Óvja meg értékeit a netes csalóktól!
Legyünk mindig óvatosak!!!

A legelterjedtebb csalási formák

Telefonos: olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. A vishing 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.

Számítógépes: a fogyasztók és a vállalkozások egyre többet vásárolnak és adnak el az interneten. Nézzen utána a dolgoknak: vásárlás előtt keressen rá a hirdetőre, olvasson értékeléseket, ismertetőket az adott termékről!
Kizárólag biztonságos fizetési szolgáltatásokkal fizessen! Gyanakodjon, ha pénzküldési szolgáltatás használatát kérik!

SMS: A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadók SMS segítségével próbálnak megszerezni személyes, pénzügyi vagy biztonsági adatokat, információkat.
Megbízható forrásnak álcázzák magukat, úgy tesznek, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkeznének.
Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot például a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében.
A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát.

E-mail: ez az adathalász csalási forma olyan, banki ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására próbálja rávenni a címzettet. Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a létező bankok küldenek: a csalók lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák.

Bűncselekmény esetén azonnal tegyen bejelentést a legközelebbi rendőrkapitányságon vagy az ingyenesen hívható 112-es segélyhívó számon!

Bővebb információk: www.kiberpajzs.hu

https://www.facebook.com/NogradMBB
Nógrád vármegyei rendőrség Facebook oldala

Óvja meg értékeit a netes csalóktól!
Legyünk mindig óvatosak!!!

Mit tegyen, hogy ne váljon csalások áldozatává?

- Kezelje óvatosan, fenntartással a kéretlen 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!
- Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet, vagy kifejezetten a családhoz is létrehozhatták.
  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!
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatról, 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!
- 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 utaljon pénzt telefonon érkező kérésre! Egy bank sosem kér ilyet.
- A csalási szándékú hívásokat azonnal jelentse a bankjának!
- 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.
- Különösen banki adatait, azonosítóit ne adja meg idegeneknek!
- Banki internetes oldal helyett használja a pénzintézet mobil applikációját, mert a csalók által készített banki oldalak megtévesztésig hasonlítanak az eredetiekhez.
- Ha azt tapasztalja, hogy a jó azonosító adatok megadása után értesítést kap, hogy nem megfelelő a bejelentkezés, akkor valószínűleg egy áloldalt hívott le és a csalók így akarják megszerezni adatait.

Bővebb információk: www.kiberpajzs.hu

Bűncselekmény esetén azonnal tegyen bejelentést a legközelebbi rendőrkapitányságon vagy az ingyenesen hívható 112-es segélyhívó számon!