

विशिंग

“विशिंग” म्हणजेच “वॉईस” आणि “फिशिंग” चे मिश्रण. फसवणूक करणाऱ्या लोकांद्वारे केलेली ही गुन्हेगारी कृती आहे. यासाठी ते टेलिफोन वापरून वॉईस कॉल द्वारे खाजगी आणि गोपनीय आर्थिक तपशील मिळवतात आणि त्याचा आर्थिक फसवणूकींसाठी गैरवापर करतात.

सामान्य शब्दांमध्ये, एक निनावी कॉलर (फसवणूक करणारा) बँकेचा प्रतिनिधी म्हणून पीडित व्यक्तीला त्यांच्या बँक खात्याशी संबंधित पडताळणी किंवा समस्येच्या बहाण्याने कॉल करू शकतो आणि वैयक्तिक / आर्थिक / खात्याची / पेमेंटविषयी माहिती किंवा पिन विचारू शकतो.

विशिंग फसवणूक करणाऱ्यांच्या जाळ्यात पडण्यापासून वाचण्यासाठी,

तुम्ही हे कधीच शेयर करू नये:

- युजर आयडी / टोपण नाव
- लॉगइन पासवर्ड ० ओटीपी (वन-टाईम पासवर्ड)
- एटीएम / आयव्हीआर पिन
- कार्ड / सीव्हीव्ही क्रमांक
- जन्मतारीख
- आईचे लग्नाआधीचे नाव

तुमच्या नेट बँकिंग तसेच पर्सनल ईमेलसचे पासवर्ड्स नियमितपणे बदला.

नेट बँकिंग आणि पर्सनल ईमेल अकाउंट्सचे सारखेच पासवर्ड्स ठेवू नका.

कृपया लक्षात ठेवा कि कोणतीही बँक ही माहिती विचारत नाही.

बळी पडू नका... कुटुंबिय आणि मित्रमैत्रिणींमध्ये सुद्धा जागरूकता पसरवा... सावध रहा आणि सुरक्षित रहा....

सायबर फसवणूक झाल्यास तात्काळ तक्रार करा:

सायबर फसवणूकीचा बळी पडल्यास त्वरित कारवाई करा. राष्ट्रीय सायबर गुन्हे हेलपलाइन 1930 वर संपर्क साधा आणि

<https://cybercrime.gov.in/> या संकेतस्थळावर तक्रार नोंदवा. तसेच, तुम्ही Sancharsaathi Portal वरूनही तक्रार दाखल करू शकता.

वेळेवर तक्रार केल्यास पुढील फसवणूक टाळता येते आणि इतरांनाही सतर्क करता येते.