न्याय सब के लिए
ACCESS TO JUSTICE FOR ALL

साइबर अपराध और साइबर सुरक्षा

राजस्थान राज्य विधिक सेवा प्राधिकरण

साइबर सुरक्षा जागरूकता क्यों महत्त्वपूर्ण है? (Why is Cyber Security Awareness Important?)

तकनीकी विकास ने आधुनिक जीवन शैली को बदल दिया है। समय के साथ इंटरनेट का प्रयोग आम जीवन में बढ़ता जा रहा है। जिसके कई लाभ हैं जैसे दोस्तों के साथ बातचीत करने, विभिन्न विषयों की जानकारी प्राप्त करने, बैंकिंग लेनदेन करने, ऑनलाइन सेवाओं का लाभ उठाने, नौकरी खोजने, जीवन साथी खोजने, यहां तक कि पूरा व्यवसाय चलाने के लिए इंटरनेट बहुत उपयोगी है। लेकिन इसके कुछ नुकसान भी हैं। नए और शक्तिशाली साइबर अपराधी नियमित रूप से इंटरनेट पर हमला कर रहे हैं। हमारी छोटी सी चूक साइबर अपराधियों के लिए डेटा चोरी के द्वार खोल सकती है। साइबर अपराधी हमारे पैसे चुरा सकते हैं। हमारी प्रतिष्ठा को नुकसान पहुंचा सकते हैं। अधिकांश साइबर अपराध मानवीय लापरवाही के कारण होते हैं। इसलिए, साइबर सुरक्षा जागरूकता महत्त्वपूर्ण है।

साइबर अपराध क्या है? (What is Cyber Crime?)

साइबर अपराध एक ऐसा अपराध है जो कम्प्यूटर और नेटवर्क के माध्यम से किया जाता है। इसमें गतिविधियों की विस्तृत श्रृंखला जैसे गैरकानूनी रूप से किसी की निजी जानकारी प्राप्त करना, जानकारी मिटाना, उसका गलत इस्तेमाल करना, उसमें फेरबदल करना, ऑनलाइन बैंक खातों से पैसे चुराना आदि सम्मिलित हैं।

साइबर अपराध हमेशा आर्थिक लाभ से प्रेरित नहीं होते हैं अपितु साइबर अपराध में गैर– आर्थिक लाभ भी शामिल हैं। इसमें नौकरी से संबंधित धोखाधड़ी, वैवाहिक धोखाधड़ी व्यक्तिगत जानकारी (आधार कार्ड का विवरण, क्रेडिट/डेबिट कार्ड का विवरण, बैंक खातों की सूचना आदि) को चुराकर उनका दुरूपयोग करना, सोशल मीडिया पर किसी व्यक्ति की मानहानि या कम्प्यूटर वायरस फैलाना आदि शामिल है। साइबर अपराध की परिणीति शारीरिक या यौन शोषण भी हो सकता है।

साइबर अपराध के प्रकार (Kinds of Cyber Crime)

पहचान की चोरी	मनोवैज्ञानिक तरकीबें	सोशल मीडिया धोखाधड़ी
डिजीटल बैंकिंग धोखाधड़ी	मोबाइल एप्लिकेशन के माध्यम से हमला	पर्सनल कम्प्यूटर/लैपटॉप पर वायरस का हमला

पहचान की चोरी (Theft of Identity)

पहचान की चोरी से आशय किसी की व्यक्तिगत जानकारी उसकी अनुमति के बिना गलत तरीके से प्राप्त करना है। व्यक्तिगत जानकारी में उसका नाम, फोन नंबर, पता, बैंक खाता नंबर, आधार कार्ड नंबर या क्रेडिट व डेबिट कार्ड नंबर आदि शामिल हो सकते हैं। पहचान की चोरी के कई गंभीर परिणाम हो सकते हैं।

धोखा देने वाला व्यक्ति चुराई गई व्यक्तिगत जानकारी का उपयोग –

- आपके बैंक खातों तक पहुंचने
- डेबिट या क्रेडिट कार्ड के अवैध उपयोग या बीमित राशि हड़पने
- आपके नाम से कर वापसी फाइल करने और धन वापसी प्राप्त करने के लिए
- ड्राइविंग लाइसेंस, पासपोर्ट या निवास प्रमाण–पत्र प्राप्त करने
- नए उपयोगिता खाते खोलने
- आपके स्वास्थ्य बीमा पर चिकित्सा उपचार प्राप्त करने
- सोशल मीडिया पर आपकी पहचान का दुरूपयोग करने
- गिरफ्तारी के दौरान पुलिस को आपका नाम देने आदि के लिए कर सकता है।

इसलिए, सभी को पहचान की चोरी के बारे में जागरूक होना चाहिए और यह जानना चाहिए कि इससे कैसे बचा जा सकता है।

सोशल मीडिया अकाउंट हैक या पहुंच प्राप्त करना (Hacking or gaining access to Social Media Accounts)

हमलावर पीड़ित का सोशल मीडिया अकाउंट हैक कर सकता है या उन तक पहुंच प्राप्त कर पीड़ित व्यक्ति की व्यक्तिगत जानकारी व फोटोग्राफ्स का दुरूपयोग कर सकता है। प्रोफाईल पर आपत्तिजनक सामग्री डाल सकता है अथवा मानहानि कर सकता है।

पहचान प्रमाणों की फोटो प्रतियों का दुरुपयोग (Misuse of photo copies of Identity Proofs)

हमलावर, पीड़ित के पहचान प्रमाणपत्र जैसे–पैन कार्ड, आधार कार्ड या अन्य किसी पहचान पत्र की फोटो प्रतियों का दुरुपयोग कर सकता है एवं धन हानि या अन्य किसी प्रकार से पीड़ित को नुकसान पहुंचा सकता है।

क्रेडिट/डेबिट कार्ड स्किमिंग (Credit/Debit Card Skimming)

क्रेडिट/डेबिट कार्ड की स्किमिंग एक छोटे उपकरण का उपयोग करके की जाती है, जिसे स्किमर कहा जाता है। क्रेडिट कार्ड की चुम्बकीय पट्टी में कार्ड की महत्त्वपूर्ण सूचना जैसे–नाम, क्रेडिट/डेबिट कार्ड नंबर और समाप्ति तिथि आदि अंकित होती है। सबसे पहले, क्रेडिट/डेबिट कार्ड को स्किमर के माध्यम से स्वाइप किया जाता है। फिर, स्किमर इन सभी विवरणों को कैप्चर करता है। अपराधी के द्वारा उपरोक्त सूचना का उपयोग ऑनलाइन लेनदेन करने/डुप्लिकेट क्रेडिट व डेबिट कार्ड बनाने/ए.टी.एम. से पैसे निकालने के लिए किया जा सकता है।

सुझाव (Tips)

- खाते को लॉग आउट किए बिना ब्राउजर विंडो को बंद न करें।
- किसी अन्य के कम्प्यूटर का उपयोग करते समय दो चरणीय सत्यापन जैसे– वन–टाइम पासवर्ड (ओटीपी) का उपयोग करें।
- वेब ब्राउजर पर उपयोगकर्ता पहचान (User ID) और पासवर्ड सेव न करें।
- सोशल नेटवर्किंग साइट पर गैर अधिकृत पहुंच की सूचना पाने के लिए अपना मोबाइल नम्बर पंजीकृत करें।
- साइबर कैफे के कम्प्यूटर पर डाउनलोड किए गए सभी दस्तावेजों को स्थायी रूप से हटा दें।
- अज्ञात व्यक्ति/संस्था को अपने पहचान प्रमाणों जैसे– आधार कार्ड, पैन कार्ड, वोटर कार्ड, ड्राईविंग लाइसेन्स आदि का विवरण या प्रतिलिपि कभी न दें।
- संदिग्ध स्थानों पर पहचान प्रमाण का उपयोग करते समय सावधान रहें।
- आपकी व्यक्तिगत सूचना जैसे– जन्म तिथि, जन्म स्थान, पारिवारिक विवरण, पता, फोन नंबर आदि किसी अज्ञात व्यक्ति/संस्था से साझा न करें।
- पहचान प्रमाण की फोटो प्रति हमेशा क्रॉस करके दें एवं उस पर देने का उद्देश्य लिखें, ताकि उसका पुनः उपयोग नहीं किया जा सके।
- अपने क्रेडिट, डेबिट या एटीएम कार्ड की रसीदों को बैंक/एटीएम या स्टोर में ना छोड़ें और ना ही सार्वजनिक स्थानों पर फेंके।
- हमेशा यह सुनिश्चित करें कि आपका क्रेडिट या डेबिट कार्ड शॉपिंग मॉल, पैट्रोल पंपों पर आपकी उपस्थिति में स्वाइप किया जाए विक्रेता को अपना कार्ड स्वाइप करने के लिए दूर ले जाने की अनुमति न दें।
- ध्यान रखें कि क्रेडिट या डेबिट कार्ड स्किमर्स पर तो प्रयोग नहीं किया जा रहा है।
- कभी भी अपना पिन नम्बर किसी के साथ साझा न करें, चाहे वह कितना भी नजदीकी क्यों न हो।

मनोवैज्ञानिक तरकीबें (Psycological Tricks)

मनोवैज्ञानिक तरकीबें वे हैं, जहां हमलावर आकर्षक प्रस्ताव के माध्यम से उपयोगकर्ता के दिमाग से खेलते हैं। एक बार फंसने के बाद हमलावर, पीड़ित के पैसे/व्यक्तिगत सूचना–नाम, आधार विवरण, बैंक खाते का विवरण आदि चोरी करके पीड़ित का शोषण कर सकते हैं। ये सभी कार्य पीड़ित को ई–मेल, फोन कॉल या एस.एम.एस के माध्यम से किए जाते हैं।

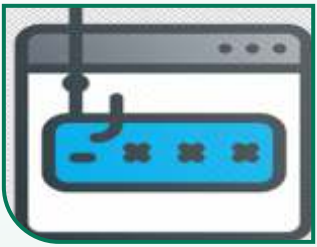
फिशिंग (Phishing)

फिशिंग धोखाधड़ी देने वाली ई–मेल के द्वारा किया जाने वाला कृत्य है, जो कि एक वैध स्रोत जैसे– बैंक, नियोजक या क्रेडिट कार्ड कंपनी इत्यादि से प्राप्त होना प्रतीत होता है। जिसके माध्यम से पीड़ित से व्यक्तिगत सूचना, बैंक खाता विवरण प्राप्त करने का प्रयास किया जाता है।

विशिंग (Wishing)

विशिंग फिशिंग के समान है। लेकिन इसमें ई–मेल के स्थान पर टेलीफोन के जरिए पीड़ित की व्यक्तिगत व वित्तीय सूचनाएं प्राप्त की जाती है।

स्मिशिंग (Smishing)



स्मिशिंग फिशिंग के समान धोखाधड़ी वाले टेक्स्ट संदेशों को भेजने के लिए एस.एम.एस. का उपयोग करता है। इसमें एस.एम.एस. प्राप्तकर्ता को एक वेबसाइट व वेबलिंक पर जाने या फोन नंबर पर कॉल करने के लिए कहा जाता है।

लॉटरी धोखाधड़ी (Lottery Fraud)

अपराधी, पीड़ित को ई–मेल, कॉल व एस.एम.एस. के माध्यम से लॉटरी जीतने के लिए बधाई देता है। पीड़ित खुश होता है और लॉटरी के पैसे पाने के लिए उत्सुक हो जाता है। अपराधी लॉटरी की राशि प्राप्त करने के लिए पीड़ित को टोकन मनी अन्तरित करने और महत्त्वपूर्ण सूचना प्रेषित करने के लिए कहता है। पीड़ित अपने पैसे व महत्त्वपूर्ण जानकारी अपराधी को उपलब्ध करवा देता है और उसे धनहानि का शिकार होना पड़ता है।

क्रेडिट/डेबिट कार्ड धोखाधड़ी (Credit/Debit Card Fraud)

हमलावर, पीड़ित को यह बताकर डराने की कोशिश करता है कि उसका क्रेडिट व डेबिट कार्ड ब्लॉक हो गया है। पीड़ित चिंतित हो जाता है और घबराने लगता है। हमलावर इसी स्थिति का फायदा उठाता है और पीड़ित को कार्ड को फिर से सक्रिय करने के लिए व्यक्तिगत जानकारी प्रदान करने के लिए कहता है और फिर यही जानकारी पीड़ित के पैसे चुराने/वित्तीय नुकसान पहुंचाने के लिए काम में ली जाती है।

नौकरी से संबंधित धोखाधडी (Job Related Fraud)

हमलावर एक आकर्षक वेतन के साथ नौकरी का प्रस्ताव पीड़ित को एक फेक ई–मेल के माध्यम से भेजता है। पीड़ित विश्वास करता है और निर्देशों का पालन करता है। फिर हमलावर पैसे चुराता है या पीड़ित को अनावश्यक परेशान करता है।

सुझाव (Tips)

- व्यक्तिगत/वित्तीय जानकारी चाहने वाले अज्ञात स्त्रोत से प्राप्त संदेश का जवाब न दें, चाहे वे आपके बैंक खाते में धन जमा होने का कथन करते हों।
- संदिग्ध ई–मेल का जवाब न दें और न ही संदिग्ध लिंक पर क्लिक करें।
- अविश्वसनीय अज्ञात बैंक खाते में कभी भी रूपए अंतरित न करें।
- ध्यान रहे आप तब तक लॉटरी नहीं जीत सकते है, जब तक कि आपने लॉटरी प्रक्रिया में भाग नहीं लिया हो।
- हमेशा ई–मेल आई.डी. के डोमेन का सही होना सुनिश्चित करें जैसे–सरकारी वेबसाईट के वैब पते में gov.in अथवा nic.in होता है।
- ई–मेल खाते में स्पैम फिल्टर इनेबल रखें।
- यदि आपके पास यह कॉल आता है कि आपका कार्ड ब्लॉक कर दिया गया है तो भ्रमित न हों। बैंक ऐसी सूचना कभी भी फोन के द्वारा नहीं देते हैं।
- किसी अजनबी से अपना पिन, पासवर्ड, कार्ड नंबर, सीवीवी नंबर, ओटीपी आदि साझा न करें, भले ही वह बैंक कर्मचारी होने का दावा करे। बैंक कभी भी ऐसी महत्त्वपूर्ण सूचना नहीं मांगता है।
- अपने बैंक के कस्टमर केयर नंबर को संभाल कर रखें ताकि आपके खाते के किसी संदिग्ध अथवा अनधिकृत लेन–देन की सूचना तुरन्त बैंक को दी जा सके।
- हमेशा प्रमाणिक जॉब पोर्टल्स, समाचार पत्रों में प्रकाशित नौकरियों के लिए ही आवेदन करें।
- सामान्यतः सभी सरकारी वेबसाइटों/ई–मेल में डोमेन ".gov.in या "nic.in होता है। अतः आवेदन करने से पूर्व वेबसाईट/ई–मेल का डोमेन भली प्रकार जांच लें।
- यदि किसी ई–मेल में वर्तनी, व्याकरणीय और विराम चिह्न की त्रुटियां हैं, तो वह धोखा देने वाली ई–मेल हो सकती है।
- स्वयं को नियोजक बताने वाली और व्यक्तिगत जानकारी या पैसे के लिए अनुरोध करने वाली फेक कॉल व ई–मेल से सावधान रहें।

सोशल मीडिया धोखाधड़ी (Social Media Fraud)

सोशल मीडिया हमारे जीवन का अभिन्न अंग बन गया है। यह संवाद करने, उसे साझा करने और हमारे जीवन में होने वाली घटनाओं के बारे में लोगों को सूचित करने का नया तरीका है। हम अपने स्वयं के दैनिक जीवन, स्वयं व परिवार की तस्वीरों, हमारे स्थान के बारे में अपडेट, वर्तमान विषयों पर हमारे विचारों आदि को सोशल मीडिया पर साझा करते हैं। कोई भी व्यक्ति किसी व्यक्ति के विचारों को उसकी सोशल मीडिया प्रोफाइल के माध्यम से समझ सकता है और अतीत के पैटर्न के आधार पर भविष्य के बारे में अनुमान लगा सकता है। यह एक व्यक्ति के लिए खतरा बन जाता है क्योंकि सोशल मीडिया प्रोफाइल के अवांछित उपयोग, जानकारी की चोरी, मानहानि या इससे भी बुरे परिणाम जैसे—शारीरिक/यौन हमला, डकैती आदि भी हो सकते हैं। इसलिए, सोशल मीडिया प्रोफाइल का संरक्षण और सुरक्षित उपयोग बहुत महत्त्वपूर्ण है।

सोशल मीडिया धोखाधड़ी के उदाहरण

हमलावर, सोशल मीडिया पर पीड़ित के साथ दोस्त बन जाता है। हमलावर लगातार भरोसा हासिल करता रहता है और बाद में हमलावर पैसों की मांग करता है या अन्यथा पीड़ित को परेशान करता है।

रोमांस धोखाधड़ी (Romance Fraud)

हमलावर, सोशल मीडिया पर पीड़ित के साथ दोस्त बन जाता है और कालान्तर में हमलावर पीड़ित का विश्वास जीत लेता है और बाद में हमलावर पीड़ित का शारीरिक, आर्थिक और भावनात्मक रूप से शोषण करता है।

साइबर स्टॉकिंग (Cyber Stalking)

साइबर स्टॉकिंग, एक ऐसा अपराध है जिसमें हमलावर इलेक्ट्रॉनिक संचार जैसे ई–मेल, इंस्टेंट मैसेजिंग (आईएम), किसी वेबसाइट या किसी ग्रुप पर पोस्ट किए गए संदेश का उपयोग करके पीड़ित को परेशान करता है।

साइबर स्टॉकर अपनी वास्तविक पहचान डिजिटल दुनिया में छुपाकर रखता है और पीड़ित को धमकी भरे/अपमानजनक संदेशों के साथ निशाना बनाता है और वास्तविक दुनिया में उसकी गतिविधियों पर नजर रखता है।

साइबर बुलिंग (Cyber Bullying)

साइबर बुलिंग डिजिटल उपकरणों के माध्यम से होती है। साइबर बुलिंग एस.एम.एस., सोशल मीडिया, फोरम्स् या गेमिंग ऐप जहां लोग कंटेंट देख सकते हैं, भाग ले सकते हैं या साझा कर सकते हैं, के माध्यम से की जाती है।

साइबर बुलिंग में नकारात्मक, हानिकारक और झूठी सामग्री भेजना, पोस्ट करना या साझा करना शामिल है, जिसका आशय पीड़ित को शर्मिंदा या अपमानित करना होता है।

सुझाव (Tips)

- सोशल मीडिया पर अनजान फ्रेंड रिक्वेस्ट प्राप्त होने पर सतर्क रहें व ऐसी रिक्वेस्ट को स्वीकार न करें।
- साइबर अपराधी, पीड़ितों को नुकसान पहुंचाने के इरादे से दोस्ती करने के लिए नकली सोशल मीडिया प्रोफाइल बनाते हैं।
- किसी अज्ञात व्यक्ति जिससे आप सिर्फ सोशल मीडिया के माध्यम से मिले हैं, के साथ अपना व्यक्तिगत/वित्तीय विवरण साझा न करें।

- यदि आप किसी सोशल मीडिया के माध्यम से बने मित्र से मिलने की योजना बना रहे हैं तो इस बाबत् अपने परिवार / दोस्तों को सूचित रखें और हमेशा सार्वजनिक स्थानों पर ही मिलें।
- कभी भी अंतरंग तस्वीरों को ऑनलाइन प्लेटफॉर्म पर किसी के साथ साझा न करें, क्योंकि बाद में इनका दुरूपयोग हो सकता है।
- अपनी प्रोफाईल को प्रतिबंधित रखें, सोशल मीडिया साईट्स आपके द्वारा प्रेषित पोस्ट, तस्वीरों और मित्रता अनुरोध प्रतिबन्धित करने के लिए विशेष सैटिंग्स प्रदान करती है।
- सुनिश्चित करें कि आपकी व्यक्तिगत सूचना, तस्वीरें एवं वीडियो किसी विश्वस्त एवं पहचान वाले व्यक्ति द्वारा ही देखी जा सके।
- अपनी तस्वीरें जिनमें आपका स्थान, लोकेशन दर्शित हो, उन्हें सोशल मीडिया पर साझा करते वक्त सावधान रहें।

मोबाइल एप्लिकेशन धोखाधडी (Mobile Application Frauds)

साइबर धोखाधड़ी के लिए मोबाइल एप्लिकेशन का उपयोग कैसे किया जा सकता है? (How mobile applications can be used for cyber frauds?)

स्मार्टफोन के उपयोग में वृद्धि और परिणामस्वरूप मोबाइल एप्लिकेशन्स के उपयोग की वृद्धि ने उससे जुड़े हुए सुरक्षा जोखिमों को भी बढ़ा दिया है। साइबर अपराधी डेटा और रूपए प्राप्त करने के लिए मोबाइल उपयोगकर्ताओं को निशाना बना रहे हैं।

मोबाइल एप्लिकेशन का उपयोग न केवल मनोरंजन के लिए बल्कि दिन–प्रतिदिन के कार्यों जैसे कि बिल भुगतान, बैंक खातों का प्रबंधन, सेवा वितरण आदि को आसान एवं सुविधाजनक बनाने के लिए भी किया जा रहा है। यह एप्लिकेशन साइबर हमलों के लिए अधिक प्रवण है। उपयोगकर्ताओं को आमतौर पर उपयोग किए जाने वाले मोबाइल एप्लिकेशन जैसे डिजिटल भुगतान एप्लिकेशन और गेमिंग पर होने वाले हमलों के प्रति जागरूक रहना चाहिए।

संक्रमित मोबाइल एप्लीकेशन के माध्यम से साइबर हमला (Cyber-attacks using Infected Mobile Applications)

आमजन कुछ मोबाईल एप्लिकेशन के उपयोग के अभ्यस्त हो जाते हैं। नतीजतन, वे सुरक्षा की अनदेखी करते हैं। धोखा देने वाले व्यक्ति ऐसी लोकप्रिय मोबाइल एप्लिकेशन का उपयोग पीड़ित पर हमला करने के लिए करते हैं।

हमलावर, संक्रमित सॉफ्टवेयर जिन्हें ट्रोजन कहा जाता है, के माध्यम से एप्लिकेशन को संक्रमित करते हैं। ये ट्रोजन आपके संदेश, ओटीपी, कैमरा, संपर्क, ई–मेल, फोटो आदि का उपयोग कर सकता है। ये आपको अश्लील विज्ञापन भी दिखाते हैं, उपयोगकर्ताओं को सःशुल्क सदस्यता के लिए साइन अप किये जाने हेतु आंमत्रित करते हैं एवं मोबाइल में से व्यक्तिगत सूचनाएं चोरी करते हैं।

सुझाव (Tips)

- हमेशा आधिकारिक एप्लिकेशन स्टोर या विश्वसनीय स्त्रोत से ही मोबाइल एप्लिकेशन इंस्टॉल करें।
- सभी अनुमति अनुरोधों, विशेष रूप से मोबाइल एप्लिकेशन इंस्टॉल/उपयोग करते समय विशेषाधिकार एक्सेस चाहने वाले मोबाइल एप्लिकेशन्स को सावधानीपूर्वक जांच लें।
- मोबाइल सॉफ्टवेयर और मोबाइल एप्लिकेशन को नियमित रूप से अपडेट करें।
- मौजूदा एप्लिकेशन में विद्वेषपूर्ण (Malicious) एप्लिकेशन या विद्वेषपूर्ण (Malicious) अपडेट से सावधान रहें।
- विद्वेषपूर्ण (Malicious) एप्लिकेशन से संबंधित सभी डेटा को हटाकर (Remove) इसे अनइंस्टॉल करें।

ऑनलाइन बैंकिंग धोखाधड़ी
(Online Banking Frauds)

आजकल सभी बैंकिंग सेवाएं जैसे– खाता विवरण, धन प्राप्त करने, अन्य खातों में अंतरण, चैक बुक का अनुरोध करना, डिमांड ड्राफ्ट तैयार करना आदि सभी सेवाएं ऑनलाइन हो चुकी हैं। इन सेवाओं में से अधिकांश सेवाओं को घर बैठे ही बिना बैंक में जाए किया जा सकता है। जैसे–जैसे सेवाएं ऑनलाइन प्लेटफॉर्म की ओर बढ़ रही हैं, बैंकिंग से संबंधित साइबर अपराध भी बढ़ रहे हैं।

ऑनलाइन बैंकिंग खाता एक मजबूत पासवर्ड के साथ होता है। अगर पासवर्ड चोरी हो जाता है तो बैंक खातों से पैसा चोरी हो जाएगा। इसलिये, मजबूत पासवर्ड सुरक्षा अत्यावश्यक हो जाती है।

डिजिटल भुगतान एप्लिकेशन संबंधित हमले
(Digital Payments Applications related Attacks)

डिजिटल भुगतान आज के जीवन में बहुत आम हो गया है। यदि अकाउंट हैक हो जाये तो यह बहुत खतरनाक है।

कमजोर पासवर्ड के कारण बैंक खाते की हैकिंग
(Hacking of Bank Account due to Weak Password)

इस प्रकार के हमले में, हमलावर अनुमान लगाकर सामान्यतः उपयोग किए जाने वाले पासवर्ड के माध्यम से खाते को हैक करने का प्रयास करता है। एक बार अकाउंट हैक होने के बाद, हमलावर पैसे चुरा सकता है या पीड़ित को बदनाम करने या फंसाने के उद्देश्य से अवैध लेनदेन कर सकता है।

समान पासवर्ड के कारण कई बैंक खातों की हैकिंग (Hacking of Multiple Accounts due to same Password)

यदि एक ही पासवर्ड कई खातों के लिए उपयोग किया जाता है, तो एक खाते की हैकिंग से अन्य सभी खाते भी हैक किए जा सकते हैं।

सुझाव (Tips)

- अपना मोबाइल अनलॉकिंग पिन या पासवर्ड कभी भी किसी के साथ साझा न करें।
- अपने बैंक के साथ अपने व्यक्तिगत फोन नंबर और ई–मेल को पंजीकृत करें और SMS सर्विस एक्टीवेट करें।
- ये सूचनाएं आपको किसी भी लेन–देन और नेट बैंकिंग खातें में लॉगिन प्रयासों के बारे में तुरंत सतर्क कर देंगी। हमेशा अपने पंजीकृत मोबाइल नंबर पर प्राप्त लेन–देन अलर्ट की समीक्षा करें।
- हमेशा अपने बैंक खाते में अधिकतम लेनदेन की सीमा रखें। अपने एप्लिकेशन को मजबूत पासवर्ड और टू–स्टेज सत्यापन (जैसे कि OTP) के साथ सुरक्षित करें। यहां तक कि आपकी अधिकतम लेनदेन सीमा से नीचे के लेनदेन के लिए भी।
- विद्वेषपूर्ण (Malicious) एप्लिकेशन को तुरंत अनइंस्टॉल करें।
- मजबूत पासवर्ड बनाने के लिए ऐसी तकनीकें, जिन्हें याद रखना आसान हो, का प्रयोग करें।
- विभिन्न खातों के लिए अलग–अलग पासवर्ड का प्रयोग करें।
- अपने पासवर्ड को कम से कम 8 अक्षर लंबा रखें।
- Uppercase एवं Lowercase अक्षरों, संख्याओं और विशेष चिन्हों के माध्यम से अपने पासवर्ड को मजबूत बनाएं।
- अपने प्रत्येक खाते और उपकरणों के लिए अलग–अलग पासवर्ड का उपयोग करें।
- जहां तक संभव हो, टू–स्टेज सत्यापन (जैसे रजिस्टर्ड मोबाईल नम्बर एवं ई–मेल पर ओटीपी) का उपयोग करें।
- यदि आपका कोई ऑनलाइन अकाउंट हैक हो गया है, तो तुरंत लॉग–इन करें और अपना पासवर्ड बदलें।
- वेब ब्राउजर में उपयोगकर्ता का नाम पहचान (User ID) और पासवर्ड को संरक्षित न करें।

पर्सनल कम्प्यूटर/लैपटॉप पर वायरस का हमला (Virus Attack on Personal Computer/Laptop)

पर्सनल कम्प्यूटर या लैपटॉप हमारे जीवन में बहुत महत्त्वपूर्ण भूमिका निभाते हैं। हम इसमें हमारी महत्त्वपूर्ण जानकारी, बैंक खाता संख्या, व्यवसाय दस्तावेज, पर्सनल फाइल जैसे फोटो, म्यूजिक, मूवी आदि संरक्षित रखते हैं। इसलिए, इन सभी डेटा की सुरक्षा अत्यधिक आवश्यक है।

बाहरी उपकरणों के माध्यम से वायरस का हमला (Virus Attack through external devices)

एक वायरस बाहरी उपकरणों जैसे–पेन ड्राइव या हार्ड डिस्क आदि के माध्यम से कम्प्यूटर में प्रवेश कर सकता है और सभी कम्प्यूटर फाइलों में फैल सकता है।

गैर–विश्वसनीय वेबसाइटों से फाइलों को डाउनलोड करके वायरस का हमला (Virus Attack by downloading files from un-trusted websites)

वायरस, गैर–विश्वसनीय वेबसाइटों से फाइलों को डाउनलोड करने पर कम्प्यूटर में प्रवेश कर सकता है। वायरस म्यूजिक फाइलों, वीडियो फाइलों या किसी भी आकर्षक विज्ञापन में छुपा होता है।

विद्वेषपूर्ण (Malicious) सॉफ्टवेयर इंस्टॉल करने से वायरस का हमला (Virus Attack by installation of malicious software)

वायरस, अविश्वसनीय स्रोतों से सॉफ्टवेयर इंस्टॉल करने से कम्प्यूटर में प्रवेश कर सकता है। अज्ञात गेम फाइलों या किसी अज्ञात सॉफ्टवेयर के अंदर वायरस छुपा हो सकता है। यह वायरस कम्प्यूटर की सभी फाइलों में फैल सकता है। वायरस/विद्वेषपूर्ण (Malicious) एप्लिकेशन के कारण कम्प्यूटर का धीमा होना, डेटा खराब होना, विलोपित या हानि हो सकती है।

सुझाव (Tips)

- अपने कम्प्यूटर पर पायरेटेड सॉफ्टवेयर, एप्लिकेशन आदि को कभी भी डाउनलोड या इंस्टॉल न करें।
- बाहरी उपकरणों जैसे– पैन ड्राईव, हार्ड डिस्क आदि को कम्प्यूटर से जोड़ने के पश्चात सर्वप्रथम उसे स्कैन करें। हमेशा ब्लूटूथ को बंद रखे, जब तक कि आपको कोई फाइल अपने फोन अथवा नेटवर्क में से अंतरित न करनी हो।
- कम्प्यूटर/मोबाइल उपकरण को डिस्पोज करने से पूर्व अपनी सारी व्यक्तिगत सूचनाएं मिटा दें। संदिग्ध ई–मेल/एसएमएस में दिए गए URL/लिंक पर क्लिक न करें, भले ही वे वास्तविक दिखाई देते हों, क्योंकि ये आपको विद्वेषपूर्ण (Malicious) वेबसाइटों तक ले जा सकते हैं।
- हमेशा ऑनलाइन लेनदेन करने से पहले वेबसाईट एड्रेस बार में दर्शित "https" जांच लें। सुरक्षित "https" यह दर्शित करता है कि वेबपेज के साथ किया गया संचार सुरक्षित है।

सामान्य सुझाव (General Tips)

1. हमेशा अपने सिस्टम/डिवाइस (डेस्कटॉप, लैपटॉप, मोबाइल) को अपडेट रखें।
2. नवीनतम एवं अपडेटेड संस्करण के साथ एंटी–वायरस जैसे– सुरक्षा सॉफ्टवेयर के माध्यम से सिस्टम/डिवाइस को सुरक्षित रखें।
3. हमेशा विश्वसनीय स्रोतों से ही सॉफ्टवेयर या एप्लिकेशन डाउनलोड करें। कभी भी पायरेटेड वर्जन का उपयोग न करें।
4. सभी उपकरण/खाते एक मजबूत पिन या पासवर्ड द्वारा सुरक्षित रखें। अपना पिन कभी किसी से साझा न करें।
5. अपने नेट–बैंकिंग पासवर्ड, वन टाइम पासवर्ड (ओटीपी), एटीएम या फोन को किसी से साझा न करें।
6. बैंकिंग पिन, सीवीवी नंबर आदि किसी भी व्यक्ति के साथ, भले ही वह बैंक का प्रतिनिधि/कर्मचारी होने का दावा करता हो, साझा न करें।

7. हमेशा अपने वाई–फाई राउटर को मजबूत पासवर्ड से सुरक्षित करें। इसके अलावा, नवीनतम एन्क्रिप्शन का उपयोग करने के लिए अपने वायरलेस नेटवर्क को हमेशा कॉन्फिगर करें। किसी भी संदेह के मामले में अपने नेटवर्क सेवा प्रदाता से तुरंत संपर्क करें।
8. सार्वजनिक वाई–फाई के माध्यम से ब्राउज करते समय सावधान रहें और व्यक्तिगत और व्यवसायिक ई–मेल व बैंकिंग खातों में लॉग–इन करने से बचें।
9. सार्वजनिक कम्प्यूटरों से नेट–बैंकिंग सुविधा का उपयोग करने के लिए हमेशा वर्चुअल की–बोर्ड का उपयोग करें और ऑनलाइन लेनदेन के पूरा होने के बाद बैंकिंग पोर्टल/वेबसाइट से लॉग–आउट करें एवं वेब ब्राउजिंग हिस्ट्री को (इंटरनेट एक्सप्लोरर, क्रोम, फायरफॉक्स आदि) से हटाना भी सुनिश्चित करें।
10. ई–मेल अटैचमेंट को खोलने से पहले वायरस स्कैन करें अज्ञात या गैर–विश्वसनीय स्रोतों से प्राप्त ई–मेल अटैचमेंट को खोलने से बचें।
11. पहचान प्रमाण दस्तावेजों को अनजान व्यक्ति/संस्था, जिनकी प्रामाणिकता सत्यापित नहीं है, से साझा करते समय सावधान रहें।
12. अपने सेल फोन का IMEI कोड सुरक्षित रखें, यदि सेल फोन चोरी हो जाता है तो ऑपरेटर इस कोड के माध्यम से फोन को ब्लैक लिस्ट, ब्लॉक या ढूंढ सकता है।
13. अपने दोस्तों और परिवार के साथ इंटरनेट के सुरक्षित उपयोग के नवाचारों के बारे में चर्चा करें और उन्हें साइबर अपराध और सुरक्षित साइबर तरीकों के बारे में जागरूक करें।
14. अपने ई–वॉलेट में अपने क्रेडिट/डेबिट कार्ड या बैंक खाते के विवरण को सेव नहीं करें।

साइबर अपराध की रिपोर्ट कहां व कैसे करें?
(Where & How to Report a Cyber Fraud?)

1. अविलम्ब निकटतम पुलिस स्टेशन पर जाएँ।
2. साइबर अपराध की ऑनलाइन रिपोर्ट करने के लिए नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर जाएं। इस पोर्टल में, दो अनुभाग हैं। एक भाग में महिलाओं और बच्चों से संबंधित अपराधों की रिपोर्ट की जा सकती है और दूसरे में अन्य प्रकार के साइबर अपराधों की रिपोर्ट की जा सकती है। आप हेल्पलाइन नंबर 155260 पर डायल करके ऑफलाइन भी शिकायत दर्ज कर सकते हैं।
3. गुम अथवा चोरी हुए मोबाइल फोन की रिपोर्ट पुलिस थाने में दर्ज करें।
4. हेल्पलाइन नम्बर 14400 के माध्यम से दूरसंचार विभाग Department of Tele Communications (DoT) को सूचित करें या केंद्रीय उपकरण पहचान रजिस्टर Central Equipment Identity Register (CEIR) पर ऑनलाइन शिकायत (CEIR) पोर्टल https://ceir.gov.in पर जाकर दर्ज करें। सत्यापन के बाद, दूरसंचार विभाग के द्वारा फोन को ब्लैकलिस्ट/आगे उपयोग के लिए अवरूद्ध कर दिया जायेगा। इसके अलावा, अगर कोई डिवाइस का उपयोग अलग सिम कार्ड का उपयोग करके करने की कोशिश करता है तो सेवा प्रदाता स्वतः ही नए उपयोगकर्ता की पहचान करेगा और पुलिस को सूचित करेगा

सूचना प्रोद्यौगिकी अधिनियम, 2000 के महत्त्वपूर्ण प्रावधान
Important provisions of the Information Technology Act, 2000

- कम्प्यूटर संसाधनों से छेड़छाड़ की कोशिश करना–धारा 65
- कम्प्यूटर में संग्रहित डेटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश करना –धारा 66
- कम्प्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को बेईमानी से प्राप्त करने के लिए दंड का प्रावधान–धारा 66B

- किसी की पहचान चोरी करने के लिए दंड का प्रावधान–धारा 66C
- अपनी पहचान छुपाकर कम्प्यूटर संसाधन या किसी संचार युक्ति की मदद से छल करने के लिए दंड का प्रावधान– धारा 66D
- किसी की एकांतता के अतिक्रमण भंग करने के लिए दंड का प्रावधान–धारा 66E
- साइबर आतंकवाद के लिए दंड का प्रावधान–धारा 66F
- अश्लील सामग्री का इलेक्ट्रॉनिक रूप में प्रकाशन के लिए दण्ड–धारा 67
- कामुकता व्यक्त करने वाले कार्य सामग्री के इलेक्ट्रॉनिक रूप से प्रकाशन के लिए दंड का प्रावधान–धारा 67A
- कामुकता व्यक्त करने वाले कार्य आदि में बालकों को चित्रित करने वाली सामग्री के इलेक्ट्रानिक रूप से प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान –धारा 67B
- मध्यवर्तियों द्वारा सूचना को बाधित करने या रोकने के लिए दंड का प्रावधान–धारा 67C
- सुरक्षित कम्प्यूटर तक अनाधिकृत पहुंच बनाने से संबंधित प्रावधान–धारा 70
- डेटा या आंकड़ों को ग़लत तरीक़े से पेश करने के लिए दण्ड का प्रावधान–धारा 71
- गोपनीयता एवं एकांतता भंग करने के लिए दण्ड का प्रावधान–धारा 72
- कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने के संबंध में दण्ड का प्रावधान–धारा 72A
- फर्ज़ी डिजिटल हस्ताक्षर का प्रकाशन–धारा 73
- कपटपूर्ण प्रयोजन से प्रकाशन के लिए दण्ड का प्रावधान–धारा 74
- इंस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों में अनुसंधान करने की अधिकारिता– धारा 78

NOTES

NOTES

हेल्पलाइन नम्बर

अजमेर : 8306002101	अलवर : 8306002102
बालोतरा : 8306002103	बांसवाड़ा : 8306002104
बारां : 8306002105	भरतपुर : 8306002106
भीलवाड़ा : 8306002107	बीकानेर : 8306002108
बूंदी : 8306002109	चूरू : 8306002110
चित्तौड़गढ़ : 8306002112	दौसा : 8306002114
धौलपुर : 8306002115	डूंगरपुर : 8306002116
हनुमानगढ़ : 8306002118	जयपुर मेट्रो I : 8306002119
जयपुर मेट्रो II : 8306008220	जयपुर जिला : 8306002120
जैसलमेर : 8306002123	जालोर : 8306002126
झालावाड़ : 8306002127	झुंझुनूं : 8306002128
जोधपुर मेट्रो : 8306002021	जोधपुर जिला : 8306002129
करौली : 8306002130	कोटा : 8306002131
मेड़ता सिटी : 8306002132	पाली : 8306002166
प्रतापगढ़ : 8306002134	राजसमंद : 8306002135
सवाई माधोपुर : 8306002136	सीकर : 8306002137
सिरोही : 8306002138	श्री गंगानगर : 8306002117
टोंक : 8306002139	उदयपुर : 8306002022

राजस्थान राज्य विधिक सेवा प्राधिकरण

राजस्थान उच्च न्यायालय परिसर

फोन : 0141–2227481, 2227602 | हेल्पलाइन नं. 9928900900,15100

ई–मेल : rj-slsa@nic.in, rslsajp@gmail.com, Website: www.rlsa.gov.in

rslsa.rajasthan | @LeglAidRajsthan | legalaidrajasthan