त्योहारों में बचें फेक आफर्स से

इन दिनों जालसाजों ने आपके बैंक खाते से पैसे ठगने के नये-नये तरीके खोज लिए हैं। स्कैमर्स इंटरनेट इंजीनियरिंग के हथकंडों का इस्तेमाल कर लोगों को अपनी बैंकिंग की गोपनीय एवं व्यक्तिगत जानकारी साझा करने के लिए लुभा रहे हैं। इसके लिए वे लोगों को अत्यधिक लुभावने आफर्स, मदद करने का लालच या फिर धमकी देकर फंसाने को कोशिश करते हैं। हाल के वर्षों में भुगतान करने और अन्य बैंकिंग एक्सचेंज के लिए डिजिटल प्लेटफार्म के उपयोग में तेजी से वृद्धि हुई है। हालांकि इससे ग्राहकों की सुविधा तो बढ़ी है, लेकिन जालसाज भी पैसे ठगने के लिए इसी डिजिटल माध्यम का इस्तेमाल करने लगे हैं। जैसे-जैसे वित्तीय लेन-देन करना ज्यादा आसान हुआ है, वैसे-वैसे ग्राहकों को ठगने की कोशिशों में भी उतनी ही बढ़ोत्तरी हुई है। इन लोगों में टेक्नो-फाइनेंशियल तरीकों को समझने वाले भी शामिल हैं और वे भी शामिल हैं, जो इससे ज्यादा परिचित नहीं हैं।

मनीष अग्रवाल
हेड, क्रेडिट इंटेलिजेंस एवं कंट्रोल, एचडीएफसी बैंक

ऐसे शुरू होता है खेल

आमतौर पर ग्राहकों को अवांछित काल, टेक्स्ट मैसेज, ईमेल आदि मिलते हैं, जिनमें एक लिंक द्वारा ग्राहकों से अपने बैंक खाते, लागइन की जानकारी, कार्ड की जानकारी, पिन और ओटीपी देने के लिए कहा जाता है। कभी-कभी पीड़ित के फोन का नियंत्रण पाकर उसकी गोपनीय जानकारी चुराने के लिए असत्यापित मोबाइल एप्स का इस्तेमाल किया जाता है। ऐसे हमलों में ये ठग बैंकर/बीमा एजेंट/स्वास्थ्य कर्मी/सरकारी अधिकारी या स्थानीय दुकानदार बनकर ग्राहकों को काल करते हैं या उनसे संपर्क करते हैं। वे नाम/जन्म की तारीख आदि विवरण साझा करके इन क्रेडेंशियल्स की पुष्टि कराते हैं और विश्वास हासिल करते हैं। इसके बाद वे महत्वपूर्ण और आवश्यक सेवा प्रस्तुत करते हैं। वे ग्राहकों को सेवा के बदले भुगतान करने के लिए कस्टमाइज्ड पेमेंट लिंक भी भेजते हैं। कुछ मामलों में ये ठग इमरजेंसी, खाता ब्लाक होने आदि का हवाला देकर ग्राहकों पर गोपनीय जानकारी साझा करने का दबाव डालते हैं। इसके बाद इन क्रेडेंशियल्स का इस्तेमाल कर ग्राहकों के साथ धोखाधड़ी की जाती है।

इन तरीकों से फंसाते हैं ठग

फिशिंग लिंक: जालसाज थर्ड-पार्टी वेबसाइट बनाते हैं, जो असली वेबसाइट की तरह दिखती है। इसके बाद इस वेबसाइट के लिंक टेक्स्ट मैसेज, ईमेल और इंटरनेट मीडिया प्लेटफार्म्स द्वारा साझा किए जाते हैं। जब ग्राहक इन लिंक्स पर क्लिक करते हैं, तो वे फिशिंग वेबसाइट पर पहुंच जाते हैं, जहां उन्हें गोपनीय जानकारी देने के लिए लुभाया जाता है। इस जानकारी का उपयोग पैसे चुराने के लिए किया जाता है।

सावधानी: किसी भी अज्ञात लिंक पर क्लिक न करें और ऐसे अज्ञात टेक्स्ट/ईमेल को डिलीट कर दें, जो बहुत लुभावने आफर का वादा करती हैं।

विशिंग काल: जालसाज बैंकर, बीमा एजेंट, सरकारी अधिकारी आदि बनकर ग्राहक को फोन करते हैं और उनका भरोसा हासिल करने के बाद उनसे सुरक्षित क्रेडेंशियल्स की पुष्टि करने के लिए कहते हैं। इसके बाद इन क्रेडेंशियल्स के जरिए ही ग्राहकों के साथ धोखाधड़ी की जाती है।

सावधानी: अपनी गोपनीय जानकारी किसी को भी न बताएं, क्योंकि बैंक/वित्तीय संस्थानों के अधिकारी ग्राहकों से कभी भी ऐसी जानकारी नहीं मांगते हैं।

सर्च इंजन का इस्तेमाल: ग्राहक अपने बैंक, इंश्योरेंस कंपनी, आधार सर्विस सेंटर आदि की कांटैक्ट डिटेल देखने के लिए अक्सर सर्च इंजन का इस्तेमाल करते हैं। कभी-कभी वे सर्च इंजन में प्रदर्शित हो रहे अज्ञात और असत्यापित नंबरों के झांसे में आ जाते हैं। सर्च इंजन पर ये कांटैक्ट डिटेल अक्सर जालसाजों द्वारा लोगों को जाल में फंसाने के लिए दिए जाते हैं।

सावधानी: सर्च इंजन का इस्तेमाल कांटैक्ट नंबर के लिए न करें। हमेशा कांटैक्ट नंबर के लिए बैंकों/कंपनियों की आधिकारिक वेबसाइट का ही इस्तेमाल करें।

क्यूआर स्कैन: जालसाज अक्सर विभिन्न बहानों से ग्राहकों से संपर्क करते हैं और उन्हें पेमेंट एप का इस्तेमाल कर क्यूआर कोड स्कैन करने के जाल में फंसा लेते हैं। इस प्रकार जालसाज ग्राहक के खाते से पैसा चुरा लेते हैं।

सावधानी: पेमेंट एप द्वारा कोई भी क्यूआर कोड स्कैन करते हुए सावधान रहें। क्यूआर कोड में किसी विशेष खाते में पैसा ट्रांसफर करने के लिए खाते की डिटेल्स समाहित की गई होती है।

डुप्लीकेट इंटरनेट मीडिया प्रोफाइल: जालसाज लोकप्रिय इंटरनेट मीडिया प्लेटफार्म पर नकली खाते बनाते हैं और सार्वजनिक रूप से उपलब्ध आपके किसी दोस्त के फोटोग्राफ एवं डिटेल का इस्तेमाल कर उसका छद्म रूप रख लेते हैं। उसके बाद वे बीमारी, दुर्घटना, आपातकालीन स्थिति आदि का बहाना बनाकर आपसे पैसे मांगते हैं।

सावधानी: इंटरनेट मीडिया प्लेटफार्म्स पर व्यक्तिगत और गोपनीय जानकारियां कभी भी साझा न करें। साथ ही, मदद के लिए भेजे गए निवेदन कितने असली हैं, इसकी जांच पैसे भेजने से पहले संबंधित दोस्तों/परिवार के सदस्यों से फोन काल या मुलाकात करके कर लें।

जूस जैकिंग: मोबाइल फोन के चार्जिंग पोर्ट को फाइल/डाटा ट्रांसफर करने के लिए भी इस्तेमाल किया जा सकता है। जूस जैकिंग एक साइबर चोरी है, जिसमें आपका मोबाइल फोन अज्ञात/असत्यापित चार्जिंग पोर्ट्स से कनेक्ट होते ही जालसाजों को उसकी एक्सेस मिल जाती है और वे संवेदनशील डाटा, ईमेल, टेक्स्ट मैसेज, सेव किए गए पासवर्ड आदि को मालवेयर की मदद से चुरा लेते हैं।

सावधानी: सार्वजनिक/अज्ञात चार्जिंग पोर्ट्स का इस्तेमाल न करें। मोबाइल फोन में पासवर्ड और अन्य गोपनीय जानकारियां सेव करके न रखें।

सिम स्वैप/सिम क्लोनिंग फ्राड: आपके खाते की ज्यादातर डिटेल्स और आथेंटिकेशन के मैसेज आपके रजिस्टर्ड मोबाइल नंबर से जुड़े होते हैं, इसलिए जालसाज सिम कार्ड की एक्सेस पाने की कोशिश करते हैं। कभी-कभी वे क्लोन करके डुप्लीकेट सिम कार्ड बना लेते हैं और इन डुप्लीकेट सिम पर ओटीपी प्राप्त करके डिजिटल ट्रांसफर कर लेते हैं। जालसाज आमतौर पर मोबाइल सर्विस कंपनी का अधिकारी बनकर ग्राहकों को काल करते हैं और सिम कार्ड को मुफ्त में अपग्रेड करने के लिए उनका विवरण मांगते हैं।

सावधानी: अज्ञात कालर्स के साथ सिम कार्ड से संबंधित विवरण साझा न करें। यदि आपके फोन में लंबे समय तक मोबाइल नेटवर्क न आए, तो सतर्क हो जाएं और अपने मोबाइल आपरेटर को काल करके इस बात की पुष्टि कर लें कि कहीं आपके नंबर पर कोई डुप्लीकेट सिम तो जारी नहीं की गई है।