साइबर–अपराधों की रोकथाम

भारत इंटरनेट इस्तेमाल करने वाला विश्व का तीसरा देश है। आप अपने मोबाइल, कंप्यूटर आदि के माध्यम से इंटरनेट से जुड़े रहते हैं। इसलिये साइबर अपराध के बारे में जानना अत्यंत आवश्यक हो गया है। विमुद्रीकरण के पश्चात बैंकिंग इंडस्ट्री में डिजिटल लेनदेन में अत्यधिक वृद्वि हुई है साथ ही साथ साइबर क्राइम भी बढ़ा है। विगत दिनों 10 करोड़ ग्राहकों का डाटा चोरी, साइबर अटैक की खबरों पर पूरी दुनिया नये सिरे से इसका समाधान निकालने में लगी है।

अ. साइबर अपराध के प्रकार

1. निजी जानकारी चुराना :- साइबर अपराधी आपके कंप्यूटर / मोबाइल नेटवर्क में प्रवेश कर आपकी निजी जानकारी जैसे – नेटबैंकिंग पासवर्ड, आपके डेबिट कार्ड क्रेडिट कार्ड की जानकारी आदि। इसे हैकिंग भी कहा जाता है।
2. फिशिंग :- इसमें साइबर अपराधी आपको फर्जी ईमेल या संदेश भेजते हैं, जो भारतीय रिजर्व बैंक, किसी प्रतिष्ठित कंपनी, आपकी बैंक, ऑन लाइन शापिंग कंपनी के तरह मिलते जुलते नाम के रहते हैं, अगर आप सतर्क नहीं हैं तो इनके झांसे में जल्दी आ जाते हैं। इन नकली ईमेल या संदेश का आश्य निजी जानकारी जैसे आपका नाम, ईमेल आई.डी, पता, जन्म तिथि, पासवर्ड, बैंक खाता नम्बर, मोबाइल या फोन नम्बर,ए.टी.एम डेबिट कार्ड तथा क्रेडिट कार्ड नम्बर, ए.टी.एम डेबिट कार्ड तथा क्रेडिट कार्ड नम्बर का वेलीडेशन कोड आदि चुराकर उनका दुरूपयोग करना होता है।
3. वायरस अटैक :- साइबर अपराधी कुछ ऐसे साफ्टवेयर आपके कंप्यूटर / मोबाइल नेटवर्क पर भेजते हैं जिससें उसकी कार्यक्षमता प्रभावित होती है, इसमें वायरस वर्म, टार्जन हार्स, लाजिक हार्स आदि कंम्युटर को काफी हानि पहुंचा सकते हैं।
4. साफ्टवेयर पाइरेसी :- साफ्टवेयर की नकल तैयार कर सस्ते दाम पर बेचना भी साइबर क्राइम है। इससे साफ्टवेयर सही काम नहीं करता था कम्युटर में रखा अन्य डाटा भी खराब हो जाता है तथा आपके कीमती उपकरण भी ठीक से काम नहीं करते।
5. फर्जी बैंक काल :- आपको जाली ईमेल, संदेश या मोबाइल काल प्राप्त हो जो आपके बैंक जैसा लगे जिसमें आपसे पूछा जाये कि आपके ए.टी.एम कार्ड नंबर और पासवर्ड की आवश्यकता है और यदि यह जानकारी नहीं दी तो आपका कार्ड ब्लाक हो जावेगा या आपका खाता बंद हो जावेगा अथवा आधार नम्बर को सिडिंग करने उक्त जानकारी आवश्यक है या किसी लिंक पर क्लिक कर सूचना दें। याद रखें कि बैंक द्वारा ऐसी जानकारी कभी भी इस तरह नहीं मांगी जाती और भूलकर इस प्रकार की जानकारी को इंटरनेट या फोनकाल या मैसेज के माध्यम से शेयर न करें।

ब. सुरक्षित इंटरनेट बैंकिंग कार्यप्रणाली (Secure Internet Banking Practices)

यह न करें :-

- अज्ञात स्त्रोतों से फाइल डाउनलोड।
- पॉपअप विंडो द्वारा ड्रायवर इत्यादि डाउनलोड।
- किसी भी वेबसाइट को अपने कम्युटर पर साफ्टवेयर इंस्टाल करने की अनुमति।
- किसी भी फेसबुक लिंक / संदेश लिंक पर क्लिक।

यह करें :-

- अपनी निजी जानकारी , पासवर्ड को सुरक्षित रखें, डेबिट कार्ड, क्रेडिट कार्ड नंबर किसी को न बतायें एवं निजी जानकारी नेट के वेबब्राउजर (एस.एस.एल का उपयोग करें या इनस्क्रीप्शन फार्म) में रखें।
- फॉयरवाल तकनीक, प्राक्सी सर्वर एवं सुरक्षित राउटर कान्फ्रीगेशन करें।

स. सुरक्षित ईमेल कार्यप्रणाली (Secure Email Practices)

E-mail पर आए Attachments को खोलते वक्त सावधानी बरतें।

यह न करें :-

- अनापेक्षित, अकारण, अज्ञात ईमेल बिना पुष्टि के न खोलें एवं न ही उनका जवाब दें।
- अज्ञात ईमेल में दिये गये अज्ञात लिंक जोक्स, विडियो पर क्लिक।
- अपना पासवर्ड किसी को न बताएं।

यह करें :-

- पासवर्ड मजबुत बनायें अथार्त पासवर्ड में करेक्टर, न्यूमरिक एवं स्पेशल करेक्टर का समावेश हो तथा पासवर्ड कभी भी किसी से शेयर न करें। पासवर्ड 8 से 10 अंकों का स्ट्रांग माना गया है । कुछ अक्षर छोटे तथा कुछ बड़े हों। (Use strong password)
- प्रत्येक यूजर का अलग कम्यूटर खाता होना चाहिये। (Use separate computer accounts for each user)
- यूजर्स को स्क्रीन लॉक ऑपशन का उपयोग करना चाहिये। (Use screen locking)
- लॉग आन और लॉग आफ सिस्टम में दिये गये मेनू से करना चाहिये। (log On and Off)
- संवेदनशील डाटा फाइल या हार्ड डिस्क ड्राइव को इंक्रीप्ट करने पर गंभीरता से विचार करें। (Seriously consider encrypting sensitive data file or entire HDD, especially for Mobile/ laptops)
- सुरक्षा हेतु सिस्टम पर Security Event Logging को Enabled रखें। (Enable security event logging)
- कार्य / दिन की समाप्ति पर कंप्यूटर सिस्टम शट डाउन करें। (Shut down the system at the end of the day)

द. ए.टी.एम का सुरक्षित प्रयोग

यह न करें :-

- कभी भी अपना ए.टी.एम कार्ड एवं पिन किसी को भी न दें । कभी भी अपना पिन पर्स या बटुआ में न रखें। यदि कोई अपने को बैंक का अधिकारी भी कहता हो तो भी कार्ड या पिन न दें।
- कार्ड पर या कार्ड के पीछे अपना पिन नंबर न लिखें।
- किसी को भी अपना पासवर्ड/पिन इंनपुट न देखने दें।
- जन्म दिन या मोबाइल नंबर आदि को पासवर्ड/पिन के रूप में न बनाएं। इसे आसानी से अनुमान लगाया जा सकता है।
- अपना कार्ड अपने पास सुरक्षित रखें, कार्ड को कहीं भी कभी भी न छोड़े।
- ए.टी.एम पिन के संबंध में प्राप्त किसी ईमेल का जवाब न दें। इसे फिशिंग प्रयास कहा जाता है।
- टेलीफोन पर ए.टी.एम कार्ड या पिन या OTP / CVV नंबर आदि की कोई जानकारी किसी को न दें।
- ए.टी.एम का उपयोग करते समय अनजान व्यक्ति या सुरक्षा गार्ड से सहायता स्वीकार न करें। बैंक को फोन करें।

यह करें :-

- अपने पिन (व्यक्तिगत पहचान संख्या) को याद रखें एवं अन्य सभी भौतिक प्रमाणों को नष्ट कर दें।
- पिन नंबर नोट करने के पश्चात तुरंत पिन मेलर को नष्ट करें।
- पिन नंबर प्राप्त होने के पश्चात उसे एक्टीवेट करें एवं तत्काल पिन नंबर बदलें।
- कार्ड का पहला उपयोग ए.टी.एम पर करें। इसके बिना प्वांइट आफ सेल (PoS **मशीन**) पर कार्ड कार्य नहीं करेगा।
- ए.टी.एम लेनदेन का sms की सुविधा प्राप्त करने के लिये बैंक में अपना वर्तमान / सही मोबाइल नंबर अवश्य पंजीकृत करावें, ताकि हर लेनदेन की आपको सूचना मिलें।
- खाते में यदि कोई अनाधिकृत कार्ड लेनदेन होता है तो बैंक को तुरंत सूचित करें। यह आपके कार्ड से की जा रही धोखाधड़ी को रोकने में मदद करता है।
- यदि आपको किसी ए.टी.एम क्षेत्र में संदिग्ध लोग दिखाई देते हैं अथवा आपको ऐसा लगता है तो ऐसे ए.टी.एम में लेनदेन न करें या प्रतिक्षा करें। ए.टी.एम में लेनदेन के समय अनजान लोगों से अनावश्यक बातचीत न करें तथा संदिग्ध गतिविधियों से सावधान रहें।
- ए.टी.एम में लेनदेन शुरू करने के बाद कोई संदेह या समस्या उत्पन्न हो जाती है तो लेनदेन को निरस्त करने का बटन दबायें।
- पिन दर्ज करते समय पूर्ण सावधानी रखें ताकि आपका पिन कोई देख न लें।
- ए.टी.एम छोड़ने से पहले नगदी एवं कार्ड लेना न भूलें।
- ATM छोड़ने के पहले यह पक्का कर लें कि कार्ड डालने के स्थान पर लाइट ब्लिंक कर रही हो।
- कृपया सुनिश्चित करें की प्वाइंट आफ सेल में कार्ड का स्वाइप आपके सामने ही किया गया है।
- यदि आपका ए.टी.एम कार्ड गुम गया है या चोरी हो गया है तो तुरंत उसे हाट लिस्ट अर्थात उस पर रोक लगवायें। इस हेतु टोल फ्री नम्बर पर काल करें एवं अपनी बैंक शाखा को सूचित करें।
- यदि आपके कार्ड की अवधि समाप्त हो जाती है या आप खाता बंद करते हैं तो ए.टी.एम कार्ड को चार टुकड़ों में इस प्रकार काटें जिससे चुंबकीय पट्टी. नष्ट हो जावे।
- ए.टी.एम से जुड़ी यदि कोई डिवाइज/ पट्टी आदि दिखाई दे तो तुरंत बैंक को सूचित करें क्योंकि यह आपके डाटा को चुराने / या रोकड़ गायब करने के लिये किया गया प्रयास हो सकता है।

य. प्वाइंट आफ सेल (PoS):-

PoS ग्राहकों को राशि जमा करने, आहरण करने, अंतरण करने की सुविधा देती है। यह एक Micro ATM भी हो सकता है। इसमें एक electronic device होती है, जो ATM Debit Card, Credit Card के जरिये किसी भी व्यक्ति से भुगतान स्वीकार करती है। इससे अपने पास नगदी रखने की आवश्यकता नहीं होती। चिल्हर की समस्या नहीं होती। PoS में Payment online होता है, इसलिये Tax की चोरी एवं भ्रष्टाचार को रोकने में भी मदद मिलती है। PoS के प्रयोग से भारतीय अर्थव्यवस्था को फायदा होता है एवं बिना cash के व्यापार किया जा सकता है।

यह न करें :-

- प्वांइट आफ सेल में राशि enter करने हेतु दुकानदार को न कहें।
- पिन नंबर दुकानदार को न बतायें, स्वयं enter करें।

यह करें :-

- ATM Debit Card, Credit Card अपने सामने प्वांइट आफ सेल में Swipe करें।
- Mobile नंबर बैंक खाते के साथ लिंक रखें एवं sms का अलर्ट की सुविधा को active रखें ताकि लेनदेन के तुरंत पश्चात से आपके मोबाइल पर प्राप्त संदेश से सही लेनदेन की तुरंत पुष्टि हो सके।
- पिन दर्ज करते समय पूर्ण सावधानी रखें ताकि आपका पिन कोई देख न लें।
- यदि आपको अहसास होता है कि कोई अन्य व्यक्ति आपके पिन को वॉच कर रहे हैं तो एक हाथ से पिन पेनल को कव्हर करें एवं दूसरे हाथ से पिन नंबर प्रविष्ट करें। संभव है कि आपको थोड़ी झिझक हो, परंतु यह आपकी सुरक्षा के लिये आवश्यक है।
- यदि आप अंतरराष्ट्रीय लेनदेन के लिये कार्ड का इस्तेमाल कर रहे हों तो पहले सुनिश्चित कर लें कि आपका कार्ड मैगनेटिक स्ट्रीप ई.एम.वी. चीप (Europay, MasterCard and Visa) वाला हो । यह निर्देश भारतीय रिजर्व बैंक द्वारा जारी किये गये हैं।

र. **ई-कॉमर्स (e-Commerce):-**

e-Commerce या ई–व्यवसाय इंटरनेट अथवा इलेक्ट्रानिक की मदद से व्यापार संचालन का एक माध्यम है इसमें खरीदी, बिक्री के अलावा अन्य सेवायें विद्य**मान रहती है,** जैसे ए.टी.एम कार्ड का उपयोग कर IRCTC tickets booking, mobile recharge, payment of Electicity bill, movie tickets, वस्तु एवं अन्य सेवायें ऑनलाइन क्रय कर सकते हैं। जिससे कैशलेस लेनदेन को बढ़ावा मिलेगा एवं नोटों की प्रिंटिंग एवं रखरखाव में होने वाले खर्चों में कमी आयेगी।

यह न करें :-

- कार्ड नम्बर एवं इसके पीछे अंकित सीवीवी (card verification value) किसी भी व्यक्ति से शेयर न करें।
- किसी भी व्यक्ति द्**वारा** किये गये लुभावने कॉल, ईमेल संदेशों से बचें जो कर्मचारियों अथवा अन्य व्यक्तिगत जानकारी शेयर करने को कहते हों।
- किसी वेबसाइट की सुरक्षा की जांच किये बिना इंटरनेट पर कोई संवेदनशील सूचना न दें।
- यदि आपको विश्वास नहीं है कि यह ई मेल कानूनी है या नही ंतो सीधे कंपनी से संपर्क कर पुष्टि करने की कोशिश करें।

यह करें :-

- ई – वॉलेट या प्लास्टिक मनी का उपयोग करें।
- बैंक खाता नंबर, कार्ड, पिन डिटेल को गोपनीय रखें। पासवर्ड नियमित अंतराल में परिवर्तित करते रहें।
- अपने खाते के स्टेटमेंट को नियमित रूप से जांच करें।
- अपने मोबाइल कम्प्यूटर पर antivirus और एंटी मालवेयर का प्रयोग करें।
- आनलाइन शॉपिंग पर फाइनल प्रिंट को सावधानी से पढ़ना चाहिये।
- शॉपिंग के पूर्व डिलीवरी टाइम, प्रभारों, आर्डर निरस्त करने के नियम एवं सामान लौटाने की नीतियों और वारंटी की जानकारी अवश्य प्राप्त करें।

ल. मोबाइल बैंकिंग (Mobile Banking):-

नोटबंदी के दौरान देश में कैश की किल्लत बढ़ने से एवं डिजिटल इंडिया अभियान से प्रभावित होकर आम आदमी "नगद रहित अर्थव्यवस्था" की ओर बढ़ा **है।** मोबाइल बैंकिंग बहुत सुरक्षित है। मोबाइल बैंकिंग के जरिये बैंकिंग सुविधा ग्राहकों की जेब तक पहुंच गयी है। कोई भी सामान खरीदने से लेकर बड़े–बड़े भुगतान, enquiry एवं fund transfer करने के लिये लोगों को बैंक जाने की जरूरत नहीं है। मोबाइल बैंकिंग सुविधा 24 *7 घर पर उपलब्ध रहती है।

यह न करें :-

1. अपना यूजर आईडी, बैंक खातों की जानकारी और पासवर्ड (MPIN/TPIN) से संबंधित जानकारी अपने फोन के डिवाइज में न रखें। किसी गलत हाथों में मोबाइल जाने से आपको नुकसान हो सकता है।
2. अगर कहीं आपके मोबाइल को नेटवर्क नहीं मिल पा रहा हो तो लालच में फ्री वाई फाई या हॉट स्पाट से मोबाइल बैंकिंग का उपयोग न करें। अगर ऐसा करते हैं तो डाटा चोरी की आशंका बनी रहती है।
3. अपने बैंक एकाउंट या मोबाइल बैंकिंग से संबंधित गुप्त/व्यक्तिगत डाटा को text message के जरिये भेजने की भी गलती न करें।
4. साइबर चोर फोन पर बात करने के दौरान भी आपके फोन से डाटा ट्रांसफर कर सकते हैं। इसलिये अनजान कॉल आने पर बातचीत करने में सावधानी रखें।

यह करें :-

1. मोबाइल बैंकिंग से संबधित एप्प डाउनलोड करने बैंक की वेबसाइट www.cgbank.in अथवा गुगल प्लेस्टोर से "CRGB m-Tej " का चुनाव करें। किसी भी सिक्योर वेबसाइट को पहचानने का सबसे सरल तरीका है इसका यूआरएल https से शुरू होता है। यहां s का मतलब सिक्योर से होता है और यह यूआरएल सिक्योर सॉकेट्स लेयर कनेक्शन का प्रयोग करता है।
2. सेफ मोबाइल बैंकिंग का इस्तेमाल करने के लिये स्क्रीन लॉक का प्रयोग करें।
3. Mpin एवं Tpin की जानकारी गोपनीय रखें।
4. एंटीवायरस साफ्टवेयर का प्रयोग करें तथा उसे अपडेट रखें ताकि मॉलवेयर आदि वायरस से मोबाइल को सुरक्षित रखा जा सके।
5. मोबाइल बैंकिंग से संबंधित कार्य के पश्चात तुरंत लागआउट करें।
6. लेनदेन के पश्चात enquiry option में जाकर बेलेंस चैक करें।
7. यदि आप अपने मोबाइल फोन का उपयोग मोबाइल बैंकिंग के लिये करते हैं तो फोन को लॉक करने के साथ एप्प को भी पासवर्ड से लॉक रखें ।