मेल आते हैं। ये सभी मेल किसी दूसरे शख्स के ई-मेल या फर्जी ई-मेल आईडी के जरिए किए जाते हैं। किसी दूसरे के ई-मेल पते का इस्तेमाल करते हुए गलत मकसद से दूसरों को ई-मेल भेजना इसी अपराध की श्रेणी में आता है। हैकिंग, फिशिंग, स्पैम और वायरस, स्पाईवेयर फैलाने के लिए इस तरह के फर्जी ई-मेल का इस्तेमाल अधिक होता है। ऐसा काम करने वाले अपराधियों का मकसद ई-मेल पाने वाले को धोखा देकर उसकी गोपनीय जानकारी हासिल करना होता है। ऐसी जानकारियों में बैंक खाता नंबर, क्रेडिट कार्ड नंबर, ई-कॉमर्स साइट का पासवर्ड वगैरह आ सकते हैं। इस तरह के मामलों में आईटी कानून 2000 की धारा 77 बी, आईटी (संशोधन) कानून 2008 की धारा 66 डी, आईपीसी की धारा 417, 419, 420 और 465 लगाए जाने का प्रावधान है। दोष साबित होने पर तीन साल तक की जेल या जुर्माना हो सकता है।

साइबर क्राइम और रिजर्व बैंक ऑफ इंडिया की पहल:-

भारतीय रिज़र्व बैंक - भारत का केंद्रीय बैंक - जनता के सदस्यों को उनके लिए उपलब्ध विभिन्न बैंकिंग नियमों और सुविधाओं के बारे में शिक्षित करने के लिए एसएमएस (SMS) के माध्यम से एक जन जागरूकता अभियान शुरू किया गया है।

सबसे पहले, रिज़र्व बैंक ने लोगों को ई-मेल/ एसएमएस/ फोन कॉल के माध्यम से प्राप्त अवांछित और काल्पनिक प्रस्तावों के शिकार होने से सावधान करते हुए संदेश भेजना शुरू किया। यह चेतावनी संदेश 'RBISAY' प्रेषक आईडी से भेजे जाते हैं।

रिज़र्व बैंक समय-समय पर जारी प्रेस विज्ञप्तियों (https://www.rbi.org.in/Scripts/RBICautions.aspx) के माध्यम से जनता को ऐसे प्रस्तावों के प्रति सचेत करता रहा है। फर्जी कॉल/ई-मेल पर इंटरएक्टिव वॉयस रिस्पांस सिस्टम (आईवीआरएस) के माध्यम से अधिक जानकारी प्राप्त करने के साथ-साथ चिट-फंड में समझदारी और सावधानी से निवेश करने के लिए जनता 8691960000 पर मिस्ड कॉल दे सकती है। वे अभियान पर अपनी प्रतिक्रिया ई-मेल द्वारा भी भेज सकते हैं।

टेलीविज़न और सोशल मीडिया साइट्स पर आरबीआई समय-समय पर लोगों को जानकारियां देती रहती है एवं सतर्क करती रहती है।

निष्कर्ष

आज के परिप्रेक्ष्य में व्यक्ति को अपने साथ-साथ दूसरों की अच्छा का भी ध्यान रखना चाहिए। जब आप खुद सतर्क होंगे तभी आप दूसरों को सतर्क कर उनकी मदद कर सकेंगे। आज का समय तेजी से बदल रहा है और अपनी के भी उसी तेजी से बढ़ रही हैं तकनीकों के बढ़ने के साथ-साथ तरह के अपराध भी बढ़ रहे हैं जानकारी एवं सतर्कता ही आज साइबर क्राइम से बचाव हैं।

साइबर अपराध बेहद निंदनीय है। लोगों में जागरूकता फैलाना ज़रूरी है कि वह इंटरनेट का इस्तेमाल जानकारी प्राप्त करने और अच्छे कार्यो के लिए करें। उन्हें इंटरनेट का उपयोग किसी को भी नुकसान पहुंचाने के लिए नहीं करना चाहिए। ऐसे कई तरीके हैं जिनका इस्तेमाल करके हम इंटरनेट पर गोपनीयता को बनाये रख सकते हैं। इंटरनेट का उपयोग सिर्फ ज्ञान विकसित करने के लिए करना चाहिए नाकि गलत चीज़ों के लिए।

मैं यह घोषणा करती हूं कि उपरोक्त विषय पर लिखा हुआ लेख मूलतः मेरे द्वारा लिखा गया है एवं कुछ सन्दर्भ लिए गए है जिनका विवरण नीचे किया गया है।

सन्दर्भ:-

1.विकिपीडिया
2. सूचना एवं प्रौद्योगिकी मंत्रालय की वेबसाइट।
3.https://www.rbi.org.in/Scripts/RBICautions.aspx

*****

अंशिता वर्मा

पदनाम:- अधिकारी
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 9827092445
ई-मेल:- ansh2902@gmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

परिचय

स्वतंत्रता से लेकर आज तक भारत के विकास की यात्रा शानदार रही है। चाहे क्षेत्र कोई भी हो, कृषि से लेकर अंतरिक्ष तक, संचार क्रांति से लेकर ट्रेन बनाने तक हर कार्य व क्षेत्र में भारत ने धीरे-धीरे सफलता प्राप्त की है। नित नए आविष्कारों और नवीनीकरण से भारत विश्व में अपनी एक अलग पहचान बना रहा है।

भारत को इस नए आकाश पर ले जाने में ग्लोबलाइज़ेशन और प्रौद्योगिकरण ने बहुत महत्वपूर्ण भूमिका निभाई है। आज के दौर मे इंटरनेट हमारी ज़रूरत बन गया है। रोटी, कपड़ा, मकान हेतु अब इंटरनेट हमारी बुनियादी जरूरत बन गया है। पर कहते हैं ना कि हर सिक्के के दो पहलू होते हैं। एक ओर जहां सूचना क्रान्ति ने समाज के सभी क्षेत्रों की कायापलट कर दी है वही इसकी सुरक्षा भी भेजा जा रहा है। आए दिन हमें साइबर संबंधित धोखे के किस्से भी सुनने को मिलते हैं। किसी भी क्षेत्र मे अनुशासन और नियम जरूरी होता है। इंटरनेट के इस दौर में उसकी सुरक्षा व बचाव के लिए कुछ नियम कायदे जरूरी है। इन्हीं नियम कायदों के लिए साइबर कानून प्रभाव में आया है ताकि इंटरनेट पर किए गए धोखेबाज़ों को सजा दिलाई जा सके।

साइबर कानून क्या है:

साइबर कानून या साइबर अपराध कानून (**cyber crime law**) ऐसा लॉ / कानून होता है जो कंप्यूटर हार्डवेयर एवं सॉफ्टवेयर, इंटरनेट और नेटवर्क सहित प्रौद्योगिकी के स्वीकार्य व्यवहार इस्तेमाल पर केंद्रित है। साइबर कानून उपयोगकर्ताओं को ऑनलाइन आपराधिक गतिविधि की जांच और अभियोजन को सक्षम करके साइबर अटैक जैसे क्राइम के नुकसान से बचाने में मदद करता है।

देश में इलेक्ट्रॉनिक कॉमर्स और गवर्नेंस के लिए अधिकतम कनेक्टिविटी और न्यूनतम साइबर सुरक्षा जोखिम सुनिश्चित करने का काम करता है, (**Indian Cyber Law**) साइबर कानून/लॉ, इसके साथ ही इस कानून की वजह से इंटरनेट के इस्तेमाल का दायरा बढ़ा है, यानि डिजिटल माध्यमों के उपयोग का विस्तार भी भारत में हुआ है।

साइबर लॉ डिजिटल कानूनी प्रणाली का एक हिस्सा है जिसे इंटरनेट, साइबर स्पेस और इसमें होने वाले दिक्कतों जैसे मुद्दों से संबंधित किया गया है। साइबर लॉ ने इंटरनेट के बहुत बड़े क्षेत्र पर अपनी पकड़ बना रखी है , मगर इसके बावजूद साइबर लॉ की जानकारी के अभाव में अपराधी प्रवृति के लोग इंटरनेट कि दुनिया में बड़े पैमाने पर अपराध को अंजाम दे रहे हैं।

आज हम बेफिक्र होकर अपनी महत्वपूर्ण जानकारी और डेटा स्टोर करने के लिए कंप्यूटर कि मदद लेते हैं और उसमें स्टोर करते हैं। हमारे महत्वपूर्ण डेटा और जानकारी फ्रॉड या धोखाधड़ी का शिकार ना हो जाए इसलिए

साइबर लॉ इससे संबंधित है। साइबर लॉ के अनुसार हर एक साइबर क्राइम के लिए अलग से धारा एवं सजा सुनिश्चित की है। इसी प्रकार के बहुत से धाराएं बनाए गए हैं, जिससे लोगों के लिए खतरा ना बढ़ने पाए।

भारत में साइबर कानून का उपयोग किसी भी साइबर क्राइम/ अपराध को रोकना है। साइबर क्राइम से बचने के लिए कानून नागरिकों को संवेदनशील जानकारी साझा न करने से बचाता है। भारत में साइबर कानून (**law for cyber crime**) की शुरूआत 2008 में, आईटी (IT) अधिनियम 2000 [**Information Technology Act 2000 (IT Act)**] के रूप में हुई थी और भारत में साइबर कानून के तहत विभिन्न प्रकार के अपराधों को कवर किया जाता है, जैसे –

- साइबर अपराध/क्राइम/जुर्म
- इलेक्ट्रॉनिक और डिजिटल हस्ताक्षर में धोखाधड़ी
- इंटेलेक्चुअल प्रॉपर्टी (IP) में धोखाधड़ी
- डेटा संरक्षण/गोपनीयता मामले में धोखाधड़ी

साइबर क्राइम लॉ (**Cyber Crime Law**) इसलिए जरुरी या महत्वपूर्ण है, क्योंकि भारत में साइबर क्राइम/अपराध अधिनियम में शामिल हैं, जो इंटरनेट पर लेनदेन के पहलू और इंटरनेट एवं साइबरस्पेस पर होने वाली गतिविधियों के मामलो को शामिल करता है। भारत में टेक्नोलॉजी के उपयोग पर निर्भरता में वृद्धि के साथ, साइबर कानून की आवश्यकता महत्वपूर्ण है।

भारत सरकार के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के अनुसार साइबर कानून (**Indian cybercrime law**) इलेक्ट्रॉनिक दस्तावेजों, ई-फाइलिंग और ई-कॉमर्स के लेनदेन का समर्थन करने के लिए एक कानूनी मान्यता देता है।

भारत में साइबर अपराधों को कम करने व उनकी जांच करने के लिए एक कानूनी संरचना प्रदान करता है। भारत में साइबर कानून का अनुबंध, बौद्धिक संपदा, डेटा संरक्षण और गोपनीयता कानूनों का एक संयोजन है। साइबर कानून सूचना, सॉफ्टवेयर, सूचना सुरक्षा, ई-कॉमर्स और मौद्रिक लेनदेन के डिजिटल संचलन की निगरानी करता हैं। सभी आपराधिक गतिविधियां जैसे कि चोरी, धोखाधड़ी, जालसाजी, मानहानि और शरारत साइबरस्पेस का हिस्सा है, इन्हें भारतीय दंड संहिता में शामिल किया हुआ है।

सभी ऑनलाइन गतिविधियां साइबर लॉ के तहत जांच के दायरे में आती हैं लेकिन कुछ ऐसे क्षेत्र भी हैं जिन पर भारत में साइबर क्राइम कानून लागू नहीं होता हैं, जैसे –

- पॉवर ऑफ़ अटॉर्नी
- विल या वसीयतनामा
- अचल संपत्ति की बिक्री या संप्रेषण का अनुबंध
- केंद्र सरकार अधिसूचित दस्तावेज और लेनदेन

भारत में साइबर कानून का इतिहास

सूचना तकनीक अधिनियम 2000 भारतीय सांसद द्वारा पारित एक अधिनियम है जो 17 अक्तूबर, 2000 को पारित हुआ। 27 अक्तूबर, 2009 को एक घोषणा द्वारा इसे संशोधित किया गया।

संयुक्त राष्ट्र संकल्प के बाद भारत ने मई 2000 में **सूचना प्रौद्योगिकी अधिनियम, 2000** पारित कर दिया और 17 अक्तूबर 2000 को अधिसूचना जारी कर इसे लागू कर दिया। सूचना प्रौद्योगिकी अधिनियम, 2000

को **सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008** के माध्यम से काफी संशोधित किया गया है जिसे 23 दिसंबर को भारतीय सांसद के दोनों सदनों द्वारा पारित किया गया था।

साइबर कानून के उद्देश्य

भारत में बनाने के कुछ खास मकसद हैं, जैसे

1. इलेक्ट्रॉनिक दस्तावेजों को कानूनी मान्यता
2. डिजिटल हस्ताक्षर को कानूनी मान्यता
3. अपराध और उल्लंघन
4. साइबर अपराधों के लिए न्याय व्यवस्था
5. सभी ई-लेनदेन (Online Transactions) के लिए कानूनी मान्यता प्रदान करना।
6. ऑनलाइन समझौतों को स्वीकार करने के लिए एक वैध हस्ताक्षर के रूप में डिजिटल हस्ताक्षर को कानूनी मान्यता देना।
7. बैंकों के साथ-साथ अन्य संगठनों द्वारा इलेक्ट्रॉनिक रूप में लेखांकन पुस्तकों को रखने के लिए कानूनी मान्यता देना।
8. ऑनलाइन गोपनीयता की सुरक्षा को बढ़ाना।
9. साइबर अपराधों (Cyber Crimes) को रोकना।

साइबर कानून की प्रभावशीलता

साइबर सुरक्षा महत्वपूर्ण है क्योंकि यह हमारे संवेदनशील डेटा, व्यक्तिगत रूप से पहचान योग्य जानकारी, संरक्षित स्वास्थ्य सूचना, व्यक्तिगत जानकारी, बौद्धिक संपदा और डेटा चोरी होने से बचाना तथा साइबर अपराधियों से डेटा को सुरक्षित रखने का एक अभ्यास और तकनीक है। इस कानून में हैकिंग, क्रेडिट कार्ड फ्रॉड, साइबर स्टॉकिंग, कम्प्यूटर सोर्स कोड के प्रसारण, बौद्धिक संपदा, कॉपीराइटर तथा ट्रेडमार्क से जुड़े अपराध के खिलाफ प्रावधान बनाए गए हैं। साइबर लॉ बनने के बाद इन कानूनी प्रावधानों तथा इनका उपयोग कर साइबर क्राइम पर रोक लगाने तथा ऐसे अपराध की पहचान कर अपराधियों को सजा दिलाने वालों की अति आवश्यकता होती है।

1. **साइबर क्राइम करना भारी पड़ेगा -:** कंप्यूटर, इंटरनेट, डिजिटल डिवाइसेज, वर्ल्ड वाइड वेब आदि के जरिए किए जाने वाले अपराधों के लिए छोटे-मोटे जुर्माने से लेकर उम्र कैद तक की सजा दी जा सकती है। दुनिया भर में रक्षा और जांच एजेंसियां साइबर अपराधों को बहुत गंभीरता से ले रही हैं। ऐसे मामलों में सूचना तकनीक कानून 2000 और सूचना तकनीक (संशोधन) कानून 2008 तो लागू होते ही हैं, मामले के दूसरे पहलुओं को रखते हुए भारतीय दंड संहिता (आईपीसी), कॉपीराइट कानून 1957, कंपनी कानून, सरकारी गोपनीयता कानून और यहां तक कि बिरले मामलों में आतंकवाद निरोधक कानून भी लागू किए जा सकते हैं। कुछ मामलों पर भारत सरकार के आईटी डिपार्टमेंट की तरफ से अलग से जारी किए गए आईटी नियम 2011 भी लागू होते हैं। कानून निर्दोष लोगों को साजिशन की गई शिकायतों से सुरक्षित रखने की भी मुनासिब व्यवस्था की है, लेकिन कंप्यूटर, दूरसंचार और इंटरनेट यूजर को हमेशा सतर्क रहना चाहिए कि उनसे जाने-अनजाने में कोई साइबर क्राइम तो नहीं हो रहा है। तकनीकी जरियों का सुरक्षित इस्तेमाल करने के लिए हमेशा याद रखें कि इलाज से परहेज बेहतर है।

2. **हैकिंग -:** हैकिंग का मतलब है किसी कंप्यूटर, डिवाइस, इंफॉर्मेशन सिस्टम या नेटवर्क में अनधिकृत रूप से घुसपैठ करना और डेटा से छेड़छाड़ करना। यह हैकिंग उस सिस्टम की फिजिकल एक्सेस के

जरिए भी हो सकती है और रिमोट एक्सेस के जरिए भी। जरूरी नहीं कि ऐसी हैकिंग के नतीजे में उस सिस्टम को नुकसान पहुंचा ही हो। अगर कोई नुकसान नहीं भी हुआ है, तो भी घुसपैठ करना साइबर क्राइम के तहत आता है, जिसके लिए सजा का प्रावधान है।

कानून - आईटी (संशोधन) एक्ट 2008 की धारा 43 (ए), धारा 66 - आईपीसी की धारा 379 और 406 के तहत कार्रवाई मुमकिन सजा: अपराध साबित होने पर तीन साल तक की जेल और/या पांच लाख रुपये तक जुर्माना।

3. **डेटा की चोरी -:** किसी और व्यक्ति, संगठन वगैरह के किसी भी तकनीकी सिस्टम से निजी या गोपनीय डेटा (सूचनाओं) की चोरी। अगर किसी संगठन के अंदरूनी डेटा तक आपकी आधिकारिक पहुंच है, लेकिन अपनी जायज पहुंच का इस्तेमाल आप उस संगठन की इजाजत के बिना, उसके नाजायज दुरुपयोग की मंशा से करते हैं, तो वह भी इसके दायरे में आएगा। कॉल सेंटरों, दूसरों की जानकारी रखने वाले संगठनों आदि में भी लोगों के निजी डेटा की चोरी के मामले सामने आते रहे हैं।

   कानून - आईटी (संशोधन) कानून 2008 की धारा 43 (बी), धारा 66 (ई), 67 (सी) - आईपीसी की धारा 379, 405, 420 - कॉपीराइट कानून सजा: अपराध की गंभीरता के हिसाब से तीन साल तक की जेल और/या दो लाख रुपये तक जुर्माना।

4. **वायरस-स्पाईवेयर फैलाना -:** कंप्यूटर में आए वायरस और स्पाईवेयर के सफाए पर लोग ध्यान नहीं देते। उनके कंप्यूटर से होते हुए ये वायरस दूसरों तक पहुंच जाते हैं। हैकिंग, डाउनलोड, कंपनियों के अंदरूनी नेटवर्क, वाई-फाई कनेक्शनों और असुरक्षित फ्लैश ड्राइव, सीडी के जरिए भी वायरस फैलते हैं। वायरस बनाने वाले अपराधियों की पूरी इंडस्ट्री है जिनके खिलाफ कड़ी कार्रवाई होती है। वैसे आम लोग भी कानून के दायरे में आ सकते हैं, अगर उनकी लापरवाही से किसी के सिस्टम में खतरनाक वायरस पहुंच जाए और बड़ा नुकसान कर दें।

   कानून - आईटी (संशोधन) एक्ट 2008 की धारा 43 (सी), धारा 66
   - आईपीसी की धारा 268
   - देश की सुरक्षा को खतरा पहुंचाने के लिए फैलाए गए वायरसों पर साइबर

आतंकवाद से जुड़ी धारा 66 (एफ) भी लागू (गैर-जमानती)। सजा : साइबर-वॉर और साइबर आतंकवाद से जुड़े मामलों में उम्र कैद। दूसरे मामलों में तीन साल तक की जेल और/या जुर्माना।

इन सभी मामलों मे कड़ी सज़ा का प्रावधान रखा गया है जिससे साइबर कानून की प्रभावशीलता बरकरार रहे और अपराधियों में एक डर बना रहे और साइबर अपराध की संभावनाएं कम हो।

उपसंहार

हमारे देश ने जैसे कि हर क्षेत्र में सफलता प्राप्त की है उसी तरह साइबर कानून के लागू होने के बाद साइबर अपराधों को काबू में किया गया है। ग्लोबलाइज़ेशन और प्रौद्योगिकरण के इस दौर में जहां हर क्षेत्र मे नयी-नयी उचाइयां प्राप्त हो रही है वही साइबर अपराध की चुनौतियों का सामना करना पड़ रहा है। ऐसी चुनौतियों से निपटने एवं अपराधियों को सजा दिलाने के लिये साइबर कानून प्रभावशाली है।

*****

अपराजिता गुप्ता

पदनाम:- प्रबंधक
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 8511290210
ई-मेल:- apra.gupta90@gmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

कंप्यूटर के अविष्कार ने मानव जीवन को अत्यंत सरल बना दिया है। प्राचीन समय में जिस कार्य को करने में मानव श्रम तथा समय लगता था, कंप्यूटर द्वारा आज वही कार्य मिनटों में करना संभव है। किन्तु प्रत्येक सकारात्मक पहल के साथ नकारात्मक कारक भी जन्म लेते हैं जो नवोन्मेषी तंत्रों के सफल कार्यान्वयन में बाधा उत्पन्न करते हैं। एक ओर तकनीकी जगत में जहां कम्प्यूटरीकरण विकसित हुआ, वहीं साइबर अपराध जैसे नकारात्मक कारक भी उत्पन्न हुए जिसने साइबर कानून का गठन करने तथा इसे प्रबल बनाने की आवश्यकता का बोध कराया।

साइबर अपराध ऐसा दुष्कर्म है जो इलेक्ट्रॉनिक या सूचना प्रौद्योगिकी तंत्रों द्वारा किसी उपकरण या इंटरनेट के माध्यम से किया जाता है। साइबर अपराध एक परिभाषा या एक प्रकार तक सीमित नहीं है। तकनीकी नवोन्मेषिता के चलते साइबर आपराधिक तंत्रों में भी नवोन्मेषिता आई है। इसी के चलते वर्तमान समय में साइबर कानून की प्रभावशीलता व उनमें सुधार होने की महत्ता उजागर हुई है।

साइबर अपराध- एक अंतर्दृष्टि

साइबर अपराध के अनेक विकल्प विद्यमान हैं। साइबर अपराध का सर्वप्रथम किस्सा अमरीका में सन् 1969 में घटित होना माना जाता है। वर्तमान में साइबर अपराधों को 4 श्रेणियों में विभाजित किया जा सकता है-

1. वैयक्तिक स्तर पर साइबर अपराध

जब साइबर अपराध किसी व्यक्ति के खिलाफ घटित हो, वह वैयक्तिक स्तर पर साइबर अपराध की श्रेणी में आता है। यह निम्न गतिविधियों द्वारा किया जा सकता है:

- **ई-मेल स्पूफिंग** – इस तंत्र में जाली ई-मेल हेडर का उपयोग किया जाता है। ई-मेल देखने से ऐसा प्रतीत होता है जैसे वह यथार्थ हो किन्तु वास्तव में वह जाली ई-मेल होता है।
- **स्पैमिंग** – ई-मेल स्पैम को जंक मेल भी कहा जाता है। इस तंत्र में अनेक व्यक्तियों को ई-मेल द्वारा किसी जाली पॉलिसी में निवेश या लाटरी जैसे आकर्षक स्कीम का लोभ दिया जाता है।
- **फिशिंग** – इस तंत्र के अंतर्गत अपराधी व्यक्तियों की गोपनीय सूचना जैसे पासवर्ड, पिन आदि प्राप्त करने की चेष्टा करता है।

2. संपत्ति आधारित साइबर अपराध

इस प्रकार के आपराधिक तंत्रों में कंप्यूटर, सॉफ्टवेयर को हानि पहुंचाई जाती है। सॉफ्टवेयर की जालसाजी, सत्त्वाधिकार उल्लंघन, ट्रेडमार्क उल्लंघन आदि माध्यमों से यह घटित होता है।

3. संस्थागत स्तर पर साइबर अपराध

इस तंत्र में संस्थाओं के आतंरिक डेटा को हानि पहुंचाई जाती है। यह निम्न गतिविधियों द्वारा किया जाता है:

- **सर्वर हाईजैक** - संस्था के आतंरिक सर्वर को हैक कर डेटा मिटाना।
- **डॉस अटैक** – इसमें अपराधी सर्वर में अनधिकृत डेटा द्वारा संस्था के कम्प्यूटरों की गति को धीमा कर देता है।
- **ई-मेल बॉम्बिंग** – इसमें अपराधी अनेक ई-मेल भेजकर मेल बॉक्स भर देता है जिससे मेल सर्वर बाधित हो जाता है।
- **सलामी अटैक** – इस तंत्र में अपराधी ऑनलाइन तकनीक के माध्यम से ग्राहकों के बैंक खाते/ कार्ड आदि की सूचना प्राप्त करता है। तत्पश्चात खातों से थोड़ी-थोड़ी राशि अंतरित कर लाभ अर्जित करता है। चूंकि राशि का मूल्य कम होता है, अतः अनेक बार ग्राहकों को अंतरण का बोध भी नहीं होता।

4. सामाजिक स्तर पर साइबर अपराध

जब साइबर अपराध का दुष्प्रभाव समस्त समाज पर होता है, वह सामाजिक स्तर पर साइबर अपराध की श्रेणी में आता है। इसमें निम्न गतिविधियां सम्मिलित हैं:

- **जालसाज़ी** – इसमें जाली दस्तावेज, हस्ताक्षर, मुद्रा, मुहर आदि के माध्यम से साइबर ठगी को अंजाम दिया जाता है।
- **वेब जैकिंग** – इसमें अपराधी जाली वेबसाइट निर्मित करता है। वेबसाइट खोलने पर उसमें भिन्न प्रकार के लिंक जनरेट होते हैं। लिंक खुलते ही अपराधी को दूसरे कंप्यूटर को परिचालित करने का साधन प्राप्त हो जाता है जिससे अपराधी उस कंप्यूटर से गोपनीय सूचना प्राप्त कर लेता है।

भारत में साइबर कानून

कंप्यूटर के बढ़ते उपयोग, आवश्यकता और साथ ही साइबर जगत में बढ़ते अपराधों की रोकथाम हेतु कानूनी प्रणाली का गठन करना महत्त्वपूर्ण था। जैसे मानवकृत अनेक अपराधों को रोकने हेतु दीवानी व फौजदारी न्यायालय बनाए गए हैं, उसी प्रकार साइबर आधारित अपराधों के लिए साइबर कानून व साइबर सेल गठित किए गए हैं।

साइबर कानून के तंत्र

1. सूचना प्रौद्योगिकी अधिनियम, 2000

यह अधिनियम साइबर अपराध, ई-कॉमर्स व डिजिटल अपराध से जूझने हेतु महत्त्वपूर्ण है। इस अधिनियम के अंतर्गत इलेक्ट्रॉनिक साधन अर्थात् कागज़-आधारित तंत्रों के वैकल्पिक साधनों द्वारा किए गए डेटा के अंतरण को कानूनी मान्यता प्रदान की जाती है। इसमें दण्डात्मक प्रणाली का भी प्रावधान है।

इस अधिनियम के अंतर्गत निम्न धाराएं अहम् हैं:

धारा	अपराध	दण्ड
धारा 65	कंप्यूटर दस्तावेजों के साथ छेड़छाड़	3 वर्ष तक का कारावास या रु. 2 लाख का जुर्माना या दोनों
धारा 66	कंप्यूटर प्रणाली को हैक करना या डेटा	3 वर्ष तक का कारावास या रु. 2 लाख का

	के साथ छेड़छाड़ करना	जुर्माना या दोनों
धारा 66ए	**किसी संचार सेवा द्वारा आपत्तिजनक संदेश भेजना**	3 वर्ष तक कारावास के साथ जुर्माना
धारा 66बी	**बेईमान तरीके से चोरी के कंप्यूटर व संचार उपकरण प्राप्त करना**	3 वर्ष तक का कारावास या रु. 1 लाख का जुर्माना या दोनों
धारा 66सी	**पहचान की चोरी**	3 वर्ष तक का कारावास या रु. 1 लाख का जुर्माना या दोनों
धारा 66डी	**कंप्यूटर संसाधनों के उपयोग द्वारा प्रतिरुपण से धोखाधड़ी**	3 वर्ष तक का कारावास या रु. 1 लाख का जुर्माना या दोनों
धारा 66ई	**गोपनीयता का उल्लंघन**	3 वर्ष तक का कारावास या रु. 2 लाख का जुर्माना या दोनों
धारा 67	**इलेक्ट्रॉनिक माध्यम द्वारा अश्लील सामग्री प्रसारित या प्रकाशित करना**	पहली बार दोषी पाए जाने पर 5 वर्ष तक कारावास तथा रु. 1 लाख तक जुर्माना। दूसरी बार दोषी पाए जाने पर कारावास की अवधि 10 वर्ष तक तथा रु. 2 लाख तक जुर्माना।
धारा 67ए	**इलेक्ट्रॉनिक माध्यम द्वारा ऐसी सामग्री का प्रसारण या प्रकाशन जिसमें यौन सामग्री या कृत्य शामिल हो**	प्रथम बार दोषी पाए जाने पर 5 वर्ष तक कारावास तथा रु. 10 लाख तक जुर्माना। दूसरी बार दोषी पाए जाने पर कारावास की अवधि 7 वर्ष तक तथा रु. 20 लाख तक जुर्माना।
धारा 67बी	**इलेक्ट्रॉनिक माध्यम द्वारा ऐसी सामग्री का प्रसारण या प्रकाशन जिसमें बच्चों को यौन सामग्री या कृत्यों में दर्शाया गया हो**	प्रथम बार दोषी पाए जाने पर 5 वर्ष तक कारावास तथा रु. 10 लाख तक जुर्माना। दूसरी बार दोषी पाए जाने पर कारावास की अवधि 7 वर्ष तक तथा रु. 10 लाख तक जुर्माना।
धारा 67सी	**मध्यस्थ द्वारा सूचना का प्रतिधारण और संरक्षण**	मध्यस्थ या बिचौलिया संस्थाओं को केंद्र सरकार द्वारा निर्धारित अवधि तक सूचना को प्रतिधारित व सुरक्षित रखना होता है। उल्लंघन होने पर 3 वर्ष तक कारावास के साथ जुर्माने का प्रावधान है।

उपरोक्त धाराओं के अतिरिक्त इस अधिनियम में धारा 43, धारा 69 , धारा 69 ए, धारा 69बी, धारा 70, धारा 71, धारा 72, धारा 73, धारा 74, धारा 75, धारा 77, धारा 77 A, धारा 85 भी महत्त्वपूर्ण हैं।

साइबर आतंक

साइबर आतंक के निम्न पहलू हैं –

- ❖ यदि कोई अपराधी इरादतन तरीके से जनता में अखंडता, एकता, संप्रभुता व सुरक्षात्मक प्रणाली को निम्न गतिविधियों द्वारा चुनौती दे-
  - व्यक्तियों को कंप्यूटर का उपयोग करने से बाधित करना
  - किसी कंप्यूटर को अनधिकृत रूप से संचालित करना

- किसी कंप्यूटर में दूषित पदार्थ जैसे ट्रोजन या वायरस द्वारा किसी व्यक्ति या संपत्ति को हानि पहुंचाना

❖ जानबूझकर किसी निजी कंप्यूटर या डिजिटल संसाधनों का अनधिकृत रूप से परिचालित करने का अधिकार प्राप्त करना, ऐसी सूचना जो राष्ट्रीय या अंतर्राष्ट्रीय स्तर की गोपनीय सूचना हो तथा जिसके अनधिकृत उपयोग से राष्ट्रीय स्तर पर हानि हो।

ऐसा करने पर अपराधी को आजीवन कारावास के दण्ड का प्रावधान है।

साइबर कानून को प्रभावशाली बनाने की आवश्यकता

भारत में साइबर अपराध की रोकथाम हेतु साइबर कानून तो गठित हुआ है किन्तु साइबर प्रणाली को अपराध मुक्त बनाने में अभी लंबा सफ़र तय करना है। निम्न तथ्यों द्वारा साइबर कानून में सुधार लाने तथा उन्हें प्रभावशाली बनाने की आवश्यकता का बोध होता है:

1. **जागरूकता**– साइबर अपराध के पीड़ितों को साइबर कानूनी तंत्र का ज्ञान नहीं होता। अनेक मामलों में शिकायत दर्ज होने पर पुलिस कर्मियों ने भी लापरवाही दिखाई है जिससे अपराधी की पहचान करने में विलंब हुआ है। ऐसे में जनता से लेकर सभी हितधारक- न्यायिक अधिकारियों तथा कानूनी पेशेवरों को साइबर कानून, निवारक एवं दण्डात्मक प्रणाली का उचित ज्ञान होना आवश्यक है।
2. **क्षेत्राधिकार** – यह एक महत्त्वपूर्ण पहलू है जो सूचना प्रौद्योगिकी अधिनियम या सूचना प्रौद्योगिकी अपीलीय अधिनियम में स्पष्ट रूप से उल्लिखित नहीं है। उदाहरणस्वरूप यदि किसी अंतर्राष्ट्रीय कंपनी जिसकी विश्व भर में शाखाएं हैं तथा किसी एक राष्ट्र के कार्यस्थल पर साइबर अपराध घटित हुआ हो तो उसकी सूचना किस पुलिस स्टेशन में दर्ज की जानी चाहिए- जहां अपराध हुआ है या जहां संस्था का कॉर्पोरेट कार्यालय है? किस देश का साइबर कानून घटना की जांच करने में लागू होगा?
3. **प्रशिक्षण का अभाव** –साइबर अपराध वायरस, हैकिंग, फिशिंग, पिन की चोरी, पहचान की चोरी इत्यादि माध्यमों द्वारा किया जाता है। ऐसे में कानूनी पेशेवरों को इन अपराधों की जांच करने हेतु उचित प्रशिक्षण देना आवश्यक है जिससे अपराध होने से पूर्व ही किसी बाहरी कारक जैसे वायरस, मैलवेयर, हैक आदि का सामयिक ज्ञान हो सके तथा अपराध होने से रोका जा सके।
4. भारत में कुछ ऐसे साइबर अपराध हुए हैं जिसने साइबर प्रणाली में विद्यमान समस्याओं पर प्रकाश डाला है तथा साइबर कानून में संशोधन करने पर विवश किया है। इनमें से प्रमुख घटनाएं निम्नलिखित हैं:

I. बैंक एन.एस.पी केस

इस केस में बैंक में कार्यरत कर्मी ने अपनी पत्नी से बातचीत करने हेतु संस्था की ई-मेल का उपयोग किया। तलाक के पश्चात् उसकी पत्नी ने संस्था की जाली ई-मेल आईडी के माध्यम से लड़के के विदेशी ग्राहकों को मेल भेजे। इससे संस्था को व्यापारिक एवं प्रतिष्ठात्मक हानि हुई तथा न्यायालय में बैंक की जाली ई-मेल आईडी के उपयोग के कारण संस्था को दोषी माना गया।

II. संसद हमला – 2001

इस हमले ने साइबर प्रणाली में व्याप्त छिद्रों को उजागर किया। इस हमले में एक लैपटॉप बरामद किया गया जिसमें गृह मंत्रालय के जाली लोगो, जाली पहचान पत्र आदि पाए गए जिसके माध्यम से संसद में प्रवेश किया गया।

इसी प्रकार मुंबई 26/11 हमलों में सैटलाइट फोन का उपयोग किया गया जो सुरक्षा प्रणाली की रडार से बाहर थे तथा जिन्हें ट्रैक करना असंभव था।

III. ई-कॉमर्स में अपराध के नवीन मामले देखे गए हैं। जाली पहचान के माध्यम से ई-कॉमर्स वेबसाइट से सामान आर्डर करना, पेमेंट ऐप द्वारा ग्राहकों के बैंक/कार्ड की जानकारी प्राप्त कर खाते से राशि अंतरित करना; ऐसे अनेक विकल्पों द्वारा ई-कॉमर्स क्षेत्र साइबर अपराध का शिकार हुआ है।

वर्ष 2021 में साइबर अपराध के मामलों की रिपोर्टिंग में 11.8% का इजाफा हुआ है। यह आंकड़ा पिछले वर्ष के 44735 मामलों की तुलना में 50035 (सितम्बर 2021 तक) दर्ज किया गया है। बढ़ते किस्से तथा कमज़ोर कानूनी तंत्र से कानूनी व्यवस्था में सुधार की महत्ता उजागर होती है।

उपसंहार

साइबर सुरक्षा राष्ट्रीय सुरक्षा के पहलू से भी महत्त्वपूर्ण है। भारतीय अर्थव्यवस्था में बैंकिंग क्षेत्र की अहम् भूमिका है और इसी क्षेत्र में साइबर अपराधों में सर्वाधिक वृद्धि हो रही है। बैंकों को हुई वित्तीय हानि का प्रभाव अर्थव्यवस्था पर भी पड़ता है। एक ओर जहां हम नकदी-रहित अर्थव्यवस्था का स्वप्न देख रहे हैं, वहीं साइबर अपराध जैसे कारक उस स्वप्न की पूर्ति में बाधक बन रहे हैं।

सभी राज्यों ने साइबर अपराध की रिपोर्टिंग हेतु पोर्टल निर्मित किया है जिसमें साइबर अपराध की शिकायत दर्ज की जा सकती है। गृह मंत्रालय द्वारा भी 'राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल' सृजित की गई है। इस पोर्टल पर शिकायत दर्ज करने के उपरांत एफ़आईआर के पश्चात् वह निर्धारित राज्यों के साइबर सेल को भेजी जाती है। अब तक इस पोर्टल पर 317439 साइबर अपराध के मामले दर्ज हुए हैं।

साइबर सुरक्षा हेतु कानूनी प्रणाली गठित करना पर्याप्त नहीं है। इसे प्रभावशाली बनाना भी अति आवश्यक है। समय के साथ-साथ जिस प्रकार आपराधिक तंत्रों में नवीनीकरण हो रहा है, उससे कानूनी तंत्रों में भी सुधार लाने की आवश्यकता है। कानूनी प्रणाली प्रबल व प्रभावी होगी तभी साइबर अपराधी ऐसे जुर्म करने का दुस्साहस नहीं करेंगे और साइबर जगत सुरक्षित बनेगा।

*****

अमरेन्द्र कुमार अमर

पदनाम:- प्रबंधक
संस्था का नाम:- बैंक ऑफ इंडिया
मोबाइल नं. :- 9673154647
ई-मेल:- amarbajigar91@gmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

इतिहास के हर आविष्कार की तरह इंटरनेट भी फायदे और नुकसान लेकर आया है। संस्थापकों को कब ही पता था कि किसी दिन उनकी रचना का उपयोग किसी को नुकसान पहुंचाने और नष्ट करने के लिए किया जाएगा। आज साइबर स्पेस में कई तरह की खतरनाक चीजें हो रही हैं। आपराधिक इरादे से वेब का उपयोग करना साइबर अपराध के रूप में जाना जाता है।

"साइबर अपराध" शब्द को भारत में किसी भी कानून के तहत परिभाषित नहीं किया गया है। लेकिन व्यापक अर्थ में इसका मतलब साइबर स्पेस में आपराधिक इरादे से की गई कोई भी गतिविधि हो सकती है, जहां कंप्यूटर एक उपकरण होने के साथ-साथ माध्यम भी हो सकता है। कभी-कभी ये अपराध मुनाफा कमाने के लिए किए जाते हैं, कभी-कभी यह सॉफ्टवेयर को नुकसान पहुंचाने के लिए किया जाता है और कभी-कभी यह मैलवेयर को एक ऐसे सिस्टम में भेजने के लिए किया जाता है जो अन्य मशीनों में प्रवेश करता है और कुछ ही समय में पूरे नेटवर्क में विस्तारित हो जाता है। साइबर अपराध में चोरी, धोखाधड़ी, शरारत, जालसाजी या मानहानि जैसी पारंपरिक आपराधिक गतिविधियां शामिल हो सकती हैं जो भारतीय दंड संहिता, 1860 के अधीन हैं और नए युग के अपराध सूचना प्रौद्योगिकी अधिनियम, 2000 के अधीन हैं।

साइबर अपराध अवैध कार्य है जहां कंप्यूटर का उपयोग या तो एक उपकरण या लक्ष्य या दोनों के रूप में किया जाता है। इलेक्ट्रॉनिक कॉमर्स (ई-कॉमर्स) और ऑनलाइन शेयर ट्रेडिंग में भारी वृद्धि के कारण साइबर अपराध की घटनाओं में असामान्य वृद्धि हुई है। हालांकि, डिवाइस को कंप्यूटर वायरस से संक्रमित होने से डेटा और कंप्यूटर नेटवर्क जैसे फायरवॉल, एंटीवायरस सॉफ्टवेयर और अन्य तकनीकी समाधानों से बचाने के लिए सिस्टम है, लेकिन भारत में मूल्यवान डेटा की सुरक्षा के लिए इन तकनीकों के प्रभावी उपयोग की दिशा में प्रयास किए जाने चाहिए।

साइबर अपराध कानून वह कानून है जो साइबर स्पेस को नियंत्रित करता है। साइबर स्पेस एक बहुत व्यापक शब्द है और इसमें कंप्यूटर, नेटवर्क, सॉफ्टवेयर और डेटा स्टोरेज डिवाइस जैसे हार्ड डिस्क, यूएसबी डिस्क, इंटरनेट, वेबसाइट, ई-मेल और यहां तक कि इलेक्ट्रॉनिक डिवाइस जैसे सेल फोन, एटीएम मशीन शामिल हैं। साइबर स्पेस पर व्यक्तियों और संगठनों की बढ़ती निर्भरता के परिणामस्वरूप कई साइबर अपराध हुए हैं।

भारत में साइबर कानून का विकास

प्रौद्योगिकी के उपयोग पर निर्भरता में वृद्धि के साथ, साइबर कानून की नितांत आवश्यकता थी। चूंकि हर सिक्के के दो पहलू होते हैं, इसलिए प्रौद्योगिकी पर निर्भरता के अपने फायदे और नुकसान हैं। 21वीं सदी के उदय ने सूचना प्रौद्योगिकी अधिनियम, 2000 (जिसे आईटी अधिनियम के रूप में जाना जाता है) के साथ भारत में साइबर कानून के विकास को चिह्नित किया। पहली बार साइबर अपराध वर्ष 1820 में दर्ज किया गया था।

भारत में साइबर कानून:-

"साइबर स्पेस में होने वाली प्रत्येक क्रिया और प्रतिक्रिया के कुछ कानूनी और साइबर कानूनी दृष्टिकोण होते हैं" । साइबर स्पेस में होने वाले कानूनी मुद्दों को संबोधित करने के लिए "साइबर लॉ" शब्द का उपयोग किया जाता है। यह हर दिन वेब पर मानवता द्वारा पेश किए गए ऐसे मुद्दों और चुनौतियों से निपटने और हल करने के लिए विभिन्न कानूनों का एकीकरण है।

चूंकि साइबर अपराध एक ऐसा क्षेत्र है जो अभी भी विकसित हो रहा है, अत: इससे निपटने के लिए आज तक दुनिया में कहीं भी कोई व्यापक कानून नहीं है। लेकिन भारत सरकार के पास इंटरनेट उपयोगकर्ता के अधिकारों का उल्लंघन करने वाली वेब पर दुर्भावनापूर्ण गतिविधियों को नियंत्रित करने के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 लागू है । कभी-कभी, कोई यह देख सकता है कि आईपीसी और आईटी अधिनियम के प्रावधान हैं जो ऐसी गतिविधियों को दंडित करते हैं जो एक-दूसरे को ओवरलैप करते हैं।

भारत में सूचना प्रौद्योगिकी अधिनियम का उद्देश्य इस प्रकार है:-

- सभी ई-लेनदेन के लिए कानूनी मान्यता प्रदान करना।
- ऑनलाइन समझौतों को स्वीकार करने के लिए वैध हस्ताक्षर के रूप में डिजिटल हस्ताक्षर को कानूनी मान्यता देना।
- बैंकरों के साथ-साथ अन्य संगठनों द्वारा लेखांकन पुस्तकों को इलेक्ट्रॉनिक रूप में रखने को कानूनी मान्यता प्रदान करना।
- ऑनलाइन गोपनीयता की सुरक्षा और साइबर अपराधों को रोकना।

निम्नलिखित अधिनियम, नियम और विनियम साइबर कानूनों के अंतर्गत शामिल हैं:-

- सूचना प्रौद्योगिकी अधिनियम, 2000
- सूचना प्रौद्योगिकी (प्रमाणन प्राधिकारी) नियम, 2000
- सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) नियम, 2004
- सूचना प्रौद्योगिकी (प्रमाणन प्राधिकारी) विनियम, 2001

सूचना प्रौद्योगिकी अधिनियम, 2000 के प्रमुख उद्देश्य इलेक्ट्रॉनिक संचार के माध्यम से किए गए लेनदेन के लिए कानूनी मान्यता प्रदान करना है, इसे "इलेक्ट्रॉनिक कॉमर्स" भी कहा जाता है और इसमें संचार एवं सूचना भंडारण के कागज-आधारित तरीकों के विकल्पों का उपयोग शामिल है । सूचना प्रौद्योगिकी अधिनियम, 2000 को सक्षम अधिनियम के रूप में भी माना जाता है जो इलेक्ट्रॉनिक रिकॉर्ड और डिजिटल हस्ताक्षर की कानूनी प्रणाली की अनुमति देता है।

प्रभावशीलता

साइबर कानून उनकी प्रभावशीलता में संदिग्ध हैं। इस तथ्य के बावजूद कि संसद ने उपयोगकर्ता की जानकारी नियंत्रित करने और परिभाषित करने के लिए एक ठोस कानूनी ढांचा प्रदान करने का प्रयास किया, जिसे साइबर स्पेस में टाला जा सकता है, वास्तव में, संसद के प्रयास प्रशंसनीय हैं, क्योंकि इसने बड़ी संख्या में कानूनों को संशोधित किया है। आईटी अधिनियम के उद्देश्य आईटी अधिनियम, 2000 उभरते साइबर खतरों के उपचार में चूक करता है । कानूनों में विविधता की कमी के अलावा, शासी निकाय द्वारा मौजूदा कानूनों का कमजोर कार्यान्वयन किया गया है। कानूनों को एक प्रौद्योगिकी तटस्थ तरीके से तैयार करने की आवश्यकता है, जिसका दायरा कम से कम सभी ज्ञात साइबर मुद्दों और उनसे उपजी हैं। यहां तक कि जो मामले पंजीकृत होते हैं, उनमें दोषसिद्धि की दर कम होती है, जो भारत में साइबर सुरक्षा कानूनों की प्रभावशीलता में बाधा उत्पन्न करती है।

इस अधिनियम के तहत दी जाने वाली सजा की मात्रा अपराधियों पर शिथिल प्रतीत होती है। इसे संशोधित करने की आवश्यकता है अन्यथा इस अधिनियम का मूल उद्देश्य ही विफल हो जाएगा। आईटी अधिनियम का संकीर्ण साइबर स्पेस मुद्दा स्पेक्ट्रम हर दिन साइबर खतरों में अप्रत्याशित वृद्धि की सुविधा प्रदान करता है। कई मुद्दे जो आज इंटरनेट को प्रभावित कर रहे हैं, उन्हें अधिनियम के तहत पर्याप्त कवरेज प्रदान नहीं किया गया है। आईटी अधिनियम में यात्रा करने के लिए एक लंबा रास्ता बचा है और भारत के साइबर स्पेस को सुरक्षित करने की क्षमता को अपने भीतर शामिल करने के लिए व्यापक संशोधनों से गुजरना पड़ता है।

कानून के लिए सुधार

भारत में साइबर अपराध से संबंधित मामलों के लिए आईटी एक्ट 2000 को बनाया गया है, जिसके माध्यम से साइबर अपराधों को नियंत्रित किया जाता है आईटी एक्ट 2000 ग्लोबल कन्वेंशन जिसे भारत द्वारा व्यापार संबंधित विषय के तहत संयुक्त राष्ट्र द्वारा ट्रेड लॉ कमीशन के अनुसार बनाया गया था। वर्तमान में उत्पन्न हो रहे नए साइबर अपराधों के अनुसार कानून में आवश्यक संशोधन करना अनिवार्य हो गया है, इसलिए ऐसा कानून बनाया जाना चाहिए जो साइबर अपराधों को रोकने के लिए ही सहायक हो और जिसमें पुलिस उस निकाय की जांच कर रही हो जो साइबर क्राइम जांच में शामिल है। संस्थाओं को अधिकार क्षेत्र और अन्य आवश्यक शक्तियां दी जानी चाहिए ताकि साइबर अपराधों को कम किया जा सके या रोका जा सके और अन्य आवश्यक तरीकों को जोड़ा जाना चाहिए जो वर्तमान और भविष्य के साइबर-अपराधों से निपटने में मददगार साबित हों।

भारत को अपने कंप्यूटिंग वातावरण और इंटरनेट ऑफ थिंग्स को वर्तमान उपकरणों, पैच, अपडेट और सर्वोत्तम ज्ञात विधियों के साथ समयबद्ध तरीके से सुरक्षित करने की आवश्यकता है। भारत सरकार के लिए समय की मांग है कि बैंकों और वित्तीय संस्थानों की सुरक्षा के लिए कड़े साइबर सुरक्षा मानकों को स्थापित करते हुए साइबर सुरक्षा, डेटा अखंडता और डेटा सुरक्षा क्षेत्रों में मुख्य कौशल विकसित किया जाए। साइबर हमलों को रोकने के लिए रीयल-टाइम इंटेलिजेंस की आवश्यकता है।

न्यायाधीशों की प्रासंगिक और सम्यक व्याख्या के बावजूद भारत के मौजूदा कानूनों की व्याख्या साइबर स्पेस में विभिन्न गतिविधियों से संबंधित सभी पहलुओं को शामिल करने के लिए उभरते साइबर स्पेस के आलोक में नहीं की जा सकती है। निर्णय के व्यावहारिक ज्ञान और अनुभव में पाया गया कि यह बड़े नुकसान के बिना नहीं होगा, अगर मौजूदा कानूनों की व्याख्या उभरते साइबर स्पेस के परिदृश्य में की जानी है, तो नए साइबर कानूनों को लागू किए बिना हमें मौजूदा कानूनों में संशोधन करने की आवश्यकता है।

उन गतिविधियों के रूप में जिन्हें साइबर स्पेस में प्रतिबंध या कानूनी वैधता दिए जाने की आवश्यकता है। उदाहरण के लिए हम अधिकांश समय इंटरनेट का उपयोग सूचना तक पहुंचने के लिए करते हैं लेकिन फिर भी आज तक हमारे देश में ई-मेल कानून ही नहीं रहा है जहां अधिकांश लोग इसका उपयोग कई व्यावसायिक उद्देश्यों और अन्य उद्देश्यों के लिए करते हैं, लेकिन यह कानूनी नहीं है। इसलिए सबसे पहले ई-मेल को वैध किया जाना चाहिए क्योंकि कई धोखाधड़ी, मेल और खाते हैक किए गए हैं। यहां तक कि अदालतें और कई अन्य प्रतिष्ठित संस्थान भी अपने संचार के लिए ई-मेल का उपयोग करते हैं। ऐसे में साइबर कानून को समय की आवश्यकता के रूप में संशोधित करने की आवश्यकता उत्पन्न हो गई है। भारत में हाल ही में कई साइबर अपराध किए गए हैं और कई लोगों के लिए खतरा हैं जहां हमें इस पहलू पर गंभीरता से विचार करने की आवश्यकता है।

*****

अश्वनी कुमार

पदनाम:- उप प्रबंधक
संस्था का नाम:- दि ओरिएंटल इंश्योरेंश कंपनी लिमिटेड
मोबाइल नं. :- 9844412640
ई-मेल:- ashwani.kumar@orientalinsurance.co.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

प्रस्तावना: साइबर क्राइम आज एक ऐसा विषय है जिससे कोई भी अछूता नहीं है। आज प्रत्येक व्यक्ति नेट यूजर है और अपना सारा कार्य साइबर के माध्यम से ही करता है। इसमें कोई संदेह नहीं कि किसी भी कार्य के दो पक्ष होते हैं एक अच्छा पक्ष तो दूसरा बुरा। दूसरे पक्ष को ध्यान में रखते हुए जिसको हम क्राइम कहते हैं, के लिए नियमों की आवश्कता पड़ती है। क्राइम आज से नहीं बल्कि बहुत पहले से हैं। यदि हम पूर्व में देखें जब टेलीफोन का जमाना था और कुछ लोग फ्री कॉल करने की वजह से उसमें गड़बड़ी करते थे वह भी क्राइम की श्रेणी में आता है। उसी प्रकार साइबर क्राइम इंटरनेट से संबंधित है क्योंकि आज इंटरनेट से ही सारे कार्य किए जा रहे हैं इसके लिए बस एक कंप्यूटर चाहिए और आज तो मोबाइल बैंकिग की भी सुविधा है। आप अपने सभी कार्य जैसे पैसे का लेन-देन, पेपर भेजना इत्यादि बड़ी आसानी से ऑनलाइन कर सकते हैं। अत: तेजी से बढ़ते हुए साइबर अपराध की रोकथाम और इसके नियंत्रण के लिए सरकार ने कई नियम बनाए हैं।

भारत में साइबर कानून : भारत में साइबर अपराध से निपटने के लिए भारतीय संसद द्वारा साइबर कानून अधिनियम 2000 पास किया गया है। यह कानून वाणिज्य लेन-देन हेतु बनाया गया था। हालांकि, वर्ष 2004 से 2005 तक व्यापारियों पर इसका नकारात्मक प्रभाव पड़ने लगा और व्यापारियों का इससे काफी नुकसान भी हुआ। वर्ष 2004 के बाद क्रेडिट कार्ड की शुरुआत हुई और काफी लोगों ने इसका प्रयोग किया और सामान्यत: आज भी कर रहे हैं। हालांकि, उस समय कार्ड की हैकिंग से लोगों का काफी नुकसान भी हुआ था। वर्ष 2010 में "ऑपरेशन आरोरा" नामक एक बड़ा साइबर हमला हुआ तथा सभी साइटों पर साइबर हमलावारों की मारामारी थी। भारत सरकार द्वारा इस पर नियंत्रण करने हेतु सूचना एवं प्रौद्योगिकी अधिनियम 2000 बनाया गया था। यह कानून खासतौर पर वाणिज्यिक लेन-देन एवं महत्वपूर्ण दस्तावेज भण्डारण हेतु बनाया गया था ताकि किसी भी प्रकार की हानि होने पर कानूनी कार्रवाई की जा सके और धोखा देने वाले को सजा मिल सके तथा लेन-देन करने वाले के हानि की क्षतिपूर्ति की जा सके।

भारत में साइबर कानूनों की प्रभावशीलता: आज हम गोपनीयता की चिंता के बारे में बात करते हैं। साइबर अपराध उस अपराध को संदर्भित करता है जिसमें एक कंप्यूटर या नेटवर्क सिस्टम द्वारा अपराध किया जाता है या अपराध करने के लिए किसी उपकरण का प्रयोग किया जाता है। साइबर-अपराधी की व्यक्तिगत जानकारी, व्यापार रहस्य या किसी अन्य दुर्भावनापूर्ण उद्देश्यों को प्राप्त करने के लिए किसी भी माध्यम का उपयोग कर सकते हैं। बुनियादी प्रश्न यह है कि साइबर हमले होने पर क्या करना चाहिए? इसमें वित्तीय धोखाधड़ी, साइबर क्राइम या कोई अन्य साइबर अपराध शामिल हो सकता है। इंटरनेट और मोबाइल की पहुंच के कारण, भारत में साइबर अपराध में तेजी से वृद्धि हुई है जिससे कई अनसुलझे मामले सामने आए हैं। भारत में सामुदायिक आपातकालीन प्रतिक्रिया दल (सीईआरटी) वह एजेंसी है जो इस प्रकार की गतिविधियों का ध्यान रखती है,

साइबर हमलों की जानकारी का विश्लेषण करती है, साइबर घटनाओं के लिए पूर्वानुमान और अलर्ट करती है। कोई भी व्यक्ति उनकी वेबसाइट पर घटना की रिपोर्ट कर सकता है। वर्ष 2007 में "अरोड़ा जनरेटर टेस्ट" किया गया जिसमे शोधकर्ताओं ने यह पाया कि दूर से बिजली जनरेटर के सॉफ्टवेयर को बदलकर टर्बाइनों को आग लगा सकते हैं और इस प्रकार अंततः जनरेटर को गंभीर नुकसान पहुंचा सकते हैं। इस प्रकार के उदाहरण औद्योगिक नियंत्रण प्रणाली (आईसीएस) और भवन नियंत्रण प्रणाली (बीसीएस) पर साइबर आतंकवादियों से एक प्रासंगिक खतरा हैं। सवाल उठता है कि किस प्रकार भविष्य में इन साइबर हमलों को होने से कैसे रोका जा सकता है? आज सबसे तेजी से बढ़ता खतरा साइबर आतंकवाद है यह न केवल व्यक्तियों या संगठनों के लिए बल्कि पूरे राष्ट्र के लिए बड़ा खतरा है। हमें यह सुनिश्चित करना चाहिए कि रोकथाम के सही तरीकों को ध्यान में रखा जा रहा है या नहीं। यह संसाधनों की कमी या किसी व्यक्ति या संगठनात्मक स्तर पर प्रेरणा की कमी के कारण होता है।

इन जोखिमों से निपटने का एक प्रभावी तरीका जिससे सुरक्षा को सही रूप से निर्माण कर सकें। सुरक्षा संस्कृति साइबर सुरक्षा के संदर्भ में मूल्यों के समुच्चय को संदर्भित करती है, जिसे संगठन में सभी के द्वारा साझा किया जाता है। यह निर्धारित करना कि कोई इसके बारे में किस प्रकार से सोच सकता है और संस्कृति के निर्माण एवं उसकी सुरक्षा हेतु जागरूकता पैदा कर महत्वपूर्ण निर्णय ले सकता है। इस प्रकार अपने कर्मचारियों को सही सुरक्षा प्रदान की जा सकती है। एक साधारण चेकलिस्ट जिसमें क्या करें और क्या न करें इस प्रकार का एक प्रश्नोत्तरी तैयार की जा सकती है।

जो संगठन को एक सुरक्षा प्रदान करने में मददगार साबित हो सकता है। एक बार इसकी सही जानकारी सभी को हो जाने पर 80-90% क्राइम को रोका जा सकता है। यह सुनिश्चित करने के लिए सरकार और सांसदों का एक बड़ा प्रयास है कि प्रौद्योगिकी स्वस्थ तरीके से विकसित हो और इसका उपयोग कानूनी और नैतिक व्यवसाय विकास के लिए किया जाए न कि अपराध करने के लिए। शुरुआत में सरकार और उद्योग जगत के नेताओं को इसमें सहयोग दिया जाना चाहिए और यह मान्यता विकसित करनी चाहिए तथा उन्हें कैप्चर द फ्लैग (सीटीएफ) गतिविधियों जैसे आयोजनों का संचालन करना चाहिए।

भारत में साइबर कानूनों में सुधारों की आवश्यकता: साइबर क्राइम को पूरी तरह से नियंत्रण करने हेतु सरकार ने विभिन्न प्रकार के कानून बनाएं हैं। कानूनों में उतनी कठोरता नहीं थी जिससे कि सभी क्राइम करने वालो के मन में भय उत्पन्न हो सके। इसलिए इसमें सुधारों की आवश्यता थी अतः उनमें कुछ संशोधन किए गए। साइबर कानून का मुख्य उद्देश्य भारत में ई-कॉमर्स के लिए कानूनी आधारभूत संरचना प्रदान करना है। संचार के इलेक्ट्रॉनिक माध्यम से व्यक्त किए गए इलेक्ट्रॉनिक रिकॉर्ड और अनुबंधों को कानूनी जामा प्रदान करने वाला आई टी एक्ट 2000 पहला कानूनी साधन था। अधिनियम को बाद में दिसंबर 2008 में आईटी (संशोधन) के माध्यम से संशोधित किया गया था। उसके मुख्य बिंदु निम्नानुसार हैं:

डिजिटल हस्ताक्षर (धारा 3 का संशोधन): एक ग्राहक द्वारा डिजिटल हस्ताक्षर लगाकर इलेक्ट्रॉनिक रिकॉर्ड को प्रमाणित किया जा सकता है। इसके अलावा ग्राहक द्वारा प्रदान की गई सार्वजनिक कुंजी का उपयोग करके हस्ताक्षर को सत्यापित किया जा सकता है।

प्रमाणन प्राधिकरण (धारा 45 ए सम्मलित करना): घरेलू और विदेशी प्रमाणन प्राधिकरण (जो डिजिटल हस्ताक्षर प्रमाण पत्र प्रदान करते हैं) कानून द्वारा मान्यता प्राप्त हैं; एक "प्रमाणक प्राधिकारी नियंत्रक" उनकी निगरानी करेगा।

इलेक्ट्रॉनिक शासन (धारा 47 ए सम्मलित करना): सरकार के किसी भी विभाग द्वारा कानून के अनुसार आवश्यक दस्तावेजों की आपूर्ति इलेक्ट्रॉनिक रूप में की जा सकती है और ऐसे दस्तावेजों को हस्तलिखित, टाइप किए गए या मुद्रित दस्तावेजों के समान माना जाना चाहिए।

अपराध और दंड (धारा 67 ए सम्मलित करना): एक न्यायनिर्णायक अधिकारी निर्णय लेगा कि क्या किसी व्यक्ति ने आईटी अधिनियम, 2000 के किसी प्रावधान के उल्लंघन में कोई अपराध किया है, कंप्यूटर या कंप्यूटर सिस्टम को किसी भी तरह की क्षति के लिए अधिकतम जुर्माना ₹1 करोड़ तक का जुर्माना है और यदि इस संबंध में कोई अपील करनी है तो अपील के लिए साइबर विनियम अपीलीय न्यायाधिकरण का गठन किया गया जो न्यायनिर्णयन अधिकारियों द्वारा पारित आदेशों के खिलाफ अपील की सुनवाई करेगा।

जांच (धारा 85 ए सम्मलित करना): अपराधों की जांच केवल पुलिस उपाधीक्षक या उससे ऊपर के रैंक के पुलिस अधिकारी द्वारा की जाएगी आईटी (संशोधन) अधिनियम, 2008 द्वारा "इंस्पेक्टर" या उससे ऊपर के रैंक में संशोधन) धारा 85ए में, "डिजिटल हस्ताक्षर" शब्दों के स्थान पर, जहां कहीं भी वे आते हैं, शब्द "इलेक्ट्रॉनिक हस्ताक्षर" को प्रतिस्थापित किया जाएगा।

धारा 85 बी का संशोधन - धारा 85 बी में, "डिजिटल हस्ताक्षर" शब्दों के स्थान पर, जहां कहीं भी वे आते हैं, शब्द "इलेक्ट्रॉनिक हस्ताक्षर" को प्रतिस्थापित किया जाएगा।

धारा 85 सी का संशोधन – धारा 85 सी में, "डिजिटल हस्ताक्षर प्रमाणपत्र" शब्दों के स्थान पर "इलेक्ट्रॉनिक हस्ताक्षर प्रमाणपत्र" शब्द रखे जाएंगे।

धारा 90 ए का संशोधन - धारा 90 ए में, शब्द "डिजिटल हस्ताक्षर", दोनों स्थानों पर जहां वे आते हैं, शब्द "इलेक्ट्रॉनिक हस्ताक्षर" को प्रतिस्थापित किया जाएगा।

अन्य कानूनों में संशोधन: भारतीय दंड संहिता, 1860, भारतीय साक्ष्य अधिनियम, 1872, बैंकर्स बुक्स एविडेंस एक्ट, 1891, भारतीय रिज़र्व बैंक अधिनियम, 1934 जैसे अन्य अधिनियमों को आईटी के साथ संरेखित करने के लिए संशोधित किया जाना आवश्यक है। इसके साथ-साथ देखा गया कि हैकिंग के मामले बढ़ गए हैं और पहचान, गोपनीयता और सूचना सुरक्षा को खतरा है:

1. **हैकिंग**: यह किसी भी आईटी अधिनियम में परिभाषित नहीं है, इसलिए भारत में साइबर अपराध कानून को काफी कमजोर कर दिया है।
2. **डेटा चोरी**: अपराध को मालिकों के बिना कंप्यूटर सिस्टम से जानकारी की प्रतिलिपि बनाने या निकालने के रूप में परिभाषित किया गया है, जिसमें कंप्यूटर चोरी और ट्रांसमिशन के दौरान डिजिटल सिग्नल की चोरी शामिल है।
3. **पहचान की चोरी (पासवर्ड की चोरी सहित):** आईटी (संशोधन) अधिनियम 2008 के अनुसार, इस अपराध को धोखाधड़ी या बेईमानी से किसी व्यक्ति के इलेक्ट्रॉनिक हस्ताक्षर, पासवर्ड या किसी अन्य विशिष्ट पहचान सुविधा का उपयोग करने के रूप में परिभाषित किया गया है।
4. **ई-मेल स्पूफिंग:** यह आमतौर पर हैकर्स द्वारा वास्तविक ई-मेल पते को छिपाने के लिए उपयोग किया जाता है जिससे फिशिंग और स्पैम संदेश भेजे जाते हैं। इसका उपयोग अन्य कपटपूर्ण तरीकों के संयोजन में भी किया जा सकता है ताकि उपयोगकर्ताओं को व्यक्तिगत/ गोपनीय जानकारी प्रदान करने के लिए छल किया जा सके।

5. **आपत्तिजनक संदेश भेजना:** आईटी अधिनियम इस अपराध को घृणा, दुर्भावना आदि पैदा करने के उद्देश्य से आपत्तिजनक या झूठी जानकारी भेजने के रूप में परिभाषित करता है।
6. **दृश्यरतिकता**: इसे किसी व्यक्ति की सहमति के बिना उसकी सहमति के छवियों/ वीडियो को प्रकाशित / प्रसारित करने के रूप में परिभाषित किया गया है।
7. **बाल अश्लीलता**: इसमें उन सभी व्यक्तियों के खिलाफ अपराध शामिल है जिन्होंने 18 वर्ष की आयु पूरी नहीं की है। सबसे गंभीर अपराधों में से एक होने के बावजूद यह किसी भी गंभीर सजा को आकर्षित नहीं करता है।
8. **साइबर आतंकवाद**: इस अपराध में दो आईटी अधिनियमों के बीच एक बड़ा अंतर था। साइबर आतंकवाद को कंप्यूटर तक पहुंच से इनकार करने, प्राधिकरण के बिना कंप्यूटर संसाधन तक पहुंचने का प्रयास करने या कंप्यूटर सिस्टम को दूषित करने के रूप में वर्णित किया गया है।
9. **सजा**: जबकि अन्य सभी अपराधों में 3-5 साल तक की कैद और/या ₹3-5 लाख तक के जुर्माने की सजा हो सकती है, साइबर आतंकवाद के लिए दोषी व्यक्ति को आजीवन कारावास की सजा हो सकती है।

उपसंहार: आधुनिक समाज तकनीक पर निर्भर है और जब तकनीक का विकास होता है तो उसमें क्राइम भी बढ़ते हैं। इसमें कोई संदेह नहीं है कि आईटी अधिनियम को अभी भी एक लंबा रास्ता तय करना है और इसमें कई संशोधनों की आवश्यकता है। हालांकि, कुछ समस्याएं हमेशा बनी रहेंगी, हम इसे पूरी तरह से समाप्त तो नहीं कर सकते लेकिन नियमों में और संशोधन करके इसको कम जरूर कर सकते हैं। भारत में आज पैसे का सारा लेन-देन एवं सभी व्यापारिक धन्धे लगभग ऑनलाइन माध्यम से ही किए जाते हैं। इसीलिए आजकल सभी क्राइम करने वालों की नजर इस पर रहती है तथा विभिन्न प्रकार के वायरस एवं दूसरी तकनीक के सहारे वे दूसरे के पैसों को हजम कर जाते हैं जिससे कि काफी नुकसान का सामना करना पड़ता है। इसमें कोई संदेह नहीं है कि आज भारत में इस पर लगाम लगाने के लिए बहुत से नए कानून बनाए जा रहे हैं। कहा जा सकता है कि वह दिन दूर नहीं जब भारत साइबर अपराध से पूरी तरह मुक्त होगा।

*****

कल्पना सी एस

पदनाम:- सहायक प्रबंधक
संस्था का नाम:- भारतीय रिज़र्व बैंक
मोबाइल नं. :- 8837419265
ई-मेल:- cskalpana@rbi.org.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

"जब परिवर्तन की हवाएं बहने लगती हैं, तो एक निराशावादी परिवर्तन के बारे में शिकायत करता है, एक आशावादी हवा के बदलने की उम्मीद करता है लेकिन एक यथार्थवादी समय को समायोजित करता है" । *अब,* भारतीय बैंकों के लिए अपने समय को समायोजित करने का समय आ गया है । प्रौद्योगिकी की प्रगति ने बैंकों को नियामक और ग्राहक दोनों को खुश रखने के प्रयास में दिन-प्रतिदिन नई टोपी पहनाने के लिए मजबूर कर रहा है ।

इंटरनेट के आविष्कार से मनुष्य के जीवन में काफी बदलाव आया है । इंटरनेट तत्काल संचार, खरीददारी, बैंकिंग, व्यापार, परामर्श, प्रशिक्षण के लिए एक आवश्यकता बन गया है । हालांकि, इंटरनेट एक दोधारी तलवार साबित हो रहा है जो दिन-प्रतिदिन जीवन में नए और अधिक जटिल मुद्दों का निर्माण कर रहा है । साइबर अपराध उन मुद्दों में से एक है जो एक बड़ी समस्या के रूप में सामने आई है । भारत दुनिया में सबसे ज्यादा इंटरनेट इस्तेमाल करने वाले राष्ट्रों में दूसरे नंबर पर है । लगभग हर चीज के लिए इंटरनेट पर अत्यधिक निर्भरता की वजह से साइबर अपराध को नज़र अंदाज़ नहीं कर सकते । इसलिए विशेष रूप से साइबर दुनिया के लिए एक मजबूत कानूनी ढांचे के साथ-साथ कार्यान्वयन रणनीति की आवश्यकता है ।

साइबर अपराध एक अवैध आपराधिक गतिविधि है जिसमें कंप्यूटर या नेटवर्क उपकरण का उपयोग किया जाता है । साइबर अपराधों की जटिलता मुख्य रूप से साइबर जगत द्वारा दी गई गुमनामी के कारण उत्पन्न होती है । धोखाधड़ी करने के लिए अपराधी को अपराध स्थल पर शारीरिक रूप से उपस्थित होने की आवश्यकता नहीं है और इसलिए कोई भौतिक और परिस्थितिजन्य साक्ष्य नहीं है जो इसे वास्तविक दुनिया के अपराधों से बहुत अलग बनाता है । आभासी दुनिया वास्तविक दुनिया की कानूनी प्रणालियों के दायरे में नहीं आती है और अपराधों की वैश्विक प्रकृति क्षेत्राधिकार की समस्याओं को प्रस्तुत करती है ।

अपराधी की पहचान के लिए कोई चेहरा या उंगलियों के निशान नहीं हैं और अपराध का कोई गवाह नहीं है । अपराध दुनिया के किसी भी कोने से और दीवारों की सीमाओं के भीतर एक बिलकुल अजनबी द्वारा हो सकता है । चूंकि समस्या तकनीकी प्रकृति की है इसलिए समाधान भी प्रौद्योगिकी में निहित है । लेकिन विडंबना यह है कि साइबर अपराधी तकनीक के मामले में अन्वेषक से हमेशा एक मील आगे रहता है और इसे एक शाश्वत दौड़ बना देता है । यह समाधान कानूनी ढांचे के साथ निहित है । इसलिए, हमें साइबर अपराधों के मुद्दे को हल करने के लिए एक मजबूत प्रौद्योगिकी और समान रूप से मजबूत वैश्विक कानूनी प्रणाली की आवश्यकता है ।

भारत में होने वाले कुछ सामान्य साइबर अपराध हैं डीडीओ हमले, पहचान की चोरी, हैकिंग, फ़िशिंग, सोशल इंजीनियरिंग, बॉटनेट, साइबर स्टॉकिंग, चाइल्ड पोर्नोग्राफ़ी, डार्क वेब का उपयोग कर नशीली दवाओं की तस्करी और ऑनलाइन से संबंधित अन्य मामले आदि।

चूंकि साइबर अपराध के मुख्य उद्देश्य मौद्रिक लाभ होता है इसलिए रणनीति मुख्यत: प्रौद्योगिकी समाधानों को आगे बढ़ाने में निहित होना चाहिए। इनमें लेनदेन के लिए मजबूत प्लेटफॉर्म सुनिश्चित करना, लेनदेन की ट्रैकिंग, ऑडिट ट्रेल्स, एम्बेडेड सुरक्षा विशेषताएं आदि शामिल हैं। यदि लेनदेन का सबूत उपलब्ध है तो इरादे को साबित किया जा सकता है और सबूत पेश किए जा सकते हैं। लेकिन यदि साइबर कानून में उपयुक्त कानूनी प्रावधान मौजूद नहीं हैं, तो अपराधी दंड से बच सकता है। सामाजिक अपराध जैसे पीछा करना, धमकाना, सोशल इंजीनियरिंग आदि हैं जो मकसद और अपराधियों को ट्रैक करने के संबंध में अधिक जटिल हैं।

भारत में, सूचना प्रौद्योगिकी अधिनियम, 2000 ई-गवर्नेंस की दिशा में पहला कदम था जिसका अर्थ था 'इलेक्ट्रॉनिक डेटा इंटरचेंज और इलेक्ट्रॉनिक संचार के अन्य माध्यमों से किए गए लेनदेन के लिए कानूनी मान्यता प्रदान करना'। इसने सरकारी एजेंसियों के साथ दस्तावेजों की ई-फाइलिंग और भारतीय दंड संहिता 1860, भारतीय साक्ष्य अधिनियम 1872, बैंकर्स बुक्स एविडेंस एक्ट 1891, भारतीय रिजर्व बैंक अधिनियम, 1934 और उनसे संबंधित मामलों में संशोधन की अनुमति दी। साइबर अपराधों की संख्या और जटिलता में वृद्धि ने 2008 में डिजिटल हस्ताक्षरों की परिभाषा और विवरण, मध्यस्थों की भूमिका पर स्पष्टता, सूचना सुरक्षा पर जोर, साइबर अपराधों की जांच करने की शक्ति और दंड के विवरण प्रदान करके आईटी अधिनियम में कुछ संशोधनों को आवश्यक बना दिया।

2018 में भारत में साइबर अपराधों से संबंधित 27,248 मामले दर्ज किए गए। 'क्राइम इन इंडिया' रिपोर्ट के अनुसार, भारत में साइबर अपराध 2020 के दौरान बढ़कर 50,035 हो गए, जो प्रचलित कानूनी ढांचे की अप्रभाविता का प्रमाण है। इसके अलावा, सीएनएन न्यूज़ 18 द्वारा विश्लेषण किए गए आंकड़ों के अनुसार 2018 और 2020 के बीच मामलों में लगभग 85 प्रतिशत की वृद्धि हुई है।

दंडनीय साइबर अपराधों का वर्णन धारा 43 के बाद से किया गया है। हालांकि, धाराएं अपराध या अपराध के प्रयास को साबित करने के लिए आवश्यक और पर्याप्त सबूत पेश नहीं करती हैं। इस वजह से जांच एजेंसियां दोषियों को पकड़ने में नाकाम रहती हैं।

आईटी अधिनियम (संशोधित) की कुछ कमियां निम्नानुसार हैं :-

1. धारा 5 एवं 6 इलेक्ट्रॉनिक हस्ताक्षर साबित किए जा सकते हैं और अदालतों में स्वीकार किए जा सकते हैं, भले ही वे डिजिटल हस्ताक्षर न हों (कुछ शर्तें पूरी हों)। जबकि इलेक्ट्रॉनिक दस्तावेज़ के लिए डिजिटल हस्ताक्षर लगाने के संबंध में एक विकल्प है, asymmetric crypto system with hash function के अलावा डिजिटल हस्ताक्षर के प्रकार को चुनने का कोई विकल्प नहीं है। इसके अलावा, पर्याप्त सबूत के रूप में डिजिटल हस्ताक्षर के बिना इलेक्ट्रॉनिक दस्तावेजों की स्वीकृति पर स्पष्टता प्रदान करने के लिए भारतीय साक्ष्य अधिनियम में आवश्यक संशोधन की आवश्यकता है।
2. धारा 43 ए, 72 और 72ए - वर्तमान परिदृश्य में डेटा सुरक्षा एक मुख्य मुद्दा है जिसमें व्यक्तिगत जानकारी सबसे मूल्यवान संपत्ति है। आईटी अधिनियम में, "sensitive personal data" और 'reasonable security practices' शब्दों में स्पष्टता नहीं है और इसे निर्दिष्ट करने की आवश्यकता है। उपयुक्त एजेंसियों द्वारा प्रमाणित होने के लिए प्रमाणन मानकों के साथ आचार संहिता और मानक प्रक्रियाओं (Code of Ethics and Standard Practices) को विकसित करना समय की आवश्यकता है।

इसलिए संवेदनशील सार्वजनिक सूचना में काम करने वाले संस्थानों के लिए प्रमाणीकरण को अनिवार्य बनाया जा सकता है।

3. धारा 21 - उप-धारा (2) के प्रावधानों के अधीन, कोई भी व्यक्ति इलेक्ट्रॉनिक हस्ताक्षर प्रमाण पत्र जारी करने के लिए लाइसेंस के लिए नियंत्रक को आवेदन कर सकता है।
4. इसके आधारित, बैंकों को डिजिटल हस्ताक्षर प्रमाण पत्र जारी करने के लिए लाइसेंस का आवेदन करने की अनुमति दी गयी है लेकिन यह स्पष्ट नहीं है कि किस को प्रमाणन प्राधिकरण बनने के लिए लाइसेंस जारी किया जा सकता है।
5. धारा 65, 66 और 67, 67बी - जो कंप्यूटर के सोर्स कोड के साथ छेड़छाड़, कंप्यूटर सिस्टम की हैकिंग, डेटा की चोरी, गोपनीयता का उल्लंघन और बाल अश्लीलता से संबंधित है, जो कि बहुत कम और हल्के सजा और दंड को आकर्षित करती है। अपराध के कृत्यों से होने वाले नुकसान के लिए यह दंड बहुत कम हैं। साइबर अपराधों को श्रेणीबद्ध करने और इससे होने वाले नुकसान की गंभीरता को ध्यान में रखते हुए सजा और दंड निर्धारित करने की आवश्यकता है। चूंकि हैकिंग के मामलों को हल करना सबसे कठिन मामलों में से एक है, इसलिए हैकिंग के तरीकों को आईटी अधिनियम में स्पष्ट रूप से समझाया जाना चाहिए। इसके अलावा, अधिनियम वास्तव में किए गए अपराधों के लिए दंडात्मक कार्रवाई का वर्णन करता है और *अपराध करने के प्रयासों के बारे में चुप* है। इस कमी के कारण, आपराधिक इरादे वाले लोग मुक्त होने और अपने प्रयास जारी रखने में सक्षम हैं।
6. धारा 67 इलेक्ट्रॉनिक रूप में अश्लील सूचना के प्रकाशन से संबंधित है। इसमें, वह शब्द *'grossly offensive and menacing character'* बहुत अस्पष्ट हैं और अलग-अलग लोगों के लिए अलग-अलग चीजें हो सकती हैं। इसमे सजा की अवधि और जुर्माने भी अस्पष्ट है।
7. उक्त अधिनियम के अनुसार अश्लील सामग्री को इलेक्ट्रॉनिक रूप में प्रकाशित या प्रसारित करना दंडनीय अपराध है, जबकि अश्लील साहित्य देखना अवैध नहीं है।
8. चूंकि साइबर अपराधों ने विभिन्न क्षेत्रों को छुआ है, इसलिए परक्राम्य लिखतों, न्यास, वसीयत, विलेखों और अचल संपत्तियों की बिक्री से संबंधित दस्तावेजों के संबंध में उपयुक्त संशोधन की आवश्यकता है जो वर्तमान में आईटी अधिनियम के दायरे से बाहर हैं।

आईटी अधिनियम में कुछ ही अपराध जैसे कि धारा 66एफ (साइबर आतंकवाद), 67 ए और बी (publishing & transmission of sexually explicit act and depicting children in sexually explicit act in e form), धारा 69 और 69ए और धारा 70 के अलावा सभी अपराध जमानती (bailable offence) है। इसे देखते हुए, अधिकांश अपराधियों को विश्वास है कि वे पकड़े जाने पर जमानत के साथ छूट सकते हैं। वे डिजिटल साक्ष्यों में हस्तक्षेप भी कर सकते हैं। बहुत सारे अपराध असंज्ञेय (non-cognizable) होते हैं और पुलिस किसी व्यक्ति को बिना वारंट गिरफ्तार नहीं कर सकती है। साइबर अपराधों से निपटने में यह एक बड़ी बाधा है।

साइबर अपराधों की वैश्विक प्रकृति को ध्यान में रखते हुए प्रभावी निवारण का मुद्दा तीन स्तरों पर हो सकता है - व्यक्तिगत, संस्था और वैश्विक।

चूंकि कई वित्तीय अपराध ग्राहकों की अज्ञानता के कारण होते हैं, साइबर अपराधों से निपटने में सबसे प्रभावी कदम साइबर अपराधों की प्रकृति, संरक्षित किए जाने वाले साक्ष्य और रिपोर्टिंग के बारे में स्कूलों/ कॉलेजों/ संगठनों में जागरूकता कार्यक्रमों को बढ़ाना है। इसके अलावा netizens के अधिकारों और जिम्मेदारियों को संकलित और प्रलेखित किया जाना चाहिए।

प्रत्येक सार्वजनिक संस्थान/ संगठन/ शैक्षणिक संस्थान के पास तकनीकी सहायता विभागों के अलावा साइबर संबंधी मुद्दों के लिए एक आपातकालीन प्रतिक्रिया दल होना चाहिए। इन टीमों को मालवेयर, बॉटनेट, फ़िशिंग साइटों और उपयुक्त साइबर वर्ल्ड शिष्टाचार के संबंध में जागरूकता पैदा करने/अद्यतन करने का काम सौंपा जा सकता है। वे साइबर मुद्दों की रिपोर्टिंग और निवारण के लिए नोडल बिंदु के रूप में कार्य कर सकते हैं। संचालन के क्षेत्र के आधार पर विभिन्न संगठनों के लिए अनुकूलित डिजिटल ऑडिट सिस्टम विकसित करने की आवश्यकता है। सतर्कता और निवारक सतर्कता उपायों में उपयुक्त साइबर व्यवहार को भी निर्दिष्ट किया जा सकता है और यदि कोई समस्या है तो उसे सतर्कता रिपोर्ट में शामिल किया जा सकता है।

नए वित्तीय डिजिटल उत्पादों और सेवाओं को तभी पेश किया जा सकता है जब अधिकांश आबादी इसे प्राप्त करने के लिए तैयार हो और प्रौद्योगिकी को संभालने में सक्षम हो। यदि नहीं, तो धोखाधड़ी के प्रजनन के लिए जमीन आसान हो जाती है। डिजिटल उत्पादों को पेश करने से पहले जागरूकता कार्यक्रम होने चाहिए ताकि अनुकूलन सुचारू रूप से हो सके।

राष्ट्रीय और वैश्विक स्तर पर, क्षेत्राधिकार से संबंधित मुद्दों को संबोधित करने की आवश्यकता है और डार्कवेब, अंतर्राष्ट्रीय ड्रग पेडलिंग, चाइल्ड पोर्नोग्राफी और साइबर आतंकवाद में हो रहे गंभीर अपराधों से निपटने के लिए एक समेकित और समन्वित दृष्टिकोण की आवश्यकता है। जैसा कि परिभाषाओं और राष्ट्रों में अपराधों के वर्गीकरण में अंतर है, एक देश में अपराध के रूप में माना जाने वाला कार्य दूसरे में नहीं माना जाता है। अपराधी भी इन मतभेदों के तहत कवर लेते हैं और इसलिए साइबर दुनिया को एक अलग और समान कानून की आवश्यकता है तथा अपराध और दंड भी राष्ट्रों में समान होते हैं जिसके तहत एक समान आचार संहिता निर्धारित की जानी चाहिए। साइबर अपराधों का पता लगाने और जांच में देशों के बीच एक समझौता ज्ञापन सभी देशों को एक साथ ला सकता है। इंटरनेट अपराध शिकायत केंद्र (IC3), साइबर इंटरपोल और एफबीआई के संचालन का दायरा सभी देशों में शाखाओं के साथ बढ़ाया जाना है।

निष्कर्षत: हम कह सकते हैं कि एक तरफ डिजिटल लेनदेन के संबंध में बरती जाने वाली सावधानियों के बारे में लोगों में जागरूकता पैदा करनी होगी। दंडों को और अधिक स्पष्ट करने की आवश्यकता है और दंड की गंभीरता अपराध के परिणामों पर आधारित होनी चाहिए। सभी जांच एजेंसियों और अदालतों को तकनीकी विशेषज्ञों द्वारा समर्थित होना चाहिए जो अपराधों के तकनीकी पहलू से निपट सकते हैं। कमियों को दूर करने के लिए आईटी अधिनियम, 2008 में उपयुक्त संशोधन/ परिवर्धन की आवश्यकता जरूर है।

सन्दर्भ:

- (https://www.statista.com/statistics/309435/india-cyber-crime-it-act/)
- https://www.law.ox.ac.uk/business-law-blog/blog/2016/09/implications-information-technology-banking-cyber-law-and-cyber#:~:text=The%20Information%20Technology%20(IT)%20Act, Business%20transactions%20and%20cyber%20crimes.&text=The%20provision%20of%20internet%20based, Bank's%20servers%20and%20network%20tap .
- RBI की आधिकारिक वेबसाइट- इलेक्ट्रॉनिक बैंकिंग पर कार्यदल की रिपोर्ट
- सूचना प्रौद्योगिकी अधिनियम 2008 (संशोधित)
- पवन दुग्गल, साइबर एडवोकेट के लेख

*****

कुणाल राहड़

पदनाम:- सहायक परामर्शदाता
संस्था का नाम:- भारतीय रिज़र्व बैंक
मोबाइल नं. :- 9929369561
ई-मेल:- kunalrahar@rbi.org.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

जब से मानव का सृजन हुआ है, अपराध होते आए हैं और अपराधों के साथ ही उनसे जुड़े नियम बनते गए हैं। उदाहरण के तौर पर 350 ईसा पूर्व के आसपास लिखे गए कौटिल्य के अर्थशास्त्र में विभिन्न अपराधों, शासकों द्वारा की जाने वाली सुरक्षा पहल, राज्य में संभावित अपराधों आदि पर चर्चा की गई है और कुछ निर्धारित अपराधों की सूची के लिए सजा की भी वकालत की गई है।

सतही हैकिंग के शुरुआती उदाहरणों का पता 1970 के दशक से लगाया जा सकता है (जब भारत में एसटीडी/आईएसडी कॉल बहुत महंगे होते थे और मुफ्त टेलीफोन कॉल करने के लिए अवैध रूप से लंबी दूरी के टेलीफोन नेटवर्क को हैक किया जाता था)। अमेरिकी खुफिया एजेंसियों का तो यहां तक कहना है कि रूस ने 2016 के राष्ट्रपति चुनाव को हैक कर लिया था और बांग्लादेश सेंट्रल बैंक के (US$81 मिलियन का साइबर हमला किसे याद नहीं है? एक फेक न्यूज के चलते पाकिस्तान के रक्षा मंत्री ख्वाजा आसिफ ने तो इजरायल को परमाणु जवाबी कार्रवाई की धमकी तक दे डाली थी।

आज आपके हाथ में रखा जो मोबाइल फोन है, उसकी संगणात्मक क्षमता विश्व के प्रथम स्पेसशिप (वोस्टोक 1) से भी ज्यादा है, जरा सोचो उस 10 मंजिला ऊंचे स्पेसशिप से ज्यादा ताकतवर ये 120 ग्राम वजनी फोन है। बैंकिंग क्षेत्र की बात करें तो आज माइक्रो सेकेंड्स में धनराशि एक खाते से दूसरे खाते में स्थानांतरित हो सकती है। ऐसे माहौल में साइबर सुरक्षा एवं साइबर कानूनों की महत्ता स्वतः ही प्रबल हो जाती है।

हालांकि 'साइबर अपराध' शब्द सूचना प्रौद्योगिकी अधिनियम 2000 में परिभाषित नहीं है और न ही आई.टी. संशोधन अधिनियम 2008 में या भारत के किसी अन्य कानून में किन्तु व्याख्या के तौर पर हम एटीएम पर क्रेडिट/डेबिट कार्ड की क्लोनिंग, रैंसमवेयर, आइडेंटिटी थेफ्ट, केवाईसी थोखाधड़ी, क्रिप्टोजैकिंग, ड्रग्स और डार्क वेब के माध्यम से अवैध हथियारों की बिक्री, सोशल-मीडिया स्टॉकिग, ऑनलाइन नौकरी धोखाधड़ी से संबंधित अपराध, वेब डिफेक्शन, साइबर आतंकवाद आदि को इसमें शामिल किया जा सकता है।

द इकोनॉमिक टाइम्स द्वारा किए गए एक हालिया विश्लेषण के अनुसार, साइबर अपराध से भारत सरकार को प्रति वर्ष लगभग रू. 1.25 लाख करोड़ का नुकसान हो रहा है यदि सोचा जाए तो यह रकम इतनी है कि भारत सरकार 3 वर्षों तक नरेगा योजना चला सकती है। सर्वप्रथम कंप्यूटर दुरुपयोग अधिनियम 1990 (ग्रेट ब्रिटेन) में आया फिर अंतर्राष्ट्रीय व्यापार कानून पर संयुक्त UE SALT (UNCITRAL) ने 1996 में ई-कॉमर्स पर मॉडल कानून अपनाया इसी तर्ज़ पर भारत ने सन् 2000 में सूचना प्रौद्योगिकी अधिनियम बनाया। सूचना प्रौद्योगिकी अधिनियम, 2000 होने के नाते भारतीय साइबर कानून मुख्य रूप से इक्कीस साल पुराना कानून है जिसे वर्ष 2008 में केवल एक बार संशोधित किया गया था।

नीति आयोग की रिपोर्ट में साइबर स्पेस और सुरक्षा के संबंध में कुछ सामान्य चुनौतियों को स्वीकार किया गया है। कॉपीराइट और ट्रेड मार्क उल्लंघन नेट पर बहुतायत में होते हैं लेकिन कॉपी राइट एक्ट 1976, याट्रेड मार्क एक्ट 1994 में इन उल्लंघन का कोई जिक्र ही नहीं है। इसलिए नेट पर डोमेन नामों की सुरक्षा सुनिश्चित करने के लिए कोई प्रवर्तन प्रणाली भी नहीं है। नेगोशिएबल इस्ट्रुमेंट एक्ट, 1881 के तहत ई-कैश और ऑनलाइन लेनदेन के प्रसारण को सुरक्षा नहीं दी गई है। ऑनलाइन गोपनीयता केवल धारा 43 (कंप्यूटर या कंप्यूटर सिस्टम को नुकसान के लिए दंड) और 72 (गोपनीयता या गोपनीयता का उल्लंघन) के बारे में बात करती है। इंटरनेट सेवा प्रदाता (ISP) जो मानव हस्तक्षेप के बिना किसी तीसरे पक्ष की जानकारी प्रसारित करते हैं, उन्हें सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत उत्तरदायी नहीं बना सकते हैं। कोई अगर यह साबित करता है कि अपराध उसकी जानकारी के बिना किया गया था या उन्होंने अपराध को रोकने के लिए उचित परिश्रम किया तो वे आसानी से छूट खंड के तहत आश्रय ले सकते हैं।

जब भारत में साइबर अपराध की घटनाओं की बात आती है तो साइबर अपराधियों द्वारा कानून के भय की कमी दिखाई देती है। इसे प्रभावहीनता ही कह सकते हैं कि अधिकांश अपराध आजीवन कारावास से दंडनीय नहीं हैं। चाहे साइबर अपराधी न्यूक्लियर प्लांट को हैक करके हजारों लोगों की जान लेले, किन्तु उस अपराध की अधिकतम सजा सिर्फ 10 साल है, इसे यदि हम अमेरिका के नियमों से तुलना करें तो पाएंगे की वहां आजीवन कारावास से लेकर मृत्युदंड तक का भी प्रावधान है। आईटी (संशोधन) अधिनियम, 2008 ने अधिकांश साइबर अपराधों के लिए सजा की मात्रा को कम कर दिया। इसमे संशोधन की जरूरत है। अधिकांश साइबर अपराधों को गैर-जमानती अपराध बनाने की जरूरत है।

साइबर अपराधों की रिपोर्टिंग में कमी, अपराध के क्षेत्राधिकार में संशय, जनता की अनभिज्ञता और अपराध की जांच की बढ़ती प्रौद्योगिकी लागत जैसी चुनौतियों के कारण पुलिस साइबर अपराधों को हल करने से जूझ रही है। अदालतों को साइबर अपराध के मामलों को अन्य अपराधों की तुलना में प्राथमिकता देने की शक्ति दी जानी चाहिए। कंप्यूटर और इंटरनेट उपयोग से संबंधित पुलिस कर्मियों हेतु साइबर प्रशिक्षण अपराध दर को कम करने का एक और महत्वपूर्ण तरीका है। भारत में कम उम्र में ही कंप्यूटर विज्ञान में शिक्षा को प्रोत्साहित करना चाहिए। आप जापान जैसे देश में देखेंगे कि छठी कक्षा का छात्र भी Coding सीखना शुरू कर देता है। सूचना प्रौद्योगिकी अधिनियम गैर-नागरिकों के लिए भी लागू होता है, लेकिन इस प्रावधान का तब तक व्यावहारिक महत्व नहीं है जब तक कि अपराधी को भारत में प्रत्यर्पित नहीं किया जा सकता। इसलिए देशों के बीच प्रत्यर्पण संधियों में साइबर अपराधियों का मुखर उल्लेख होनी चाहिए। रंजीत डी. उदेशी बनाम महाराष्ट्र राज्य के मामले में सुप्रीम कोर्ट ने स्वीकार किया कि भारतीय दंड संहिता अश्लीलता को परिभाषित नहीं करती है, हालांकि यह अश्लील सामग्री के प्रकाशन के लिए सजा का प्रावधान करती है। एक सामग्री जिसे अश्लील कहा जा सकता है और जो कलात्मक भी है, उनके बीच बहुत पतली रेखा मौजूद है ऐसे में अधिनियम 2000 का इस्तेमाल करना नामुमकिन सा है और इसमें संशोधन की आवश्यकता है।

सबसे महत्वपूर्ण मुद्दा है, इंटरनेट कानूनों के एकीकरण की तत्काल आवश्यकता। उदाहरण के लिए हानिकारक साइटों के लिए हमारे पास भारतीय दंड संहिता (आईपीसी), अश्लीलता कानून, संचार शालीनता कानून, स्व-विनियमन, सूचना प्रौद्योगिकी अधिनियम 2000, डेटा संरक्षण अधिनियम, भारतीय दंड संहिता, आपराधिक प्रक्रिया संहिता आदि है। विषय से संबंधित कई कानूनों के कारण उनकी प्रयोज्यता के बारे में भ्रम होता है और कोई भी कानून इस विषय से विशेष रूप से पूर्ण रूप से संबंधित नहीं है। समस्या से निपटने के लिए विभिन्न इंटरनेट कानूनों के एकीकरण का सुझाव दूंगा जैसे आयकर के लिए एक डीटीसी की संरचना की जा रही है।

भारतीय रिज़र्व बैंक ने "बैंकों में साइबर सुरक्षा ढांचा" नामक एक अधिसूचना भी जारी की जिसमें कई

दिशानिर्देश और सर्वोत्तम प्रथाओं को निर्दिष्ट किया गया और बैंकों पर एक रिपोर्टिंग दायित्व लगाया गया। अक्तूबर 2020 में खबरें सामने आई कि एटीएम से जुड़े बैक-एंड सिस्टम के उल्लंघन के कारण 3.2 मिलियन डेबिट कार्ड जोखिम में हैं। यह घटना केवल इसलिए प्रकाश में आई क्योंकि जनता को अपने बैंकों से अपना पिन बदलने का निर्देश मिला। यदि किसी ई-कॉमर्स साइट का डेटा चोरी हो जाता है तो उसे आपको या सरकार को बताकर कुछ हासिल नहीं होता है। और अगर बाद में आपके क्रेडिट या डेबिट कार्ड से किसी दूर देश में या यहां किसी अन्य शहर में चार्ज किया जाता है, तो आप अनजान होंगे और ईकॉमर्स साइट पर उल्लंघन का पता लगाने का कोई तरीका नहीं होगा। एसएमएस आधारित वन टाइम पासवर्ड भी सेफ नहीं है। 557 सिस्टम असुरक्षित है और सिम स्वैप एक ज्ञात भेद्यता है। हाल ही में अमेरिका में एक सुरक्षा फर्म ने पाया कि कुछ एंड्रॉइड फोन में पहले से इंस्टॉल किए गए सॉफ्टवेयर के कारण चीन में एक सर्वर पर फोन में एसएमएस संदेश भेज रहे थे। यदि ऐसे डेटा लीक की जिम्मेदारी साबित नहीं की जाएगी तो सजा देना भी कठिन होगा।

प्रभावी साइबर अपराध नियंत्रण के लिए राष्ट्रीय और अंतर्राष्ट्रीय स्तर पर कानून प्रवर्तन एजेंसियों के बीच समन्वय को तेज करने की त्वरित आवश्यकता है। चूंकि साइबर अपराध अंतर्राष्ट्रीय सीमा को नहीं पहचानता है तो इसकी रोकथाम के लिए बने कानून क्यों सिर्फ एक देश के लिए हों। साइबर कानूनों का वो प्रारूप होना चाहिए जो जलवायु परिवर्तन के कानूनों का है अर्थात् 'Global Commons' का।

रक्षा जोखिम पर विचार करते हुए आइए थोड़ी कल्पना करते हैं। विचार करें कि यदि कई स्रोतों से एकत्र किए गए डेटा को एक साथ रखा जाए तो क्या होगा। यहां से आपका ई मेल पता और पासवर्ड, वहां से आपका मोबाइल नंबर और सोशल नेटवर्किंग साइट से आपके मित्र और परिवार का ब्यौरा, जिन्हें साझा करने में हम भारतीय ऐसे ही बहुत खुश हैं। इनमें से कई डेटा डार्कनेट पर बिक्री के लिए आता है, टार्गेटेड मार्केटिंग की अनुमति देने वाले समान डेटा माइनिंग टूल को लागू करके, कोई आपराधिक संगठन आपकी एक प्रोफाइल बना सकता है जो उन्हें आपके पासवर्ड का अनुमान लगाने में मदद कर सकता है जिसमें किसी प्रियजन का नाम और जन्म तिथि शामिल है। वे आपके पासवर्ड को रीसेट करने के लिए सुरक्षा प्रश्नों के उत्तर का अनुमान तक लगा सकते हैं। ये खौफनाक मंजर आर्टिफिशियल इंटेलिजेंस (एआई), इंटरनेट ऑफ थिंग्स (आईओटी) और ब्लॉकचैन जैसी नई तकनीकों की जमाने में वास्तविकता से दूर नहीं है, करोड़ रुपये का सवाल यह है कि क्या हमारे कानून इन सब से लड़ने में सक्षम हैं? मुझे लगता है बहुत बदलाव की जरूरत है। वैश्विक साइबर सुरक्षा सूचकांक में डेनमार्क, जर्मनी, इजराइल, अमेरिका जैसे देश अव्वल आते हैं और भारत जो विश्वभर में आईटी के क्षेत्र में अग्रणी है किंतु यहां आकर पिछड़ जाता है।

कोविड -19 महामारी के आगमन के बाद, वर्क फ्रॉम होम कल्चर उभरा, जिसने मनुष्य के काम, शिक्षा, मनोरंजन और संचार की जरूरतों को पूरा करने के लिए तकनीक-आधारित उपकरणों के जाल में फंसा दिया। ऐसे में साइबर अपराधों में करीब 56 प्रतिशत का इजाफा हुआ। किन्तु सुरक्षा नियम ऐसे माहौल में ज्यादा सार्थक साबित न हो पाये। 2020 में नई साइबर सुरक्षा नीति की घोषणा जरूर की गयी थी परंतु इसका क्रियान्वयन अभी बाकी है। भारत में कोई डेटा संरक्षण अधिनियम नहीं है, केवल डेटा सुरक्षा के बारे में बात करने वाले प्रावधान सूचना प्रौद्योगिकी अधिनियम, 2000 की थारा 72 और थारा 43 हैं | ऐसे ही सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 69 में संशोधन की आवश्यकता है। हाल ही में बजट 2022 में हुई घोषणा के मुताबिक आरबीआई डिजिटल मुद्रा लाने वाला है, ऐसे में नीति निरधाताओं के लिए यक्ष प्रश्न यह है कि क्या पहले आईटी अधिनियम में संशोधन करना जरूरी नहीं है क्या?

ऐसा नहीं है कि हमारे कानून में सिर्फ खामियां ही हैं। 140 करोड़ की जनसंख्या वाले विविध देश में वर्ष 2020 में CERT-IN ने करीब 12 लाख हमलों का सामना किया यानि यूं देखा जाए तो प्रति मिनट 140 हमले। कुछ

समय पहले की बात है कि पूर्वोत्तर के हजारों लोग हिंसा की धमकी के बाद दहशत में बैंगलोर से भागने पर मजबूर हुए थे। कारण था सोशल नेटवर्किंग वेबसाइटों पर एक फेक विडियो का वायरल होना। किन्तु सतर्कता और राजनीतिक इच्छाशक्ति के चलते आईटी नियमों के तहत पुलिस असली अपराधियों का पकड़ने में सफल रही।

अतः साइबर सुरक्षा की जिम्मेदारी में ग्राहक, बैंक, सरकार और रिज़र्व बैंक ऑफ इंडिया सभी को योगदान देना होगा। यह मान कर कार्य करना होगा कि इन सब प्रयासों के बावजूद भी साइबर हमले जड़ से खत्म नहीं होंगे। जिस तरह नई-नई दवाइयों के बावजूद बीमारियां नए रूप में देश विदेश के कोनों में उत्पन्न होती रहती हैं उसी प्रकार सर्वांगीण चौकसी और तत्परता के बावजूद साइबर हमलों का खतरा हमेशा रहेगा पर हां ये जरूर है कि कोरोना के टीके की तरह हम इन वायरस के हमलों को नगण्यता की ओर ले जा सकते हैं। हमने 2025 तक 5 ट्रिलियन अमेरिकी डॉलर की अर्थव्यवस्था का लक्ष्य रखा है। सुरक्षित डिजिटल देश के रूप में उभरने के लिए नीति, कानूनी ढांचे, निगरानी बुनियादी ढांचे और प्रौद्योगिकी के संबंध में हमें तैयार रहना ही होगा।

*****

जया मिश्रा

पदनाम:- मुख्य प्रबंधक एवं शिक्षण प्रमुख
संस्था का नाम:- बैंक ऑफ़ बड़ौदा
मोबाइल नं. :- 9990932573
ई-मेल:- jayabadelhi@gmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

आज हम तकनीक के उस युग में जी रहे हैं जहां आए दिन नए-नए आविष्कार हो रहे हैं और दुनिया मोबाइल के माध्यम से हमारी हथेली में समा चुकी है। इन आविष्कारों से जीवन इतना आसान हो चुका है कि हम एक साधारण काम से लेकर कठिनतम काम तक जैसे कि विदेशों के सर्वोत्तम विश्वविद्यालयों के शैक्षणिक सत्र तक में अपने घर बैठकर सहभागिता कर सकते हैं। लेकिन जैसे हर सिक्के के दो पहलू होते हैं वैसे ही तकनीक भी दोधारी तलवार है। जहां डिजिटलीकरण ने जीवन को बहुत आसान किया है वहीं इसके दुष्परिणाम भी सामने आ रहे हैं जिसका नाम है साइबर क्राइम।

यद्यपि साइबर अपराध को न तो सूचना प्रौद्योगिकी अधिनियम 2000 में परिभाषित किया गया है, न ही राष्ट्रीय साइबर सुरक्षा नीति 2013 और न ही भारत में किसी अन्य विनियम में लेकिन वैसी आपराधिक गतिविधि जहां कंप्यूटर तथा कंप्यूटर नेटवर्क को साधन या लक्ष्य बनाकर गलत मानसिकता के साथ दूसरों की ऑनलाइन गोपनीयता को भंग किया जाता है, साइबर अपराध कहलाता है। साइबर अपराध पिछले कुछ वर्षों में उभरकर सामने आया है क्योंकि भारत में इंटरनेट का उपयोग करने वालों की संख्या काफी बढ़ी है। यदि हम विश्व स्तर पर देखें तो इंटरनेट उपभोक्ताओं की सर्वाधिक संख्या के मामले में विश्व में अमेरिका और चीन के बाद भारत का तीसरा स्थान है। बैंकिंग संबंधित साइबर अपराधों की संख्या नोटबंदी के बाद काफी बढ़ी है क्योंकि लोगों में ऑनलाइन पेमेंट की आदत बहुत बढ़ गई है।

भारत के साइबर कानून

भारत में साइबर अपराधों के निपटान के लिए दो कानूनों में प्रावधान किया गया है। प्रथम, सूचना तकनीक कानून 2000 और दूसरा भारतीय दंड संहिता।

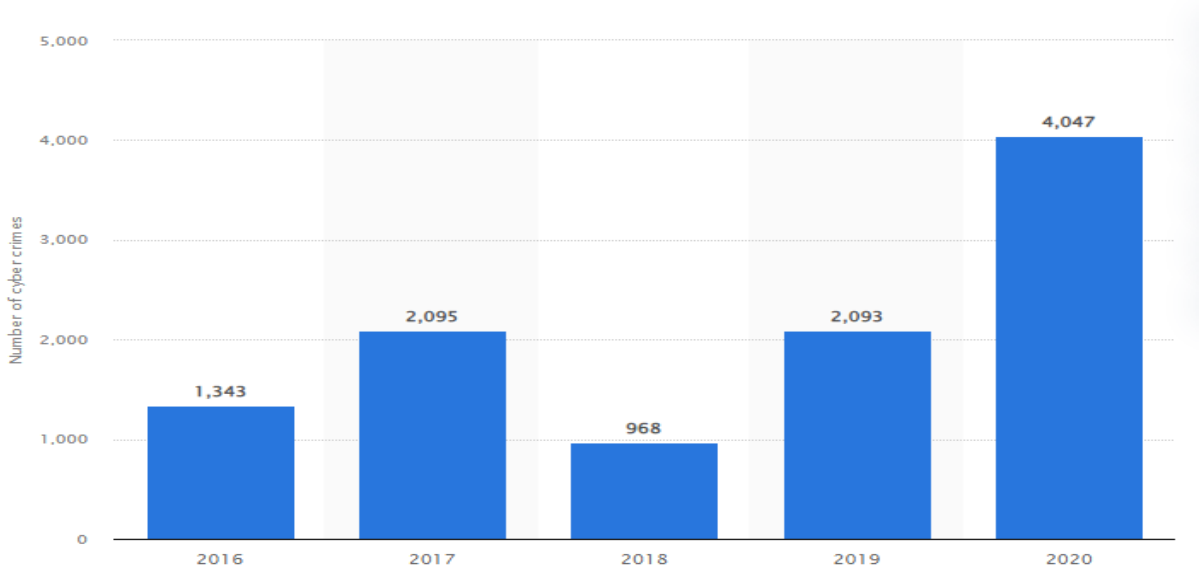
सूचना तकनीक कानून, 2000 के अंतर्गत साइबर अपराधों से संबंधित प्रावधान

- कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश
- कंप्यूटर में संग्रहित डेटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश
- कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को गलत तरीके से हासिल करने के लिए दंड का प्रावधान
- किसी की पहचान चोरी करने के लिए दंड का प्रावधान
- अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डेटा तक पहुंच बनाने के लिए दंड का प्रावधान
- साइबर आतंकवाद के लिए दंड का प्रावधान

- इलेक्ट्रॉनिक माध्यमों से सेक्स या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान
- इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो
- सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान
- फर्जी डिजिटल हस्ताक्षर का प्रकाशन
- भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान
- ई-मेल के माध्यम से धमकी भरे संदेश भेजना
- ई-मेल के माध्यम से ऐसे संदेश भेजना जिससे मानहानि होती हो
- फर्जी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल
- फर्जी वेबसाइट्स या साइबर फ्रॉड
- ई-मेल का गलत इस्तेमाल

यदि भारत में साइबर अपराधों की संख्या के बारे में बात करें तो "इलेक्ट्रॉनिक्स और आईटी राज्य मंत्री" श्री राजीव चंद्रशेखर द्वारा लोकसभा को दिये गए लिखित जवाब का संदर्भ लिया जा सकता है जिसमें उन्होंने बताया है कि वर्ष 2018, 2019, 2020 और 2021 (अक्तूबर तक) के दौरान कुल 17,560, 24,768, 26,121 और 25,870 भारतीय वेबसाइटों को हैक किया गया था। यदि हम बैंकिंग से संबंधित धोखाधड़ी की चर्चा करें तो यह संख्या भी कम नहीं है। बैंकों में साइबर अपराध के 2016 से 2020 तक के निम्नांकित आंकड़े दर्शाते हैं कि यह संख्या बड़ी तेजी से बढ़ रही है। यह संख्या रिपोर्ट किए गए अपराधों की है जबकि न रिपोर्ट किए गए अपराधों की संख्या शायद इससे कहीं ज्यादा है।

2016 से 2020 तक पूरे भारत में ऑनलाइन बैंकिंग से संबंधित साइबर अपराधों की संख्या



निःसन्देह जहां अपराधों की संख्या इतनी ज्यादा है वहां एक सख्त कानून की भी आवश्यकता है। भारत में भी साइबर अपराधों के नियंत्रण के लिए उपरोक्त कानून मौजूद है लेकिन आज जब हम तकनीकी रूप से इतने आगे निकल चुके हैं यह समय आत्ममंथन का है कि क्या हमारे साइबर कानून प्रभावकारी हैं?

साइबर कानून सूचना प्रौद्योगिकी अधिनियम, 2000 को समय-समय पर अद्यतन भी किया जाता रहा है और इसकी कमियों को दूर करने का प्रयास किया गया है लेकिन स्थिति **"तू डाल डाल मैं पात पात"** वाली है। कानून उतनी जल्दी अद्यतन नहीं किए जा रहे जितनी जल्दी-जल्दी धोखाधड़ी के नए तरीके ढूंढ लिए जा रहे हैं। यदि हम बैंक के संदर्भ में देखें तो हम पाते हैं कि बैंक ग्राहक सेवा को अधिकतम सहज, सुलभ व लोकलुभावन बनाने के लिए तकनीक का सहारा लेकर नित नई डिजिटल सेवाएं शुरू कर रहे हैं लेकिन हमारे साइबर कानून उसके लिए तैयार नहीं हैं। कुछ नई तकनीक जिसके सहारे बैंक अपने ग्राहकों को सहज सेवा उपलब्ध करा रहे हैं परंतु भारत का साइबर कानून इसके लिए तैयार नहीं है:

- **विडियो केवाईसी में डीपफेक तकनीक द्वारा धोखाधड़ी**: आजकल बैंक विडियो केवाईसी के माध्यम से ग्राहकों को शाखा में बिना बुलाये ही खाता खोलने की सुविधा दे रहे हैं। इस सिस्टम में ग्राहक विडियो द्वारा केवाईसी पूरा करवाते हैं और बैंक द्वारा मांगी गई जानकारी प्रदान कर खाता खुलवाते हैं। साइबर अपराधियों ने इस तकनीक का फाइदा उठाया है जिसमें डीपफेक तकनीक द्वारा कोई दूसरा व्यक्ति किसी और व्यक्ति का प्रतिरूपण कर अपना खाता खुलवा लेता है और बैंक के साथ धोखाधड़ी करता है। इस तकनीक में वास्तविक ध्वनि वाले ऑडियो और वीडियो का उत्पादन करने के लिए कृत्रिम बुद्धिमत्ता का उपयोग किया जाता है।

- **स्मार्ट वॉच के माध्यम से बैंकिंग सेवा:** कई बैंकों ने स्मार्ट घड़ी के माध्यम से ग्राहकों को बैंकिंग सेवा प्रदान करना शुरू किया है जैसे कि बैंक ऑफ़ बड़ौदा द्वारा बॉब वर्ल्ड वेव। इस उत्पाद में वन क्लिक में भुगतान की सुविधा प्रदान की गई है। निःसन्देह, यह सुविधा डिजिटल भुगतान को अत्यधिक आसान बनाएगी लेकिन यदि स्मार्ट वॉच चोरी हो जाए या किसी और व्यक्ति द्वारा उपयोग की जाए तो क्या भारत का साइबर कानून इतना सशक्त है कि लोगों को इसके दुरुपयोग से हुई हानी से बचा सके। निःसन्देह नहीं।

- **यूपीआई रिक्वेस्ट पेमेंट ऑप्शन व अन्य पेमेंट ऑप्शन**: नोटबंदी के बाद डिजिटल भुगतानों में अत्यधिक वृद्धि हुई है। भुगतान के साथ-साथ यदि किसी से पैसे उधार लेने हो तो भी डिजिटल माध्यम का ही उपयोग किया जा रहा है जैसे यूपीआई रिक्वेस्ट पेमेंट ऑप्शन। अंतरण की यह प्रक्रिया बेहद आसान है और यदि मोबाइल फोन हैक कर लिया जाए तो साइबर अपराधियों के लिए लोगों के परिश्रम से कमाए गए पैसे को हड़प लेना अत्यधिक आसान हो जाता है। ऐसे ज़्यादातर अपराधों में एक छोटी धनराशि ही संलिप्त होती है जिसे साइबर सेल बहुत ही हल्के में लेता है और उचित कार्रवाही नहीं हो पाती है। ऑनलाइन पेमेंट पर साइबर कानून पूर्णतया स्पष्ट भी नहीं है।

- **क्रेडिट व क्रेडिट कार्ड में ऑटो डेबिट फैसिलिटी**: आजकल बहुत सारी सुविधाओं के उपयोग के लिए क्रेडिट व डेबिट कार्ड से ऑटो डेबिट सुविधा उपलब्ध है। कई बार हम किसी सुविधा को बंद करना चाहते हैं लेकिन उन कंपनियों द्वारा हमें उस सुविधा को बंद करने का कोई विकल्प नहीं दिया जाता। हमारे न चाहते हुए भी हमें उस सुविधा का उपयोग करना पड़ता है क्योंकि हमारे पास भुगतान को रोकने का कोई विकल्प नहीं होता। यह भी एक तरीके का अप्रत्यक्ष साइबर अपराध है और ऐसे अपराधों के लिए साइबर कानून में कोई प्रावधान नहीं है। यदि हम ऐसे अपराधों की शिकायत करते भी हैं तो वो कंपनियां हमारे एक बार की सहमति का प्रमाण देकर बच जाती हैं।

  उपरोक्त क्षेत्रों के अलावे भी ऐसे बहुत से क्षेत्र हैं जो नियमित नवोन्मेषिता के परिणाम हैं लेकिन भारत का साइबर कानून इसके लिए पूर्णतया तैयार नहीं है। साइबर कानून की प्रभावशीलता सैद्धांतिक कारणों से तो

कम होती ही है लेकिन कई व्यावहारिक कारण भी इसकी प्रभावशीलता को कम करने में महत्वपूर्ण भूमिका निभाते हैं। जिसमें कुछ कारण निम्नलिखित हैं:

- **साइबर सेल व साधारण पुलिस थानों का अलग होना व साइबर सेलों की संख्या कम होना**: साइबर सेल व साधारण पुलिस थाने अलग-अलग हैं व साइबर सेल की संख्या भी पुलिस थानों की तुलना में काफी कम हैं। यदि हम दिल्ली की बात करें तो पूरी दिल्ली में केवल 15 साइबर सेल मौजूद हैं जबकि रिपोर्ट की गई साइबर अपराधों की संख्या काफी है। रिपोर्ट नहीं किए गए साइबर अपराधों की तो बात ही क्या की जाए। रिपोर्ट किए गए अपराधों पर भी तत्काल कार्रवाही नहीं की हो पा रही है क्योंकि शायद साइबर कानून में हर कार्य के लिए समय सीमा निश्चित नहीं की गई है। साइबर सेल के साधारण पुलिस थानों से अलग होने के कारण लोगों की पहुंच इन सेलों तक सीमित है।

- **साइबर कानून में प्रचार-प्रसार की नीति का अभाव होना**: भारत में यद्यपि वर्ष 2000 से साइबर कानून उपलब्ध है लेकिन यदि हम इसके प्रचार-प्रसार की स्थिति को देखें तो हम पाते हैं कि अभी भी साइबर सेल व साइबर क़ानूनों के प्रति जागरूकता का बेहद अभाव है। छोटे शहरों व गांवों की क्या बात की जाए महानगरों तक में हर व्यक्ति को साइबर सेल व साइबर कानून की जानकारी नहीं है जिसके कारण काफी संख्या में साइबर अपराध रिपोर्ट ही नहीं हो पाते। किसी भी समस्या को पहचानना जितना महत्वपूर्ण है उससे भी महत्वपूर्ण है उसका समाधान ढूंढना। यक्ष प्रश्न यह है कि कैसे साइबर कानून की प्रभावशीलता को बढ़ाया जा सकता है।

साइबर सुरक्षा कानून की प्रभावशीलता को बढ़ाने के उपाय

राष्ट्रीय साइबर सुरक्षा नीति, 2013 ने स्पष्ट किया कि भारत को एक समर्पित राष्ट्रीय साइबर सुरक्षा रणनीति की आवश्यकता है, हालांकि इसे अभी तक जारी नहीं किया गया है। अतः साइबरस्पेस के महत्त्व को देखते हुए नई रणनीति में सभी प्रमुख मुद्दों को शामिल किया जाना चाहिए, जिनमें से कुछ निम्नलिखित हैं:

- **साइबर कानून में बैंक से संबंधित अपराधों के लिए विशेष अध्याय एवं उसे कम समयांतराल पर अद्यतन करने की आवश्यकता:** यदि साइबर अपराध धन से संबंधित है तो वो वह किसी न किसी खाते के द्वारा ही हो सकता है। अतः साइबर कानून में बैंक से संबंधित अपराधों के लिए एक विशेष अध्याय जोड़ने की आवश्यकता है जो बहुत विस्तृत और स्पष्ट हो। चूंकि बैंकों के डिजिटल उत्पाद बहुत ही जल्दी अद्यतन होते रहते हैं और बैंक ग्राहकों को नियमित नवोन्मेषिता का सहारा लेकर नित नए डिजिटल उत्पाद प्रदान करते रहते हैं, इसलिए साइबर कानून के बैंक से संबंधित अध्याय की कम समय के अंतराल पर, जैसे की हर 6 महीने में, समीक्षा की जानी चाहिए।

- **जागरूकता में वृद्धि:** यद्यपि वर्ष 2000 से भारत में साइबर कानून उपलब्ध है लेकिन यदि जागरूकता की बात करें तो यह संतोषजनक नहीं है। अतः साइबर कानून में ही ऐसा प्रावधान होना चाहिए कि इसकी जागरूकता को बढ़ाना सभी संस्थाओं के लिए अनिवार्य हो। विभिन्न संस्थाओं को भी साइबर अपराधों, इससे बचाव के उपाय और साइबर कानून के प्रति जागरूकता बढ़ाने पर ध्यान देना चाहिए। जागरूकता बढ़ाने के लिए जो लक्ष्य समूह निर्धारित किए जाने चाहिए वो केवल कर्मचारी न होकर ग्राहक भी होने चाहिए क्योंकि अगर बैंकों के संदर्भ में देखें तो साइबर अपराध के शिकार अधिकांशतः ग्राहक ही होते हैं।

- **मौजूदा साइबर सुरक्षा ढांचे को मजबूत करना:** यद्यपि सरकार का प्रयास रहा है कि भारत में एक शसक्त साइबर सुरक्षा ढांचा मौजूद हो लेकिन अभी भी यह पूर्णतया संभव नहीं हो पाया है। साइबर सेलों की संख्या

जरूरत से काफी कम है। अलग साइबर सेल बनाने से बेहतर है कि हर बड़े थाने में दो साइबर एक्सपर्ट और छोटे थानों में एक साइबर एक्सपर्ट की व्यवस्था की जाए जो साइबर अपराधों को सुलझा सकें।

- **साइबर अपराधों को सुलझाने के लिए अधिकतम समय सीमा का निर्धारण**: साइबर कानून में किसी भी अपराध का निपटान करने के लिए अधिकतम समय सीमा का निर्धारण होना चाहिए जिससे पीड़ित के केस पर जल्द-जल्द से कार्रवाही सुनिश्चित हो सके।

- **शैक्षिक पाठ्यक्रमों में साइबर सुरक्षा को शामिल करना:** विद्यालयों, केंद्रीय विश्वविद्यालयों, निजी विश्वविद्यालयों, उद्योग संघों, औद्योगिक प्रशिक्षण संस्थानों सहित अन्य सभी शैक्षिक संस्थानों में साइबर सुरक्षा संबंधी पाठ्यक्रमों को शामिल करना चाहिए जिससे लोगों में जागरूगता बढ़ाई जा सके।

आज हम तकनीक के उस युग में जी रहे हैं जहां इसके बगैर जीना असंभव है। अतः आवश्यकता है कानून को और सशक्त बनाने की और लोगों की इसके प्रति जागरूकता बढ़ाने की जिससे अपराधी बच न सकें और अपराध की संख्या न्यूनतम की जा सके।

*****

डॉ. प्रशांत रामटेके

पदनाम:- प्रबंधक
संस्था का नाम:- भारतीय रिज़र्व बैंक
मोबाइल नं. :- 9822790150
ई-मेल:- prashantramteke@rbi.org.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

भारत में साइबर कानून

सूचना प्रौद्योगिकी अधिनियम, 2000 भारत का प्रधान कानून है जो कंप्यूटर, कंप्यूटर सिस्टम और कंप्यूटर नेटवर्क के साथ-साथ इलेक्ट्रॉनिक प्रारूप में डेटा और सूचना के उपयोग को नियंत्रित करता है। इस कानून ने इलेक्ट्रॉनिक प्रमाणीकरण, डिजिटल हस्ताक्षर, साइबर अपराध और नेटवर्क सेवा प्रदाताओं की जवाबदेही से संबंधित विभिन्न पहलुओं को छुआ है। अधिनियम की प्रस्तावना में कहा गया है कि इसका उद्देश्य इलेक्ट्रॉनिक डेटा इंटरचेंज और इलेक्ट्रॉनिक संचार के अन्य माध्यमों के माध्यम से किए गए लेनदेन के लिए कानूनी मान्यता प्रदान करना है, जिसे आमतौर पर "इलेक्ट्रॉनिक कॉमर्स" कहा जाता है, जिसमें पेपर-आधारित विधियों के विकल्पों का उपयोग शामिल है। इस अधिनियम को सूचना प्रौद्योगिकी संशोधन विधेयक, 2008 द्वारा संशोधित किया गया था।

कई कानूनों और यहां तक कि विभिन्न नियामकों द्वारा बनाए गए नियमों में साइबर अपराधों को दंडित करने वाले कानून मिलते हैं। सूचना प्रौद्योगिकी अधिनियम, 2000 और भारतीय दंड संहिता, 1860 कई साइबर अपराधों को दंडित करता है और आईपीसी और आईटी अधिनियम में इस संबंध में कई प्रावधान हैं।

कंप्यूटर एवं इंटरनेट के आगमन के साथ रोजमर्रा की जिंदगी में काम और तौर-तरीके आसान, सुविधाजनक एवं सुलभ हो गए हैं। लेकिन, कुटिल और चालाक प्रवृत्ति के लोगों को अपराधों का अभ्यास करने एवं व्यक्तियों या व्यवसायों के कामकाज में तबाही मचाने के लिए एक और मंच मिल गया है। भारत में साइबर अपराधों में वृद्धि हुई है। साइबर आतंकवाद, बौद्धिक संपदा अधिकारों का उल्लंघन, मनी लॉन्ड्रिंग धोखाधड़ी, एक्सचेंज फंड ट्रांसफर धोखाधड़ी, अश्लील साहित्य आदि साइबर धोखाधड़ी द्वारा किए जाने वाले कुछ लोकप्रिय साइबर अपराध हैं। हैकिंग, वायरस अटैक, डॉस अटैक आदि ऐसे तरीके हैं जिनसे साइबर फ्रॉड आपके सिस्टम के लिए खतरा लाते हैं।

उपरोक्त अपराधों का उदय 'साइबर कानूनों' को जन्म देता है जो साइबर स्पेस से संबंधित कानूनी मुद्दों या पहलुओं से संबंधित होते हैं और इसे परिभाषित करते हैं। ये साइबर कानून कई अन्य कानूनी क्षेत्रों के संबंधित बिंदु हैं जो एक तरह से या किसी अन्य बौद्धिक संपदा, गोपनीयता, भाषण और अभिव्यक्ति की स्वतंत्रता के संवैधानिक अधिकार एवं अन्य कानूनी अधिकार क्षेत्र को प्रभावित करते हैं।

भारत में साइबर कानून के तहत विभिन्न प्रकार के अपराधों को शामिल किया जाता है, जैसे

साइबर अपराध

- इलेक्ट्रॉनिक एवं डिजिटल हस्ताक्षर में धोखाधड़ी

- इंटेलेक्चुअल प्रॉपर्टी में धोखाधड़ी
- डेटा संरक्षण/ गोपनीयता मामले में धोखाधड़ी
- सभी ऑनलाइन गतिविधियां साइबर कानून के तहत जांच के दायरे में आती है लेकिन कुछ ऐसे क्षेत्र भी हैं जिन पर भारत में साइबर क्राइम कानून लागू नहीं होता हैं, जैसे –
- पॉवर ऑफ़ अटॉर्नी
- विल या वसीयतनामा
- अचल संपत्ति की बिक्री
- केंद्र सरकार अधिसूचित दस्तावेज एवं लेनदेन

साइबर अपराध कानून का उद्देश्य-

- सभी ई-लेनदेन के लिए कानूनी मान्यता प्रदान करना।
- ऑनलाइन समझौतों को स्वीकार करने के लिए एक वैध हस्ताक्षर के रूप में डिजिटल हस्ताक्षर को कानूनी मान्यता देना।
- बैंको के साथ-साथ अन्य संगठनों द्वारा इलेक्ट्रॉनिक रूप में लेखांकन पुस्तकों को रखने के लिए कानूनी मान्यता देना।
- ऑनलाइन गोपनीयता की सुरक्षा को बढ़ाना।
- साइबर अपराधों को रोकना।

प्रभावशीलता

भारत में, हमारे पास मुख्य रूप से सूचना प्रौद्योगिकी अधिनियम, 2000 है। जिसने एक हद तक इन साइबर अपराधों से निपटने में मदद की है। इसने साइबर-आतंकवादियों के मन में भय पैदा कर दिया है और इस तरह के कृत्यों को करने से पहले कानूनी नतीजों का डर लाएगा। आज, अधिकांश लेन-देन और संप्रेषण साइबरस्पेस के माध्यम से किए जाते हैं और इलेक्ट्रॉनिक माध्यमों से किए जाते हैं। यह प्रवृत्ति सरकारी विभागों सहित संचालन के लगभग सभी क्षेत्रों में प्रचलित है। इस अधिनियम ने डिजिटल हस्ताक्षर, एन्क्रिप्शन मोड, आदि के माध्यम से इलेक्ट्रॉनिक रिकॉर्ड को प्रमाणित करने, पर्यवेक्षण करने, सुरक्षित करने के लिए एक कानूनी ढांचा पेश किया है।

साइबर कानून ई-व्यवसायों के लिए पर्याप्त लाभ लाते हैं और उनका सर्वोत्तम और संरक्षात्मक उपयोग सुनिश्चित करना चाहिए।

साइबर कानून ई-कॉमर्स कंपनियों के लिए अपने आभासी व्यवसायों को सुरक्षित रूप से चलाने के लिए एक कानूनी ढांचा और सेट-अप प्रदान करते हैं।

आईटी अधिनियम ने डिजिटल हस्ताक्षर आरंभ किए हैं जिससे ऑनलाइन लेनदेन में वैध सुरक्षा को बढ़ाया है और यह कंपनियों के लिए डेटा सुरक्षा को काफी हद तक सुनिश्चित करता है।

भारत में साइबर कानूनों के आगमन के साथ, इलेक्ट्रॉनिक लेनदेन को कम से कम परेशानी और अधिक सुरक्षा के साथ सफलतापूर्वक किया जा सकता है।

यह अधिनियम कंपनियों को वैधानिक उपाय और कानूनी सहायता प्रदान करता है। आईटी अधिनियम, 2000 के अध्याय ग्यारह में ऐसे अपराधों से निपटने के तरीकों और सुरक्षात्मक उपायों का उल्लेख है।

भारत में, कम्युनिटी इमरजेंसी रिस्पांस टीम (सीईआरटी) वह एजेंसी है जो संग्रह का ध्यान रखती है, साइबर हमलों की जानकारी का विश्लेषण करती है, साइबर घटनाओं के लिए पूर्वानुमान और सचेत करती है। कोई उनकी वेबसाइट पर घटना की रिपोर्ट कर सकता है।

वर्तमान परिप्रेक्ष्य में सबसे तेजी से बढ़ता खतरा साइबर आतंकवाद है, यह न केवल व्यक्तियों या संगठनों के लिए बल्कि पूरे राष्ट्र हेतु हमें यह सुनिश्चित करना चाहिए कि इसकी रोकथाम के लिए यथोचित उपायों को कार्यान्वित किया जा रहा है।

अभी हाल ही में हमने देखा है कि नोट विमुद्रीकरण एवं कोरोना काल में डिजिटल लेन-देन में संव्यवहार काफी बढ़ा है। भारत सरकार द्वारा नकद रहित संव्यवहार पर जोर दिया जा रहा है। भारतीय रिज़र्व बैंक द्वारा वित्तीय समावेशन एवं वित्तीय साक्षरता पर जोर दिया जा रहा है। बैंकिंग एवं साइबर अपराधों से संबंधित शिकायतों के निराकरण के लिए पूर्ववर्ती तीनों लोकपाल योजनाओं को एकीकृत करके हाल ही में रिज़र्व बैंक एकीकृत योजना। 2021 को लागू किया गया है। सभी शिकायतों को डिजिटल प्लेटफार्म- शिकायत प्रबंधन प्रणाली (सीएमएस) के माध्यम संसाधित किया जाता है। भारतीय रिज़र्व बैंक ने प्रौद्योगिकी के इस्तेमाल को आसान बनाने के लिए आईडीआरबीटी, एनपीसीआई, सीसीआईएल आदि जैसी संस्थाओं की स्थापना करके महत्वपूर्ण भूमिका अदा की है। भारत सरकार के प्रयासों से जन-धन खातों में वृद्धि हुई और सभी सरकारी लाभ सीधे उनके खातों में जमा किए जा रहे हैं। इस वर्ष के बजट में माननीय वित्त मंत्री द्वारा सेंट्रल बैंक डिजिटल करेंसी (सीबीडीसी) की घोषणा की है जिसे भारतीय रिज़र्व बैंक द्वारा चलन में लाया जाएगा। मोबाइल एवं इंटरनेट बैंकिंग के उपयोग में बढ़ोत्तरी हुई है और इस संदर्भ में साइबर कानून काफी महत्वपूर्ण हो जाता है।

सुधारों की आवश्यकता

भारत को एक समर्पित एवं प्रासंगिक साइबर सुरक्षा कानून की आवश्यकता है। इस तरह के कानून की आवश्यकता बहुत अधिक है क्योंकि यह भारत, इसकी साइबर सुरक्षा एवं साइबर संप्रभु हितों की रक्षा के लिए एक महत्वपूर्ण होगा। ऐसे समय में जब कई अन्य देशों ने साइबर सुरक्षा पर समर्पित कानूनों के साथ आना शुरू कर दिया है, भारत इस मामले में थोड़ा पीछे है। इस संबंध में उचित कार्रवाई की आवश्यकता है।

फ़िशिंग, पहचान की चोरी एवं धोखाधड़ी सहित साइबर अपराध पिछले कुछ वर्षों में बड़े पैमाने पर बढ़े हैं। हालांकि, मौजूदा कानूनों के तहत इसका कवरेज न तो पर्याप्त है और न ही व्यापक।

सूचना प्रौद्योगिकी क्रांति ने वैश्विक समुदाय में बदल दिया है और इंटरनेट ने साइबर अपराध के खतरे को जन्म दिया है। साइबर अपराध का खतरा एक या दो देशों तक ही सीमित नहीं है बल्कि पूरी दुनिया इस विशाल समस्या का सामना कर रही है। ऐसा नहीं है कि इस कानून से पहले इन अपराधों से निपटने के लिए कोई कानून नहीं था। भारतीय दंड संहिता, 1860 में पहले से ही साइबर अपराधों को रोकने और नियंत्रित करने के प्रावधान थे लेकिन वे साइबरस्पेस अपराधों की सभी प्रकारो से निपटने के लिए पर्याप्त नहीं थे। इसका स्पष्ट कारण यह है कि जिस समय भारतीय दंड संहिता लागू की गई थी उस समय कंप्यूटर या इंटरनेट के बारे में कोई नहीं जानता था। साइबर कानूनों में सुधार लाने के लिए निम्नलिखित सुधारों की आवश्यकता हैं।

सुरक्षा कड़ी की जाए

अधिकांश वाणिज्यिक, औद्योगिक और व्यावसायिक लेनदेन राष्ट्रीय एवं अंतर्राष्ट्रीय स्तर पर इंटरनेट सेवाओं के माध्यम से किए जाते हैं। व्यापार एवं वाणिज्य के क्षेत्र में कंप्यूटर के बढ़ते उपयोग ने एक ही समय में अपराधियों द्वारा अपने व्यक्तिगत मौद्रिक लाभ के लिए साइबर अपराधों के अपराध के लिए नए रास्ते खोल दिए हैं। वाणिज्यिक क्षेत्र में कंप्यूटर पर बढ़ती निर्भरता के साथ, अधिकांश धनराशि का लेन-देन कंप्यूटर नेटवर्क की मदद

से किए जा रहे हैं, जिससे साइबर अपराधियों के लिए अवैध रूप से वित्तीय धोखाधड़ी को करना संभव हो गया है। इसलिए, यह आवश्यक है कि ई-कॉमर्स एवं ई-बैंकिंग को संभावित ऑनलाइन धोखाधड़ी, जालसाजी या धन के दुरुपयोग आदि से बचाने के लिए एक पर्याप्त सुरक्षा तंत्र विकसित किया जाए।

तलाशी और जब्ती से संबंधित कानून में संशोधन

व्यापक साइबर अपराध को नियंत्रित करने के लिए सरकार के नियामक प्रणाली को और तेज करने की जरूरत है। सबसे महत्वपूर्ण बात यह है कि मौजूदा कानूनी व्यवस्थाओं को कानून प्रवर्तन एजेंसियों को बिना किसी बाहरी दबाव के अपने कार्यों को निडरता से पूरा करने में सक्षम बनाना चाहिए। कानून प्रवर्तन एजेंसियों को सेवा प्रदाताओं से ऐसे विवरण प्राप्त करने का अधिकार होना चाहिए। पूरे विश्व में फिनटेक संबंधी क्रांति के आने से एक बार फिर से साइबर के क्षेत्र में स्थिति चुनौतीपूर्ण बन गई है।

एक सार्वभौमिक कानूनी नियामक प्रणाली की आवश्यकता

कानून और आपराधिक न्याय वितरण प्रणाली ने पिछले वर्षों के दौरान दुनिया भर में हुई तकनीकी प्रगति के साथ तालमेल नहीं रखा है, जिसने इंटरनेट के दुरुपयोग के लिए पर्याप्त गुंजाइश प्रदान की है। विभिन्न राष्ट्रों के कानूनों और प्रक्रियाओं के विचलन के कारण उत्पन्न होने वाली समस्या को काफी हद तक समाप्त किया जा सकता है यदि कम से कम प्रमुख साइबर अपराधों को सभी देशों द्वारा उनके दंड कानूनों में समान रूप से मान्यता दी जाती है और शामिल किया जाता है।

इसलिए, साइबर अपराधों में शामिल क्षेत्राधिकार संबंधी चुनौतियों का सामना करने के लिए यह सुझाव दिया जाता है कि साइबर अपराध से संबंधित अपराधियों की जांच करने और उन्हें दंडित करने की शक्ति के साथ वैश्विक अधिकार क्षेत्र के साथ एक अंतर्राष्ट्रीय आपराधिक न्यायाधिकरण स्थापित किया जाए।

साइबर कानून के सार्वभौमिकरण की आवश्यकता

आमतौर पर यह देखा गया है कि साइबर अपराध के अपराधी आमतौर पर कंप्यूटर में निहित कमजोरियों का फायदा उठाते हैं। इसलिए कंप्यूटर सिस्टम के अनधिकृत उपयोग को रोकने के लिए कुछ विशेष सुरक्षा उपाय अपनाए जा सकते हैं। इसलिए साइबर कानून सहित विभिन्न देशों के आपराधिक कानूनों को सार्वभौमिक बनाया जाना चाहिए ताकि साइबर अपराध के खतरे के खिलाफ नागरिकों, संस्थानों, संगठनों, सरकारी एवं गैर-सरकारी एजेंसियों और समाज को पर्याप्त सुरक्षा प्रदान की जा सके।

सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008

यद्यपि 2008 में संशोधित सूचना प्रौद्योगिकी अधिनियम, 2000 लगभग सभी ऑनलाइन आपराधिक गतिविधियों के लिए कानून की पहुंच बढ़ाकर और लोगों में जागरूकता बढ़ाकर कंप्यूटर मालिकों / उपयोगकर्ताओं को राहत प्रदान करने में काफी हद तक सफल रहा है, अधिनियम अभी भी कुछ कमियों से ग्रस्त है जिसका निराकरण किए जाने की आवश्यकता है।

मौजूदा कानूनों के आधुनिकीकरण एवं नए कानूनों के अधिनियमन की आवश्यकता

कंप्यूटर के आगमन से पहले के देशों के दंड कानूनों को आधुनिक बनाने की आवश्यकता है। एक ओर कंप्यूटर से संबंधित धोखाधड़ी जैसे हैकिंग, डेटा चोरी, सॉफ्टवेयर चोरी आदि से निपटने के लिए मौजूदा कानूनों को बदलना होगा और दूसरी ओर डेटा सुरक्षा एवं गोपनीयता सुनिश्चित करने के लिए नया कानून भी आवश्यक है।

लोगों को जागरूक और साक्षर करना

विकसित राष्ट्रों की तुलना में भारत में साक्षरता दर कम है और इसका असर वित्तीय साक्षरता पर भी पड़ता है। विश्व में आई सूचना क्रांति के कारण बैंकिंग एवं आर्थिक जगत में नए तकनीकयुक्त उत्पादों का सृजन हो रहा है

और साइबर अपराधी अपने आप को इस क्षेत्र में विकसित कर रहे है। अतः इस क्षेत्र में आम आदमी एवं सामान्य जनता को साक्षर किए जाने की आवश्यकता है ताकि वे किसी धोखाधड़ी का शिकार होने से बच सकें।

निष्कर्ष

अंत में, यह निष्कर्ष निकाला जा सकता है कि 21 वीं सदी के वर्तमान कंप्यूटर युग में इंटरनेट ने मानव जीवन के हर पहलू को प्रभावित किया है और कोई भी कंप्यूटर के उपयोग के बिना जीवन के बारे में सोच भी नहीं सकता है। इसलिए, वर्तमान परिदृश्य में यह अत्यधिक वांछनीय है कि आपराधिक माध्यमों द्वारा इसके दुरुपयोग के बजाय कंप्यूटर प्रौद्योगिकी को समाज की प्रगति और समृद्धि के लिए संरक्षित किया जाना चाहिए।

इंटरनेट एवं साइबरस्पेस लोगों को ऐसे असंख्य लेन-देन करने में सक्षम बनाता है जो व्यापार को बढ़ावा दे सकते हैं, इसे सुविधाजनक बना सकते हैं और ज्ञान की दुनिया तक पहुंच प्रदान कर सकते हैं। कुछ कमियों के बावजूद ये साइबर कानून साइबर अपराधों के खिलाफ आवश्यक सुरक्षा प्रदान करते हैं। फिर भी, अधिनियमों में सुधार की व्यापक गुंजाइश है और इन प्रावधानों के प्रभावी क्रियान्वयन के साथ-साथ प्रभावी प्रावधानों की आवश्यकता है। साइबर अपराध के खिलाफ जंग तो शुरू हो चुकी है लेकिन इन पर सख्ती से अंकुश लगाने के लिए यथोचित कानूनी हथियारों की जरूरत है।

परिवर्तन ही संसार का नियम है और समय के साथ-साथ नए-नए आविष्कारों का सृजन होता है और साइबर जगत इससे अछूता नहीं है। तकनीक का विकास निरंतर होता है और इसी कारणवश इससे संबंधित कानूनों में समय-समय पर संशोधन या नए कानूनों की आवश्यकता होती हैं। अतः हमें आवश्यक दूरदृष्टि रखकर और लोकहित को ध्यान में रखकर प्रासंगिक कानूनों का निर्माण करना है और यह समग्र राष्ट्र के विकास में निहित होता है।

संदर्भ:

1. भारतीय दंड संहिता, 1860
2. सूचना प्रौद्योगिकी अधिनियम, 2000

*****

पूनम कुमारी प्रसाद

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- यूको बैंक
मोबाइल नं. :- 9903434911
ई-मेल:- zovaranasi.ol@ucobank.co.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

हम जितनी तेजी से डिजिटल दुनिया की ओर बढ़ रहे हैं, ठीक उतनी ही तेजी से साइबर अपराध की संख्या में भी वृद्धि हो रही है। जिस गति से तकनीक ने उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। एक ही जगह पर बैठकर इंटरनेट के जरिये मनुष्य की पहुंच विश्व के हर कोने तक आसान हुई है। आज के समय में हर वो चीज जिसके विषय में इंसान सोच सकता है, उस तक उसकी पहुंच इंटरनेट के माध्यम से हो सकती है, जैसे कि सोशल नेटवर्किंग, ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब इत्यादि। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।

वर्तमान में भारत की बड़ी आबादी सोशल नेटवर्किंग साइट्स का उपयोग करती है। भारत में सोशल नेटवर्किंग साइट्स के उपयोग के प्रति लोगों में जानकारी का अभाव है। इसके साथ ही अधिकतर सोशल नेटवर्किंग साइट्स के सर्वर विदेश में हैं, जिससे भारत में साइबर अपराध घटित होने की स्थिति में इनकी जड़ तक पहुंच पाना कठिन होता है।

साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था। साइबर अपराधों के मामलों में भारत भी उन देशों से पीछे नहीं है जहां साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है। साइबर अपराध के मामलों में एक साइबर अपराधी किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के लिए कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध है।

इसमें कोई संशय नहीं है कि यह एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिये कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहां इनके (कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क) जरिये ऐसे अपराधों को अंजाम दिया जाता है वहीं इन्हें लक्ष्य बनाते हुए इनके विरुद्ध अपराध भी किया जाता है।

ऐसे अपराध में साइबर जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फिशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियां शामिल हैं। गौरतलब है कि सॉफ्टवेयर चोरी भी साइबर अपराध का ही एक रूप है, जिसमें यह जरूरी नहीं है कि साइबर अपराधी, ऑनलाइन पोर्टल के माध्यम से ही अपराध करे।

साइबर विशेषज्ञों के अनुसार, अपराध की श्रेणी को दो वर्गों में विभाजित किया जा सकता है-

- वे अपराध जिनमें कंप्यूटर पर हमला किया जाता है। इस तरह के अपराधों के उदाहरण हैकिंग, वायरस हमले आदि हैं।
- वे अपराध जिनमें कंप्यूटर को एक हथियार/उपकरण के रूप में उपयोग किया जाता है। इस प्रकार के अपराधों में साइबर आतंकवाद, आईपीआर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी आदि।

साइबर अपराध के अंतर्गत 3 प्रमुख श्रेणियां आती हैं जिसमें व्यक्ति विशेष, संपत्ति और सरकार के विरुद्ध अपराध शामिल हैं।

- **व्यक्ति विशेष के विरुद्ध साइबर अपराध:-** ऐसे अपराध, यद्यपि ऑनलाइन होते हैं परंतु वे वास्तविक लोगों के जीवन को प्रभावित करते हैं। इनमें से कुछ अपराधों में साइबर उत्पीड़न और साइबर स्टॉकिंग का वितरण, विभिन्न प्रकार के स्पूफिंग, क्रेडिट कार्ड धोखाधड़ी, मानव तस्करी, पहचान की चोरी और ऑनलाइन बदनाम किया जाना शामिल हैं। साइबर अपराध की इस श्रेणी में किसी व्यक्ति या समूह के खिलाफ दुर्भावनापूर्ण या अवैध जानकारी को ऑनलाइन लीक कर दिया जाता है।
- **संपत्ति विशेष के विरुद्ध साइबर अपराध:-** कुछ ऑनलाइन अपराध संपत्ति के खिलाफ होते हैं, जैसे कि कंप्यूटर या सर्वर के खिलाफ या उसे जरिया बनाकर किये जाते हैं। इन अपराधों में हैकिंग, वायरस ट्रांसमिशन, साइबर और टाइपो स्क्वाटिंग, कॉपीराइट उल्लंघन, आईपीआर उल्लंघन आदि शामिल हैं। उदाहरण- कोई आपको एक वेब-लिंक भेजे, जिस पर क्लिक करने के पश्चात एक वेब पेज खुले जहां आपसे आपके बैंक खाते/गोपनीय दस्तावेजों संबंधित सारी जानकारी मांगी जाए और ऐसा कहा जाए कि यह जानकारी रिज़र्व बैंक ऑफ़ इंडिया या सरकार की ओर से मांगी जा रही है, आप वहां सारी जानकारी दे दें और फिर उस जानकारी के इस्तेमाल से आपके दस्तावेज़ एवं बैंक खाते के साथ छेड़छाड़ की जाए, तो यह संपत्ति के विरूद्ध साइबर हमला कहा जायेगा।
- **सरकार विशेष के विरुद्ध साइबर अपराध:-** यह सबसे गंभीर साइबर अपराध माना जाता है। सरकार के खिलाफ किये गए ऐसे अपराध को साइबर आतंकवाद के रूप में भी जाना जाता है। सरकारी साइबर अपराध में सरकारी वेबसाइट या सैन्य वेबसाइट को हैक किया जाना शामिल हैं। गौरतलब है कि जब सरकार के खिलाफ एक साइबर अपराध किया जाता है, **तो इसे उस राष्ट्र की संप्रभुता पर हमला और युद्ध की कार्रवाई माना जाता है**। ये अपराधी आमतौर पर आतंकवादी या अन्य शत्रु देशों की सरकारें होती हैं। इस प्रकार के साइबर अपराधों पर नियंत्रण के लिये प्रत्येक देश की सरकार द्वारा कठोर साइबर कानून बनाए गए हैं।

साइबर अपराधों को बढ़ावा देने में सोशल मीडिया की भूमिका भी अति संवेदनशील हो चुकी है। बड़े पैमाने पर सोशल नेटवर्किंग साइट्स का उपयोग करने वाली जनसंख्या साइबर अपराध के खतरों से अनजान है। विभिन्न सोशल नेटवर्किंग साइट्स के सर्वर अन्य देशों में केंद्रित हैं, जिससे यह डर रहता है कि कहीं ये देश लोगों की व्यक्तिगत जानकारी का दुरुपयोग न करें।

- विभिन्न सोशल नेटवर्किंग साइट्स पर लोग अपनी व्यक्तिगत जानकारियां साझा करते हैं, जिससे हैकर्स इन सोशल नेटवर्किंग एकाउंट्स को आसानी से हैक कर लेते हैं और फिर प्राप्त सूचना का दुरुपयोग करते हैं।
- लोगों को सोशल नेटवर्किंग साइट्स पर हैकर्स ऑनलाइन ठगी का शिकार बनाते हैं।
- सुरक्षा एजेंसियों द्वारा यह भी पता लगाया गया है कि ऑनलाइन मुद्रा स्थानांतरित करने वाले विभिन्न ऐप के माध्यम से आतंकवादियों और देशविरोधी तत्वों को फंडिंग की जाती है।

- साइबर अपराधी विभिन्न ऑनलाइन गेम्स के माध्यम से बच्चों को अपराध करने के लिये प्रोत्साहित करते हैं।

साइबर अपराधों से निपटने के लिए कई स्तरों पर नीतियों का निर्माण कर प्रभावी उपाय किए गए हैं:-

वैधानिक उपाय

- भारत में 'सूचना प्रौद्योगिकी अधिनियम, 2000' पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिये पर्याप्त हैं। सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएं 43, 43ए, 66, 66बी, 66सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए और 74 हैकिंग और साइबर अपराधों से संबंधित हैं।
- सूचना प्रौद्योगिकी अधिनियम, 2000 (2008 में संशोधित) को साइबर सुरक्षा के लिए डेटा पहुंच प्रदान करने, इलेक्ट्रॉनिक डेटा इंटरचेंज के माध्यम से किए गए लेन-देन के लिए कानूनी ढांचा प्रदान करने आदि उद्देश्यों से अधिनियमित किया गया था। प्रमाणन प्राधिकरणों के कामकाज को लाइसेंस प्रदान करने और विनियमित करने के लिए इस अधिनियम के तहत प्रमाणन प्राधिकरणों हेतु एक नियंत्रक स्थापित किया गया है जो उपयोगकर्ताओं के इलेक्ट्रॉनिक प्रमाणीकरण के लिए डिजिटल हस्ताक्षर प्रमाणपत्र जारी करता है।
- राष्ट्रीय साइबर सुरक्षा नीति 2013: यह नीति निम्नानुसार प्रस्तावित करती है।
  - सभी साइबर सुरक्षा मामलों को समन्वित करने के लिए एक राष्ट्रीय नोडल एजेंसी के साथ खतरों के विभिन्न स्तरों से निपटने के लिए विभिन्न निकायों की स्थापना करना। एक राष्ट्रीय महत्वपूर्ण सूचना मूल संरचना संरक्षण केंद्र का सृजन।
  - मानक सुरक्षा प्रथाओं और प्रक्रियाओं को अपनाने के लिए व्यवसायों को वित्तीय लाभ प्रदान करना।
  - देश में उपयोग में आने वाले उपकरणों की सुरक्षा की नियमित जांच करने के लिए परीक्षण प्रयोगशालाएं स्थापित करना।
  - देश में एक सुरक्षित साइबर पारिस्थितिकी तंत्र सृजित करना तथा तकनीकी एवं प्रचालन सहयोग के माध्यम से प्रभावी सार्वजनिक-निजी भागीदारी और सहयोगात्मक सहभागिता विकसित करना।
  - अनुसंधान के माध्यम से स्वदेशी सुरक्षा प्रौद्योगिकियों का विकास करना।
- देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय के तहत भारत सरकार की डिजिटल इंडिया मुहिम का एक हिस्सा है।
- जनवरी 2020 में गृह मंत्रालय द्वारा साइबर क्राइम से निपटने के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Coordination Centre-I4C) का उद्घाटन किया गया है। इस योजना को संपूर्ण भारत में लागू किया गया है। साइबर क्राइम से बेहतर तरीके से निपटने के लिए तथा I4C को समन्वित और प्रभावी तरीके से लागू करने हेतु इस योजना के निम्नलिखित सात प्रमुख घटक हैं-
  - नेशनल साइबरक्राइम थ्रेट एनालिटिक्स
  - नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल
  - संयुक्त साइबर अपराध जांच दल के लिए मंच
  - राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र
  - राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र
  - साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट
  - राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र

अंतर्राष्ट्रीय उपाय

- साइबर - कूटनीतिः भारत सरकार ने संयुक्त राज्य अमेरिका, यूरोपीय संघ और मलेशिया जैसे देशों के साथ साइबर सुरक्षा सहयोग हेतु विभिन्न कदम उठाए हैं। उदाहरण के लिए- US-इंडिया साइबर रिलेशनशिप फ्रेमवर्क।
- ग्लोबल कांफ्रेंस ऑन साइबर स्पेस - ग्लोबल कांफ्रेंस ऑन साइबर स्पेस में भाग लेना यह एक प्रतिष्ठित वैश्विक कार्यक्रम है, जिसमें अंतराष्ट्रीय नेता, नीति निर्माता, उद्योग विशेषज्ञ, थिंक टैंक, साइबर विशेषज्ञ इत्यादि साइबर स्पेस का अधिकतम उपयोग करने के लिए मुद्दों और चुनौतियों पर विचारविमर्श करने के लिए एकत्रित होते हैं।
- ग्लोबल सेंटर फॉर साइबर सिक्योरिटी: इसे विश्व आर्थिक मंच (WEF) द्वारा भविष्य की परिस्थितियों में साइबर सुरक्षा के लिए प्रयोगशाला और अर्ली वार्निंग थिंक टैंक के रूप में कार्य करने तथा एक सुरक्षित वैश्विक साइबर स्पेस के निर्माण में सहायता करने हेतु प्रारंभ किया गया था।
- बुडापेस्ट कन्वेंशन साइबर क्राइम पर एक कन्वेंशन है जिसे साइबर अपराध पर बुडापेस्ट कन्वेंशन के नाम से जाना जाता है। यह अपनी तरह की पहली ऐसी अंतर्राष्ट्रीय संधि है जिसके अंतर्गत राष्ट्रीय कानूनों को सुव्यवस्थित करके, जांच-पड़ताल की तकनीकों में सुधार करके तथा इस संबंध में विश्व के अन्य देशों के बीच सहयोग को बढ़ाने हेतु इंटरनेट और कंप्यूटर अपराधों पर रोक लगाने संबंधी मांग की गई है।
- कन्वेंशन का अनुच्छेद 32B डेटा तक पहुंच की अनुमति देता है और इस प्रकार यह राष्ट्रीय संप्रभुता का उल्लंघन करता है, इसलिये भारत ने अभी तक इस पर हस्ताक्षर नहीं किए हैं।

सरकार द्वारा किए गए अन्य उपाय

- नेशनल एसोशिएसन ऑफ सॉफ्टवेयर एंड सर्विस कंपनी (नेसकॉम) ने अपनी साइबर प्रयोगशालाओं में साइबर फोरेंसिक टूल्स और पद्धतियों के उपयोग में हाल के रुझानों पर ध्यान केंद्रित करने के साथ उन्नत प्रशिक्षण कार्यक्रम प्रारंभ करने की योजना बनाई है।
- साइबर प्रतिरोधी क्षमताओं को और मजबूत किया जाना। साइबर प्रतिरोध दो प्रकार का होता है - रक्षात्मक और आक्रामक। भारत को विभिन्न देशों द्वारा अपनाए गए आक्रामक साइबर सिद्धांत का उचित आकलन करने की आवश्यकता है। ये 'साइबरवेपन्स' नामक सॉफ्टवेयर के बिट्स बनाकर आक्रामक क्षमताओं का संग्रहण कर रहे हैं ताकि विरोधी नेटवर्क को अत्यधिक नुकसान पहुंचाया जा सके।
- वर्तमान में साइबर स्पेस संबंधी बेहतर विनियमन और मानदंडों को अपनाने की आवश्यकता है। साइबर स्पेस संबंधी व्यवहारिक रूप से स्वीकार्य कोई भी मानदंड नहीं है। अतः राज्य के साथ-साथ विभिन्न कंपनियां भी अपनी क्षमताओं का विकास कर रही हैं। इससे सम्पूर्ण साइबर स्पेस को अस्थित करने की क्षमता रखने वाले आक्रामक साइबर उपकरणों और पद्धतियों का अनियंत्रित प्रसार हो रहा है।
- विभिन्न संस्थानों के मध्य आवश्यक समन्वय करने और साइबर प्रतिरोध सहित समन्वित दृष्टिकोण विकसित करने हेतु राष्ट्रीय साइबर सुरक्षा को ऑर्डिनेटर (एनसीसी) सुदृढ़ बनाया जा सकता है।
- व्यवसायों द्वारा साइबर सुरक्षा में निवेश को बढ़ावा देना वर्तमान में सुरक्षा बजट का केवल एक छोटा हिस्सा कंपनियों द्वारा आईटी सुरक्षा के लिए उपयोग किया जा रहा है।
- सरकार द्वारा 'कंप्यूटर इमरजेंसी रिस्पॉन्स टीम की स्थापना की गई जो कंप्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।

- भारत में 2025 तक साइबर सुरक्षा क्षेत्र में लगभग दस लाख रोजगारों के अवसर के सृजन का अनुमान है। इन अवसरों का अन्य देशों के पेशेवरों से संरक्षण और भारतीयों को इनका लाभ प्राप्त करने में सक्षम बनाने हेतु भारत को आवश्यक कौशल विकास हेतु उचित परिवेश स्थापित करना होगा। आईटी पेशेवरों की एक रिपॉजिटरी के रूप में एक राष्ट्रीय साइबर रजिस्ट्री के विचार को भी लागू किया जा सकता है।
- भारत में साइबर इंश्योरेंस: उद्योग के अनुमानों के अनुसार अभी तक भारत में 300-400 साइबर पॉलिसियां ही बेची गई हैं। भारत में साइबर इंश्योरेंस की औसत लागत लगभग 7.5 मिलियन डॉलर है। हालांकि, विकसित देशों की तुलना में यह अभी भी 20-25% कम है। इस क्षेत्र के द्वारा सामना की जाने वाली चुनौतियों में शामिल हैं- विश्वसनीयता संबंधी मुद्दे, प्रतिभा की कमी, प्रौद्योगिकी को वृहद पैमाने पर स्वीकार करने की आवश्यकता।

भारत इंटरनेट का तीसरा सबसे बड़ा उपयोगकर्ता है और हाल के वर्षों में साइबर अपराध कई गुना बढ़ गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिये सरकार की ओर से कई कदम उठाए गए हैं। कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी अतः भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा। वहीं दूसरी ओर सोशल मीडिया ने अभिव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है, आज प्रत्येक व्यक्ति बिना किसी डर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हजारों लोगों तक पहुंचा सकता है, परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी तथा साइबर अपराध के गंभीर खतरों से बचा सकता है।

*****

प्रवीण भाटी

पदनाम:- रोकड़िया
संस्था का नाम:- बैंक ऑफ इंडिया
मोबाइल नं. :- 9829665753
ई-मेल:- paryog@rediffmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

"अपराध मानवीय समूहों के व्यवहार के आदर्श नियमाचारों का उल्लंघन हैं"

---------- थोर्सटन सेलिन

मनुष्यता के इतिहास के साथ अपराध भी जुड़े रहे हैं। एक सभ्य समाज के साथ-साथ अपराध भी निरंतर बढ़ रहे हैं। समय और परिस्थितियों के अनुसार अपराधों में भी परिवर्तन होता रहा है। प्रौद्योगिकी और इलेक्ट्रॉनिक मीडिया के विकास के बाद कंप्यूटर से संबंधित अपराधों का जन्म हुआ है जिसे आमतौर पर "साइबर अपराध" कहा जाता है। साइबर अपराध एक नई चुनौती के रूप में विश्वभर के सामने आए हैं। यह अपराध अजीब है अपराधी शारीरिक रूप से उपस्थित हुए बिना गुमनाम रूप से और पीड़ित से बहुत दूर रहकर अपराध कर देता है। ये साइबर अपराधी पकड़े जाने के भय के बिना दूर से ही किसी अपराध को कुशलता से कार्यान्वित कर देते हैं।

साइबर अपराध :- 'साइबर अपराध' शब्द संसद द्वारा अधिनियमित किसी भी क़ानून या अधिनियम में कहीं भी परिभाषित नहीं है। यह पारंपरिक अपराध की अवधारणा से मौलिक रूप से अलग नहीं है क्योंकि दोनों में आचरण शामिल हैं चाहे वह कार्य हो या लोप, जो कानून के उल्लंघन का कारण बनता है और इसलिए यह दंडनीय है। साइबर अपराध में कंप्यूटर का उपयोग या तो एक उपकरण, लक्ष्य या आगे अपराध करने के साधन के रूप में होता है। इसमें तकनीक के माध्यम से किसी भी व्यक्ति की निजी जानकारी को प्राप्त करना और उसका गलत इस्तेमाल करना, किसी की भी निजी जानकारी को बिना अनुमति के ही कंप्यूटर से निकाल लेना या चोरी कर लेना भी साइबर अपराध है।

बैंकिंग में साइबर अपराधों के स्वरुप :-

स्पैम ई-मेल- इसमें साइबर अपराधी बैंक के हजारों खाताधारको को ई-मेल भेजते हैं जिसका उद्देश्य खाताधारकों के कंप्यूटर को नुकसान पहुंचाना होता है। उन ई-मेल से खाताधारको के कंप्यूटर में खराबी आ जाती है, इससे बैंक की प्रतिष्ठा को भी नुकसान होता है। बैंक के प्रति खाताधारकों के विश्वास में कमी आती है।

फर्जी बैंक कॉल - आपको जाली ई-मेल, मैसेज या फोन कॉल प्राप्त हो जो आपकी बैंक जैसा लगे जिसमें आपसे साइबर अपराधी द्वारा बैंक का अधिकारी/ कर्मचारी बन कर पूछा जाता है कि आपके एटीएम नंबर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपका खाता बन्द कर दिया जायेगा या इस लिंक पर सूचना दें। याद रखें किसी भी बैंक द्वारा ऐसी जानकारी कभी भी इस तरह से नहीं मांगी जाती है और भूलकर भी अपनी ऐसी किसी भी जानकारी को इन्टरनेट या फोनकॉल या मैसेज के माध्यम से नहीं बताएं। इस संबध में बैंक द्वारा समय-समय पर सभी खाताधारको को दिशानिर्देश जारी किए जाते हैं लेकिन फिर

भी ग्राहक साइबर अपराधियों के झांसे में आ जाते हैं और सबसे बड़ी गलती यह है कि इसकी समय पर रिपोर्ट नहीं करते इसके लिए सभी से निवेदन हैं कि यदि ऐसी कोई घटना हो जाये तो बिना विलम्ब किए 155260 पर कॉल कर अपनी रिपोर्ट दर्ज करा सकते हैं, जिससे वसूली की सम्भावना अधिक रहती है।

हैकिंग- इसमें साइबर अपराधी खाताधारक की निजी जानकारी को हैक करता है जैसे कि इन्टरनेट बैंकिंग के उपयोगकर्ता नाम या पासवर्ड और फिर उसमें फेर बदल कर देता है और उपलब्ध राशि का हस्तांतरण अपने खाते में कर देता है ।

साइबर फिशिंग- इसमें साइबर अपराधी खाताधारक को आकर्षक स्पैम ई-मेल भेजता है ताकि वो अपनी निजी जानकारी दे और उस जानकारी से उसका नुकसान हो सके।

साइबर धोखाधड़ी - आजकल विभिन्न अन्य माध्यमों से साइबर अपराध होते जा रहे हैं और खाताधारकों को चुना लगाया जा रहा है, इन साइबर अपराधियों की हिम्मत की भी दाद देनी पड़ेगी इनके हाथ सांसद महोदयों के बैंक खाते तक भी पहुंच गये हैं तो इससे आम आदमी भला कैसे सुरक्षित रह पायेगा।

बैंकिंग में साइबर अपराधों हेतु अपनाये गए सुरक्षात्मक उपाय:- आज के आधुनिक दौर में सभी बैंक द्वारा खाताधारकों को कई सुविधाएं घर बैठे-बैठे ही दी जा रही हैं जैसे - इन्टरनेट बैंकिंग, फोन बैंकिंग आदि जिससे समय की काफी बचत होती है और भीड़-भाड से दूर भी रहा जा सकता है, हाल ही में आई विश्व की सबसे भयानक महामारी कोविड -19 में भी यह ऑनलाइन सुविधाएं बहुत उपयोगी और कारगर साबित हुईं। इन सुविधाओं के उपयोग के साथ-साथ उपयोगकर्ताओं को कुछ सुरक्षात्मक उपायों को भी ध्यान रखना होगा:-

1. बैंक द्वारा जारी इन्टरनेट बैंकिंग उपयोग हेतु आई.डी. और पासवर्ड, टी-पिन, ई-पिन किसी भी व्यक्ति के साथ साझा न करें, यदि किन्ही विशेष प्रयोजन हेतु साझा करें तो भी उन्हें तुरंत अद्यतन कर लें।
2. अपने टेलीफोन नं., जन्मतिथि या अपने वाहन संख्या के आधार पर पासवर्ड कभी न बनाएं क्योंकि ऐसे पासवर्ड को हैक करना अत्यंत सरल हो जाता है।
3. नियमित अन्तराल पर अपने पासवर्ड बदलते रहें।
4. पासवर्ड को लम्बा रखें और उनमें अक्षर, संख्या और विशिष्ठ चिह्न का समावेश कर उन्हें एक योजक कुंजी के रूप में उपयोग करें।
5. आपके डिवाइस पर फायरवॉल का अवश्य उपयोग करें।
6. समय-समय पर बैंक द्वारा अपने खाताधारकों को सेमिनार, प्रेजेंटेशन के माध्यम से जागरूक किया जाये।
7. सबसे आवश्यक होता है वन टाइम पासवर्ड (ओ.टी.पी.), वो कभी भी किसी को न बताएं। यह अंतिम सुरक्षा चक्र होता है आपके खाते से निकासी का।
8. सभी ग्राहकों को यह सूचित करें कि ऐसी किसी भी अपरिहार्य घटना यदि जाने-अनजाने में हो भी जाए तो 72 घन्टे के भीतर बैंक को सूचित करें जिससे वसूली सरलता से हो सके।

कानूनी प्रावधान :- सूचना तकनीक कानून, 2000 की धारा 1 (2) के अनुसार, उल्लिखित अपवादों को छोड़कर इस कानून के प्रावधान पूरे देश में प्रभावी हैं। साथ ही उपरोक्त उल्लिखित प्रावधानों के अंतर्गत देश की सीमा से बाहर किए गए किसी अपराध की हालत में भी उक्त प्रावधान प्रभावी होंगे और ऐसे अपराधियों को पकड़ने के लिए विश्व स्तर पर समिति का गठन कर उन तक पहुंचना होगा।

उपसंहार :- भारत इन्टरनेट का तीसरा सबसे बड़ा उपयोगकर्ता है, आज के समय में सभी बैंकों के लिए यह आवश्यक कदम है कि वे अपने ग्राहकों को साइबर अपराधों से कैसे बचाएं। इसके लिए बैंकिंग नियामक रिज़र्व बैंक का निर्देश कहता है कि अगर आपके बैंक खाते से अवैध निकासी की जाती है तो तीन दिन के अंदर अगर बैंक को इसकी शिकायत की जाए तो ग्राहक को कोई नुकसान नहीं उठाना पड़ेगा। बशर्ते थर्ड पार्टी धोखाधड़ी बैंक या ग्राहक की चूक की वजह से नहीं, बल्कि बैंकिंग सिस्टम की किसी चूक की वजह से हुई हो। इसके साथ ही शिकायत की समय सीमा के अनुपात में बैंक की देनदारी तय की गई है। गृह मंत्रालय ने भी साइबर फ्रॉड से जुड़ी शिकायतों के निपटारे के लिए एक केंद्रीकृत हेल्पलाइन नंबर जारी किया हुआ है। इसका संचालन संबंधित राज्य की पुलिस द्वारा किया जाता है, सरकार की मानें तो इस हेल्पलाइन के जरिए बैंक तथा पुलिस को आपस में कनेक्ट होकर रियल टाइम एक्शन में मदद मिलेगी. शायद इसलिए कहते हैं, "ऐसी कोई भी व्यवस्था तब कारगर होगी जब तय समय-सीमा के अंदर फ्रॉड के संबंध में पता चल जाए। यहां तो पता ही तब चलता है जब समय बीत जाता है। इस परिस्थिति में शिकायतों का समाधान कैसे होगा।" जाहिर है, ऐसी घटनाओं को रोकने और ग्राहकों को अपराधियों से होने वाले नुकसान से बचाने के लिए बैंकिंग व्यवस्था में बदलाव की जरूरत है और इसके लिए आर्टिफीसियल इंटेलिजेंस और रोबोटिक्स की मदद ली जा सकती है। कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण बैंकों द्वारा साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निभर करेगी। अतः बैंक को इस क्षेत्र में तीव्रगति से कार्य करना होगा।

याद रखिये सबसे बड़ा अपराध,
अन्याय सहना
और
उसके खिलाफ आवाज नहीं उठाना।

- नेताजी सुभाष चन्द्र बोस

*****

रजनी बाला

पदनाम:- सहायक प्रबंधक
संस्था का नाम:- इण्डियन ओवरसीज़ बैंक
मोबाइल नं. :- 9416804040
ई-मेल:- rajnibala@iobnet.co.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

भारत देश में डिजिटल इंडिया अभियान वर्ष 1 जुलाई, 2015 में शुरू हुआ जिसका मुख्य उद्देश्य दूर-दराज़ के गांवों में इन्टरनेट के प्रयोग को बढ़ावा देना था क्योंकि देश की जनसंख्या का एक बहुत बड़ा भाग अधिकतर गांवों में ही निवास करता है। डिजिटल इंडिया के विकास में आजकल सब एक ही चीज़ से जुड़े हैं और वो है मोबाइल और तकनीक। आजकल बहुत से मुफ्त एप मौजूद हैं, जिन्हें अपने मोबाइल में डाउनलोड करने पर व्यक्तिगत जानकारी लेते हैं और **मुफ्त** - यह शब्द जहां हमने पढ़ा नहीं कि कूद पड़े लाइन में।

हम मुफ्त के एप डाउनलोड करके अपनी सारी निजी जानकारी विदेशी कंपनियों को मुफ्त में दे रहे हैं। हमारी जानकारी को बेचने का एक बड़ा बाजार है। एक अनुमान के मुताबिक एड बाजार की इकॉनमी कुछ 3–4 ट्रिलियन डॉलर्स सालाना है और इसमें कोई प्रोडक्ट नहीं बिकता, कोई सर्विस नहीं मिलती सिर्फ आपका डेटा बिकता है।

जब भी आप कोई एप डाउनलोड करते हैं तो उसमें आप अपना फोन नंबर और ई-मेल एड्रेस और व्यक्तिगत जानकारी डालते हैं और फिर आप उसके ग्राहक हो जाते हैं। अब वो एप वाली कंपनी इस डेटा को आगे दूसरी कंपनियों को मोटे दामों में बेच देती है। जो कंपनी इस डेटा को खरीदती है, वो पहले इसको (डेटा) अपने हिसाब से अलग करती है। इसमें अलग-अलग ग्रुप बनाए जाते हैं उम्र के हिसाब से, पसंद के हिसाब से आदि और फिर यह कंपनी अपने कच्चे ख़रीदे हुए डेटा को "रिफाइन" करके आगे बेचती है।

अब बात करते हैं दूसरे तरीके की। ज़्यादातर लोग फेसबुक और अन्य वेबसाइट पर ढेर सारे पर्सनालिटी टेस्ट आदि करते हैं। उन्हें इस बात का ज़रा भी इल्म नहीं होता कि वो अपने हाथ से अपनी सारी जानकारी दूसरों को मुफ्त में दे रहे हैं।

इस प्रकार हमारी व्यक्तिगत जानकारी को बेचा जाता है ये जानकारियों नेटवर्क और कंप्यूटर से जुड़ी होती हैं और साइबर अपराध को जन्म देती हैं। इन अपराधों में संचार सेवाओं की चोरी, औद्योगिक जासूसी, साइबर स्पेस में अश्लील और आपत्तिजनक सामग्री का प्रसार, इलेक्ट्रोनिक मनी लॉन्ड्रिंग और कर चोरी, आतंकवाद से संबन्धित गतिविधियों आदि की एक लंबी सूची है। इन साइबर अपराधों की रोकथाम करना अत्यंत आवश्यक है।

वर्तमान में भारत की कुल अर्थव्यवस्था में 14-15 फीसदी हिस्सेदारी डिजिटल अर्थव्यवस्था की है और साल 2024 तक इसे 20 प्रतिशत तक पहुँचाने का लक्ष्य है। इसके लिए सरकार डिजिटल इंडिया और कैशलेस अर्थव्यवस्था की तरफ कदम बढ़ा रही है, जबकि दूसरी तरफ साइबर सुरक्षा पर खतरा दिनोंदिन बढ़ता जा रहा है।

इंटरनेट उपभोक्ताओं के बढ़ने के साथ-साथ साइबर अपराध निरंतर बढ़ रहे हैं। साइबर स्पेस का खतरा कितना बड़ा है इसका अंदाजा इस बात से लगाया जा सकता है कि हमारे देश में पीएमओ से लेकर विदेश व रक्षा मंत्रालय, भारतीय दूतावासों, यहां तक की खुफिया एजेंसी- सीबीआई के कंप्यूटरों पर भी साइबर अटैक कर उनकी जासूसी हो चुकी है। राहत की बात यह है कि प्रधानमंत्री नरेंद्र मोदी ने देश में नई साइबर नीति लाने की घोषणा की है। इंटरनेट ऑफ थिंग्स, क्लाउड कम्प्यूटिंग, आर्टिफिशियल इंटेलिजेंस और 5 जी जैसी सूचना प्रौद्योगिकी के उपयोग बढने के साथ देश के लिए मजबूत समन्वित साइबर सुरक्षा व्यवस्था का होना बहुत जरूरी है।

भारत में साइबर कानून :

भारत में, साइबर कानून सूचना प्रौद्योगिकी अधिनियम, 2000 ("आईटी अधिनियम") में निहित हैं जो 17 अक्टूबर, 2000 को लागू हुए। अधिनियम का मुख्य उद्देश्य सरकार के पास रिकॉर्ड के इलेक्ट्रॉनिक कॉमर्स को कानूनी मान्यता प्रदान करना और इलेक्ट्रॉनिक फाइलिंग की सुविधा प्रदान करना है।

पिछले दो दशकों में भारत ने साइबर सुरक्षा की अनुकूलता पर ध्यान केंद्रित करते हुए संस्थागत मशीनरी तैयार करने का एक महत्त्वपूर्ण प्रयास किया है, साथ ही इस पहल का विस्तार कई सरकारी संस्थाओं तक है।

- प्रधानमंत्री कार्यालय के अंतर्गत ही कई साइबर पोर्टफोलियो शामिल हैं। राष्ट्रीय सुरक्षा परिषद भी इनमें से एक है, इसकी अध्यक्षता आमतौर पर राष्ट्रीय सुरक्षा सलाहकार (NSA) द्वारा की जाती है, और यह भारत की साइबर नीति पारिस्थितिकी तंत्र को आकार देने में महत्त्वपूर्ण भूमिका निभाती है।
- NSA द्वारा राष्ट्रीय सूचना बोर्ड की अध्यक्षता भी की जाती है, जो साइबर सुरक्षा नीति पर अंतर-मंत्रालयी समन्वय के लिये सर्वोच्च निकाय के रूप में कार्य करता है।
- राष्ट्रीय तकनीकी अनुसंधान संगठन के अंतर्गत जनवरी 2014 में स्थापित राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र को महत्त्वपूर्ण सूचना बुनियादी ढाँचे के संरक्षण का कार्य सौंपा गया है।
- वर्ष 2015 में भारतीय प्रधानमंत्री द्वारा राष्ट्रीय साइबर सुरक्षा समन्वयक कार्यालय की स्थापना की गई, जो प्रधानमंत्री को रणनीतिक साइबर सुरक्षा मुद्दों पर सलाह देता है।
- केंद्रीय इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MEITY) के अंतर्गत स्थापित कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In) गैर-प्राथमिकता वाले बुनियादी ढाँचे से जुड़े विभिन्न साइबर सुरक्षा खतरों से निपटने के लिये कार्य करती है।
- केंद्रीय रक्षा मंत्रालय द्वारा 'डिफेंस साइबर एजेंसी' की स्थापना के लिये डिफेंस इंफॉर्मेशन एश्योरेंस एंड रिसर्च एजेंसी को अपग्रेड किया गया है। DCA संयुक्त सशस्त्र अभियानों का समन्वय और नियंत्रण करने के लिये भारतीय सशस्त्र बलों की एक त्रि-सेवा कमान है, साथ ही यह भारत की साइबर नीति के निर्धारण में भी सहायक होगी।
- इसके अतिरिक्त केंद्रीय गृह मंत्रालय की निगरानी में कई समन्वय केंद्रों का संचालन किया जाता है जो साइबर अपराध, जासूसी और आतंकवाद के खातमे के लिये कानून प्रवर्तन प्रयासों पर ध्यान केंद्रित करते हैं। जबकि केंद्रीय विदेश मंत्रालय भारत की साइबर कूटनीति को दोनों रूपों में (द्विपक्षीय रूप से अन्य देशों के साथ, और संयुक्त राष्ट्र जैसे अंतर्राष्ट्रीय मंचों पर) समन्वित करता है।
- राष्ट्रीय साइबर सुरक्षा रणनीति 2020 : इस रणनीति को और अधिक कठिन ऑडिट प्रकिया के माध्यम से साइबर जागरूकता एवं साइबर सुरक्षा में सुधार के लिये तैयार किया गया है।
- नागरिकों के डेटा को सुरक्षित करने के लिये व्यक्तिगत डेटा संरक्षण विधेयक मसौदा, 2018।

- सभी प्रकार के साइबर अपराधों से व्यापक और समन्वित तरीके से निपटने के लिये अक्तूबर 2018 में भारतीय साइबर अपराध समन्वय केंद्र स्थापित करने की योजना को मंज़ूरी दी गई थी।
- भारतीय कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-In) सभी साइबर सुरक्षा प्रयासों, आपातकालीन प्रतिक्रियाओं और संकट प्रबंधन के समन्वय के लिये नोडल एजेंसी के रूप में कार्य करती है।
- राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre- NCIIPC) की स्थापना के साथ महत्त्वपूर्ण सूचना अवसंरचनाओं को संरक्षण प्रदान किया जाता है।

साइबर कानून का महत्व:

1. यह इंटरनेट पर सभी लेनदेन को कवर करता है।
2. यह इंटरनेट पर सभी गतिविधियों पर नजर रखता है।
3. यह साइबरस्पेस में हर क्रिया और हर प्रतिक्रिया को छूता है

साइबर कानून का क्षेत्र:

साइबर कानूनों में विभिन्न प्रकार के उद्देश्य होते हैं। कुछ कानून नियम बनाते हैं कि कैसे व्यक्ति और कंपनियां कंप्यूटर और इंटरनेट का उपयोग कर सकते हैं जबकि कुछ कानून लोगों को इंटरनेट पर अनैतिक गतिविधियों के माध्यम से अपराध का शिकार बनने से बचाते हैं। साइबर कानून के प्रमुख क्षेत्रों में शामिल हैं:

धोखा:

उपभोक्ता ऑनलाइन धोखाधड़ी से बचने के लिए साइबर कानूनों पर निर्भर हैं। पहचान की चोरी, क्रेडिट कार्ड की चोरी और ऑनलाइन होने वाले अन्य वित्तीय अपराधों को रोकने के लिए कानून बनाए गए हैं। उन्हें पीड़ित द्वारा लाई गई नागरिक कार्रवाई का भी सामना करना पड़ सकता है। साइबर वकील इंटरनेट का उपयोग करके धोखाधड़ी के आरोपों के खिलाफ बचाव और मुकदमा चलाने दोनों के लिए काम करते हैं।

कॉपीराइट:

इंटरनेट ने कॉपीराइट उल्लंघन को आसान बना दिया है। ऑनलाइन संचार के शुरुआती दिनों में, कॉपीराइट उल्लंघन बहुत आसान था। कॉपीराइट उल्लंघन साइबर कानून का एक क्षेत्र है जो व्यक्तियों और कंपनियों के अपने रचनात्मक कार्यों से लाभ प्राप्त करने के अधिकारों की रक्षा करता है।

मानहानि:

मानहानि कानून नागरिक कानून हैं जो व्यक्तियों को नकली सार्वजनिक बयानों से बचाते हैं जो किसी व्यवसाय या किसी की व्यक्तिगत प्रतिष्ठा को नुकसान पहुंचा सकते हैं। जब लोग इंटरनेट का उपयोग ऐसे बयान देने के लिए करते हैं जो नागरिक कानूनों का उल्लंघन करते हैं, तो इसे मानहानि कानून कहा जाता है।

उत्पीड़न और पीछा :

कभी-कभी ऑनलाइन बयान उन आपराधिक कानूनों का उल्लंघन कर सकते हैं जो उत्पीड़न और पीछा करने से मना करते हैं। जब कोई व्यक्ति ऑनलाइन किसी और के बारे में बार-बार धमकी भरे बयान देता है, तो नागरिक और आपराधिक दोनों कानूनों का उल्लंघन होता है।

अभिव्यक्ति की स्वतंत्रता:

अभिव्यक्ति की स्वतंत्रता साइबर कानून का एक महत्वपूर्ण क्षेत्र है। साइबर वकीलों को अपने मुवक्किलों को अश्लीलता को प्रतिबंधित करने वाले कानूनों सहित अभिव्यक्ति की स्वतंत्रता की सीमाओं के बारे में सलाह देनी चाहिए।

व्यापार के रहस्य:

ऑनलाइन कारोबार करने वाली कंपनियां अक्सर अपने व्यापार रहस्यों की सुरक्षा के लिए साइबर कानूनों पर निर्भर रहती हैं। उदाहरण के लिए, Google और अन्य ऑनलाइन खोज इंजन खोज परिणाम उत्पन्न करने वाले एल्गोरिदम को विकसित करने में बहुत समय व्यतीत करते हैं। साइबर कानून इन कंपनियों को अपने व्यापार रहस्यों की रक्षा के लिए आवश्यक कानूनी कार्रवाई करने में मदद करते हैं

भारत के साइबर सुरक्षा ढाँचे से जुड़ी चुनौतियां:

- **एकीकृत प्रतिक्रिया का अभाव**: राष्ट्रीय स्तर पर साइबर सुरक्षा खतरों का मुकाबला करने और उन्हें कम करने के लिये एक एकीकृत प्रतिक्रिया को लागू करने में प्रभावी समन्वय, उत्तरदायित्वों का अधिव्यापन और स्पष्ट संस्थागत सीमाओं व जवाबदेही की कमी जैसी चुनौतियों का सामना करना पड़ सकता है।
- **आवश्यक क्षमता का अभाव**: भारत में हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों व तकनीकों के मामले में स्वदेशी क्षमता (आत्मनिर्भरता) का अभाव है।
- यह भारत के साइबर क्षेत्र को शत्रु राष्ट्रों और अन्य अराजक समूहों द्वारा प्रेरित साइबर हमलों के लिये असुरक्षित बनाता है।
- भारत में यूरोपीय संघ के 'सामान्य डेटा संरक्षण विनियमन : (GDPR) या अमेरिका के 'क्लेरीफाइंग लॉफुल ओवरसीज़ यूज़ ऑफ डेटा (CLOUD) एक्ट' की तरह एक सक्रिय साइबर सुरक्षा ढाँचा नहीं है।
- **एक प्रभावी साइबर डिटरेंस रणनीति का अभाव**: इसके अतिरिक्त एक विश्वसनीय साइबर रणनीति के अभाव का अर्थ है कि राज्य प्रायोजित और गैर-राजकीय अराजक तत्त्वों को कई उद्देश्यों के लिये कम पैमाने पर साइबर हमलों का संचालन (जैसे-जासूसी, साइबर अपराध और महत्त्वपूर्ण सूचना अवसंरचनाओं के संचालन को बाधित करना आदि) करने के लिये प्रोत्साहन मिलता रहता है।
- भारतीय कंपनियां भी साइबर सुरक्षा चुनौतियों का सामना कर रहीं हैं, क्योंकि कोविड-19 के कारण कंपनियों के अधिकांश कर्मचारियों को 'वर्क फ्रॉम होम' मोड में स्थानांतरित कर दिया गया है।
- भारत में हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों में स्वदेशीकरण का अभाव है। यह भारत के साइबरस्पेस को राज्य और गैर-राज्य अभिकर्त्ताओं द्वारा प्रेरित साइबर हमलों के प्रति संवेदनशील बनाता है।

निष्कर्ष : इक्कीसवीं सदी में साइबर जासूसी, साइबर अपराध, साइबर आतंकवाद और साइबर युद्ध जैसे बढ़ते खतरे के साए में साइबर दुनिया को सुरक्षित बनाना आज विश्व के सामने बड़ी चुनौती बन गया है। सरकारी आंकड़ों के मुताबिक, इनमें सबसे ज्यादा अपराध फेसबुक के जरिए हुए। सरकार के खिलाफ आतंकी गतिविधियां करने हेतु इंटरनेट का प्रयोग करना व ई-मेल, ई-बैंकिंग आदि के द्वारा साइबर आतंकवाद को बढ़ावा देने संबंधी पहलू भी उजागर हो रहे हैं। जाहिर है साइबर सुरक्षा को मजबूत करना हमारी सबसे बड़ी चुनौती है। कैशलेस अर्थव्यवस्था में साइबर स्पेस में अस्थिरता का मतलब है आर्थिक अस्थिरता और कोई भी देश आर्थिक

अस्थिरता बर्दाश्त नहीं कर सकता। ऐसे परिदृश्य में समावेशी डिजिटल भारत के सपने को साकार करने के लिए कुशल और सुरक्षित साइबर इंफ्रास्ट्रक्चर की आवश्यकता है। ऐसी नीति विकसित करने की जरूरत है जो साइबर सुरक्षा क्षेत्र में कैरियर बनाने वाले छात्रों को भी प्रोत्साहित करें। शैक्षिक संस्थानों को साइबर सुरक्षा को पाठ्यक्रमों में शामिल करना चाहिये। साथ ही समय की मांग है कि देश के प्रमुख शहरों में साइबर अपराध से संबंधित मामलों के लिए विशेष साइबर न्यायालय की स्थापना भी की जाए। साइबर ठगों के बढ़ते हौसले का मुख्य कारण यह है कि देश में साइबर अपराधों को रोकने और अपराधियों को दंडित करने के लिए प्रभावी कानूनों का अभाव है। यह दुर्भाग्य की बात है कि देश में अभी भी साइबर अपराध गैर जमानती नहीं है और इसके लिए अधिकतम सजा तीन साल है। ऐसे में साइबर अपराध को गैर जमानती बनाने के साथ भारत में एक मजबूत साइबर सुरक्षा कानून की जरूरत है जो विभिन्न प्रकार के साइबर खतरों, हमलों और अपराधों से निपटने के लिए प्रभावी हों।

*****

विकास महांगरे

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- यूनियन बैंक ऑफ इंडिया
मोबाइल नं. :- 7775970978
ई-मेल:- vikas.mahangare@unionbankofindia.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

परिचय :

इंटरनेट की कंप्यूटरयुक्त दुनिया को साइबरस्पेस के रूप में जाना जाता है और इस क्षेत्र में प्रचलित कानूनों को साइबर कानून के रूप में जाना जाता है। इस स्थान के सभी उपयोगकर्ता इन कानूनों के दायरे में आते हैं क्योंकि यह एक प्रकार का विश्वव्यापी अधिकार क्षेत्र रखता है। साइबर कानून, कानून की वह शाखा है जो इंटरनेट, सूचना प्रौद्योगिकी के उपयोग से संबंधित कानूनी मुद्दों से संबंधित हैं। संक्षेप में, साइबर कानून कंप्यूटर और इंटरनेट को नियंत्रित करने वाला कानून है।

इलेक्ट्रॉनिक कॉमर्स के विकास को प्रभावी नियामक तंत्र की आवश्यकता है जो कानूनी बुनियादी ढांचे को और मजबूत करेगा। इलेक्ट्रॉनिक कॉमर्स की सफलता के लिए यह महत्वपूर्ण भी है। यह सभी तंत्र और कानूनी संरचनाएं साइबर कानून के दायरे में आती हैं। साइबर कानून महत्वपूर्ण हैं क्योंकि ये लेनदेन और गतिविधियों के लगभग सभी पहलुओं को छूता है जिसमें इंटरनेट, वर्ल्ड वाइड वेब और साइबर स्पेस शामिल हैं।

साइबर अपराध क्या है ?

साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था। साइबर अपराधों के मामलों में भारत भी उन देशों से पीछे नहीं है, जहां साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है।

साइबर अपराध के मामलों में एक साइबर अपराधी, किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के लिये कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध है।

इसमें कोई संशय नहीं है कि यह एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है, एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिये कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहां इनके (कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क) जरिए ऐसे अपराधों को अंजाम दिया जाता है वहीं इन्हें लक्ष्य बनाते हुए इनके विरुद्ध अपराध भी किया जाता है।

इंटरनेट और सोशल मीडिया का दुष्प्रभाव आर्थिक, सामाजिक, राजकीय क्षेत्र में भी बढ़ रहा है। साइबर अपराध का उद्देश्य ज्यादा तर आर्थिक लाभ तथा गलत तरीके से पैसा कमाने के लिए किया जाता है। इसके अलावा किसी की बदनामी के लिए भी ऐसे अपराध किए जाते हैं। ऐसे कुछ अपराध मानसिक विकृति से भी होते हैं।

भारत में साइबर कानून की प्रभावशीलता:

साइबर कानून में निम्नलिखित से संबंधित कानून शामिल हैं :

- साइबर अपराध
- इलेक्ट्रॉनिक और डिजिटल हस्ताक्षर
- बौद्धिक सम्पदा
- डेटा सुरक्षा और गोपनीयता

साइबर कानून इलेक्ट्रॉनिक दस्तावेजों को कानूनी मान्यता प्रदान करते हैं और ई-फाइलिंग और ई-कॉमर्स लेनदेन का समर्थन करने के लिए एक ढांचा प्रदान करते हैं। साइबर अपराधों को कम करने, रोकने के लिए एक कानूनी ढांचा भी प्रदान करते हैं। साइबर स्पेस में कंप्यूटर, नेटवर्क, सॉफ्टवेयर, डेटा स्टोरेज डिवाइस (जैसे हार्ड डिस्क, यूएसबी डिस्क, आदि), इंटरनेट, वेबसाइट, ई-मेल और यहां तक कि इलेक्ट्रॉनिक डिवाइस जैसे सेलफोन, एटीएम मशीन आदि शामिल हैं।

तालिका 1 : विविध माध्यमोंसे डिजिटल लेनदेन :

क्रम संख्या	अवधि	डिजिटल लेनदेन-संचयी (रु.करोड़ में)	भीम लेनदेन - संचयी (रु.करोड़ में)	डेबिट कार्ड - (रु.करोड़ में)
1	जुलाई -2021	17,688.98	5,234.73	1,822.56
2	अगस्त -2021	18,374.5	5,590.27	1,858.44
3	सितंबर -2021	19,050.27	5,955.69	1,893.34
4	अक्तूबर -2021	19,854.35	6,377.54	1,931.87
5	नवंबर -2021	20,671.21	6,796.18	1,968.31
6	दिसंबर -2021	21,519.12	7,252.8	2,005.96

(स्रोत: इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार)

आज इंटरनेट ने पूरी दुनिया में तूफान लाया है। विविध माध्यमों से डिजिटल लेनदेन बढ़ रहा है। *(तालिका 1)* खासकर कोरोना महामारी के बाद शिक्षा से लेकर बैंकिंग तक लगभग हर काम ऑनलाइन हो रहा है। इंटरनेट के बढ़ते इस्तेमाल के साथ साइबर क्राइम की दर भी बढ़ी है। साइबर अपराध कंप्यूटर और नेटवर्क के उपयोग द्वारा किया जाने वाला कोई भी अपराध है जहां कंप्यूटर का उपयोग हथियार के रूप में या लक्ष्य के रूप में किया जाता है।

भारत में साइबर कानून व साइबर कानून से संबंधित साइबर कानून एवं उनकी प्रभावशीलता :

सूचना प्रौद्योगिकी अधिनियम, 2000 और सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 :

संशोधन अधिनियम का उद्देश्य मौजूदा भारतीय साइबर कानून ढांचे में क्रांतिकारी परिवर्तन करना है। कई साइबर अपराध जिनके लिए सूचना प्रौद्योगिकी अधिनियम, 2000 में कोई स्पष्ट प्रावधान मौजूद नहीं थे, अब सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 में शामिल हो गए हैं। सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008 (आईटी अधिनियम 2008) भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी-इन) द्वारा प्रशासित है। भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) साइबर सुरक्षा घटनाओं को संबोधित करने के लिए एक राष्ट्रीय एजेंसी के रूप में कार्य करता है। सीईआरटी-इन के पास सूचनाओं की निगरानी, संग्रह, विश्लेषण और ब्लॉक करने की शक्तियां है।

राष्ट्रीय साइबर सुरक्षा रणनीति, 2020:

इसका लक्ष्य अधिक कड़े ऑडिट के माध्यम से साइबर जागरूकता और साइबर सुरक्षा में सुधार करना है।

राष्ट्रीय साइबर सुरक्षा नीति, 2013:

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी विभाग (डीईआईटीवाई) द्वारा एक नीति ढांचा है। इसका उद्देश्य साइबर हमलों से सार्वजनिक और निजी बुनियादी ढांचे की रक्षा करना है।

यदि सूचना प्रौद्योगिकी अधिनियम विशिष्ट साइबर अपराधों को कवर करने के लिए अपर्याप्त है, तो कानून प्रवर्तन एजेंसियां **भारतीय दंड संहिता (आईपीसी), 1860** धाराओं का सहारा ले सकती है।

भारतीय टेलीग्राफ अधिनियम, 1885:

भारतीय टेलीग्राफ अधिनियम काफी पुराना है। यह कानून एक अक्तूबर 1885 को लागू किया गया था हालांकि इसमें समय-समय पर संशोधन होते रहे हैं। भारतीय टेलीग्राफ अधिनियम, 1885 के तहत केंद्र सरकार या राज्य सरकार को आपातकाल में या लोक-सुरक्षा के हित में फोन संदेश को प्रतिबंधित करने एवं उसे टेप करने तथा उसकी निगरानी का अधिकार हासिल है।

"साइबर सुरक्षित भारत" पहल:

भारत में साइबर सुरक्षा प्रणाली को सुदृढ़ बनाने की आवश्यकता महसूस करते हुए तथा प्रधानमंत्री नरेंद्र मोदी के 'डिजिटल इंडिया' के विज़न के अनुरूप, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) द्वारा राष्ट्रीय ई-गवर्नेंस डिविज़न (एनईजीडी) एवं उद्योग जगत के सहयोग से साइबर सुरक्षित भारत पहल की घोषणा की गई। इसमें साइबर सुरक्षा के महत्त्व पर जागरूकता कार्यक्रम, सर्वश्रेष्ठ प्रचलनों पर कार्यक्रम की एक श्रृंखला तथा साइबर खतरों को प्रबंधित करने तथा इनमें कमी लाने के लिये साइबर सुरक्षा हेल्थ टूल किट्स के साथ अधिकारियों की सक्षमता जैसे पक्षों को शामिल किया गया है।

तालिका 2 :विभिन्न प्रकार की साइबर सुरक्षा घटनाएं :

साइबर सुरक्षा घटनाएं	**2020**
फ़िशिंग	280
अनधिकृत नेटवर्क स्कैनिंग /जांच/कमजोर सेवाएं	1028881
वायरस/ माल्यासीअस कोड	99986
वेबसाइट विरूपण	25969
वेबसाइट घुसपैठ और मैलवेयर प्रोपेगेशन	152
अन्य	2940
कुल	1158208

(स्रोत: कंप्यूटर इमरजेंसी रिस्पॉन्स टीम - इंडिया)

वर्ष 2020 में, सीईआरटी-इन ने 1158208 साइबर घटनाओं को संभाला। साइबर कानूनों के लागू होने के साथ भी, साइबर अपराध की दर में भारी वृद्धि हो रही है। *(तालिका 2)* । पुलिस साइबर अपराधों को हल करने के लिए जूझ रही है क्योंकि उनके सामने आने वाली चुनौतियों जैसे अंडररिपोर्टिंग, अपराध के अधिकार क्षेत्र, सार्वजनिक अज्ञानता और अपराध की जांच करने की बढ़ती प्रौद्योगिकी लागत। इसलिए, भारत में साइबर कानून में सुधारों की भी आवश्यकता है।

भारत में साइबर कानून में सुधारों की आवश्यकता :

साइबर हमलों को रोकने के लिए रीयल-टाइम इंटेलिजेंस की आवश्यकता है। रैंसमवेयर के समाधान के लिए समय-समय पर 'डेटा का बैकअप' जरूरी है । हमलों की भविष्यवाणी और सटीक पहचान के लिए आर्टिफिशियल इंटेलिजेंस (एआई) का उपयोग करना जरूरी है। प्रभावी साइबर सुरक्षा के लिए पहले ही हो चुके वास्तविक हमलों से प्राप्त ज्ञान और सीख का उपयोग करना जरूरी है । साइबर खतरों के बारे में जागरूकता बढ़ाना जिसके लिए सबसे पहले डिजिटल साक्षरता की आवश्यकता है। भारत को अपने कंप्यूटिंग वातावरण और इंटरनेट ऑफ थिंग्स को वर्तमान उपकरणों, पैच, अपडेट और सर्वोत्तम ज्ञात विधियों के साथ समयबद्ध तरीके से सुरक्षित करने की आवश्यकता है। यह सुधार साइबर कानून में करने की आवश्यकता है।

बैंकों और वित्तीय संस्थानों की सुरक्षा के लिए कड़े साइबर सुरक्षा मानकों को स्थापित करते हुए साइबर सुरक्षा, डेटा अखंडता और डेटा सुरक्षा क्षेत्रों में मुख्य कौशल विकसित किया जाए। यह राष्ट्रीय सुरक्षा का अभिन्न अंग है। डिजिटल अर्थव्यवस्था का महत्त्व बढ़ रहा है। आर्टिफिशियल इंटेलिजेंस , मशीन लर्निंग ,डेटा एनालिटिक्स, क्लाउड कंप्यूटिंग और इंटरनेट ऑफ थिंग्स की अधिक समावेशी प्रकृति के कारण साइबर स्पेस एक जटिल डोमेन बन गया है, जो तकनीकी व कानूनी प्रकृति की समस्याओं को जन्म देगा। डेटा, मुद्रा के समान महत्त्वपूर्ण है। भारत की विशाल जनसंख्या के कारण कई अंतरराष्ट्रीय कंपनियां यहां अपनी पहुँच बनाने की कोशिश कर रही हैं । इसलिये डेटा संप्रभुता ,डेटा स्थानीयकरण और इंटरनेट गवर्नेंस आदि से संबंधित मुद्दों का समाधान आवश्यक है। इस क्षेत्र के लिये आवश्यक विभिन्न सॉफ्टवेयर और हार्डवेयर से संबंधित तकनीकी पहलुओं को समझने के लिये भारतीय सैन्य बलों, केंद्रीय पुलिस संगठनों, कानून प्रवर्तन एजेंसियों में कुशल लोग बढ़ाए जाना जरूरी है। भारत में कई केंद्रीय निकाय है जो साइबर मुद्दों से निपटते हैं। इसलिये प्रत्येक निकाय में एक अलग रिपोर्टिंग संरचना होती है, जिससे विनियामक संगठनों की कार्यप्रणाली में एकरूपता का अभाव नज़र आता है। इस एकरूपता को बढ़ावा देना चाहिए। भारत में हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों में स्वदेशीकरण का अभाव है। यह भारत के साइबर स्पेस को राज्य अभिकर्ताओं और गैर-राज्य अभिकर्ताओं से प्रेरित साइबर हमले से निपटने में दुर्बल कर देता है। हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों में स्वदेशीकरण को बढ़ावा देने की आवश्यकता है। साइबर कानून में इन महत्वपूर्ण मुद्दों कों जोड़के तथा संशोधन करके साइबर कानून प्रभावशीलता बढ़ाने के लिए सुधार करने की आवश्यकता है।

सोशल मीडिया 'सूचना' के प्रसार का एक शक्तिशाली उपकरण बन रहा है, जिससे भ्रामक समाचार तेज़ी से फैलते हैं, जो साइबर सुरक्षा को खतरा उत्पन्न करते रहते हैं। भारत में सोशल मीडिया का बहुत ज्यादा उपयोग होता है। लेकिन बहुत सारे सोशल मीडिया के सर्वर दूसरे देशों में है। साइबर अपराध सोशल मीडिया के माध्यम से बढ़ रहे हैं। ऐसे अपराधों की जांच में उपयुक्त जानकारी इन सोशल मीडिया ऐप या वेबसाइट से मिलती है। यह सर्वर दूसरे देशों में होने के कारण भारत सरकार का इस पर अंकुश नहीं है। इसलिए कानून में सुधार करना बहुत ही आवश्यक है। भारतीय संस्कृति अलग है। भारतीय संस्कृति के मूल्यों पर सोशल मीडिया से आघात हो रहे हैं। संवेदनशील सोशल मीडिया पोस्ट मिटाने का अधिकार भारत सरकार के पास होना चाहिए तथा भारत के सोशल मीडिया उपयोगकर्ताओं की जानकारी (रिपॉजीटरी) भारत सरकार के पास होनी चाहिए और इसके लिए साइबर कानून में सुधारों की आवश्यकता है, नहीं तो भविष्य में कानून एवं व्यवस्था खतरे में आ सकती है। बहुत सारे पेमेंट ऐप, पेमेंट वॉलेट, पेमेंट गेटवे के जरिए होने वाले लेन देन की विस्तार में जानकारी मिलना जरूरी है। जैसे - लेन देन किसने की और उसका लाभार्थी कौन है। इसके अलावा लेनदेनकर्ता और लाभार्थी दोनों के बैंक खाता क्रमांक, आईएफएससी कोड के विवरण में पारदर्शिता होनी चाहिए। कोई पेमेंट वॉलेट या दूसरे कोई लेनदेन के जरिए व्यवहार कर रहे हैं तो उसके बारे में विस्तृत जानकारी होनी चाहिए। लेनदेन के विविध

प्रणालियों का का साइबर अपराधी उपयोग करता है। साइबर अपराध की जांच में उस लेन देन की पूरी जानकारी न होने के कारण पुलिस यंत्रणा को अपराधी की तलाश मे मुश्किले आती है और जो इस अपराध का शिकार हुआ है उसको न्याय नही दे पाते, इसलिए ऐसी पेमेंट प्रणालियों पर भारत सरकार, भारतीय रिज़र्व बैंक का नियंत्रण होना चाहिए और साइबर कानून में सुधार करके ऐसी जानकारी को साइबर कानून के दायरे में लाना जरूरी है। साइबर अपराध से जुड़ी लेन देने की प्रणालियों को जैसे - पेमेंट वॉलेट, पेमेंट ऐप को बंद (ब्लॉक) करने का अधिकार भारत सरकार के पास होना चाहिए और ऐसे सुधार साइबर कानून में करने आवश्यक हैं।

बहुत बार मोबाइल नंबर दूसरों के नाम पर लिए जाते हैं और ऐसे मोबाइल नंबर का हथियार के रूप में उपयोग करके साइबर अपराध होते हैं। इसलिए दूरसंचार संबंधित कानून और साइबर संबंधित कानून में बहुत बड़े सुधार की आवश्यकता है। जिससे मोबाइल से होने वाले अपराधों पर नियंत्रण लाया जा सके। मोबाइल नंबरों से जो साइबर अपराध किए गए हैं, ऐसे मोबाइल नंबरों को तुरंत ब्लॉक करने के लिए उचित रिपोर्टिंग प्राधिकरण होना चाहिए।

साइबर कानून में साइबर अपराध के अपराधी की संपत्ति को सील करने का प्रावधान होना चाहिए। सूचना प्रौद्योगिकी अधिनियम के तहत धाराएं गैर जमानती होनी चाहिए क्योंकि अधिकांश साइबर अपराध संगठित अपराध होते हैं। साइबर अपराधियों के लिए सजा बढ़ाई जानी चाहिए। साइबर अपराध विभाग द्वारा बैंकों से मांगी गई आवश्यक जानकारी उपलब्ध कराने के लिए कॉमन पोर्टल होना चाहिए ताकि उसे तत्काल उपलब्ध कराया जा सके। भारत में साइबर कानून की प्रभावशीलता बढ़ाने के लिए ऐसे सुधारों की आवश्यकता हैं।

गूगल प्ले स्टोर या अन्य ऐप के जरिए भी साइबर अपराध होते हैं। ऐसे एप्लिकेशन की निगरानी और नियंत्रण के लिए साइबर कानून में सुधार करने की आवश्यकता है। वित्तीय संस्थानों में लागू नियमों में भी सुधार की आवश्यकता है जिससे मनी लॉन्ड्रिंग (काले धन को वैध बनाना) को और इससे जुड़े साइबर अपराधों को रोका जा सके। साइबर धोखाधड़ी / अपराध का शिकार प्रत्येक नागरिक हो सकता है। भारत के आर्थिक, सामाजिक, राजकीय स्थितियों के अहित में साइबर अपराध हो रहे हैं। इस आधुनिक दुनिया के साथ आगे बढ़ते हुए साइबर अपराध से नागरिकों की सुरक्षा करना एवं उनमें जागरूकता बढाना आवश्यक है। साइबर कानून में ऐसे सुधारों को कार्यान्वित करके देश की आर्थिक, सामाजिक, राजकीय अहित से हिफाजत होगी जिससे भारत की संपन्नता को और बढ़ावा दिया जा सकता है।

संदर्भ:

i. *https://meity.dashboard.nic.in*
ii. *Violating these cyber laws can land you in jail! (indiatimes.com)*
iii. *https://www.drishtiias.com/hindi/daily-news-analysis/national-cyber-security-strategy-2020*
iv. *https://www.indiacode.nic.in*
v. *https://meity.gov.in*
vi. *https://en.m.wikipedia.org*

*****

विनोद चन्द्रशेखर दीक्षित

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- बैंक ऑफ इंडिया
मोबाइल नं. :- 9427800749
ई-मेल:- vinod.dixit@bankofindia.co.in

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

प्रस्तावना

वर्तमान समय में साइबर अपराध जैसा शब्द अक्सर सुनने को मिलता है। विश्व के लगभग सभी देशों ने साइबर अपराध से निपटने हेतु कानून बनाए हैं। इस आलेख के अंतर्गत उन जानकारियों को प्रस्तुत किया जा रहा है जो साइबर अपराध को स्पष्ट करती है। प्रौद्योगिकी और इलेक्ट्रॉनिक मीडिया के विकास के बाद कंप्यूटर से संबंधित अपराधों का जन्म हुआ है जिसे आमतौर पर "साइबर अपराध" कहा जाता है। साइबर अपराध एक गैरकानूनी कार्य है जिसमें कंप्यूटर या तो एक उपकरण या लक्ष्य है या दोनों साइबर अपराध में आपराधिक गतिविधियों की एक विस्तृत विविधता शामिल है। कंप्यूटर डेटा या सिस्टम, कंप्यूटर की गोपनीयता, अखंडता और उपलब्धता संबंधित अपराध, सामग्री संबंधी अपराध, कॉपीराइट संबंधी अपराध सभी इसमें शामिल है। बढ़ते साइबर अपराधों के साथ, डेटा गोपनीयता के मुद्दे और ऑनलाइन प्रतिरूपण से पहचान की सुरक्षा एक गंभीर चिंता का विषय बन गई है। वास्तव में नई तकनीक के आगमन के साथ, धोखे और भेष को पहचानना आसान नहीं है, साथ ही वित्तीय संसाधन हमेशा लक्ष्य पर होते हैं। इसलिए, विचार करने का एक वास्तविक बिंदु यह है कि सभी प्रकार की सूचनाओं को नेटवर्क पर संपत्ति के रूप में माना जाना चाहिए। आज कंप्यूटर और इंटरनेट हमारे दैनिक जीवन के लिए बहुत ही सामान्य और आवश्यक हो गया है। 1990 में, दुनिया भर में 1 लाख से भी कम लोग इंटरनेट का उपयोग करने में सक्षम थे। अब दुनिया भर में लगभग 2.5 मिलियन लोग नेट सर्फ करने के लिए जुड़े हुए हैं।

साइबर अपराधों का ऐतिहासिक पहलू

इस बात से इंकार नहीं किया जा सकता है कि इंटरनेट के आगमन ने वास्तव में हमारे जीवन को मौलिक रूप से बदल दिया है। सूचनाओं के आदान-प्रदान की तीव्र क्षमता के साथ इंटरनेट संचार का एक प्रभावी माध्यम बन गया है। हर दूसरे अपराध की तरह, साइबर अपराधों का एक घटनापूर्ण इतिहास है।

साइबर अपराध

'साइबर अपराध' शब्द संसद द्वारा अधिनियमित किसी भी कानून या अधिनियम में कहीं भी परिभाषित नहीं है। एक मायने में, यह पारंपरिक अपराध की अवधारणा से मौलिक रूप से अलग नहीं है क्योंकि दोनों में आचरण शामिल है चाहे वह कार्य हो या लोप, जो कानून के उल्लंघन का कारण बनता है और इसलिए यह राज्य द्वारा दंडनीय है। साइबर अपराध को किसी भी अवैध आपराधिक गतिविधि के रूप में परिभाषित किया जा सकता है जो कंप्यूटर का उपयोग या तो एक उपकरण, लक्ष्य या आगे अपराध करने के साधन के रूप में करता है। कंप्यूटर डेटा या सिस्टम, कंप्यूटर की गोपनीयता, अखंडता और उपलब्धता संबंधित अपराध, सामग्री संबंधी अपराध, कॉपीराइट संबंधी अपराध सभी इसमें शामिल है।

क्यों होते हैं सायबर अपराध:-

सायबर अपराध अनेक प्रकार के हैं। इस आलेख के अंतर्गत साइबर अपराध पर परिचय प्रस्तुत किया जा रहा है। इसके भाग 2 में साइबर अपराध के प्रकारों का उल्लेख किया जाएगा। परंतु साइबर अपराधों के प्रकारों को जानने के पूर्व इन अपराधों के होने के कारणों को जानना आवश्यक है। विद्वानों की राय और परिस्थितियों के अवलोकन से साइबर अपराध के निम्न कारण प्रतीत होते हैं-

1. कंप्यूटर में बहुत कम जगह में डेटा स्टोर करने की अनूठी विशेषता है। यह भौतिक या आभासी माध्यम से अधिक आसानी से जानकारी प्राप्त करने और निकालने की सुविधा देता है इसलिए इससे संबंधित अपराध करना भी आसान होता है।
2. कंप्यूटर तक पहुंच आसान है और इसलिए जटिल साइबर स्पेस प्रौद्योगिकी के उपयोग से अनधिकृत पहुंच सुरक्षा प्रणाली को दरकिनार करना आसानी से संभव है।
3. कंप्यूटर ऑपरेटिंग सिस्टम पर काम करते हैं जो जटिल होते हैं और लाखों कोड से बने होते हैं। साइबर अपराधी इसका सदोष लाभ उठाते हैं।
4. कंप्यूटर प्रणाली की एक महत्वपूर्ण विशेषता यह है कि साक्ष्य कुछ ही समय में नष्ट हो जाते हैं। अपराधियों के लिए अपराध होने के तुरंत बाद सबूतों को नष्ट करना आसान हो जाता है जिससे जांच एजेंसियों के लिए अपराधी पर मुकदमा चलाने के लिए प्रासंगिक सामग्री साक्ष्य एकत्र करना मुश्किल हो जाता है।
5. कंप्यूटर सिस्टम की सुरक्षा सुनिश्चित करने में कंप्यूटर उपयोगकर्ता की ओर से थोड़ी सी भी लापरवाही के विनाशकारी परिणाम हो सकते हैं क्योंकि साइबर अपराधी अपने आपराधिक लक्ष्य को पूरा करने के लिए कंप्यूटर सिस्टम पर अवैध पहुंच और अनधिकृत नियंत्रण प्राप्त कर सकता है।

भारत में साइबर कानून

उस ऐतिहासिक पृष्ठभूमि को समझना महत्वपूर्ण है जिसके खिलाफ भारत सरकार को सूचना प्रौद्योगिकी अधिनियम, 2000 को अधिनियमित करने के लिए राजी किया गया था। अधिनियम के मुख्य उद्देश्य इसकी प्रस्तावना में ही दिए गए हैं।

1. इलेक्ट्रॉनिक डेटा इंटरचेंज के माध्यम से किए जाने वाले इलेक्ट्रॉनिक वाणिज्यिक लेनदेन के लिए आवश्यक कानूनी मान्यता प्रदान करना। इस तरह के लेनदेन में कागज आधारित दस्तावेज भंडारण प्रणाली के विकल्प के रूप में इलेक्ट्रॉनिक भंडारण सुविधाओं का उपयोग शामिल है।
2. सरकारी एजेंसियों और कानून की अदालत में भी दस्तावेजों की इलेक्ट्रॉनिक फाइलिंग की सुविधा के लिए।
3. मौजूदा अपराधी के साथ-साथ भारत में कुछ विशिष्ट कानूनों में संशोधन करने के लिए। उदाहरण के लिए आईटी अधिनियम, 2000 ने भारतीय दंड संहिता, बैंकर्स बुक्स एविडेंस एक्ट, 1891, भारतीय साक्ष्य अधिनियम, 1872 और भारतीय रिज़र्व बैंक अधिनियम, 1934 में संशोधन किया।
4. आईटी अधिनियम अनिवार्य रूप से निम्नलिखित क्षेत्रों पर जोर देता है:
   [1] इलेक्ट्रॉनिक दस्तावेज़ों की कानूनी मान्यता, [2] साइबर अपराधों के लिए न्याय व्यवस्था प्रणाली [3] डिजिटल हस्ताक्षरों की कानूनी मान्यता

अपराध और उल्लंघन

यह ध्यान रखना दिलचस्प है कि सूचना प्रौद्योगिकी अधिनियम 2000 के तहत 'साइबर अपराध' के सामूहिक शब्द को कोई ठोस परिभाषा प्रदान नहीं की गई है। संशोधनों के बाद भी, यह बिंदु चूक गया था।

धारा 66 इस अधिनियम के तहत सबसे महत्वपूर्ण धाराओं में से एक है क्योंकि यह कंप्यूटर से संबंधित अपराधों से संबंधित है। हैकिंग का अपराध धारा 66 के तहत कहा गया है।

ये कानून कितने प्रभावी रहे हैं?

साइबर कानूनों की प्रभावशीलता बहस का विषय है। भले ही संसद ने उपयोगकर्ता जानकारी के मानक को विनियमित करने और निर्धारित करने के लिए एक उचित कानूनी ढांचा प्रदान करने का प्रयास किया है जिसे साइबरस्पेस के भीतर दरकिनार किया जा सकता है। वास्तव में, संसद का प्रयास सराहनीय है क्योंकि इसने आईटी अधिनियम के उद्देश्य को पूरा करने के लिए बहुत सारे कानूनों में संशोधन भी किया है।

क्या कहते हैं आंकड़े

भारत ने 2020 में साइबर अपराध के 50,035 मामले दर्ज किए, पिछले वर्ष की तुलना में इस तरह के अपराधों में 11.8% की वृद्धि हुई। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) के आंकड़ों के अनुसार, देश में साइबर अपराध (प्रति लाख जनसंख्या पर घटनाएं) की दर भी 2019 में 3.3% से बढ़कर 2020 में 3.7% हो गई। 2019 में, देश में साइबर अपराध के 44,735 मामले दर्ज किए गए, जबकि 2018 में यह आंकड़े 27,248 थे, जो कि संबंधित वर्षों के आंकड़ों से पता चलता है।

वर्ष में ऑनलाइन बैंकिंग धोखाधड़ी के 4,047 मामले, 1,093 ओटीपी धोखाधड़ी और 1,194 क्रेडिट/डेबिट कार्ड धोखाधड़ी के मामले देखे गए, जबकि 2020 में एटीएम से संबंधित 2,160 मामले सामने आए, जैसा कि एनसीआरबी के आंकड़ों से पता चलता है।

इसमें कहा गया है कि सोशल मीडिया पर फर्जी खबरों के 578 मामले, साइबर स्टॉकिंग या महिलाओं और बच्चों को डराने-धमकाने के 972 मामले, फर्जी प्रोफाइल की 149 घटनाएं और डेटा चोरी के 98 मामले सामने आए।

2020 में दर्ज किए गए अधिकतम 60.2% साइबर अपराध धोखाधड़ी (50,035 मामलों में से 30,142) के लिए किए गए थे, एनसीआरबी, जो गृह मंत्रालय के तहत कार्य करता है।

राज्यों में, उत्तर प्रदेश में सबसे अधिक 11,097 साइबर अपराध के मामले दर्ज किए गए, उसके बाद कर्नाटक (10,741), महाराष्ट्र (5,496), तेलंगाना (5,024) और असम (3,530) का स्थान रहा। हालांकि, कर्नाटक में अपराध दर सबसे अधिक 16.2% थी, जिसके बाद तेलंगाना (13.4%), असम (10.1%), उत्तर प्रदेश (4.8%) और महाराष्ट्र (4.4%) का स्थान था।

राष्ट्रीय राजधानी दिल्ली में वर्ष के दौरान 0.8 प्रतिशत की अपराध दर के साथ 168 ऐसे मामले दर्ज किए गए, एनसीआरबी के अनुसार, जो भारतीय दंड संहिता और देश में विशेष और स्थानीय कानूनों द्वारा परिभाषित अपराध डेटा एकत्र करने और विश्लेषण करने के लिए जिम्मेदार है।

राष्ट्रीय सुरक्षा चिंताएं और सामान्य चुनौतियां

साइबर सुरक्षा राष्ट्रीय सुरक्षा के दृष्टिकोण से भी एक महत्वपूर्ण चिंता है। वास्तव में, साइबर स्पेस और प्रौद्योगिकी में सूचना संचार ने राष्ट्रीय सुरक्षा के संबंध में नई तरह की चिंताओं को जन्म दिया है। इस बात में कोई संदेह नहीं है कि साइबरस्पेस नए प्लेटफॉर्म और अवसर प्रदान कर रहा है, जैसा पहले कभी नहीं हुआ और वास्तव में इसने हमारे जीवन में क्रांति ला दी है। हालांकि, साथ ही, यह राष्ट्रीय सुरक्षा के लिए भी एक चुनौती है।

अब जबकि दुनिया भर की सरकारों के पास अपनी योजनाओं, कल्याणकारी गतिविधियों और रिपोर्टों के बारे में जानकारी प्राप्त करने और फैलाने के लिए एक आवश्यक साइबर प्लेटफॉर्म है; इतना ही नहीं, यहां तक कि संवेदनशील जानकारी भी साइबर स्पेस में स्टोर की जाती है; हैकर्स और साइबर आतंकवादी ऐसी सूचनाओं तक आसानी से पहुंच सकते हैं और निर्दोष नागरिकों को नुकसान पहुंचा सकते हैं।

हार्डकॉपी के रूप में संग्रहीत जानकारी की तुलना में साइबरस्पेस पर कोई भी जानकारी अपेक्षाकृत अधिक सुलभ है। साइबर युद्ध, साइबर आतंकवाद आदि के साथ-साथ डेटा गोपनीयता आजकल एक उभरता हुआ मुद्दा है। हैक्टिविज्म भी एक नए प्रकार का खतरा है जो राजनीतिक मुद्दों के नाम पर किया जाता है। हालांकि इसके पीछे असली मकसद राजनीतिक अस्थिरता पैदा करना है।

राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIPC) और राष्ट्रीय साइबर समन्वय केंद्र (NCCC) जैसी विभिन्न राष्ट्रीय परियोजनाओं को अभी अमल में लाना बाकी है। दिसंबर 2019 में कुडनकुलम साइबर हमले पर एक गहन रिपोर्ट से पता चला कि महत्वपूर्ण बुनियादी ढांचे जैसे बिजली संयंत्र, वित्तीय संस्थान, पावर ग्रिड आदि को साइबर हमलों से बचाने की जरूरत है।

भारतीय रक्षा क्षेत्र को ऐसी धमकियां मिलती हैं जो या तो बाहरी लोगों से राजनीतिक रूप से प्रेरित होती हैं जो संवेदनशील जानकारी चुराते हैं या अपराधियों द्वारा अपने देश का व्यापार करते हैं। 2012 में भारतीय नौसेना पर "पब्बी" नामक साइबर हमले का सामना करना पड़ा था। इन हमलों के बाद, यह भी भविष्यवाणी की गई थी कि भविष्य में राष्ट्रीय सुरक्षा एजेंसी और भारतीय वायु सेना को भी निशाना बनाया जा सकता है। पब्बी 2012 में भारतीय नौसेना ने वास्तव में कभी यह नहीं बताया कि किस तरह की जानकारी को निशाना बनाया गया था।

साइबर पोर्टल में कई प्रवेश बिंदु हैं। इस प्रकार, सुरक्षा का स्तर चाहे जो भी हो, संवेदनशील जानकारी तक पहुंचने का एक तरीका हमेशा रहेगा। कंप्यूटर नेटवर्क रक्षा तकनीकें, रणनीति और प्रथाएं महत्वपूर्ण संचालन (मिशन) के बजाय व्यक्तिगत सिस्टम और नेटवर्क की रक्षा करती हैं।

सबसे महत्वपूर्ण विकासों में से एक यह है कि रक्षा प्रौद्योगिकी के धीमे-धीमे विकास की तुलना में साइबर हमले के तरीके बड़े पैमाने पर विकसित हुए हैं। हमले की तकनीक के नए तरीकों के साथ तालमेल रखने के लिए साइबर सुरक्षा मॉड्यूल को खुद को अपडेट करना होगा।

विभिन्न राष्ट्रों, राज्यों, बाहरी संगठनों के साथ-साथ सहकर्मी स्तर पर व्यक्ति साइबर स्पेस पर आंतरिक सरकारी सॉफ्टवेयर के हमलों को छेड़ने में पूरी तरह से सक्षम हैं।

निष्कर्ष

आज का समाज तकनीक पर निर्भर है। इस प्रकार, इलेक्ट्रॉनिक माध्यम से किए गए अपराध में वृद्धि होना तय है। साइबर कानूनों और साइबरस्पेस के पेशेवरों और विपक्षों को तौलने के बाद यह स्पष्ट है कि आईटी अधिनियम को अभी भी एक लंबा रास्ता तय करना है और इसमें कई संशोधनों की आवश्यकता है। जबकि कुछ समस्याएं इस तथ्य के कारण हमेशा बनी रहेंगी कि साइबरस्पेस अपेक्षाकृत खुला है और कुछ स्तर की भेद्यता हमेशा शामिल रहेगी और इसे पूरी तरह से रद्द नहीं किया जा सकता है। इस प्रकार, साइबरस्पेस के नैतिक उपयोग को प्रोत्साहित किया जाता है। कानूनी तंत्र का प्रयास बदलते समय के अनुसार होना चाहिए और अपेक्षाओं को पूरा करना चाहिए। अपराध दर को रोकने के लिए दोषसिद्धि दर को बढ़ाने की जरूरत है।

स्त्रोत :

- ✓ साइबर क्राइम रिपोर्ट
- ✓ ईकोनोमिक टाइम्स
- ✓ राजस्थान पत्रिका
- ✓ अमर उजाला
- ✓ जागरण जोश
- ✓ अहमदाबाद मिरर
- ✓ मनी भास्कर

*****

वैभव द्विवेदी

पदनाम:- प्रक्रिया सहायक
संस्था का नाम:- भारतीय रिज़र्व बैंक
मोबाइल नं. :- 7355303935
ई-मेल:- vaibdwivedi786rh@gmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

संदर्भ:-

हम जितनी तेजी से डिजिटल दुनिया की ओर बढ़ रहे हैं, ठीक उतनी ही तेजी से साइबर अपराध की संख्या में भी वृद्धि हो रही है। जिस गति से तकनीक ने उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। एक ही स्थान से इंटरनेट के जरिए मनुष्य की पहुंच विश्व के हर कोने तक आसान हुई है। आज के समय में हर वो चीज जिसके विषय में इंसान सोच सकता है, उस तक उसकी पहुंच इंटरनेट के माध्यम से हो सकती है। जैसे कि सोशल नेटवर्किंग, ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब इत्यादि। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।

वर्तमान में भारत की बड़ी आबादी सोशल नेटवर्किंग साइट्स का उपयोग करती है। भारत में सोशल नेटवर्किंग साइट्स के उपयोग के प्रति लोगों में जानकारी का अभाव है। इसके साथ ही अधिकतर सोशल नेटवर्किंग साइट्स के सर्वर विदेश में है। जिससे भारत में साइबर अपराध घटित होने की स्थिति में इनकी जड़ तक पहुंच पाना बहुत कठिन होता है।

साइबर अपराध क्या है?

- साइबर अपराध विभिन्न रूपों में किए जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में भारत भी उन देशों से पीछे नहीं है, जहां साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है। साइबर अपराध के मामलों में एक साइबर अपराधी, किसी टूल का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यवसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के लिए कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध है।
- इसमें कोई संशय नहीं है कि यह एक अपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के माध्यम से अंजाम दिया जाता है। साइबर अपराध, जिसे "इलेक्ट्रानिक्स अपराध" के रूप में भी जाना जाता है।
- ऐसे अपराध में जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फिसिंग, अवैध डाउनलोडिंग, साइबर स्टांकिग, वायरस प्रसार सहित कई प्रकार की गतिविधियां शामिल हैं।

साइबर अपराध का वर्गीकरण:-

- साइबर अपराध की श्रेणी को दो वर्गों में विभाजित किया जा सकता है।
  - वे अपराध जिसमें कंप्यूटर पर हमला किया जाता है। उदाहरण – हैकिंग, वायरस हमले आदि।

- वे अपराध जिसमें कंप्यूटर को हथियार या उपकरण के रूप में प्रयोग किया जाता है। उदाहरण – साइबर आतंकवाद, आईपीआर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी आदि।

साइबर अपराध की श्रेणियां –

इसके अंतर्गत तीन प्रमुख श्रेणियां आती है।

1. **व्यक्ति विशेष के विरूद्ध साइबर अपराध** –

   व्यक्ति विशेष के विरुद्ध साइबर अपराध, यद्यपि ऑनलाइन होते हैं, परंतु वह वास्तविक लोगों के जीवन को प्रभावित करते हैं। इनमें से कुछ अपराधों में साइबर उत्पीड़न और साइबर उत्पीड़न और साइबर स्टाकिंग, चाइल्ड पोनोग्राफी का वितरण, विभिन्न प्रकार के स्पूकिंग, क्रेडिट कार्ड धोखाधड़ी, मानव तस्करी आदि शामिल हैं।

2. **संपत्ति विशेष के विरूद्ध साइबर अपराध:-**

   कुछ ऑनलाइन अपराध संपत्ति के खिलाफ होते हैं, जैसे कि संप्यूटर या सर्वर के खिलाफ या उसे जरिया बना के किए जाते हैं। इसमें हैकिंग, वायरस ट्रासमिशन, कॉपी राइट उल्लंघन आदि शामिल हैं।

3. **सरकार विशेष के विरूद्ध साइबर अपराध:-**

   यह सबसे गंभीर साइबर अपराध माना जाता है जब सरकार के खिलाफ कोई साइबर अपराध किया जाता है, तो इसे उस राष्ट्र की संप्रभूता पर हमला और युद्ध की कार्यवाही माना जाता है। सरकार के खिलाफ ऐसे अपराध को साइबर आतंकवाद के रूप भी जाना जाता है।

सोशल मीडिया की भूमिका:-

1. विभिन्न सोशल नेटवर्किंग साइट्स के सर्वर अन्य देशों में केंद्रित है जिससे यह डर है कि यह देश लोगों की व्यक्तिगत जानकारी का दुरूपयोग न करें।
2. लोगों को सोशल नेटवर्किंग साइट्स पर हैकर्स ऑनलाइन ठगी का शिकार बनाते हैं।
3. ऑनलाइन मुद्रा स्थानांतरित करने वाले विभिन्न ऐप के माध्यम से आतंकवादी और देश विरोधी तत्वों को फीडिंग की जाती है।

सरकार के साइबर अपराधों से निपटने के प्रयास:-

- भारतीय सूचना प्रौद्योगिकी नियम, 2000 पारित किया गया जिसके प्रावधनों के साथ-साथ भारतीय दंड सहिंता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिए पर्याप्त हैं।
- सूचना प्रौद्योगिकी अधिनियम, 2000 की धाराएं **43, 43A, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, 72, 72A और 74** हैकिंग और साइबर अपराधों से संबंधित हैं।
- सरकार द्वारा **राष्ट्रीय साइबर सुरक्षा नीति, 2013** जारी की गई, जिसके तहत सरकार ने अतिसंवेदनशील सूचनाओं के संरक्षण के लिए **राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र का गठन किया।**
- इसके अंतर्गत 2 वर्ष से लेकर उम्रकैद तथा दण्ड अथवा जुर्माने का भी प्रावधान है।
- विभिन्न स्तरों पर सूचना एवं सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने **सूचना सुरक्षा शिक्षा और जागरूकता परियोजना** प्रारंभ की है।
- सरकार द्वारा कंप्यूटर इमरजेंसी रिस्पोंस टीम (CERT IN) की स्थापना की गई है जो कंप्यूटर सुरक्षा के लिए राष्ट्रीय स्तर की मॉडल ऐजेंसी है।

- देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए साइबर सुरक्षा केंद्र भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय के तहत भारत सरकार की डिजिटल इंडिया मुहिम का हिस्सा है।
- भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्यप्रणाली अपनाने के लिए अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है।
- अंतर-ऐजेंसी समन्वय के लिए **भारतीय साइबर अपराध समन्वय केंद्र की स्थापना की गई है।**

भारतीय साइबर अपराध समन्वय केंद्र:-

- साइबर क्राइम से बेहतर तरीके से निपटने के लिए तथा 14 C को समन्वित एवं प्रभावी तरीके से लागू करने हेतु इस योजना के 7 घटक हैं।
    1. नेशनल साइबर क्राइम थ्रेट ऐनालिटिक्स यूनिट
    2. नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल
    3. संयुक्त साइबर अपराध जांच दल के लिए मंच
    4. राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र
    5. राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र
    6. साइबर क्राइम इको सिस्टम मैनेजमेंट यूनिट
    7. राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र

बुडापेस्ट कन्वेशन क्या है?

- बुडापेस्ट कन्वेशन साइबर क्राइम पर एक कन्वेशन है जिसे साइबर अपराध पर बुडापेस्ट कन्वेशन के नाम से जाना जाता है।
- यह पहली एक ऐसी अंतर्राष्ट्रीय संधि है जिसके अंतर्गत कानूनों को सुव्यवस्थित करके जांच पड़ताल की तकनीकों में सुधार कर तथा इस संबंध विश्व के अन्य देशों को बीच सहयोग को बढ़ाने हेतु इंटरनेट और कंप्यूटर अपराधों पर रोक लगाने संबंधी माँग की गई है।
- कन्वेशन का अनुच्छेद 32बी डेटा में एक्सेस करने की अनुमति देता है और इस प्रकार यह राष्ट्रीय संप्रभुता का उल्लंघन करता है, इसीलिए भारत ने अब तक इस पर हस्ताक्षर नहीं किए हैं।

निष्कर्ष:-

भारत इंटरनेट का तीसरा सबसे बड़ा उपयोगकर्ता है और हाल के वर्षों में साइबर अपराध कई गुना बढ़ गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिए सरकार की ओर से कई कदम उठाये गए हैं। कैशलेश अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी। अतः भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा। वहीं दूसरी ओर सोशल मीडिया ने अभिव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है। आज प्रत्येक व्यक्ति बिना किसी डर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हजारों लोगों तक पहुँचा सकता है, परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी तथा साइबर अपराध के गंभीर खतरों से बचा सकता है।

*****

स्नेहा सिंह

पदनाम:- वरिष्ठ प्रबंधक
संस्था का नाम:- पंजाब नैशनल बैंक
मोबाइल नं. :- 9712469696
ई-मेल:- snehasingh1812pnb@gmail.com

भारत में साइबर कानून: प्रभावशीलता एवं सुधारों की आवश्यकता

साइबर अपराध तकनीकी प्रगति का परिणाम है। हम जितनी तेजी से डिजिटल दुनिया का उपयोग कर रहे हैं ठीक उतनी ही तेजी से साइबर अपराध की संख्या में वृद्धि भी हो रही है। आज इंटरनेट और फोन का बड़े पैमाने पर इस्तेमाल किया जाता है। इंटरनेट ने इंसानी जीवन को हर जगह से घेर रखा है। लेकिन डिजिटल हो रही इस दुनिया का गलत उपयोग भी किया जा रहा है जैसे कि लोगों के साथ धोखाधड़ी, निजी डेटा की चोरी और ठगने जैसे संगीन अपराध को अंजाम भी दिया जा रहा है।

साइबर अपराध के मामलों में एक साइबर अपराधी किसी उपकरण का उपयोग कर उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक एवं सरकारी जानकारी को गैर-कानूनी रूप से हासिल करता है अथवा डिवाइस को डिसेबल कर देता है।

साइबर अपराध के प्रकार

- फर्जी बैंक कॉल- आपको जाली ई-मेल, मैसेज या फोन कॉल के माध्यम से यह पूछा जाए कि आपके एटीएम नंबर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपका खाता बंद कर दिया जाएगा, कृपया इस लिंक पर सूचना दें। याद रखें किसी भी बैंक द्वारा ऐसी जानकारी कभी भी नहीं मांगी जाती है और भूलकर भी इस प्रकार की जानकारी को इन्टरनेट, फोनकॉल या मैसेज के माध्यम से न बताएं।
- साइबरफिशिंग- स्पैम ई-मेल भेजकर किसी व्यक्ति से उसकी निजी जानकारी प्राप्त करना ताकि उस जानकारी का प्रयोग कर उसका नुकसान किया जा सके। ये ई-मेल बहुत आकर्षक होते हैं।
- स्पैम ई-मेल के अंतर्गत कई प्रकार के मेल आते हैं जिसमें ऐसे ई-मेल भी होते हैं जो सिर्फ कंप्यूटर को नुकसान पहुचाते हैं। उन ई-मेल से सारे कंप्यूटर में खराबी आ जाती है।
- हैकिंग-किसी की भी निजी जानकारी जैसे उपयोगकर्ता के नाम या पासवर्ड को हैक करना और उसमें फेर बदल करना।
- सोशल नेटवर्किंग साइटों पर अफवाह फैलाना- बहुत से लोग साइट पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं, लेकिन उपयोग उनके इरादें समझ नहीं पाते हैं और जाने-अनजाने में ऐसे लिंक्स को शेयर करते रहते हैं, यह भी साइबर अपराध और साइबर-आतंकवाद की श्रेणी में आता है।
- साइबर बुलिंग-सोशल नेटवर्किंग पर अशोभनीय कमेंट करना, धमकियां देना, किसी का इस स्तर तक मजाक बनाना कि तंग हो जाए, दूसरों के सामने शर्मिंदा करना, इसे साइबर बुलिंग कहते हैं। अक्सर बच्चे इसका शिकार होते हैं।

- वायरस फैलाना -साइबर अपराधी कुछ ऐसे सॉफ्टवेयर आपके कम्प्युटर पर भेजते हैं जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस, वर्म, टार्जन हॉर्स, लॉजिक हॉर्स आदि वायरस शामिल हैं, यह आपके कंप्यूटर को काफी हानि पहुंचा सकते हैं।
- सॉफ्टवेयर पाइरेसी-सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है, इससे सॉफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है। साथ ही साथ आपके कीमती उपकरण भी ठीक से काम नहीं करते हैं।

साइबर कानून

साइबर कानून डिजिटल कानून प्रणाली का एक हिस्सा है जो इंटरनेट साइबर स्पेस और इसमें होने वाली दिक्कतों जैसे मुद्दों से संबंधित है साइबर कानून होने के बावजूद अपराधी प्रवृत्ति के लोग बड़े पैमाने पर अपराध को अंजाम दे रहे हैं। आज हम बेफिक्र होकर अपनी महत्वपूर्ण जानकारी और डेटा स्टोर करने के लिए कंप्यूटर की मदद लेते हैं। यह डेटा और जानकारी फ्रॉड या धोखाधड़ी का शिकार न हो जाए इसलिए साइबर कानून बहुत ही आवश्यक है। साइबर अपराधों पर नियंत्रण के लिए प्रत्येक देश की सरकार द्वारा कठोर साइबर कानून बनाए गए हैं। भारत में 'सूचना प्रौद्योगिकी अधिनियम, 2000' पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिए पर्याप्त हैं।

भारतीय दंडसंहिता (आईपीसी) में साइबर अपराधों से सम्बंधित प्रावधान:

- ई-मेल के माध्यम से धमकी भरे सन्देश भेजना–आईपीसी की धारा 503
- ई-मेल के माध्यम से ऐसे संदेश भेजना जिससे मानहानि होती हो-आईपीसी की धारा 499
- फर्ज़ी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल-आईपीसी की धारा 463
- फर्ज़ी वेबसाइट्स या साइबर फ्रॉड-आईपीसी की धारा 420
- चोरी-छुपे किसी के ई-मेल पर नज़र रखना-आईपीसी की धारा 463
- वेब जैकिंग-आईपीसी की धारा 383
- ई-मेल का गलत इस्तेमाल - आईपीसी की धारा 500
- दवाओं को ऑनलाइन बेचना - एनडीपीएस एक्ट
- हथियारों की ऑनलाइन ख़रीद-बिक्री-आर्म्स एक्ट

सरकार द्वारा 'राष्ट्रीय साइबर सुरक्षा नीति, 2013' जारी की गई जिसके तहत सरकार ने "राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र" का गठन किया है।

भारत सरकार के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के अनुसार साइबर कानून इलेक्ट्रॉनिक दस्तावेजों, ई-फाइलिंग, ई-कॉमर्स तथा एक वैध हस्ताक्षर के रूप में डिजिटल हस्ताक्षर को कानूनी मान्यता देना है और सरकार के लिए अधिकतम कनेक्टिविटी और सुरक्षा जोखिम सुनिश्चित करने का काम करता है। भारत में साइबर कानून किसी भी साइबर अपराध को होने से रोकता है और नागरिकों की संवेदनशील जानकारी किसी अजनबी को ऑनलाइन भेजने से बचाता है। इस कानून के तहत विभिन्न प्रकार के अपराधों को कवर किया जाता है:

- साइबर अपराध
- इलेक्ट्रॉनिक और डिजिटल हस्ताक्षर में धोखाधड़ी
- इंटेलेक्चुअल प्रॉपर्टी में धोखाधड़ी
- डेटा संरक्षण गोपनीयता मामले में धोखाधड़ी

साइबर अपराध संसद द्वारा अधिनियमित किसी भी कानून या अधिनियम में कहीं भी परिभाषित नहीं है, पर यह पारंपरिक अपराध की अवधारणा से अलग नहीं है एवं दंडनीय है। साइबर अपराध को किसी भी अवैध गतिविधि के रूप में परिभाषित किया जा सकता है जो कंप्यूटर का उपयोग या तो एक उपकरण या आगे अपराध करने के साधन के रूप में काम करता है। साइबर अपराध का दायरा दुनिया के विभिन्न हिस्सों पर प्रभाव डालता है।

मनुष्यता के इतिहास के साथ अपराध भी जुड़े रहे। समय और परिस्थितियों के अनुसार अपराधों में भी परिवर्तन होता रहा है। अपराधों की व्यापक वृद्धि वैश्विक चिंता का विषय बन गयी। यहां अपराधी बिना शारीरिक उपस्थिति के गुमनाम रूप से बहुत दूर रहकर भी अपराध कर देता है। उसे पकड़े जाने का भय भी नहीं होता विभिन्न देशों के साइबर अपराध के लिए अंतर्राष्ट्रीय दृष्टिकोण में एक रणनीति विकसित करने से तथा संयुक्त प्रयासों के कारण अंतर्राष्ट्रीय स्तर पर एक मानवीकृत, सार्वभौमिक, एंटी साइबर अपराध कानून का पारित होना आवश्यक है। साइबर अपराध के खिलाफ लड़ने के लिए कई अंतर्राष्ट्रीय सम्मेलन आयोजित किए जाने के बावजूद वांछित सफलता नहीं मिली क्योंकि इन अपराधियों को पकड़ना अत्यंत कठिनाई भरा कार्य है जिसे केवल कानून प्रवर्तन एजेंसियों के अंतर्राष्ट्रीय सहयोग से ही पता लगाया जा सकता है।

साइबर सुरक्षा में अंतर्राष्ट्रीय उपाय:

भारत ने संयुक्त राज्य अमेरिका, यूरोपीय संघ, मलेशिया आदि देशों के साथ साइबर सुरक्षा सहयोग स्थापित किया है। साइबर स्पेस पर आयोजित वैश्विक सम्मलेन में अंतर्राष्ट्रीय नेतृत्वकर्ता नीति निर्माता, उद्योग विशेषज्ञ, साइबर विशेषज्ञ इत्यादि एकत्रित होते हैं और साइबर स्पेस के इष्टतम उपयोग संबंधी मुद्दों तथा चुनौतियों पर विचार करते हैं। पांचवें सम्मेलन का आयोजन भारत में किया गया। इसे वैश्विक, आर्थिक मंच द्वारा भविष्य के सुरक्षा परिदृश्य हेतु एक थिंक टैंक तथा एक प्रयोगशाला के रूप में कार्य करने के लिए लांच किया गया था। इनका उद्देश्य सुरक्षित वैश्विक साइबर स्पेस के निर्माण में सहायता करना है। साइबर हमलों के विरुद्ध अपने ग्राहकों की गोपनीयता तथा सुरक्षा को इंटरनेट तथा तकनीक उपयोग द्वारा बेहतर रूप से सुनिश्चित करने के उद्देश्य से माइक्रोसॉफ्ट ने साइबर सिक्योरिटी टेक समझौते के साथ-साथ डिजिटल पीस अभियान को आरंभ किया है। वर्ष 2015 में संयुक्त राष्ट्र में सरकारी विशेषज्ञों के एक दल द्वारा साइबर स्पेस संबंधी शांति कालीन मानकों को निर्धारित किया गया है:

- राष्ट्रों द्वारा एक दूसरे की महत्वपूर्ण अवसंरचना में हस्तक्षेप नहीं किया जाना चाहिए।
- साइबर हमलों की जांच में अन्य देशों की सहायता करना।
- एक दूसरे के कंप्यूटर आपात अनुक्रिया दल को लक्षित नहीं किया जाना चाहिए।
- राष्ट्रों को उनके क्षेत्रों से हो रहे किसी भी कार्रवाई के प्रति उत्तरदायी होना।

साइबर कानून में सुधारों की आवश्यकता:

डिजिटल दुनिया जहां एक तरफ सबको आकर्षित करती हैं वहीं दूसरी ओर व्यापक स्तर पर डिजिटल निरक्षरता भारतीय नागरिकों को साइबर अपराधों के प्रति अधिक संवेदनशील बना देती है। भारत में ज्यादा जनता गरीबी रेखा के नीचे है अतः वह निम्न गुणवत्ता वाले उपकरणों का प्रयोग करते हैं और इन पर डिजिटल लेन-देन करते समय उनकी मालवेयर के संपर्क में आने का खतरा अधिक हो जाता है।

भारत में लाखों ऐप डाउनलोड करने वाले हैं। हालांकि, इन ऐप्स में से 80% ऐप्स सुरक्षित हैं। परंतु शिक्षा के अभाव एवं गरीबी के कारण हमारी आम जनता को इनका प्रयोग करना पड़ता है अतः वह साइबर अपराध में आसानी से फंस जाते हैं।

भारत की बैंकिंग अवसंरचना इतनी मजबूत नहीं है कि बढ़ते डिजिटल अपराधों का सामना कर सके। डेबिट तथा क्रेडिट कार्ड में से 75 प्रतिशत मैग्नेटिक स्ट्रिप पर आधारित है जिनका प्रतिरूप सरलता से बनाया जा सकता है। भिन्न-भिन्न मानकों के साथ प्रयुक्त होने वाले उपकरणों की संख्या अत्यधिक है जिससे एक समान सुरक्षा प्रोटोकॉल स्थापित करना कठिन हो जाता है। ऊर्जा, रक्षा तथा महत्वपूर्ण अवसंरचनात्मक क्षेत्रों में प्रयुक्त अधिकांश इलेक्ट्रॉनिक उपकरणों से लेकर मोबाइल फोन तक आयात किए जाते हैं जिससे भारत की सुभेद्यता बढ़ जाती है। वर्तमान में भारत में साइबर सुरक्षा के क्षेत्र में लगभग 30000 पद रिक्त हैं तथा आवश्यक कौशल युक्त लोगों की आपूर्ति उनकी मांग से बहुत कम है। निजी क्षेत्र के साइबर स्पेस में महत्वपूर्ण हितधारक होने के बावजूद साइबर सुरक्षा के संबंध में सक्रिय भूमिका का निर्वहन नहीं किया जा रहा है। उपर्युक्त के अलावा भौगोलिक बाधाओं की अनुपस्थिति, अधिकांश सर्वरों का भारत के बाहर स्थापित होना, साइबर स्पेस के क्षेत्र में तेजी से विकसित होती प्रौद्योगिकी तथा साइबर स्पेस के समग्र परिवेश में विद्यमान विविध प्रकार की सुभेद्यता के कारण एक अभेद साइबर सुरक्षा संरचना की स्थापना इत्यादि भी महत्वपूर्ण चुनौतियां हैं।

निष्कर्ष: देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी के तहत भारत सरकार की डिजिटल इंडिया मुहिम का एक हिस्सा है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी। अतः भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा। सोशल मीडिया ने अभिव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है, आज प्रत्येक व्यक्ति बिना किसी डर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हज़ारों लोगों तक पहुँचा सकता है, परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी तथा साइबर अपराध के गंभीर खतरों से बचा सकता है। **हमें हमेशा जागरूकता पर ध्यान देना चाहिए, क्योंकि, 'रोकथाम इलाज से बेहतर है', खासकर तब जब इलाज उपलब्ध नहीं है।**

*****

सरकारी क्षेत्र के बैंकों / वित्तीय संस्थानों / बीमा कंपनियों के स्टाफ सदस्यों हेतु अखिल भारतीय सेमिनार का आयोजन

दिनांक 07.03.2022 को मैसूरू (कर्नाटक) में भारतीय रिज़र्व बैंक/ सरकारी क्षेत्र के बैंकों/ वित्तीय संस्थानों/ बीमा कंपनियों के सभी स्टाफ सदस्यों के लिए **'बैंकिंग में साइबर अपराध'** विषय पर अखिल भारतीय सेमिनार का आयोजन किया गया. सेमिनार का शुभारंभ बैंक के मुख्य महाप्रबंधक (परिचालन) श्री अजय कुमार खोसला एवं विशिष्ट अतिथि के रूप में उपस्थित कर्नाटक पुलिस की आर्थिक अपराध शाखा (सीआईडी) के पुलिस अधीक्षक श्री एम डी शरत द्वारा किया गया. इस अवसर पर मुख्य अतिथि के रूप में क्षेत्रीय कार्यान्वयन कार्यालय (कार्यान्वयन), दक्षिण, राजभाषा विभाग, गृह मंत्रालय, भारत सरकार के सहायक निदेशक श्री नरेंद्र मेहरा उपस्थित रहे. साथ ही, सेमिनार में बैंक के मुख्य सूचना सुरक्षा अधिकारी श्री सर्वेश गुप्ता, बेंगलुरू अंचल के महाप्रबंधक श्री सुधाकर डी नायक ए तथा मैसूरू क्षेत्र के क्षेत्रीय प्रमुख श्री आर मुरलीकृष्णा भी उपस्थित रहे. इस अवसर पर पिछले वर्ष के सेमिनार के लिए प्राप्त और चयनित आलेखों के संकलन की पुस्तक **'बैंकिंग में अनुपालन संस्कृति'** का विमोचन भी किया गया.