VISHING: HAMIS BANKI HÍVÁSOK

Vishing: csalárd telefonhívások, amelyek érzékeny (személyes, banki, stb) adatok megszerzését célozzák.

A vishing (az angol „voice” és „phishing”, vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására, vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. Tipikus formája a vishingnek, amikor a csaló az adathalász hívás során megpróbálja elhitetni a felhasználóval, hogy ténylegesen egy banki alkalmazottal beszél, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonál.

Mit tegyen hamis banki hívás esetén?

- Kezelje óvatosan a kéretlen telefonhívásokat!
- Minél sürgetőbb a hívás és az üzenet annál gyanúsabb! Lassítson és gondolja át mit kérnek Öntől!
- Gyanús hívás esetén ne adjon meg személyes adatokat, és szakítsa meg a beszélgetést!
- Ha a kijelzett telefonszám valóban a banki ügyfélszolgálati telefonszáma, az sem garancia, hogy tényleg onnan keresik. Ellenőrzésként keresse meg a szervezet telefonszámát és azon keresztül lépjen vele kapcsolatba!
- Ne használja az ellenőrzéshez a hívó által adott telefonszámot. A szám hamis lehet!
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről, vagy a vállalatáról, amelynek dolgozik..például közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- Soha ne adja meg a betéti vagy hitelkártyája PIN kódját, CW kódját, vagy az online banki jelszavát. A bankok, banki ügyintézők sosem kérik el ezeket az adatokat!
- Soha ne telepítsen mások kérésére olyan programot számítógépére vagy telefonjára, amit nem ismer!
- Soha ne utaljon pénzt telefonon érkező kérésre! Egy bank sosem kér ilyet!

- Csalási szándékú hívásokat jelentse a bankjának!
  (Forrás: kiberpajzs.hu)

Esetpéldánk:

Sértettünket felhívta egy banki ügyintéző adategyeztetési céllal. A hívó elmondta, hogy a bejelentő számlájáról adathalászat segítségével egy nagyobb összeget próbáltak elutalni, de ez nem sikerült. Viszont ezt a bank észlelte, így segíteni szeretnének.

Az elmúlt 24 óra tranzakcióinak átvizsgálása érdekében elkérte a bejelentő internetbankos belépési adatait. Ezt sms formájában kérte elküldeni (arra a telefonszámra, ahova az áldozatunk banki visszaigazoló sms érkezik).

Az ügyintéző a további támadás kivédése ellen - a vírusvédelemre hivatkozva - egy telefonra letölthető programot ajánlott a sértettünknek, és megkérte, hogy ezt töltse le a telefonjára.

Sértettünk mind az internetbankos adatokat megadta, mind pedig a javasolt programot letöltötte a telefonjára.

Ezt követően számlájáról több millió forintot vettek le és utaltak el.