इंटरनेट और ईमेल द्वारा धोखाधड़ी (फिशिंग)

इंटरनेट ने ऑनलाइन बैंकिंग और शॉपिंग जैसी सेवाओं के साथ हमारे जीवन को सुविधाजनक बनाया है, लेकिन इसमें हमेशा ऐसे सुरक्षा जोखिम होते हैं जिनसे अपराधी हमारे निजी बैंकिंग विवरणों का एक्सेस पाने के लिए इंटरनेट का दुरुपयोग करेंगे और इसका उपयोग हमारी मेहनत की कमाई को चुराने के लिए करेंगे।

धोखाधड़ी करने वाले लोग खुद को इलेक्ट्रॉनिक संचार की भरोसेमंद संस्था के रूप में दिखाकर उपयोगकर्ता के नाम, पासवर्ड और अन्य बैंकिंग विवरण जैसी जानकारी पाने का प्रयास करते हैं। इस कार्रवाई को "फिशिंग" कहा जाता है।

फिशिंग आमतौर पर ईमेल या इंस्टेंट मैसेजिंग द्वारा की जाती है और इसमें अक्सर उपयोगकर्ताओं को नकली वेबसाइट पर जानकारी दर्ज करने के लिए कहा जाता है जिसका रूप-रंग काफी हद तक असली वेबसाइट की तरह होता है।

फिशिंग करने वाले लोग ग्राहक की जानकारी, जैसे कि खाता नंबर, लॉगिन आईडी, लॉगिन और लेनदेन पासवर्ड, मोबाइल नंबर, पता, डेबिट कार्ड ग्रिड वैल्यू, क्रेडिट कार्ड नंबर, सीवीवी नंबर, पैन, जन्म तिथि, माता का नाम, पासपोर्ट नंबर इत्यादि, पाने के लिए ईमेल फिशिंग, विशिंग (वॉयस फिशिंग) और स्मिशिंग (एसएमएस फिशिंग) के संयोजन का उपयोग करते हैं।

फिशिंग के प्रयास की पहचान कैसे करें?

a. अनचाहे ईमेल, अजनबियों या वेबसाइटों से कॉल जिनमें गोपनीय बैंकिंग जानकारी मांगी गई हो
b. वे संदेश जिनमें सुरक्षा कारणों से तुरंत कार्रवाई करने के लिए कहा गया हो
c. ज्ञात वेबसाइटों के एक्सेस के लिए ईमेल में प्राप्त लिंक
d. असली वेबसाइट की जांच करने के लिए, लिंक पर कर्सर को ले जाएं या उस पर https:// देखें जहां "s" का मतलब 'सुरक्षित साइट' है।

फिशिंग हमलों का शिकार होने से बचने के तरीके

a. कभी भी इन ईमेल का जवाब न दें और किसी भी लिंक पर क्लिक न करें।

b. कभी भी ईमेल द्वारा या इन ईमेल में किसी भी लिंक पर अपना पिन या खाता विवरण जैसा अपना व्यक्तिगत विवरण न दें।

c. ते में हमेशा बैंक की वेबसाइट टाइप करें।

d. स्पैम ईमेल तुरंत हटाएं। मेलिंग सूची से ईमेल पता हटाने के अनुरोध से भी धोखा देने वाले व्यक्तियों को इस बात की पुष्टि होगी कि आपका ईमेल खाता सक्रिय है और आप पर अधिक हमलों का जोखिम हो सकता है।

e. कभी भी ईमेल अटैचमेंट न खोलें जब तक आप यह न जानते हों कि संदेश किसने भेजा है।

f. आने वाले नवीनतम ब्राउजरों का उपयोग करें

अगर आपके साथ इस तरह की फिशिंग गतिविधि होती है, तो तुरंत अपना पासवर्ड बदलें और बिना किसी देरी के अपनी शाखा को रिपोर्ट करें।

फिशिंग हमलों का शिकार होने से बचने के लिए आपकी जागरूकता महत्वपूर्ण है।

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।