प्लास्टिक मुद्रा के प्रयोग से जुड़ी चुनौतियाँ

✍ डॉ. साकेत सहाय*

तकनीक, जोखिम और परिवर्तन को एक ही सिक्के के दो पहलू माना जा सकता है। इतिहास गवाह है कि दुनिया के तमाम बड़े परिवर्तन बदलती आवश्यकता के परिप्रेक्ष्य में समय, तकनीक एवं आवश्यकता के समन्वय के आधार पर हुए हैं और अधिकांश परिवर्तनों के साथ मानवीय सुविधा एवं समन्वय जुड़े हुए होते हैं। बीते दशक की बैंकिंग भी इन ऐतिहासिक बदलावों, परिवर्तनों से अछूती नहीं रही है। यह बैंकिंग तकनीक में आए बदलाव का ही असर है कि आज बैंकिंग सेवा किसी-न-किसी रूप में 24x7 उपलब्ध है। इन बदलावों, परिवर्तनों से बैंकिंग सेवा में हर रोज नए बदलाव परिलक्षित हो रहे हैं, जिससे आम जनता के साथ-साथ देश की अर्थव्यवस्था भी लाभान्वित हो रही है।

हम सभी इस तथ्य से परिचित हैं कि विकसित अर्थव्यवस्था की पहली पहचान है नकदी विहीन अर्थव्यवस्था, क्योंकि यह काले धन के प्रवाह को नियंत्रित करती है। साथ ही, देश की कर-व्यवस्था को मजबूती प्रदान करती है। जैसे-जैसे भारतीय अर्थव्यवस्था विकासशील से विकसित होने की ओर अग्रसर हो रही है, यहाँ नकदी विहीन अर्थव्यवस्था एवं भुगतान व्यवस्था को एकीकृत करने पर जोर दिया जा रहा है। भारतीय अर्थव्यवस्था में प्लास्टिक मुद्रा यानि डेबिट/क्रेडिट कार्ड के प्रयोग पर जोर दिया जा रहा है। युवा वर्ग भी प्लास्टिक मुद्रा के इस्तेमाल में अधिक सुविधा का अनुभव करता है। इसी का नतीजा है कि आज सभी बैंक ग्राहकों को प्लास्टिक मुद्रा प्रयोग करने पर जोर दे रहे हैं। नकदी के बिना किए जाने वाले लेन-देन के लिए भी इन कार्डों का उपयोग लगातार बढ़ता जा रहा है। इन सभी का एकमात्र सार है: आधुनिक युग में प्लास्टिक मुद्रा या इलेक्ट्रॉनिक मुद्रा, वास्तविक मुद्रा का मजबूत विकल्प बनते जा रहे हैं।

बीते 08 नवंबर, 2016 को केंद्र सरकार द्वारा भ्रष्टाचार, कालाधन और जमाखोरी जैसी समस्याओं से छुटकारा पाने हेतु घोषित की गई विमुद्रीकरण या अखबारी शब्दों में कहें तो नोटबंदी ने बैंकिंग सेवा का एक नया रूप पेश किया है। देश में 1000 और 500 रूपए के नोट बंद होने पर हर तरफ मचे हड़कंप से निपटने में बैंकिंग क्षेत्र ने कारगर भूमिका निभाई है। नोटबंदी की वजह से नगदी की समस्या से जूझ रही जनता को भी प्लास्टिक मुद्रा के रूप में बेहतर विकल्प दिखाई दिया। यही कारण है कि सरकार भी इस विकल्प को अपनाने पर ज्यादा जोर दे रही है। पर, इस काम में कई बड़ी चुनौतियाँ हैं। बड़े शहरों में तो प्लास्टिक मुद्रा का चलन है लेकिन छोटे शहरों और ग्रामीण क्षेत्रों में लोग अभी भी इसके इस्तेमाल से कतराते हैं। सरकार ने बैंकिंग

* वरिष्ठ प्रबंधक (राजभाषा) ओरियन्टल बैंक ऑफ कॉमर्स

से जुड़ी कई महत्वाकांक्षी योजनाओं की शुरूआत की है, जिससे आम जनता को बैंकिंग की मुख्यधारा से जोड़ा जा सके। इसके बावजूद भारत में प्लास्टिक मुद्रा को जन-जन तक पहुंचाने के लिए अभी कई बड़ी चुनौतियाँ हैं। साइबर क्षेत्र के विशेषज्ञों के मुताबिक, प्लास्टिक मुद्रा हो या फिर डिजिटल लॉकर - इन सभी में सूचना की सुरक्षा एक प्राथमिक जरूरत है।

आर्थिक मामलों के जानकारों के मुताबिक प्लास्टिक मुद्रा की प्राथमिक जरूरत एटीएम, कार्ड स्वैपिंग मशीन, अच्छी इंटरनेट स्पीड और सुरक्षा के फीचर्स हैं। अगर समुचित संसाधनों की पूर्ति होगी तो शहरी ही नहीं, ग्रामीण क्षेत्रों में भी लोग इसे स्वीकारेंगे। विशेषज्ञों के मुताबिक, इनके प्रयोग से कई बड़ी चुनौतियाँ जुड़ी हुई हैं। ऐसे में बैंकिंग की इस नई सुविधा के प्रति लोगों को जागरूक करने की आवश्यकता है। इन कार्डों के प्रयोग में वृद्धी से जुड़ी सबसे प्रमुख चुनौती है, प्लास्टिक मुद्रा पर आसानी से विश्वास नहीं करना तथा इससे जुड़ी कई प्रकार की भ्रांतिया रखना। प्लास्टिक मुद्रा भले ही लेन-देन हेतु एक सुविधाजनक माध्यम है। साथ ही, धोखाधड़ी एवं जालसाजी इन कार्डों के व्यापक प्रयोग वृद्धी में एक बड़ी समस्या है। इसके बढ़ते प्रयोग के साथ-साथ इससे जुड़े जोखिम भी बढ़ते जा रहे हैं। प्रस्तुत आलेख में हम उपर्युक्त वजहों को विस्तार से समझने का प्रयास करेंगे।

प्लास्टिक मुद्रा का कम इस्तेमाल

जनधन योजना से अधिकतर लोगों तक बैंकिंग सुविधा पहुंचाने के बावजूद देश में डेबिट और क्रेडिट कार्ड का इस्तेमाल करने वालों की संख्या कम है। भारतीय रिज़र्व बैंक की एक रिपोर्ट के मुताबिक वर्ष 2016 की शुरूआत तक देश में लगभग 23 करोड़ क्रेडिट कार्ड धारक हैं जबकि डेबिट कार्ड की पहुंच 64 करोड़ लोगों तक ही है। आंकड़ों से जाहिर है कि प्लास्टिक मुद्रा का चलन सीमित है।

25 फीसदी लोग बैंक से दूर

रिपोर्ट के मुताबिक भारत में 75 फीसदी लोग बैंक खाताधारक हैं जो कि बैंकिंग सेवा का प्रत्यक्ष रूप से बैंक में जाकर पैसा निकालने और जमा करने के तौर पर इस्तेमाल करते हैं। ऐसे में बड़ी संख्या में लोगों को प्लास्टिक मुद्रा की तरफ मोड़ना बहुत बड़ी चुनौती है। नोटबंदी की घोषणा के समय मे भी सरकार ने इस तथ्य को महसूस किया। 500 और 1000 के नोटों को बदलवाने की बजाय अगर जनता केवल अपनी जरूरत के हिसाब से पैसा बदलती और बाकी पैसा अपने खाते में जमा करती, तो विमुद्रीकरण के समय उत्पन्न आसन्न संकट से एक हद तक बचा जा सकता था। लोग अपनी मेहनत से जमा किए गए पैसे को बदलवाने के लिए घबरागए। अगर ऐसे लोग अपने खाते का महत्व समझते तो इन पैसों को अपने खाते में जमा कर सकते थे और प्लास्टिक मुद्रा यानि एटीएम के अलावा पीओएस, मनी ट्रांसफर या पेटीएम के विकल्प का प्रयोग कर सकते थे। हालांकि इसके प्रयोग से दूसरी चुनौतियाँ भी जुड़ी हुई हैं, जिस पर चर्चा हम आगे के उद्धरणों में करेंगे।

नेट बैंकिंग की समझ न होना

देश भर में लोग ऑनलाइन बैंकिंग को अभी भी शक की नजरों से देखते हैं। ये लोग पैसों के लेनदेन के लिए अपने पारंपरिक तरीकों जैसे चेक, ड्राफ्ट और कैश इस्तेमाल करते हैं। देश में कुल सक्रिय बैंकिंग

सेवा धारकों में से 7 फीसदी लोग ही ऑनलाइन बैंकिंग का इस्तेमाल करते हैं।

स्वैपिंग की सुविधा का सीमित होना

भारतीय रिज़र्व बैंक के आंकड़ों के मुताबिक देश भर में वर्ष 2016 के शुरूआत तक सभी व्यावसायिक बैंकों द्वारा कुल 12,36,933 स्वैपिंग मशीन जारी किए गए थे; जो कि अधिकतर टियर-1 और टियर-2 शहरों में लगे हुए हैं। स्वैपिंग मशीन की कम उपलब्धता भी प्लास्टिक मुद्रा के इस्तेमाल में एक बड़ा रोड़ा है।

धोखाधड़ी और जालसाजी का डर

देश में बैंकिंग की नई टेक्नोलॉजी को लेकर अभी भी कई प्रकार की भ्रांतियां हैं, जिससे लोग ऑनलाइन बैंकिंग और प्लास्टिक मुद्रा पर आसानी से विश्वास नहीं करते। बैंकिंग की नई सुविधाओं के साथ लोगों को जागरूक करने की जरूरत है। धोखाधड़ी एवं जालसाजी इन कार्डों के प्रयोग में बहुत बड़ी बाधा है। प्लास्टिक मुद्रा लेनदेन हेतु एक सुविधाजनक माध्यम है। इसके बढ़ते प्रयोग के साथ-साथ इससे जुड़े जोखिम भी बढ़ते जा रहे हैं। इन जोखिमों में शामिल हैं- क्रेडिट कार्ड और डेबिट कार्ड के प्रयोग से संबंधित धोखाधड़ी। इसी जोखिम की कड़ी में हाल में देश भर में तकरीबन 32 लाख एटीएम के पिन चोरी होने की आशंका की खबरों से डेबिट कार्ड की सुरक्षा को लेकर नए प्रश्न उभरे हैं, जो क्रेडिट कार्ड के मुकाबले कहीं ज्यादा सुरक्षित माने जाते थे।

भारत में सभी तरह की खुदरा भुगतान प्रणालियों का शीर्ष संगठन, भारतीय राष्ट्रीय भुगतान निगम (एनपीसीआई) के अनुसार चोरी किए गए एटीएम-डेबिट कार्ड के डेटा की मदद से 19 बैंकों के 641 ग्राहकों को साइबर अपराधियों ने 1.3 करोड़ रूपए का चूना लगाया। यह मामला इसलिए भी उल्लेखनीय है कि इसमें ग्राहक की बिना गलती के एटीएम-डेबिट कार्ड डेटा चुरा कर बड़े पैमाने पर भारत में धोखाधड़ी का पहला मामला सामने आया। ज्ञात हो कि इसमें उन्नीस बैंकों के एटीएम -डेबिट कार्ड के डेटा चुराने की खबर अखबारों में आई थी। यह खबर पिछले अक्टूबर, 2016 में तब सुर्खियों में आई जब इस खबर के आने के बाद भारतीय स्टेट बैंक ने अपने छः लाख एटीएम-डेबिट कार्ड्स को ब्लॉक कर दिया। मीडिया माध्यमों में इस दुर्घटना से प्रभावित एटीएम-डेबिट कार्ड की संख्या पैंसठ लाख तक बताई गई।

मीडिया रिपोर्टों के मुताबिक, चीन के हैकरों ने यह सेंधमारी की है जिससे निजी एवं सार्वजनिक क्षेत्र के बैंकों के 32 लाख से अधिक डेबिट कार्ड के प्रभावित होने की आंशका है। डाटा में यह सेंध कुछ एटीएम प्रणालियों में साइबर मालवेयर हमले के रूप में बताई गई। फिलहाल, मालवेयर नामक वायरस को सेंधमारी का कारण माना जा रहा है। इस घपले के बाद एटीएम-डेबिट कार्ड का क्लोन बना कर देश व विदेशों से पैसों की निकासी या ऑनलाइन खरीदारी की बात सामने आई तथा विदेश में सबसे ज्यादा क्लोन कार्ड्स के इस्तेमाल का मामला चीन में रिकार्ड किया गया।

इस घटना के बाद सरकार एवं बैंक दोनों ही ग्राहक की सुरक्षा को लेकर सतर्क हो गए हैं तथा एहतियाती कदम के रूप में सभी प्रभावित बैंकों ने संदेहास्पद एटीएम-डेबिट कार्डों पर रोक लगा दी तथा ग्राहकों को इनके इस्तेमाल से पहले अपना पासवर्ड बदलने

की सलाह दी। नोटबंदी की वजह से मीडिया माध्यमों ने इस घटना को उतनी तवज्जो नहीं दी परंतु इस घटना ने भारत में वित्तीय सुरक्षा के लिए चेतावनी का संकेत जरूर दे दिया है तथा बैंकिंग उद्योग को इससे निपटने का समय भी दिया है।

आमतौर पर विश्व के अधिकतर वित्तीय संस्थानों की प्लास्टिक मुद्रा से जुड़ी शर्तों में धोखाधड़ी का शिकार होने पर मुआवजा देने की व्यवस्था नहीं होती हैं। साथ ही ग्राहक भी ऐसी सुविधा लेने के समय बैंक द्वारा प्रभारित शर्तों को ठीक से पढ़ते तक नहीं है। परंतु, भारत में स्थिति इतनी बुरी नहीं है। भारतीय रिज़र्व बैंक ने 11 अगस्त, 2016 को जारी अपने एक परिपत्र (सर्कुलर) में साफ तौर पर कहा है कि यदि किसी बैंक की सूचना प्रौगिकी की कमजोर सुरक्षा प्रणाली की वजह से कोई ऑनलाइन धोखाधड़ी होती है, तो उसकी जवाबदेही ग्राहक की न होकर संबंधित बैंक की होगी और धोखाधड़ी की भेंट चढ़ी राशि का हर्जाना बैंक को पीड़ित ग्राहक को देना होगा। परंतु, इस प्रकार की सूचना ग्राहक को तीन दिनों के भीतर बैंक को देनी होगी।

प्लास्टिक मुद्रा के प्रयोग से जुड़े खतरे :

आलेख में ऊपर दिए गए आंकड़ों से स्पष्ट है कि प्लास्टिक मुद्रा का चलन सीमित वर्ग तक है। पर, इससे इंकार नहीं किया जा सकता कि इन कार्डों की लोकप्रियता धीरे-धीरे बढ़ रही है तथा ये कार्ड भविष्य की जरूरत है। इन कार्डों के बढ़ते प्रयोग से जहां एक ओर कार्डधारकों को अनेक प्रकार की नई बैंकिंग सुविधाएं प्राप्त हुई हैं वहीं दूसरी ओर कई बार उन्हें नए प्रकार के खतरों का भी सामना करना पड़ता है। हालांकि, हमारे देश में इन खतरों से निपटने हेतु बैंकिंग लोकपाल, उपभोक्ता फोरम, अदालतें एवं साइबर सुरक्षा कानून आदि हैं। भारत में कार्ड धोखाधड़ी की वारदातें अरसे से होती आ रही हैं। लिहाजा, इन फोरमों में ऐसे मसलों पर ही ग्राहकों की शिकायतों की सुनवाई ज्यादा की जाती है। बैंकिंग लोकपाल के आंकड़ों के मुताबिक, बैंकिंग लोकायुक्त के पास सबसे ज्यादा शिकायतें एटीएम-डेबिट कार्ड से संबंधित आती हैं। इसमें शामिल है एटीएम मशीन से पैसे नहीं निकलने, कार्ड की क्लोनिंग, एटीएम-डेबिट कार्ड के पास में रहने के बावजूद पैसे की निकासी हो जाने जैसी शिकायतें सबसे अधिक दर्ज की जाती हैं।

कई बार लोगों के खाते से बिना उनकी जानकारी के पैसे निकल जाते हैं एवं पीड़ित ग्राहकों को इसकी भनक तक नहीं लग पाती हैं जो हमारी वित्तीय साक्षरता के स्तर को दिखाता है। आज भी अधिकांश ग्राहक अपने खातों की विवरणी को नियमित रूप से नहीं देखते है, जबकि लगभग सभी बैंकों ने अनेक तरह के एप्स ग्राहकों को मुहैया करा रखे हैं। गौरतलब है कि बैंकिंग एप्स की मदद से खातों से जुड़ी अनेक तरह की सूचनाएं हासिल की जा सकती हैं। भारतीय स्टेट बैंक ने हाल ही में 'एसबीआई क्विक' के नाम से एक ऐसा एप विकसित किया है जिसकी मदद से एटीएम कार्ड को बिजली की स्वीच की तरह ऑन व ऑफ किया जा सकता है। अर्थात् एटीएम से पैसे निकालने के समय आप एटीएम कार्ड का स्वीच ऑन कर पैसे निकाल सकते हैं और उसके तुरंत बाद उसके स्वीच को ऑफ भी कर सकते हैं, जिससे धोखाधड़ी से बचा जा सकता है।

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 हमेशा बनी रहती है, लेकिन आवश्यक सावधानी बरत कर इस तरह की धोखाधड़ी से बचा जा सकता है। देखा जाए तो दिनचर्या के सारे काम करते समय हम सावधानी बरतते हैं। खाना बनाने से लेकर सड़क पार करने तक में सावधानी बरतने की जरूरत होती है, लेकिन वित्तीय मामलों में आज भी अधिकांश भारतीय निरक्षर है। बड़ी-बड़ी डिग्रियां हासिल करने वाले लोग भी एटीएम का इस्तेमाल करना नहीं जानते है, जबकि एटीएम का इस्तेमाल कैसे करें, क्या-क्या सावधानियां बरतें, तमाम जानकारियां एटीएम कार्ड के साथ संलग्न विवरण पुस्तिका में दी हुई रहती हैं। लेकिन कोई भी इसे पढ़ने की जहमत नहीं उठाता। इतना ही नहीं, एटीएम मशीन के केबिन की दीवारों में भी तमाम जानकारियां व एहतियात बरतने के नुस्खे पोस्टरों में लिखे रहते हैं। वर्तमान में लोग अपने एटीएम कार्ड को दोस्त, रिश्तेदार आदि को देने से नहीं हिचकते है। पॉइंट ऑफ सेल में भी इसका बेहिचक इस्तेमाल करते हैं। ई-कॉमर्स में इजाफा होने के बाद से ग्राहक इंटरनेट के जरिए ऑनलाइन खरीदारी कर रहे हैं, परंतु इस क्रम में किस प्रकार की सावधानियां उन्हें बरतनी चाहिए इससे वे अनजान हैं। यथा, मोबाइल नंबर अंजान व्यक्तियों के साथ साझा करते वक्त हम सभी को सावधानी रखनी चाहिए। उदाहरण के लिए आज भारत के बाजारों में चीन के मोबाइलों का कब्जा है, जिनकी सुरक्षा प्रणाली कमजोर होती हैं एवं ऐसे मोबाइलों से डेटा चुराना आसान होता है।

प्लास्टिक मुद्रा से संबंधित धोखाधड़ी की परिभाषा अगर मूल रूप में तय की जाए तो इसमें शामिल है, प्रथम-खो गए अथवा चोरी किए कार्डों के द्वारा; द्वितीय- नकली या क्लोन किए गए कार्डों द्वारा आर्थिक लाभ के लिए किसी व्यक्ति की निजी पहचान सूचना का अधिग्रहण तथा इसका इस्तेमाल करना।

व्यक्ति की पहचान से संबंधित जानकारी की चोरी द्वारा, आर्थिक लाभ के लिए किसी व्यक्ति की निजी पहचान की सूचना के अधिग्रहण द्वारा व्यक्ति के ऐप्लिकेशन की जालसाजी तब की जाती है, जब कोई अपराधी किसी चुराई या नकली दस्तावेजों के जरिए किसी अन्य व्यक्ति के नाम से खाता खुलवाता है। अपराधी यूटीलिटी बिल तथा बैंक विवरणी चुराने की कोशिश कर आपकी जरूरी जानकारी हासिल कर लेते हैं।

खाते के अधिग्रहण में किसी अन्य व्यक्ति के खाते पर अपराधी अधिग्रहणारा अधिकार कर लेता है, जिसके लिए पहले तो वह लक्ष्यित व्यक्ति की जानकारी इका करता है, और कार्ड जारी करने वाले से उसी व्यक्ति के रूप में संपर्क करता है और उससे सभी पत्राचार को नए पते पर भेजने का अनुरोध करता है। तब वह व्यक्ति कार्ड के खो जाने की सूचना देता है और वह उससे नए कार्डों को भेजने की मांग करता है।

कार्ड की धोखाधड़ी में अवैध तरीके से किसी अन्य व्यक्ति के क्रेडिट/डेबिट कार्ड से वस्तु या सेवा प्राप्त करना शामिल है। कार्ड धोखाधडी के अन्य तरीकों में शामिल हैं, जैसे, कार्ड की कॉपी निकाल कर, किसी साधारण नियमित व्यवहार के समय 'स्किमिंग' द्वारा, जिसमें एक अत्यंत छोटे से उपकरण पर असली कार्ड को गुजार कर कार्ड पर लिखी सूचनाओं की चोरी की जाती है, कार्ड चोरी एवं डाक या कूरियर में ही इसके साथ हस्तक्षेप करके तथा अन्य कुटिल माध्यमों द्वारा धोखाधड़ी की जा सकती है।

फिशिंग विशेषत: ई-मेल स्पूफिंग या तत्काल संदेश के साथ की जाती है जिसके द्वारा यूज़रनेम, पासवर्ड एवं क्रेडिट कार्ड की जानकारी जैसा, विवरण इलेक्ट्रॉनिक कम्युनिकेशन की मदद से चुराया जाता है एवं इसमें यूजर को वैध लगनेवाली एक अवैध वेबसाईट की ओर निर्देशित किया जाता है।

स्किमिंग में चोर अपने शिकार के क्रेडिट कार्ड का नंबर रसीदों की नकल कर या और अधिक विकसित तरीकों से जैसे एक छोटा-सा इलेक्ट्रॉनिक उपकरण (स्किमर) के प्रयोग द्वारा सैकड़ों क्रेडिट कार्ड नंबर अपने पास संग्रहित कर सकते हैं। स्किमिंग होटल, शॉपिंग मॉल या ऐसी जगह जहां आपके कार्ड को आपकी नजरों से कुछ समय के लिये दूर किया जाता है, वहां संभव है।

इसके अतिरिक्त, सोशल इंजिनियरिंग में 'विशिंग' जैसे धोखाधड़ी के तरीके अपना कर यथा, वॉयस ओवर आइपी (वीओआईपी) द्वारा समर्थित फीचरों का इस्तेमाल कर निजी तथा वित्तीय जानकारी प्राप्त की जाती है और उसका दुरूपयोग किया जाता है। सोशल इंजीनियरिंग में धोखाधड़ी करनेवाला पहले कर्मचारी होने का नाटक कर ग्राहक का विश्वास जीतता है। सोशल इंजीनियरिंग के माध्यम से ही अपराधी एटीएम पर स्कैनिंग यंत्र यानि स्किमर का उपयोग करके कार्ड की सारी जानकारी चुरा लेते हैं। स्कैंनिग के माध्यम से धोखेबाज सारी जानकारी और पिन नंबर मिल जाने पर डुप्लीकेट कार्ड बनाकर एटीएम से पैसा निकालते हैं या खरीदारी करते हैं। इस प्रकार सोशल इंजीनियरिंग से बचने हेतु सतर्क रहना ही एकमात्र विकल्प है।

प्लास्टिक मुद्रा की धोखाधड़ी से बचाव हेतु सुझाव

अगर प्रयोक्ता सचेत एवं सतर्क रहें एवं बैंकिंग तकनीक में नित नए हो रहे बदलावों से अपने को अतन रखें तो ऑनलाइन या ऑफलाइन दोनों ही प्रकार की ठगी या धोखाधड़ी से काफी हद तक बचा जा सकता है।

- इसकी प्रारंभिक शुरूआत के रूप में प्रयोक्ता को यह सुनिश्चित करना चाहिए कि बैंक से प्राप्त होने वाला किसी भी प्रकार का लिफाफा(कवर) पूरी तरह से सीलबंद हो और उस पर किसी भी प्रकार का फाड़ने या चिपकाने का निशान न हो, विशेष रूप से जब कार्ड संबंधित चीजें प्राप्त होने वाली हों।
- कार्ड प्राप्ति के बाद तुरंत उस पर अपना हस्ताक्षर कर दें। कार्ड के आखिरी तीन नम्बर को सदैव कवर करने की कोशिश करें।
- खाते के लेन-देन विवरण की जानकारी लेने हेतु अपने मोबाइल नम्बर रजिस्टर्ड करा लें तथा मोबाइल नंबर में किसी भी प्रकार का बदलाव होने पर बैंक को तुरंत सूचित करें।
- वेंडर द्वारा कार्ड स्वाइप करते वक्त उस पर पैनी नजर रखें। कभी भी क्रेडिट कार्ड की खाली रसीद पर हस्ताक्षर न करें। खाली स्थान पर एक लाइन खींच लें ताकि वहां किसी प्रकार की अतिरिक्त जानकारी न लिखी जा सके।
- जब लेनदेन के लिए दो बार पिन मांगा जाए तो लेनदेन को तुरंत रद्द कर दें। हमेशा किसी भी कैमरे से बचने हेतु की-पैड को कवर करें और आसपास के लोगों की मदद लेने से परहेज करें।
- निश्चित अंतराल पर अपने एटीएम कार्ड का पासवर्ड बदलते रहना चाहिए। वित्तीय कार्यों

हेतु यथासंभव अपने बैंक की एटीएम मशीन का इस्तेमाल करने की कोशिश करनी चाहिए। विशेष रूप से उस एटीएम का जोकि बैंक शाखा से जुड़ा हो और वहां वैध सुरक्षा गार्ड हो।

- एटीएम का उपयोग करने से पहले मशीन में किसी भी तरह की आशंका, परिवर्तन और क्षति के संकेत की जांच करें। वहां स्कीमिंग डिवाइस लगा हो सकता है।
- किसी भी प्रकार की गड़बड़ी या धोखाधड़ी का पता चलने पर तुरंत अपने एटीएम कार्ड को टोल फ्री नंबर पर फोन करके ब्लॉक कराएं तथा इसकी शिकायत बैंकिंग लोकपाल व पुलिस से भी करें।
- कार्ड के खो जाने या खाते अथवा कार्ड की जानकारी जाहिर हो जाए तो टोल फ्री हेल्पलाइन पर कार्ड को तुरंत ब्लॉक करा दें।
- एकदिवसीय आयोजन/कार्यक्रम जैसे, खेलकूद गतिविधियां, त्योहार, सेमिनार, कार्यशाला, मेला एवं प्रदर्शनी आदि में मुहैया कराई गई अस्थायी वित्तीय सुविधाओं के उपयोग से बचा जाना चाहिए।
- सार्वजनिक वाई–फाई माध्यमों में इंटरनेट बैंकिंग का उपयोग न करें।
- होटल, रेस्तरां, पेट्रोल पंप आदि स्थानों में एटीएम कार्ड का इस्तेमाल करते समय किसी दूसरे से पासवर्ड साझा न करें।
- बैंक विवरणी(स्टेटमेंट) की नियमित रूप से जांच करें तथा किसी भी अनधिकृत लेनदेन का पता लगते ही तुरंत बैंक को खबर करें। दुकानों या पेट्रोल पंप पर अपने सामने ही कार्ड का इस्तेमाल करें।
- रिस्तरां /शॉपिंग मॉल में प्रस्तुत किए गए किसी सर्वे फॉर्म में आप अपनी निजी जानकारी न भरें।
- अपने एटीएम पिन, सीवीवी या पासवर्ड का खुलासा किसी से न करें। बैंकों द्वारा भी इस प्रकार के विज्ञापन जारी किए जाते हैं कि बैंक या क्रेडिट कार्ड फर्म ग्राहकों से फोन या ई-मेल पर कार्ड का विवरण मांगने के लिए अधिकृत नहीं हैं। बावजूद, कई बार पढ़े-लिखे ग्राहक भी इसके शिकार हो जाते हैं।
- कार्ड की वैधता समाप्त होने, नया जारी होने पर पुराने कार्ड को काट कर इसके टुकड़े कर दें ताकि इसका दुरूपयोग न किया जा सके।

ऑनलाइन सावधानी

ई-शॉपिंग के लिए केवल सुरक्षित, स्थापित और वैध साइट का उपयोग करना ही समझदारी है। जिन साइटों में सिक्योर सॉकेट लेयर (एसएसएल) हो और जो एचटीटीपीएस का प्रयोग करती हैं, उन्हीं साइटों का उपयोग करना चाहिए। सिक्योरिटी क्लूज़ की पहचान, जैसे- आपके ब्राउजर के सबसे नीचे लॉक इमेज, यूआरएल का आरंभ https: से होना चाहिए। ऐसे संकेतों से पता चलता है कि आपकी खरीद को एंक्रिप्शन के साथ सुरक्षित किया गया है और आपके खाते की जानकारी सुरक्षित है। अर्थात् लेन-देन एवं खरीदारी हेतु केवल सुरक्षित वेबसाइट का इस्तेमाल करें। किसी भी साइट पर कार्ड के विवरण को सेव करने के लिए यदि पूछा जाए तो उस पर कदापि

क्लिक न करें। साथ ही, साइट के पेमेंट वेरीफिकेशन टूल्स, जो पेमेंट को सत्यापित करता है, पर भी सतर्कता से नजर रखनी चाहिए। आप उसी मर्चेंट या शॉप में खरीदारी करें जिन्हें आप जानते हैं और जिन पर आपको भरोसा हो। अपने क्रेडिट/डेबिट कार्ड से खरीदारी करने के बाद उस वेबसाइट से लॉग-ऑफ हो जाएं और ब्राउजर कुकीज़ को डिलीट कर दें। ऑनलाइन माध्यमों में निजी जानकारी प्रदान करते समय सावधान रहें।

कम्प्यूटर और स्मार्टफोन से बैंकिंग करते वक्त सावधानी

कम्प्यूटर और स्मार्टफोन में सदैव एंटी वायरस सॉफ्टवेयर डालकर रखें, ताकि किसी भी प्रकार के मालवेयर से बचा जा सके। आज कई ऐसे ऐप हैं जो मोबाइल चोरी हो जाने के बाद भी दूर से ही डेटा खत्म कर देते हैं। ऐसा कोई ऐप स्मार्टफोन में इंस्टॉल करना अच्छा होता है ताकि संभावित खतरों से बचा जा सके। बैंक में मोबाइल और ई-मेल अलर्ट अपडेट करके रखें ताकि कोई ट्रांजेक्शन हो तो तुरंत पता चल सके। सोशल मीडिया और अन्य ऑनलाइन खातों में लॉग-आउट करना भी खाते की सुरक्षा के लिए अत्यंत जरूरी है। मोबाइल फोन पर गोपनीय पासवर्ड रखने से परहेज करना चाहिए। कार्ड धोखाधड़ी से बचने के लिए नियमित रूप से पासवर्ड बदलते रहना भी फायदेमंद रहता है।

सभी ई-मेल संदेशों को ध्यान से देखें ताकि आपको फिशिंग स्कैम का पता लग जाए। ऐसे किसी मेल का जबाव न दें जिसमें आपसे आर्थिक जानकारी समेत आपकी निजी जानकारी मांगी गई हो। क्योंकि बैंक कभी ऐसी जानकारी आपसे नहीं मांगता। भुगतान जानकारी कभी-भी ई-मेल के जरिए न भेजें। इंटरनेट (जैसे कि ई-मेल) से भेजी जाने वाली सूचना हमेशा पूरी तरह से सुरक्षित नहीं होती; कोई भी तीसरा पक्ष इन्हें पढ़ सकता है। प्रमोशनल स्कैम से सावधान रहें। पहचान की चोरी के लिए आपसे फोन पर निजी जानकारी मांगी जा सकती है और सबसे ज्यादा जरूरी कि अपने पासवर्ड को सदैव गोपनीय रखें। कुछ ऑनलाइन स्टोर यूज़रनेम तथा पासवर्ड के साथ रजिस्टर करने की मांग करते हैं। ऑनलाइन पासवर्ड को दूसरों से छुपा कर दें, उसी प्रकार आप एटीएम पासवर्ड को भी दूसरों से सुरक्षित रखें। नेटबैंकिंग के लिए सदैव वर्चुअल की-बोर्ड का इस्तेमाल करें।

इसके अलावा, यदि अपने प्लास्टिक मुद्रा कार्ड को धोखाधड़ी से बचाने हेतु हम निम्न रेडी रेकनर का इस्तेमाल करें, तो बहुत हद तक अपने कार्ड को सुरक्षित बना सकते हैं।

ऐसा करें

- एटीएम का इस्तेमाल करने से पहले आप यह देख लें कि इंसर्शन पैनेल पर किसी प्रकार की दूसरी वस्तु न रखी हो (स्किमिंग से बचने हेतु)।
- ट्रांजैक्शन के समय एटीएम पिन नम्बर को हथेली से छुपा दें। ट्रांजैक्शन रसीद न छोड़ें।
- अपने एटीएम पिन को हर तीन महीने पर बदल दें।
- केवल ऐसे ही क्रेडिट कार्ड को साथ में रखें जिनकी आपको ज्यादा आवश्यकता हो।
- अपने घर को बदलने से पहले ही अपने कार्ड निर्गतकर्ता (जारीकर्ता) को पता बदलने की सूचना दे दें।

ऐसा न करें

- अपना कार्ड नंबर एवं पिन किसी को न दें, भले ही वह अपनी पहचान बैंक के कर्मचारी के रूप में बताए।
- किसी अजनबी व्यक्ति द्वारा एटीएम मशीन में आपको मदद करने की पेशकश के बहकावे में आने से बचें। किसी अज्ञात/अवैध स्रोत के साथ आप अपने खाते के विवरण को साझा न करें।
- किसी सार्वजनिक स्थान में स्थित किसी शेयर्ड या असुरक्षित कम्प्यूटर से आप नेट-बैंकिंग एक्सेस न करें अथवा वहां अपने क्रेडिट/डेबिट कार्ड से भुगतान न करें।
- किसी अनपेक्षित स्रोत से आए अजनबी ई-मेल अटैचमेंट को न खोलें या इन्स्टेंट मैसेज डाउनलोड लिंक पर क्लिक न करें। किसी भी संदेहास्पद ई-मेल को तुरंत डिलीट कर दें।
- अपनी खाता संख्या की जानकारी किसी को फोन पर तब तक न दें, जब तक कि आप कॉल करके सुनिश्चित न कर लें कि अमुक कंपनी प्रतिष्ठित है और उसे यह जानकारी देनी चाहिए। जब आपको कोई फोन कॉल आए और क्रेडिट कार्ड का विवरण मांगा जाए तो आप उसे कोई जानकारी न दें (इसे विशिंग कहते हैं।)।
- किसी भी ई-मेल में अपने खाते से संबंधित मांगी गई कोई भी गोपनीय सूचना जैसे कि- पासवर्ड, कस्टमर आइडी, डेबिट कार्ड नम्बर, पिन, CVV2, DOB की जानकारी कभी न दें, भले ही वह ई-मेल किसी भी सरकारी प्राधिकारों जैसे कि आयकर विभाग, भारतीय रिज़र्व बैंक या वीजा या मास्टर कार्ड से जुड़ी किसी कंपनी का ही क्यों न हो।
- अपने बैंक खाते से जुड़ी किसी समस्या या खाते के विवरण तथा पासवर्ड आदि किसी सोशल नेटवर्किंग साइट या ब्लॉग पर नहीं दें।

कुछ सुझाव

कार्ड की धोखाधड़ी से बचाव हेतु कार्ड जारीकर्ताओं, सरकार एवं नियामक संस्थाओं तथा कार्ड धारकों द्वारा किए जाने वाले उपाय :-

कार्ड जारीकर्ताओं द्वारा किए जाने वाले उपाय -

- धोखाधड़ी की छानबीन एवं रोकथाम हेतु सॉफ्टवेयर लगाना जो ग्राहक के सामान्य एवं असामान्य व्यवहार का विश्लेषण करें एवं संभावित धोखाधड़ी से बचने हेतु लेन-देन पर नजर रखें।
- कार्डधारक द्वारा सत्यापन न किए जाने तक कार्ड को ब्लॉक रखना ।
- कार्ड लेनदेन के सुदृढ अधिप्रमाणन (Authentication) संबंधी सख्त उपाय, जैसे कि कार्डधारक से खाता नंबर, पिन, जिप नंबर, व्यक्तिगत प्रश्न आदि पूछना तथा इस तथ्य का सत्यापन करना कि लेनदेन कार्डधारक द्वारा ही किया गया है तथा इसकी पुष्टि टेक्स्ट संदेश, फोन कॉल या सुरक्षा टोकन डिवाइस जैसे परिचित या विश्वस्त माध्यमों से ही हुई है।
- सभी ज्ञात एवं संभावित धोखेबाजों की सूचनाओं का आदान-प्रदान संपूर्ण उद्योग स्तर पर हो।

सरकार एवं नियामक संस्थाओं तथा व्यापारियों द्वारा किए जानेवाले उपाय-

- कार्ड धोखाधड़ी से ग्राहक को बचाने हेतु सशक्त कानून व्यवस्था।
- डेबिट कार्ड/क्रेडिट कार्ड/गिफ्ट कार्ड कंपनियों की कार्य-प्रणाली एवं जोखिम क्षमताओं का नियमित निरीक्षण।
- कार्ड धारकों के हितों की रक्षा हेतु आवश्यक दिशानिर्देशों का प्रकाशन एवं धोखाधड़ी की गतिविधियों की निगरानी।

कार्डधारकों द्वारा किए जानेवाले उपाय

- गुम हुए या चोरी हुए कार्ड की तत्काल सूचना देना ।
- अनधिकृत लेनदेनों की त्वरित रिपोर्टिंग।
- अपना खाता नंबर, कार्ड समाप्त होने की तारीख तथा संबंधित कंपनी का फोन नंबर और पता सुरक्षित स्थान पर दर्ज करके रखना।

उपसंहार

इस प्रकार हम देखते हैं कि तकनीकी रूप से कार्ड धोखाधड़ी रोकने हेतु कई सारे उपाय सृजित किए गए हैं। बावजूद इसके धोखाधड़ी की संख्या दिन-प्रतिदिन बढ़ती ही जा रही है। ऐसे समय में, इन उपायों के साथ ही देश में एक कठोर कानून बनाने की भी आवश्यकता है। ध्यान से अगर देखें तो यह कड़वा सच सामने आता है कि इस अपराध से भारतीय कानून अंजान है। इसे सूचना प्रौगिकी अधिनियम के दायरे तक सीमित कर दिया गया है। जिसका नतीजा है कार्ड धोखाधड़ी की बढ़ती घटनाएं।

हालांकि, कार्ड धोखाधड़ी से बचाव एवं नकदी रहित अर्थव्यवस्था में इस विकल्प की बेहतर भूमिका हेतु समय-समय पर सरकार बैंकों को त्वरित कार्रवाई करने का निर्देश देती रहती है। इसी दिशा में सरकार द्वारा ओटीपी के माध्यम से एटीएम में जालसाजी रोकने हेतु निवारक उपाय अपनाने पर विचार किया जा रहा है। साथ ही केंद्र सरकार डेबिट कार्ड के जरिये बैंक ग्राहक के खाते में सेंध लगाने की कोशिशों को वन टाइम पासवर्ड (ओटीपी) द्वारा सुलझाने पर भी विचार कर रही है। इस व्यवस्था में एटीएम के जरिये कोई भी लेन-देन एक ही बार होगा और अगली बार पासवर्ड बदल जाएगा। इस व्यवस्था में पासवर्ड मोबाइल के जरिये ग्राहक को प्राप्त होगा। अगर यह व्यवस्था लागू हो गई तो यह अत्यंत क्रांतिकारी साबित होगा।

इसके अतिरिक्त केंद्र सरकार द्वारा देश में बैंकिंग सेवाओं को बढ़ाने और ग्राहक सुविधा सुधारने की कवायद में भौगोलिक सूचना प्रणाली मानचित्रण (जी.आई.एस. मैपिंग) की भी तैयारी की जा रही है। इसके माध्यम से विभिन्न पहलुओं पर बैंकों से रोजाना की जानकारी मिलेगी। साथ ही शहरी और ग्रामीण क्षेत्रों में बैंकिंग सेवाओं की पहुंच के बारे में भी जानकारी मिलेगी।

अंत में धोखाधड़ी से बचाव हेतु एकमात्र सूत्र वाक्य है - बैंक सुरक्षा व तकनीक पर बढ़ाएं निवेश, ग्राहक सावधानी बरतें। उदाहरण के लिए, डेटा हैकिंग को लिया जा सकता है। डेटा हैकिंग के लिए एक प्रवेश बिंदु की जरूरत होती है, जो कई बार ग्राहक लापरवाही बरतते हुए उपलब्ध करा देता है। इससे बचने के लिए उपभोक्ताओं को एटीएम, क्रेडिट कार्ड व नेटबैंकिंग पासवर्ड किसी को नहीं देना चाहिए और समय-समय पर इसे बदलते भी रहना चाहिए और

ये ऐसा नहीं होना चाहिए कि कोई भी इसका अंदाजा लगा सके। कार्ड के पीछे मैग्नेट चिप होती है, जिस पर खाता संबंधी सारी जानकारी होती है। इसलिए इस पर डबल आइडेंटिफिकेशन होनी चाहिए। नेट बैंकिंग उपभोक्ताओं को डेटा चोरी रोकने लिए सबसे ज्यादा कदम बैंक स्तर पर उठाए जाने चाहिए। ग्राहकों को ऑनलाइन लेनदेन सुरक्षित वेबसाइट के जरिये करना चाहिए। बैंकिंग में इलेक्ट्रॉनिक लेनदेन सिस्टम एक स्विच के माध्यम से होता है। हैकर इसी स्वीच को हैक कर बैंक ग्राहकों की जानकारी प्राप्त कर लेते हैं। इसलिए बैंकों को प्रत्येक लेनदेन का एसएमएस अलर्ट ग्राहकों को भेजना चाहिए। स्विच प्रबंधनकर्ता या स्विच सुरक्षा प्रबंधक को किसी खाते में सामान्य के मुकाबले अचानक अधिक लेनदेन होने पर सतर्क रहना होगा। उसे इसकी जांच कर यह सुनिश्चित करना चाहिए कि कहीं हैकिंग तो नहीं हुई है?

बैंकों में इस समय 30 फीसदी से ज्यादा लेन-देन ऑनलाइन हो रहे हैं। भविष्य में ऑनलाइन लेनदेन में और इजाफा होने वाला है। ऐसे में बैंकों को तकनीक और सुरक्षा पर निवेश बढ़ाना होगा। बैंकों ने इस पर काफी कम निवेश किया हुआ है। जबकि यह भविष्य की बैंकिंग है। ऐसे में, इस प्रकार के नियम बनने चाहिए जिसमें बैंकों को उनके कारोबार का निश्चित हिस्सा सुरक्षा एवं तकनीक पर निवेश करने का प्रावधान हो।

फिर भी इस तथ्य को नजरअंदाज नहीं किया जा सकता कि कार्ड संबंधित धोखाधड़ी एवं गड़बड़ी पूरी दुनिया की समस्या बन चुकी है। ऐसे में इस समस्या से निपटने की तुरंत जरूरत है और इसके लिए सबसे बड़ी जरूरत है कि डाटा के रूप में मौजूद सूचना के संरक्षण पर पूरा ध्यान दिया जाए। एटीएम-डेबिट कार्ड की डेटा चोरी बैंकों की तकनीकी सुरक्षा प्रणाली की कमी को जरूर दर्शाती है, लेकिन इससे ग्राहकों को घबराने की जरूरत नहीं है, क्योंकि भारतीय बैंकों की सुरक्षा प्रणाली अत्यंत मजबूत है। ग्राहकों का भी दायित्व है कि धोखाधड़ी के प्रति ज्यादा जागरूक व सतर्क रहें तथा बैंकिंग क्षेत्र में आए दिन हो रहे तकनीकी बदलावों से अपने को अतन रखें तथा बैंक द्वारा बताई जा रही सावधानियों का भी अनुपालन करें। निष्कर्षतः "यह हमारा कर्तव्य है कि इसे धोखाधड़ी करने वालों के लिए अतिसंवेदनशील स्थिति में न छोड़ दें।" सावधान एवं जागरूक रहना ही एकमात्र उपाय है।