स्मिशिंग (SMShing) क्या है?

यह फिशिंग का वह रूप है जिसमें धोखा देने वाला व्यक्ति धोखाधड़ी वाले एसएमएस अलर्ट द्वारा किसी व्यक्ति से उनकी निजी जानकारी मांगने के लिए चालबाजी करने का प्रयास करता है।

क्योंकि इस रूप में ईमेल पर टेक्स्ट मैसेज / एसएमएस / फोन नंबर पाना शामिल है, इसलिए इसे भरोसेमंद स्रोत से माना जाता है। इसमें आपकी केवाईसी अपडेट करने, आपके डेबिट / क्रेडिट कार्ड रिवॉर्ड पॉइंट्स को रिडीम करने, इत्यादि के लिए प्रेरित करके आपका ऑनलाइन पासवर्ड, ओटीपी, इत्यादि जैसी आपकी व्यक्तिगत जानकारी आपसे पाने के उद्देश्य से सोशल इंजीनियरिंग के तत्वों का उपयोग किया जाता है।

सावधान रहें!!!

- अपना पिन, पासवर्ड, कार्ड नंबर, सीवीवी नंबर, ओटीपी इत्यादि किसी भी अजनबी को न बताएं, भले ही वह बैंक कर्मचारी होने का दावा करता/करती हो। बैंक कोई भी महत्वपूर्ण जानकारी कभी नहीं मांगेगा।
- व्यक्तिगत या वित्तीय विवरण का अनुरोध करने वाले अज्ञात स्रोत से मिलने वाले संदेशों का जवाब न दें, भले ही उनमें आपके बैंक खाते में पैसे क्रेडिट करने का आश्वासन दिया जा रहा हो।
- अपने फोन पर मिलने वाले लिंक पर तब तक क्लिक न करें जब तक आप भेजने वाले व्यक्ति को नहीं जानते। संदेश की प्रामाणिकता की जांच करें, भले ही किसी ज्ञात व्यक्ति से प्राप्त किया गया हो।
- टेक्स्ट मैसेज द्वारा भेजे गए लिंक से कभी भी ऐप्स इंस्टॉल न करें। आपके द्वारा अपने डिवाइस पर इंस्टॉल किया गया कोई भी ऐप सीधे आधिकारिक ऐप स्टोर से होना चाहिए।

साइबर अपराध की शिकायत करें:

यदि आप साइबर अपराध का शिकार हो जाते हैं, तो तुरंत काररवाई करें। राष्ट्रीय साइबर अपराध हेल्पलाइन 1930 पर कॉल करें और अपनी शिकायत https://cybercrime.gov.in/ पर दजर करें। आप Sancharsaathi Portal के माध्यम से भी शिकायत दजर कर सकते हैं। समय पर की गई शिकायत से आगे की ठगी रोकी जा सकती है और दूसरों को भी सुरक्षित रखा जा सकता है।