

Hamis banki telefonhívás

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, 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, HOGY NE VÁLJON ILYEN CSALÁS ÁLDOZATÁVÁ?

- ✓ Kezelje óvatosan, fenntartással a kéréstelen telefonhívásokat!
- ✓ Minél sürgetőbb a hívás, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!
- ✓ Gyanús telefonhívás esetén ne adjon meg személyes adatokat, és szakítsa meg a beszélgetést!
- ✓ Ha a kijelzett telefonszám valóban a bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát (a weboldalán vagy online kereséssel), és lépjen vele kapcsolatba közvetlenül!
- ✓ Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták.
- ✓ A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatáról, amelynek dolgozik, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- ✓ Ha hitelesnek gondolja a telefonhívást, akkor is kérjen keresztazonosítást, melynek során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét az intézmény ügyintézője adja meg, a válaszok másik felét pedig az ügyfél! Kérdezzünk rá olyan adatokra, amiket a bank tud, de egy csaló nem (pl. számlaszámunk, számla egyenlegünk, utolsó kártyahasználatunk). Ha „átkapcsolnak” vagy nem tudják a választ, akkor bontsa a vonalat.
- ✓ Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV-kódját, online banki jelszavát vagy egyszer használható, második hitelesítési kódot! A bankok sosem kérik ezeket az információkat!
- ✓ Soha ne telepítsen mások kérésére programot számítógépére vagy telefonjára! A csalók sokszor vírusvédelmi megoldásnak beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
- ✓ Soha ne utaljon pénzt (pl. biztonsági számlára) telefonon érkező kérésre! Egy bank sosem kér ilyet.
- ✓ A csalási szándékú hívásokat azonnal jelentse a bankjának!

Az internetes csalásokkal kapcsolatban a kiberpajzs.hu oldalon találnak hasznos információkat.