विशिंग (Vishing)

"विशिंग" शब्द "वॉइस" और "फिशिंग" का संयोजन है। यह धोखेबाजों द्वारा निजी और गोपनीय वित्तीय विवरणों का एक्सेस करने और वित्तीय धोखाधड़ी के लिए इसका दुरुपयोग करने के उद्देश्य से टेलीफोन द्वारा वॉयस कॉल का उपयोग करके की जाने वाली आपराधिक गतिविधि है। सामान्य शब्दों में, गुमनाम कॉलर (धोखाधड़ी करने वाला व्यक्ति) किसी पीड़ित व्यक्ति को उनके बैंक खाते से संबंधित सत्यापन या समस्या के बहाने बैंकिंग प्रतिनिधि बनकर कॉल कर सकता है और व्यक्तिगत/ वित्तीय / खाता / भुगतान की जानकारी या पिन मांग सकता है।

विशिंग से जुड़े धोखाधड़ी करने वाले व्यक्तियों के जाल में फंसने से बचने के लिए,

आपको ये चीजें कभी भी साझा नहीं करना चाहिए:

- उपयोगकर्ता आईडी / उपनाम
- लॉगिन पासवर्ड o ओटीपी (वन-टाइम पासवर्ड)
- एटीएम/आईवीआर पिन
- कार्ड / सीवीवी नंबर
- जन्म की तारीख
- माता का नाम

अपने नेट बैंकिंग के साथ-साथ व्यक्तिगत ईमेल के पासवर्ड नियमित रूप से बदलें

नेट बैंकिंग और व्यक्तिगत ईमेल खातों के लिए समान पासवर्ड न रखें

कृपया ध्यान रखें, कोई भी बैंक यह जानकारी नहीं मांगता है....

शिकार न बनें... परिवार के सदस्यों और दोस्तों को भी यह जानकारी दें.... सतर्क रहें और सुरक्षित रहें....

साइबर अपराध की शिकायत करें:

यदि आप साइबर अपराध का शिकार हो जाते हैं, तो तुरंत कारवाई 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।