INTESA SANPAOLO BANK

Ce este vishing (voice phishing) si care sunt masurile pentru protejare impotriva acestor fraude

Voice phishing – sau mai pe scurt vishing – e o metoda frauduloasa prin care poti fi contactat telefonic de catre persoane care pretind a fi din partea autoritatilor (politisti, procurori) sau angajati ai bancii sau ai unor companii IT si care iti solicita accesul de la distanta pe calculatorul tau sub diferite pretexte,, scopul lor real fiind accesarea datelor bancare si efectuarea tranzactiilor frauduloase.

Aceasta metoda a evoluat si in domeniul bancar, atacatorii incercand sa obtina date financiare sau confidentiale, parole si coduri de acces, pentru a sustrage ulterior bani din conturile dumneavoastra.

Cele mai frecvente “scenarii” inventate sunt:

- ✓ **Castig neasteptat** – ai castigat o suma mare de bani, iar pentru a intra in posesia ei trebuie sa oferi datele tale confidentiale.
- ✓ **Calculator virusat** – din cauza unor virusi din calculatorul tau, a aparut o eroare in sistemul bancii si e nevoie de datele tale pentru a remedia problema.
- ✓ **O urgenta a bancii** – atacatorii vor invoca nevoia rapida la informatiile tale, punand asta pe seama unor proceduri bancare false (de exemplu: cont bancar blocat).
- ✓ **Apelurile false de suport** - metoda prin care atacatorii încearca sa obtina date sau bani de la posibile victime sunt apelurile care simuleaza contactarea pentru suport tehnic.
- ✓ **Frauda cu apeluri pierdute** - un utilizator gaseste un apel pierdut de la un numar de telefon din afara tarii. In momentul in care incearca sa contacteze inapoi acel numar, pentru a intelege scopul apelului, victima suna de obicei la un numar de telefon cu suprataxa.

Pentru a va proteja de astfel de metode frauduloase, va transmitem mai jos o serie de masuri de securitate pe care sa le puneti in aplicare in acest sens:

- ✓ NU raspundeti la apeluri din afara tarii, mai ales daca nu cunoasteti persoane din tarile respective.
- ✓ Ulterior, verificati identitatea acestuia cu organizatia din partea caruia a specificat ca va apeleaza.
- ✓ NU divulgati niciun fel de date confidentiale cum ar fi userul si parola de Internet Banking, codul de activare, numarul cardului, codul CVV2 sau PIN-ul. Banca niciodata nu va solicita informatii sensibile in acest mod de la clientii sai.
- ✓ Nu transferati bani catre necunoscuti, daca vi se solicita acest lucru.
- ✓ Verificați mereu cu banca orice solicitare suspecta privind furnizarea de informatii.
- ✓ NU instalati aplicatii si NU accesati site-uri la indicatiile persoanelor care va contacteaza telefonic.
- ✓ NU presupuneti ca persoanele care va contacteaza sunt de incredere doar pentru ca stiu cateva informatii despre dumneavoastra pe care le pot afla foarte usor de pe retelele de socializare.

In cazul in care ati fost victima unui astfel de atac:

- Notati orice date va amintiti din apelul respectiv: numarul sau numerele de telefon cu care ati luat contact in cadrul acestei scheme de vishing, data si durata apelului, ce date ati furnizat, ce software vi s-a sugerat sa instalati, orice date furnizate de atacator si mai ales ce actiuni ati facut, la cererea interlocutorului.
- Ulterior, mergeti la cea mai apropiata sectie de Politie pentru a depune o plangere si specificati aceste detalii. Sesizati Poliția la orice incercare de frauda, chiar daca nu ati devenit victima acesteia.
- In cazul in care ati oferit detalii legate de contul dvs. de Internet Banking sau date de card, contactati cat mai curand Banca pentru a bloca orice tranzactie suspecta. Rapiditatea cu care faceti acest pas este esentiala.
- Atentie la tentativele viitoare! Daca ati fost victima unei fraude, foarte probabil autorii va vor tinti din nou sau va vor vinde datele altor infractori.