****

**HOGYAN KERÜLD EL HOGY**

**TELEFONOS, E-MAILES VAGY INTERNETES CSALÁS ÁLDOZATÁVÁ VÁLJ!**

Az utóbbi időben egyre több olyan esettel találkozunk, amelynek során ismeretlen csalók nagyvállalatok, mobilszolgáltatók, bankok, vagy éppen közüzemi szolgáltatók nevében telefonon, vagy a cégek arculati elemeit (nevét, logóját, stb.) felhasználva interneten keresnek fel gyanútlan ügyfeleket, és kifinomult trükkökkel pénzt vagy személyes adatokat próbálnak megszerezni tőlük.



**Mire utaznak a csalók?**

* Vagy **pénzt szeretnének kicsalni tőled**.
* Vagy a **személyes adataidat szeretnék megszerezni**.

A pénzre utazó csalók válogatott módszerekkel dolgoznak: van, aki veled töltetné fel a saját feltöltőkártyás egyenlegét, más a bankszámládhoz szeretne hozzáférni, míg a legmerészebbek akár személyes találkozót is szerveznek készpénz átvételére – ha kellően sikeresen meggyőztek, hogy önszántadból fizess nekik valamiért.

A személyes adat nagy érték a csalóknak, azaz úgynevezett adathalászoknak! A csalás útján megszerzett személyes adatokkal vagy közvetlenül visszaélnek, vagy tömegesen eladják azokat az  internetes feketepiacokon. Mit kezdenek a jogosulatlanul megszerzett személyes adatokkal? Sok módja van a visszaélésnek, például a jelszóval védett ügyfél-felületek belépési adatait megszerezve részletre vásárlással rendelnek új, nagyértékű telefont – csak éppen nem neked, hanem saját címükre kérik a szállítást, míg a telefon árának további részletfizetését meghagyják neked.

**Kiket céloznak a csalók?**

Mivel a csalók alapvetően nem rendelkeznek hivatalos ügyféladatbázissal, teljesen véletlenszerűen célozzák hívásaikat és küldenek e-maileket, vagy adnak fel hamis online hirdetéseket. Így gyakran előfordul, hogy egy potenciális áldozat egy olyan szolgáltatótól kap számlát, amelynek nem is az ügyfele.

**Hogyan zajlik egy ilyen átverés?**

A támadások érkezhetnek telefonon, e-mailen, internetezés közben a böngészőben felugró ablakban, vagy akár egy mobilalkalmazásban megjelenő kamuhirdetésben is. Az utóbbi időben a telefonos csalások helyett inkább az online módszerek felé fordulnak a csalók. Mi is ezekkel kezdjük a felsorolást!

**Netes csalások körében a következő módszerekkel találkoztunk eddig:**

* Hamis vírusriasztás okostelefonon böngészés közben, vagy appban megjelenő reklámban („Új vírust találtunk a telefonodon, azonnal kattints ide!”)
* Hamis fizetési felszólítás e-mailben egy szolgáltató nevében
* Értesítés egy állítólagos nagyértékű nyereményről (e-mailben vagy online hirdetési felületen), amelyet csak valamilyen – a nyeremény értékéhez képest aprónak tűnő – költség megfizetése után vehet át az áldozat, de valójában soha nem kap meg
* Egy szolgáltató (közmű, telefon, bank, stb.) nevében arról értesítenek, hogy feltörték a fiókodat, és – mielőbb – meg kell adnod a jelszavad az általuk megadott felületen

**Telefonos csalási kísérletek:**

* Hamis értesítés egy állítólagos nagyértékű nyereményről
* Telefonon kérnek el személyes adatokat, (például a feltöltőkártyás ügyfelekét) a kötelező adategyeztetés miatt
* A telefonszámlád másolatát kérik tőled faxon, kedvezőbb tarifát ígérve
* Valaki a hívott fél ismerősének adja ki magát, vagy azonnali pénzbeli segítséget kér egy állítólagosan bajba került rokonnak
* Megcsörgetik az áldozatot egy olyan telefonszámról, aminek előhívója ismeretlen, valószínűleg egy távoli országhoz tartozik

A fenti esetek mögött átverés van! A csalók ezekkel a módszerekkel  személyes adatokat, vagy pénzt próbálnak szerezni.

**Ezeket a módszereket használják az internetes csalók**

Ebben a részben nem a számítógépes vírusokat terjesztő csalók megoldásait (pl. zsarolóvírusok) mutatjuk be, hanem azokat a módszereket, amikkel egyes cégek, szolgáltatók ügyfeleit célozzák meg, a cég nevében elkövetve. Egyes csalók kifejezetten az online fizetésre használható bankkártya-adatokat próbálják kicsalni, mások a szolgáltatók oldalán regisztrált fiókod online belépési adatait akarják megszerezni, hogy más nevében saját maguknak rendeljenek valamilyen drága telefont, de a törlesztőrészletek fizetését már az áldozatukra bíznák. Lássuk az ismert eseteket!

**1, Hamis fizetési felszólítás e-mailben egy szolgáltató nevében:**

Ez a csalástípus az adathalászok kedvelt módszere. Lemásolnak egy valós céges számlalevelet, felhasználják az adott cég logóját, betűtípusát, azaz a kamu számlaértesítő szinte minden eleme megegyezik az eredeti levéllel. Mivel a csalóknak nincs valódi ügyfélazonosító-adatbázisuk, ide valótlan azonosítószámokat írnak, arra számítva, hogy azt úgysem ellenőrzi senki. A hamis számlalevéllel két céljuk lehet: vagy az, hogy rávegyék áldozatukat egy általuk kért összeg befizetésére (ami jellemzően nem gyanút keltően magas, de a csalók számláján landol), vagy az, hogy átirányítsák egy külső, ugyancsak hamis weboldalra, amelyet a személyes adatok ellopásához használnak (ehhez elég begépelni a felhasználónevet és a jelszót a csalók által készített űrlapon).  A hamis számlaértesítő e-mailben lévő linkek valamilyen külső honlapra vezetik a látogatót. Ezek a hamis oldalak kinézetre teljesen megegyezhetnek a szolgáltató weboldalával, csak éppen a csalók üzemeltetik abból a célból, hogy megszerezzék az adatait.

**Megoldás: E-mailes értesítő esetében több ponton is meggyőződhetsz arról, hogy valódi értesítésről van-e szó.**

1. Ellenőrizd, hogy a számlalevélen a te pontos számlázási azonosítód szerepel-e! Ha ezt a számsort nem ismered fejből, bármely korábbi havi számládon megtalálhatod!

2. Nézd meg alaposan azt is, hogy a levélben lévő link – ami az ígéret szerint a szolgáltatód online felületére visz, valójában – milyen honlapra mutat.

3. Ellenőrizd a levél, üzenet feladóját, tárgyát, címzettjét! Ha nem a te helyes e-mail címedet látod ott, akkor valószínűleg csalóktól érkezik az üzenet, akik jellemzően elrejtik az üzenetek címzettjét.

4. Az is gyanút kelthet, ha a  számlád jellemző összegétől eltérő nagyságrendű „számla” érkezik.

5. A szolgáltató általában nem kéri ügyfeleit arra, hogy levélben küldje meg a jelszavát vagy más személyes adatot, hiszen ez egyáltalán nem lenne biztonságos. Ha ilyesmit kérnek tőled, ne válaszolj a levélre! Ha bármilyen gyanúd merül fel egy online érkezett számlával kapcsolatban, érdemes felkeresni a szolgáltató ügyfélszolgálatát, ahol meg tudják mondani, hogy az adott értesítő valós volt, vagy sem.

**2, E-mailben értesítenek egy állítólagos nagy összegű nyereményről, amelyet csak kezelési költség vagy postaköltség megfizetése után vehetsz át:**

Távközlési szolgáltatók, vagy szerencsejáték szervezésével foglalkozó cég nevében üzenő csalók gyakran állítják azt, hogy áldozatuk nagy összeget  nyert valamilyen játékon. A nyeremény átvételének feltételéül azonban vagy valamilyen kezelési vagy regisztrációs költség, vagy egy feltöltőkártyás telefon egyenlegének feltöltését szabják.

**Megoldás:**egy ilyen hirtelen, váratlan nagy nyeremény (vagy örökség) mindig gyanús. Úgy senki sem sorsolhat ki téged, hogy ne tudnál arról, hogy egyáltalán részt vettél a játékban – hiszen ez azt jelentené, hogy valaki eleve visszaélt az adataiddal. Semmilyen esetben se tölts fel egyenleget idegen feltöltőkártyára, és ne adj kisebb összegű pénzt sem egy nagy nyeremény átvételének reményében, mert ezek átverések!

**3, Egy szolgáltató nevében arra figyelmeztetnek, hogy valaki feltörhette a fiókodat, azonnal meg kell adnod egy új jelszót az általuk megadott felületen:**

A csalók ebben az esetben egy hamis honlapra irányítanak téged, amely többnyire csupán egyetlen űrlapot tartalmaz, ahol megadhatja a régi és új jelszavát. Persze az egész egy átverés, a begépelt adatok valójában a csalóknál kötnek ki.

**Megoldás:**Nézd meg alaposan, hogy milyen cég nevében érkezik a figyelmeztetés; a céghez tartozhat-e az értesítést feladó e-mail cím. Ami a legfontosabb: hogy mi a weboldal címe, ahol az adatokat kérik tőled: ezt a böngésző felső címsorában láthatod. Ha az adott cég weboldalának címe szerepel itt, akkor jó helyen jársz!

**4, Mobilon böngészés közben vagy egy alkalmazásban a hirdetés helyén hamisan jelez vírust a mobilodon egy honlap/reklám:**

Az asztali PC-k, laptopok mellett már az okostelefonokat is célozzák a csalók olyan hamis  rendszerüzenetekkel, amelyekben általában arra hívják fel hamisan a látogató figyelmét, hogy készüléküket valamilyen kártevő fertőzte meg. Megoldásként általában egy vírusirtónak álcázott program lefuttatását javasolják. A javasolt program azonban általában nem legitim, és sok esetben valójában egy adott felületre kattintva egy emelt díjas számra küld SMS-üzenetet az áldozat.  Más esetben ezzel a módszerrel valamilyen fizetős SMS-szolgáltatásra lehet feliratkozni, amely esetében az üzenetek fogadásáért akár több ezer forintot kell fizetni. Az is előfordul, hogy olyan mobilalkalmazást telepíttetnek fel az áldozattal, amely valójában nem tisztítja meg semmitől a készüléket, ellenben jelszavakat és más privát adatokat továbbít illetékteleneknek.

**Megoldás:**Gondolj bele, egy egyszerű honlap hogyan lenne képes kimutatni azt, hogy a telefonod fertőzött? Ha emiatt aggódsz, telepíts fel a Google Play-ről vagy az Apple App Store-ból valamilyen legitim biztonsági appot (pl.  Avas), és hagyd figyelmen kívül a honlapokon felbukkanó félrevezető figyelmeztetéseket!

**Így próbál meggyőzni egy telefonos csaló**

A telefonos (hívásalapú) csalások népszerűsége abban rejlik, hogy az áldozat egyetlen érzékszervére, a hallására támaszkodhat, miközben a csalóknak számos technikájuk van arra, hogy a legkevesebb ideje maradjon a hívott félnek gyanús jeleket észrevenni a hívás során.

**A telefonos átverések** legelterjedtebb formájában ismeretlen vagy rejtett telefonszámról hívják fel a potenciális áldozatot. Nagyon résen kell lenni, hogy észrevegyük a turpisságot, mert ilyenkor igen gyakorlott csalók vannak a vonal túlsó végén. Sokszor (valójában nem is létező) azonosítószámukat, felettesük nevét is bemondják, és olyan szófordulatokat használnak, amivel a hívott fél bizalmába férkőzhetnek; pl. „az Ön biztonsága érdekében a telefonbeszélgetést rögzítjük”. A csalók jellemzően **igen határozottan és gyorsan beszélnek,**a lehető legkevesebb esélyt adva arra, hogy félbeszakíthassuk őket.

Jellemzően olyan helyzet elé állítanak a hívás során, amiben **gyorsan kell döntést hoznunk**, ezzel arra próbálnak rávenni, hogy ne is a hívás valódiságán, hanem annak tartalmán – szerencsés vagy megoldandó helyzeten – gondolkodjunk. Ha a csalók érzik, hogy a hívott fél gyanút fogott, a legtöbb esetben azonnal bontják a vonalat, és valószínűleg nem is jelentkeznek újra.

**Mit tehetsz, hogy ne válj áldozattá?**

Sajnos a csalók folyamatosan finomítják módszereiket, így kihívást jelent lépést tartani velük. Alapvetően azt javasoljuk mindenkinek, hogy online befizetés, átutalás, adatbekérés előtt legyen fokozottan körültekintő! Győződj meg arról, hogy valóban az a cég áll-e a megkeresés mögött, aki a pénzt vagy az adatokat kéri.

**Mit tegyek, ha megtörtént a baj?**

Ez attól is függ, milyen kárt okoztak neked. Első lépésben mindenképpen ahhoz a céghez/szolgáltatóhoz érdemes fordulnod, akinek a nevében a csaló fellépett. A szolgáltatóval való egyezetetés alapján érdemes megkeresni a rendőrséget, ha pedig kisebb-nagyobb összeget is ki tudtak csalni belőled, nélkülözhetetlen feljelentést tenni a rendőrségen.

Lássuk a fent említett csalási módszereket részletesebben: hogyan lehet felismerni a csalók próbálkozásait, és hogyan lehet elkerülni, hogy áldozattá váljunk?

**Ezeket a módszereket használják a telefonos csalók:**

**1, Hamis értesítés egy állítólagos nagy összegű nyereményről:**

Az ilyen esetekben közös, hogy egy ismert cég nevében hívnak fel, és azt állítják, hogy nagyértékű nyereményt nyertél. Ez elsőre jól hangzik, de minden esetben **valamilyen feltételt szabnak** **a nyeremény átvételéhez.** Például egy frissen vásárolt feltöltőkártya kódját kérik bediktálni, vagy a nyeremény átadásához kezelési költség címén egy meghatározott telefonszámra való egyenlegfeltöltést kérnek. Más esetekben trükkösebbek: egy olyan kód feltöltését kérik, amelynek begépelésével bármilyen kártyás előfizetés egyenlegét növelni lehet a befizetett összeggel. Ez a csalási módszer azért működik, mert a váratlan nagy nyeremény/szerencse híre azonnal a gyermeki énünket hozza felszínre, így csökkent realitás-érzékkel hajlamosakká válhatunk irracionális kéréseknek is eleget tenni.

 **Megoldás:**Alapvető, hogy a hatályos törvények értelmében nem nyerhetünk olyan játékon, amiről nem is tudtuk, hogy részt vettünk benne. Ez ugyanis azt jelentené, hogy valaki a tudomásunkon kívül kezeli az adatainkat, ami visszaélést jelent, tehát valami turpisság van a dologban. **Egyszerűen nem szabad ismeretlen emberek egyenlegét feltölteni, és ugyanígy  nem szabad az állítólagos nagyértékű nyeremény reményében pénzt utalni, küldeni, vagy akár személyesen átadni senkinek.**

**2, Telefonon kérnek el személyes adatokat, például a feltöltőkártyás ügyfeleknek kötelező adategyeztetés miatt:**

A 2017-ben hatályba lépett hazai jogszabályok értelmében a szolgáltatóknak évente be kell azonosítani a feltöltőkártyás ügyfeleiket, hogy ne legyen mód idegenek nevére vásárolt SIM-kártyákkal való visszaélésre. Egyes csalók magukat valamelyik szolgáltató munkatársának kiadva a kötelező adategyeztetésre hivatkozva mindenféle bizalmas adatot, például nevet, címet, bankkártya-adatokat próbálnak kiszedni az ügyfelektől.

Ha valamelyik szolgáltató feltöltőkártyás adategyeztetés miatt keres, akkor biztos, hogy korábban kaptál már tőlünk értesítő SMS-t emiatt. Ha mégsem kaptál ilyet, és mégis erre hivatkozik a telefonáló, akkor a hívás jó eséllyel hamis!

**Megoldás:** Ne adj meg semmilyen adatot addig, amíg nem győződtél a hívás valódiságáról! Ha feltöltőkártyás adategyeztetés miatt hívnak, már biztosan küldtek a telefonszámra SMS-t emiatt. Kérjük, ellenőrizd!

**3, A telefonszámlád másolatát kérik tőled faxon, kedvezőbb tarifát ígérve:**

Hidd el, nem jótékonykodni szeretnének veled! Még akkor sem, ha azt is állítják, hogy jótékonyságból szeretnék helyetted kifizetni a havi telefonszámládat, és arra kérnek, hogy faxold el nekik a számlád másolatát. Sokszor a jelenleginél kedvezőbb tarifát is ígérnek, de valójában a számlán lévő adatokra (név, lakcím, ügyfélszám stb.) fáj a foguk. Ezek birtokában például saját címükre rendelnek akciós készüléket, a törlesztőrészletek kifizetését persze az áldozatra, vagyis rád bíznák!

**Megoldás:**Semmiképp ne küldd el a telefonszámládat, de még a másolatát sem idegeneknek, és tudd, hogy egyetlen szolgáltató sem kér ilyet az ügyfeleitől. Aki mégis ezt teszi, annak biztosan visszaélés, csalás a célja.

**4, Ismeretlen telefonáló egy rokonnak vagy egy rokon ismerősének adja ki magát, és azonnali pénzbeli segítséget kér, jellemzően valamilyen hirtelen előállt baj, baleset miatt. Ez az úgynevezett „unokázós csalás”.**

Ezzel a módszerrel általában idős embereknél próbálkoznak, illetve bárkinél, akiben a hívás során érzik a bizonytalanságot – hiszen a csalók azt gondolják, sok vesztenivalójuk nincs. Idősek esetében kihasználják azt is, ha a hívott fél nem érti, nem hallja teljesen jól, amit mondanak neki, és nem mindig tűnik fel számukra, hogy valójában nem a saját rokonuk, ismerősük beszél hozzájuk. Más esetekben pedig csak egy rokon jóbarátjának adják ki magukat a csalók, így kérnek azonnali segítséget az állítólag bajba került rokonnak. Szinte mindig kitalálnak valamilyen hamis történetet arra vonatkozólag is, hogy az ismerős vagy rokon miért nem tud személyesen telefonálni, miért nem tud eljönni az összegért, és ezekben az esetekben a csalók személyesen vennék át a kicsalt készpénzt. Az ilyen esetekben mindig azonnali döntést sürgetnek, és amint érzik, hogy bedőlt a hívott fél, már jönnének is a pénzért.

**Megoldás:**Egyáltalán ne adj pénzt ismeretlen embernek! Ha mégis esélyét látod, hogy igaz a történet, mielőtt rokonnak, ismerősnek szánt pénzt adnál egy idegen ember kezébe, próbáld meg felvenni a kapcsolatot a hivatkozott emberrel, vagy a rokonságból bárkivel, akit ismer, és akinek tudomása lehet egy olyan esetről, amire az ismeretlen hivatkozik. Szükség esetén a rendőrséget is érdemes értesíteni!

**5, Megcsörgetnek egy olyan telefonszámról, aminek előhívója ismeretlen, valószínűleg egy távoli országhoz tartozik:**

Előfordul, hogy teljesen ismeretlen telefonszámról csörgetik meg a telefonodat, és mielőtt felvennéd, meg is szakítják a hívást. Ez esetben nagy valószínűség szerint ún. visszahívásos csalással próbálkoznak. Ezek elkövetői egy távoli országból véletlenszerűen hívnak fel telefonszámokat, de csöngés után a hívást rögtön bontják, mert **az a céljuk, hogy te visszahívd őket!**A csalók a hívott fél által indított, nemzetközi irányú (2-3-as díjzóna) hívások díja után kapnak részesedést. Ezek minimális összegek, de ha sokan hívják őket vissza, szép kis summát zsebelnek be egy távoli ország szolgáltatójától. Az ilyen típusú csalásoknál sokszor még azzal is trükköznek, hogy egy automata ugyan fogadja a hívást, ám ők továbbra is bejátsszák a kicsöngés hangját. Ezzel az a céljuk, hogy a visszahívó minél tovább tartsa a vonalat, és fizesse a nemzetközi hívás percdíját.

 **Megoldás:**Könnyű a védekezés, egyszerűen **ne hívd vissza az ilyen idegen előhívójú számokat!** Ha valakit gyakran hívhatnak külföldi számról, ezért egy ismeretlen számról érkező hívás önmagában nem kelt gyanút, akkor az lehet gyanús, ha a csalók olyan rövid ideig csörgetnek meg,  hogy esélyed sincs felvenni a hívást. Ha mégis szeretnél meggyőződni a megkeresés valódiságáról, érdemes megkeresni az interneten, hogy melyik országból hívták, és javasoljuk, hogy gondolja át, hogy mennyire valószínű az a helyzet, hogy abból az országból keresnek téged!

**Hivatalosnak tűnő ál-mailek:**

Ennél az átverésnél a potenciális áldozatok rendszerint egy e-mailt kapnak, amely látszólag egy hivatalos intézménytől, leggyakrabban banktól érkezik. A felhasználót azután egy linkkel átcsalják egy hamis weboldalra, amely egyébként megtévesztésig hasonlít az eredetihez, így csak ritkán kelt gyanút. Az e-mail hitelesnek tűnik az eredeti logók vagy a cég szokásos betűtípusának használata miatt, így a felhasználók meglehetősen könnyen félrevezethetők. Ám a hamis weboldalon rendszerint bankkártyaszámot, jelszót, PIN-kódot kérnek: itt bukik meg a dolog, ugyanis a valóságban a bank sosem kér ilyet mailben.



**Ha mégis bűncselekmény áldozatává válik,**

**azonnal értesítse a rendőrséget a 112-es segélyhívó számon!**