Bűnmegelőzési hírlevél
2019.08.06.
Ne dőljön be a csalóknak!

Az elmúlt néhány év adatai és a szakmai tapasztalatok azt mutatják, hogy a bűnözésen belül egyre nagyobb arányt képviselnek a megtévesztéssel, az emberek jóhiszeműségének kihasználásával elkövetett bűncselekmények, egyre gyakrabban fordulnak elő a telekommunikációs eszközök felhasználásával („feltöltőkártyás" csalások) és az online elkövetett bűncselekmények, amelyek célja

az áldozat pénzének és/vagy személyes adatainak megszerzése.

A személyes adat nagy érték a csalóknak. A csalás útján megszerzett személyes adatokkal vagy közvetlenül visszaélnek, vagy tömegesen eladják azokat az internetes feketepiacokon.
A támadások érkezhetnek telefonon, e-mailen, internetezés közben a böngészőben felugró ablakban, vagy akár egy mobilalkalmazásban megjelenő kamuhirdetésben is.

Módszerek:

Hamis fizetési felszólítás e-mailben egy szolgáltató nevében:
Lemásolnak egy valós céges számlalevelet, felhasználják az adott cég logóját, betűtípusát, azaz a kamu számlaértesítő szinte minden eleme megegyezik az eredeti levéllel.
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 számlájára érkezik), **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**).
Kérjük:

- Ellenőrizze, hogy a számlalevélen az Ön pontos számlázási azonosítója szerepel-e?
- Nézze meg alaposan azt is, hogy a levélben lévő link valójában milyen honlapra mutat?
- Az is gyanút kelthet, ha a számla jellemző összegétől eltérő nagyságrendű „számla" érkezik

Ne feledje:
A szolgáltató soha nem kéri ügyfeleit arra, hogy e-mailben küldje meg a jelszavát vagy más személyes adatát, hiszen ez egyáltalán nem lenne biztonságos. Ha ilyesmit kérnek, ne válaszoljon a levélre! Ha gyanú merül fel egy online érkezett számlával kapcsolatban, keresse fel a szolgáltató ügyfélszolgálatát, ahol meg tudják mondani, az adott értesítő valós volt, vagy sem.

E-mailben értesítik egy állítólagos nagy összegű nyereményről, amelyet csak kezelési költség vagy postaköltség megfizetése után vehet 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.
Egy ilyen váratlan nyeremény (vagy örökség) legyen mindig gyanús! Ellenőrizze le a hivatkozott szolgáltatónál a nyeremény valódiságát.

Egy szolgáltató nevében arra figyelmeztetik, valaki feltörhette a fiókját, azonnal meg kell adnia egy új jelszót az általuk megadott felületen:

A csalók ebben az esetben egy hamis honlapra irányítják, amely többnyire csupán egyetlen űrlapot tartalmaz, ahol megadhatja a régi és új jelszavát.

Ne feledje, a szolgáltatók soha nem kérik, hogy írja meg a jelszavát és a PIN kódját!
Ellenőrizze, hogy a hivatkozott céghez tartozhat-e az értesítést feladó e-mail cím!
Érdeklődjön közvetlenül a szolgáltató ügyfélszolgálatánál!

Mobilon böngészés közben vagy egy alkalmazásban a hirdetés helyén hamisan jelez vírust a mobilján 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 legális 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**

Egy egyszerű honlap nem képes kimutatni azt, hogy a telefonja fertőzött! Ha emiatt aggódik, javasoljuk, telepítsen fel a Google Play-ről vagy az Apple App Store-ból valamilyen legális biztonsági appot (pl. Avas), és hagyja figyelmen kívül a honlapokon felbukkanó félrevezető figyelmeztetéseket!

Telefonon kérnek el személyes adatokat, például a feltöltőkártyás ügyfeleknek kötelező adategyeztetés ürügyén:

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 keresi, akkor biztos, hogy korábban már kapott már tőlük értesítő SMS-t. Ha mégsem kapott ilyet, és mégis erre hivatkozik a telefonáló, akkor a hívás jó eséllyel hamis!

Ne adjon meg semmilyen adatot addig, amíg nem győződött meg a hívás valódiságáról!

A telefonszámlája másolatát kérik Öntől, kedvezőbb tarifát ígérve:

Állításukkal ellentétben nem jótékonykodni szeretnének! Még akkor sem, ha jótékonyságból felajánlják a számla kifizetését és arra kérik, faxolja el nekik a számlája másolatát. Sokszor a jelenleginél kedvezőbb tarifát is ígérnek, de valójában a számlán lévő adatokra (név, lakcím, ügyfélszám stb.) van szükségük, amelyekkel vásárolni tudnak, az árut a saját címre rendelve, a számlát pedig Önre hagyva.

Semmiképp ne küldje el a telefonszámláját, de még a másolatát sem idegeneknek, és **ne feledje, egyetlen szolgáltató sem kér ilyet az ügyfeleitől**. Aki mégis ezt teszi, annak biztosan visszaélés, csalás a célja.

Megcsörgetik egy olyan telefonszámról, aminek előhívója ismeretlen és valószínűleg egy távoli országhoz tartozik:

Előfordul, hogy teljesen ismeretlen telefonszámról csörgetik meg a telefonját, és mielőtt felvenné, 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 is, mert **az a céljuk, hogy Ön visszahívja őket!** A csalók a hívott fél által indított, nemzetközi irányú (2-3-as díjzóna) hívások díja után kapnak részesedést. 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.

Ne hívja 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, hogy a csalók olyan rövid ideig csörgetik meg, hogy esély sincs fogadni a hívást.
Ha mégis szeretne meggyőződni a hívás valódiságáról, érdemes megkeresni az interneten, melyik országból hívták, és javasoljuk, gondolja át, mennyire valószínű az a helyzet, hogy abból az országból keresik Önt!

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 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. **A valóságban a bankok sosem kérnek ilyet mailben.**

Online vásárlás

Az utóbbi időben megszaporodtak azok a bűncselekmények, amikor ismeretlenek mások nevében, mások személyes adatainak felhasználásával vásároltak drága mobil telefont előfizetéssel részletre, előleg fizetése nélkül online a szolgáltatótól. Akinek az adataival visszaéltek, csak néhány hónap késéssel értesül a történtekről, amikor a szolgáltató elkezdi követelni rajta a tartozást, mert természetesen az álvásárló nem fizet.
Ezeket a típusú bűncselekményeket kivédeni csak úgy lehet, **ha kellő körültekintéssel óvják személyes adataikat.**

Az online térben és a valóságban is ügyeljenek arra, kinek adják meg személyes adataikat, vigyázzanak az okmányaikra, bankkártyájukra, hogy mások ne tudjanak vele visszaélni!

Heves Megyei Rendőr-főkapitányság
Bűnügyi Osztály Bűnmegelőzési Alosztály

☎:112