बैंकों में साइबर जोखिम एवं बचाव प्रबंधन

✍ डॉ. साकेत कुमार सहाय*

पृष्ठभूमि

बैंकिंग का जो स्वरूप हम सभी के समक्ष आज उपस्थित है ऐसा माना जाता है कि इसकी शुरूआत 17वीं शताब्दी में हुई होगी। लेकिन, आज की समस्त आधुनिक बैंकिंग प्रथाएं जैसे- जमा, ब्याज, ऋण और साख पत्र आदि प्राचीन काल में भी मौजूद थीं। भारत में कौटिल्य ने 300 ईसा पूर्व उनके द्वारा लिखित अर्थशास्त्र में मर्चेंट बैंकरों की सशक्त प्रतिभूतियों के बारे में लिखा है कि वे जमाराशियां स्वीकार करते थे और ऋण देते थे तथा हुंडियां (अंतरण-पत्र) जारी किया करते थे।

तब से अब तक बैंकिंग क्षेत्र में अनेक क्रांतिकारी बदलाव परिलक्षित हुए हैं, जिससे बैंकिंग क्षेत्र आज उत्कृष्ट ग्राहकोन्मुखी सेवा के रूप में उपस्थित हैं। इस ग्राहकोन्मुखी सेवा का ही परिणाम है कि बैंकिंग क्षेत्र ने तमाम विपरीत परिस्थितियों में भी आगे बढ़कर नागरिक आकांक्षाओं की प्रतिपूर्ति में श्रेष्ठ योगदान दिया है। जब ग्राहकोन्मुखी बैंकिंग की बात की जाती है तो हम दो शब्दों को प्रमुखता से पाते हैं – ''सहज एवं सुरक्षित'' और इसी से जन्म होता है ''ग्राहक संतुष्टि'' का। इसी सहज एवं सुरक्षित सेवा तथा ग्राहक संतुष्टि के उद्देश्य से बीते दशकों में भारतीय बैंकिंग में अभूतपूर्व बदलाव परिलक्षित हुए हैं। इस बदलाव को निम्न प्रकार से समझा जा सकता है-

- ब्रिक व मोर्टार - क्लिक व ऑर्डर - ई-बैंकिंग
- जमा व ऋण - भुगतान
- भौतिक चेक समाशोधन – इलेक्ट्रॉनिक समाधान
- उच्च संव्यवहार लागत – कम संव्यवहार लागत
- उत्पाद केंद्रित – ग्राहक केंद्रित
- बहु प्रदाता – एकल प्रदाता
- शाखा कोर – डिजिटल चैनल कोर
- फेस टू फेस इंगेजमेंट – डिजिटल माध्यम से इंगेजमेंट

बैंकिंग संरचना एवं कार्य-प्रणाली के डिजिटलीकरण का भविष्य 1950 के दशक में सबसे पहले इलेक्ट्रॉनिक कंप्यूटर के विकास के साथ ही महसूस किया जाने लगा था। दूसरे शब्दों में कहें कि इसे निर्धारित किया जा चुका था और बैंकों द्वारा मेनफ्रेम कंप्यूटरों का उपयोग करके अपने बैक-ऑफ़िस संचालन को स्वचालित करना इस बात की पुष्टि करता है। हालाँकि, समय के परिवर्तन के साथ बैंकिंग तकनीक ने डिजिटल परिवर्तन की दिशा में और अधिक महत्वपूर्ण कदम उठाना शुरू किया। इस परिवर्तन की क्रमबद्धता को हम निम्नलिखित रुप में समझ सकते हैं -

1. 1950 और 1960 के दशक में, बैंकों ने लेखांकन और लेनदेन प्रसंस्करण के लिए इलेक्ट्रॉनिक कंप्यूटरों का उपयोग करना शुरू किया, जिससे अधिक कुशल और सटीक रिकॉर्ड-कीपिंग हुई।
2. 1970 के दशक में, बैंकों द्वारा ग्राहकों को 24/7 नकदी आहरण की सेवा प्रदान करने के लिए स्वचालित टेलर मशीन (एटीएम) का उपयोग करना शुरू किया गया।
3. 1980 के दशक में, ऑनलाइन बैंकिंग के साथ ग्राहकों को अपने खातों का 24/7 परिचालन करने और

*मुख्य प्रबंधक (राजभाषा), पंजाब नैशनल बैंक।

कंप्यूटर नेटवर्क के माध्यम से लेनदेन करने की अनुमति मिली।

4. 1990 के दशक में, बैंकों ने ग्राहक संबंधों को बेहतर ढंग से प्रबंधित करने और ग्राहक सेवा में बेहतरी लाने हेतु ग्राहक संबंध प्रबंधन (सीआरएम) प्रणाली का उपयोग करना शुरू किया।

5. 2000 के दशक की शुरुआत में, मोबाइल बैंकिंग की शुरुआत हुई, जिससे ग्राहकों को मोबाइल उपकरणों के माध्यम से अपने खातों का परिचालन करने और लेन-देन करने की अनुमति मिली ।

6. 2000 के दशक के अंत में, सोशल मीडिया के उदय ने बैंकों को ग्राहकों के साथ जुड़ने और उनके उत्पादों और सेवाओं को बढ़ावा देने के लिए सोशल मीडिया प्लेटफॉर्म का उपयोग करने के लिए प्रेरित किया।

7. 2010 के दशक में, बैंकों ने अपने परिचालन में सुधार करने और ग्राहकों को बेहतर सेवाएं प्रदान करने के लिए क्लाउड कंप्यूटिंग और बिग डेटा एनालिटिक्स को अपनाना शुरू किया।

8. इसके साथ ही कृत्रिम मेधा (आर्टिफिशियल इंटेलीजेंस) एवं अन्य तकनीकी प्रयुक्तियों के माध्यम से बैंकिंग सेवाएं समय के साथ और भी सुगम एवं अद्यतित हो रही हैं।

इन बदलावों से, जहां बैंकों ने अपने दृष्टिकोण में भारी परिवर्तन किए हैं वहीं बैंकिंग सेवाओं के प्रति ग्राहकों के दृष्टिकोण में भी व्यापक बदलाव आए हैं। इसी का परिणाम है कि बैंक एक वित्तीय सुपर-बाजार के रूप में हमारे समक्ष खड़े हैं। बैंक द्वारा दी जा रही सेवाएं ग्राहकों की जरूरतों के मुताबिक है, जो विभिन्न डिलीवरी चैनलों द्वारा उपलब्ध करवाई जा रही है। इनमें से अधिकांश डिज़िटल माध्यमों से संचालित हो रही है। जिससे बैंकिंग सेवाएं ज्यादा सहजता से उपलब्ध हो पा रही हैं। परंतु इस बदलाव एवं प्रगति ने इस सेवा के समक्ष अनेक सवाल भी खड़े किए हैं जिसका एक प्रमुख पक्ष है बैंकिंग में बढ़ता साइबर अपराध।

आज के युग में यदि हम अपना व्यक्तिगत या सार्वजनिक विकास हेतु कुछ भी प्रगतिशील कार्य करते हैं तो यह सब बिना डिजिटल तकनीक के मानो असंभव-सा लगता है। बैंकिंग के साथ भी यही है। बैंकिंग की शुरुआत ग्राहकों को वित्तीय सहायता एवं सेवाएं देने के उद्देश्य से की गई थी परन्तु तब से लेकर अभी तक बैंकिंग व्यवस्था ने स्वयं को डिजिटल क्रांति के विविध आयामों से जोड़ा और अपने साथ-साथ अपने बहुमूल्य ग्राहकों को भी डिजिटल तकनीक से पूरी तरह से लैस करने का अद्‌भुत कार्य किया है। यह डिजिटल भुगतान व्यवस्था का ही परिणाम है कि आज बैंकिंग सेवा किसी-न-किसी रूप में 24x7 उपलब्ध है।

डिजिटल भुगतान लेन-देन हेतु एक सुविधाजनक माध्यम है। इसके बढ़ते प्रयोग के साथ-साथ इससे जुड़े जोखिम भी बढ़ते जा रहे है। धोखाधड़ी एवं जालसाजी डिजिटल बैंकिंग के समक्ष व इनके प्रयोग में बहुत बड़ी बाधा के रूप उपस्थित हो रही है। कभी भारतीय रिज़र्व बैंक के पूर्व गवर्नर श्री रघुराम राजन ने अपने कार्यकाल में यह बात रखी थी कि ''साइबर ठग रिज़र्व बैंक गर्वनर को भी आम ग्राहक समझकर लुभावनी पेशकश करते हैं।''

आज डिजिटल या साइबर अपराध भारत में ही नहीं बल्कि पूरे विश्व में एक केंद्रीय मुद्दा बन चुका है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) के अनुसार, वर्ष 2020 में ही भारत में साइबर अपराध के 50,035 मामले सामने आए थे, जो एक साल पहले की तुलना में 11.8 फीसदी अधिक थे। आरबीआई की वार्षिक रिपोर्ट-2022-23 के अनुसार धोखेबाजों की नजर में डिजिटल भुगतान निशाने पर रहा। रिपोर्ट के अनुसार, ऑनलाइन भुगतान में धोखाधड़ी की रकम भले घटी है, परंतु इसकी संख्या में वृद्धि हुई है। आंकड़ों के अनुसार, बैंकिंग में धोखाधड़ी के मामले वित्तीय वर्ष-2022- 23 में बढ़कर 13,530 हो गए। धोखाधड़ी के इन मामलों में शामिल कुल राशि ₹30,252 करोड़ रही, जो इससे पिछले वित्तीय वर्ष (2021-22) के मुकाबले करीब आधा रहा।

वर्ष	मामले	राशि (₹ करोड़ में)
2022-23	13,530	30,252
2021-22	9,097	59,819
2020-21	7,338	1,32,389

स्रोत: बिज़नेस स्टैण्डर्ड (31 मई, 2023)

भारत सरकार, भारतीय रिज़र्व बैंक एवं बैंक भी इस विषय पर निरंतर सतर्क एवं निगरानी में है। भारतीय रिज़र्व बैंक एवं बैंक भी उपभोक्ताओं को धोखाधड़ी के प्रति सजग रहने को लेकर निरंतर आह्वान करते रहते हैं। तमाम घटनाओं को देखकर यह भी निष्कर्ष निकलता है कि वास्तव में एक विशेष प्रकार की धोखाधड़ी जो दूसरों की तुलना में अधिक होती है और उनको लेकर जागरूक रहना ही खुद को सुरक्षित रखने की दिशा में पहला कदम है।

आरबीआई की वित्तीय स्थिरता रिपोर्ट-2021 के अनुसार, अक्तूबर, 2020 से ही बैंकिंग क्षेत्र उच्च जोखिम क्षेत्र में शामिल है। कोरोना महामारी के बाद से ही बैंकिंग प्रणाली के लिए साइबर अपराध को ज्यादा बड़ा खतरा माना जा रहा है। ऑनलाइन तकनीक के प्रयोग में बढ़ोत्तरी के साथ ही बैंकिंग क्षेत्र में साइबर आक्रमणों की संख्या, अंतराल एवं प्रभाव में वृद्धि हुई है।

बैंकों में साइबर अपराधों का स्वरूप एवं सुरक्षात्मक उपाय

बिज़नेस स्टैण्डर्ड, 07 जून, 2023 में प्रकाशित रिपोर्ट के अनुसार, भारतीय परिवार अपना 35 फीसदी लेनदेन औसतन डिजिटल माध्यम से करते हैं और रिपोर्ट के अनुसार, वित्त वर्ष 2026 तक यह आंकड़ा बढ़कर 50 फीसदी के पार होने की उम्मीद है। रिपोर्ट में यह भी कहा गया है कि स्मार्टफोन और इंटरनेट के बढ़ते इस्तेमाल तथा सरकारी नीतियों के कारण वित्त वर्ष 2026 तक भारत में कम से कम 85 फीसदी व्यवसाय डिजिटल रूप से सक्षम हो जाएंगे। आज चीन के बाद भारत में इंटरनेट प्रयोक्ताओं (70 करोड़ से अधिक) की दूसरी सबसे बड़ी संख्या है।

यह स्पष्ट है कि डिजिटल बैंकिंग की लोकप्रियता धीरे-धीरे बढ़ रही है। भारत में हुई डिजिटल क्रान्ति को देखते हुए यह कहा जा सकता है कि 'भारत ने बगैर किसी शोर-शराबा किए ऑनलाइन लेनदेन में क्रांति ला दी है और सभी हितधारक इसमें अपनी सक्रिय भूमिका निभाने को लेकर उत्साहित हैं।' परंतु इसी के साथ यह भी स्थिति निर्मित हुई है कि जहां डिजिटल बैंकिंग से इसके धारकों को कई प्रकार की बैंकिंग सुविधाएं प्राप्त हुई हैं वहीं कई बार उन्हें नए प्रकार के खतरों का भी सामना करना पड़ता है। भारत में ग्राहकों के अधिकारों की रक्षा के लिए बैंकिंग लोकपाल, उपभोक्ता फोरम, अदालतें आदि मौजूद हैं। बैंकिंग लोकपाल के आंकड़ों के मुताबिक, बैंकिंग लोकायुक्त के पास सबसे ज्यादा शिकायतें एटीएम-डेबिट कार्ड से संबंधित ही आती हैं। इसमें शामिल है - एटीएम मशीन से पैसे नहीं निकलने, कार्ड की क्लोनिंग होने, एटीएम-डेबिट कार्ड के पास में रहने के बावजूद दूसरों द्वारा पैसे की निकासी हो जाने जैसी शिकायतें सबसे अधिक हैं।

सबसे अधिक चुनौतीपूर्ण स्थिति यह है कि आज वैश्विक स्तर पर बैंकिंग प्रणाली ऑनलाइन हो चुकी है और ग्राहकों से जुड़ी तमाम वित्तीय जानकारियां सर्वर में मौजूद हैं, जिसके हैक होने की आशंका निरंतर बनी रहती है। आए दिन समाचार पत्रों में प्रकाशित रिपोर्टों से यह स्पष्ट है कि वर्तमान में बैंक इलेक्ट्रॉनिक एवं पेपर दोनों ही माध्यमों के धोखाधड़ी से जूझ रहे है। पर, इसमें बड़ी समस्या है साइबर धोखाधड़ी की, 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 जाए।

हालांकि, इस चुनौती से निपटने हेतु बैंकों ने साइबर जोखिम प्रबंधन की ओर विशेष ध्यान दिया है एवं जी. गोपाल कृष्ण समिति के निर्देशों के अनुरूप सुरक्षा, इलेक्ट्रॉनिक बैंकिंग, तकनीकी जोखिम प्रबंधन एवं साइबर धोखाधड़ी से निपटने हेतु उपाय भी लागू किए है। फिर भी यह कहा जा सकता है कि बैंकों द्वारा उठाए गए ये उपाय फिलहाल शुरूआती

दौर में ही है और इसमें निरंतर अनुप्रयोग अपनाए जाने शेष है। क्योंकि जिस प्रकार से डिजिटल बैंकिंग अपनाने वालों की संख्या तथा इससे जुड़े साइबर अपराध के खतरे बढ़ते जा रहे है 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 नए आधार पर सक्रिय रूप से तैयार एवं संशोधित करना ही 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 एक जटिल कार्य है और इसकी जटिलता तब और ज्यादा बढ़ जाती है जब 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''।

बैंकों 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: बैंकों में धोखाधड़ी के कारण निम्न हैं, अपने ग्राहक को जानिये तथा अपने कर्मचारियों को जानिये, नीति का सुचारु रुप से पालन नहीं होना, निर्धारित आंतरिक एवं बाह्य प्रक्रियाओं का पालन नहीं करना, अति विश्वास, धोखाधड़ी की जानकारी न देना, ग्राहकों का जागरूक नहीं होना आदि एवं डिजिटल धोखाधड़ी में एटीएम डेबिट/क्रेडिट कार्ड से संबंधित धोखाधड़ी, स्किमिंग, कार्ड क्लोनिंग, ऑनलाइन पासवर्ड या पिन की चोरी, मोबाइल धोखाधड़ी, फिशिंग, विशिंग आदि शामिल किए जा सकते हैं। आज सहज, सुरक्षित एवं विश्वसनीय डिजिटल बैंकिंग सेवा प्रदान करने के बीच साइबर अपराध एक बड़ी चुनौती के रूप में उपस्थित है।

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

यह भी कहा जा सकता है कि आवश्यक सावधानी बरत कर इस प्रकार की धोखाधड़ी से बचा जा सकता है। देखा जाए तो दिनचर्या के सारे कार्य करते समय हम सभी पूर्ण सावधानी बरतते हैं। खाना बनाने से लेकर सड़क पार करने तक में सावधानी बरतने की जरूरत होती है, लेकिन वित्तीय मामलों में आज भी अधिकतर भारतीय निरक्षर की भांति व्यवहार करते हैं। बड़ी-बड़ी डिग्रियां हासिल करने वाले लोग भी एटीएम के इस्तेमाल में आवश्यक सावधानी नहीं बरतते। लोग अपने एटीएम कार्ड को दोस्त, रिश्तेदार आदि को देने से नहीं हिचकते हैं। पीओएस (प्वाइंट ऑफ सेल्स) के इस्तेमाल में असावधानी बरतते हैं। ई-कॉमर्स में भी ग्राहक ऑनलाइन खरीदारी करते वक्त सावधानी नहीं बरतते।

बैंकों में साइबर अपराधों के 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 तीन स्तरों पर जरूरी है- बैंक, विनियामक एवं ग्राहक। साइबर अपराध के समुचित निपटान, कार्रवाई, समाधान एवं नियंत्रण में बैंकों, हितधारकों एवं विनियामकों तीनों की महत्वपूर्ण भूमिका है। ग्राहक स्तर पर यदि देखें तो पहला उपाय है – 'अपने डाटा को सुरक्षित रखें' और उससे भी महत्वपूर्ण है 'थोड़े अविश्वासी बने'। साथ ही, ग्राहकों को साइबर सुरक्षा को जीवन जीने की शैली के रूप में अपनाना होगा। 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) द्वारा उठाए गए कदम

भारत सरकार द्वारा उठाए गए कदम

- **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 (कंप्यूटर आपात कार्रवाई टीम-भारत) गठित है। यह संगठन साइबर सुरक्षा को दुरूस्त करने की दिशा में सक्रिय एवं प्रतिक्रियात्मक सेवाओं के साथ-साथ दिशानिर्देश प्रदान करते हुए, खतरे की आसूचना और वित्तीय क्षेत्रों सहित सभी क्षेत्रों में विभिन्न एजेंसियों की तैयारी का मूल्यांकन करते हुए कदम उठा रही है।

- **साइबर संकट प्रबंधन योजना**

बैंक साइबर संकट प्रबंधन योजना (सीसीएमपी) को प्रभावी रुप से अपना रहे है। 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

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

- **एसओसी (सिक्यूरिटी ऑपरेशन सेंटर)**

बैंकों द्वारा गठित सिक्यूरिटी ऑपरेशन सेंटर (एसओसी) से रीयल टाइम में साइबर जोखिमों की निगरानी तथा प्रबंधन सुनिश्चित हो रही है। बैंकों के समन्वय के उपरांत इन केंद्रों को मजबूत किया जाना और भी आवश्यक हो गया है।

- **साइबर सुरक्षा मुस्तैदी संकेतक**

बैंक साइबर खतरों से अपने डाटा को सुरक्षित रखने हेतु साइबर रेसिलिएन्स फ्रेमवर्क के तहत साइबर सुरक्षा मुस्तैदी संकेतक भी अपना रहे है।

- **साइबर-अपराधों से संबंधित सूचनाओं को आरबीआई के साथ साझा करना**

बैंकों द्वारा साइबर–अपराधों से संबंधित जानकारी आरबीआई के साथ साझा करने से (सफल/असफल प्रयास) 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 के अन्य कदम

- **ग्राहक सूचना की सुरक्षा सुनिश्चित करना**

जब से बैंकिंग उद्योग ने प्रौद्योगिकी आधारित सेवाएँ देना शुरू किया है तब से इस क्षेत्र में साइबर खतरे बढ़े है। इसका बड़ा कारण है कि देश में प्रौद्योगिकी आधारित सेवाओं के प्रति लोगों की अनभिज्ञता एवं अरूचि। आज भी बहुत लोगों को एटीएम कार्ड का उपयोग नहीं आता और वे पैसा निकालने के लिए एटीएम में जाकर अपना कार्ड किसी दूसरों के हवाले कर देते हैं या अपने कार्ड पर या डायरी में लिखी पिन संख्याएं उन्हें दिखा देते हैं जिसके कारण उनके कार्ड का दुरूपयोग बेहद आसान हो जाता है। इन घटनाओं की गंभीरता को देखते हुए बैंकों एवं भारत सरकार के साथ ही स्थानीय पुलिस संगठनों के समन्वय से इस हेतु वित्तीय साक्षरता अभियान भी चलाया जाना चाहिए।

- **भारत में आम आदमी के स्तर पर सूचना प्रौद्योगिकी इंफ्रास्ट्रक्चर एवं जागरूकता**

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

- **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 उपाय -

- एटीएम के प्रयोग से पूर्व ग्राहक इसकी सुरक्षा स्थिति जांच लें।
- कार्ड एवं पिन नंबर किसी भी व्यक्ति को न दें।
- पासवर्ड मजबूत रखें 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 प्रदान न करें।
- कार्ड प्राप्ति के तुरंत बाद कार्ड के पीछे या चेकबुक पर दर्ज नंबर पर कॉल कर इसकी पुष्टि करें।

साइबर धोखाधड़ी की शिकायत

- साइबर अपराध/धोखाधड़ी की घटना होने पर 1930 पर संपर्क करें या cybercrime.gov.in पर लॉग इन कर तुरंत शिकायत दर्ज करवानी चाहिए।
- गलत या धोखे से गलत व्यक्ति के खाते में यूपीआई से धनराशि ट्रांसफर होने पर www.npci.org.in पर ऑनलाइन शिकायत दर्ज करें।

अन्य सावधानियाँ

1) ओटीपी/पिन/सीवीवी नंबर साझा न करें।
2) ऑनलाइन खाते/नेटबैंकिंग के अल्फान्यूमैरिक स्पेशल कैरेक्टर के साथ जटिल पासवर्ड रखें।
3) नाम/मोबाइल नंबर/जन्मतिथि को पासवर्ड नहीं बनाये।
4) लॉटरी/कैशबैक/रिफ़ंड/जॉब्स/गिफ्ट इत्यादि ऑनलाइन प्रलोभनों से सावधान रहें।
5) सोशल मीडिया खाते पर टू स्टेप वेरीफिकेशन/टू फैक्टर प्रमाणीकरण ऑन रखें।
6) कस्टमर केयर के नंबर कभी भी गूगल से सर्च नहीं करें, केवल आधिकारिक वेबसाइट से प्राप्त करें।
7) मोबाइल डिवाइस का जीपीएस/ब्लूटुथ/एनएफसी/

हॉटस्पॉट वाई–फाई आवश्यक होने पर ही ऑन रखें।

8) अंजान लोगों से प्राप्त होने वाली वीडियो कॉल रिसीव न करें और न ही फ्रेंड रिक्वेस्ट स्वीकार करें।

9) पब्लिक वाई-फ़ाई में ऑनलाइन शॉपिंग या बैंकिंग ट्रांजेक्शन न करें।

10) अंजान क्यू आर कोड स्कैन/लिंक पर क्लिक न करें।

11) अंजान व्यक्ति के कहने पर रिमोट एक्सेस, एपीके एनी डेस्क, टीम व्यूयर, एयर ड्रॉप, मीडमिन, एयरमाइनर इत्यादि एप्लीकेशन इंस्टाल न करें।

12) ऑटोमैटिक फारवर्डिंग एप्लीकेशन इंस्टाल या डाउनलोड न करें।

13) व्हाट्सअप, इन्स्टाग्राम, फेसबुक, ट्रू कॉलर की डीपी में वरिष्ठ पुलिस अधिकारियों के नाम वर्दी पहने फोटो या किसी परिचित व्यक्ति का फोटो दिखाई देने पर तत्काल विश्वास न करें।

14) ऑनलाइन सोशल साईट पर पर्सनल फोटो/वीडियो शेयर न करें।

15) लाइक/रीव्यू/रेटिंग के नाम पर घर बैठे रुपए कमाने के लालच में न जाए और न ही पूंजी लगाए।

16) आरबीआई द्वारा स्वीकृत बैंकिंग/नॉन बैंकिंग वित्तीय संस्थानों के अधिकृत लोन ऐप से लोन लें।

इन सभी के साथ यह कहा जा सकता है कि धोखाधड़ी से जागरूकता ही बचाव का महत्वपूर्ण समाधान है। साथ ही सरकार को कठोर नियम बनाने होंगे।

जागरूकता ही बचाव

साइबर अपराध रोकने के लिए हम खुद भी जागरूक बनें और दूसरों को भी जागरूक बनाएं। किसी भी अवांछित लिंक या ई-मेल को न खोलें। ऐसे ई-मेल अटैचमेंट को डाउनलोड भी नहीं करना चाहिए। पुलिस अधिकारियों को साइबर अपराध रोकने का गहन व विधिवत प्रशिक्षण दिया जाना चाहिए। पीड़ितों को हेल्पलाइन पर घटना की जानकारी देने के लिए प्रोत्साहित करना जरूरी है।

'साइबर हाइजीन' ही बचाव का तरीका

साइबर धोखाधड़ी को पूरी तरह रोक पाना लगभग नामुमकिन है। तकनीकी बचाव के तहत साइबर धोखाधड़ी के प्रचलित तरीकों की रोकथाम और नई किस्म की संभावित धोखाधड़ी से निपटने के लिए उपाय किए जाते हैं लेकिन यह पूरी तरह कारगर नहीं है क्योंकि धोखेबाज नित नए तरीके खोज ही लेते हैं। नीतिगत स्तर पर भी अभी कई चीजें स्पष्ट नहीं हैं। जागरूकता के अभाव में लोग खुद अपनी निजी जानकारी धोखेबाजों के साथ साझा कर बैठते हैं। यह भी कहा जा सकता है कि कोविड काल में जिस प्रकार हमने अपने स्वास्थ्य सुरक्षा हेतु विभिन्न नियमों को अनुशासन के साथ अपनाया था उसी प्रकार से साइबर धोखाधड़ी से बचने के लिए हमें साइबर स्वच्छता (हाइजीन) का भी विशेष ध्यान रखना होगा। इसके तहत हम सभी को अपने स्तर पर अनजान नंबर से आने वाले लिंक, संदेश या तस्वीरों को क्लिक करने या खोलने से बचना होगा। साथ ही, किसी भी ऐप को आधिकारिक वेबसाइट से ही डाउनलोड करें। कई बार मिलते जुलते नाम से भी धोखा हो सकता है इसलिए यह जरूरी है कि नाम की वर्तनी को विशेष रूप से मिला लें।

जागरूकता व सरकार की जवाबदेही

साइबर धोखाधड़ी को पूरी तरह से रोका तो नहीं जा सकता है लेकिन इसे कम जरूर किया जा सकता है। इसके लिए सबसे बड़ा उपाय है - जागरूकता। सरकारी संगठनों के साथ निजी संगठनों को भी लोगों को साइबर धोखाधड़ी के प्रति जागरूक करना होगा कि वे किस प्रकार से इससे बच सकते हैं। सबसे अधिक यह जरूरी है कि धोखाधड़ी करने वालों पर सख़्त कार्रवाई हो। इसके लिए सरकार को तुरंत समर्पित साइबर बल का गठन करना चाहिए। जिससे कि साइबर अपराधियों के विरुद्ध यथाशीघ्र कार्रवाई हो सके। बैंकों को भी लिंक या ऐप आधारित भुगतान प्रणाली को और अधिक सुरक्षित बनाने की जरूरत है। यदि बैंकों को साइबर धोखाधड़ी के संबंध में क्षतिपूर्ति के लिए बाध्य किया जाए तो वे अधिक जिम्मेदार बनकर सुरक्षा उपाय कर सकते हैं। साथ ही पुन: यह जरूरी है कि लोग खुद भी सावधान व सतर्क रहें।

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 मिलकर कार्य करना होगा। साइबर अपराध से जुड़े विभिन्न मामलों में यह देखा गया है कि अधिकांश अपराध पेमेंट कार्ड की जानकारी चुराने एवं एटीएम ढाँचे के जरिए नुकसान पहुंचाने जैसी चीजों से जुड़े हैं। सरकार ने धोखाधड़ी का पता लगाने और जांच करने के लिए लिए एक राष्ट्रीय हेल्पलाइन नंबर 155260 शुरू किया है। यह कदम साइबर अपराध नियंत्रण में बेहद उपयोगी है। बैंक साइबर सुरक्षा संबंधी घटनाओं को देखते हुए साइबर सुरक्षा जोखिम प्रबंधन हेतु बीमा भी ले सकते हैं। आज की सबसे बड़ी आवश्यकता है कि साइबर अपराध से निपटने हेतु सभी हितधारकों में एक संतुलित एवं दूरगामी सोच विकसित हो और यह कार्य सबके सहयोग से ही संभव है।

प्रसंगवश, सरकार, विनियामक, बैंक एवं ग्राहक सभी को यह समझना होगा कि ''आपदाएं बताकर नहीं आती, उपाय यही है कि हम आपदाओं से एक हद तक बचाव ही कर सकते हैं और इस हेतु सबसे जरूरी है - समेकित प्रयास।'' व्यवस्थाएं, साइबर संसार से दूर नहीं जा सकती, अब हम सभी को इसी में जीना, इसी के साथ जीना सीखना पड़ेगा और इसका एकमात्र समाधान है-डिजिटल कौशल बढ़ाना। इसी डिजिटल कौशल में निहित है साइबर जोखिम से बचाव एवं प्रबंधन। यह कौशल एवं समेकित प्रयास ही हमें साइबर जोखिम से नियंत्रित कर पाएगा। साथ ही समन्वित डिजिटल जोखिम प्रबंधन भी जरूरी है।

संदर्भ स्रोत

- दैनिक हिंदुस्तान
- बिजनेस स्टैंडर्ड दैनिक के विभिन्न अंक
- भारतीय रिजर्व बैंक की वेबसाइट

☯