Az online csalások, módszerek, megelőzés

Mi az adathalászat?

Az adathalászat lényege, hogy a támadások megbízható forrásnak álcázott csalóktól származnak (saját bank, saját közmű szolgáltató, egyéb) és megtévesztéssel a gyanútlan felhasználó bizalmas adataihoz férnek hozzá. Leggyakrabban bankkártya adatokat próbálnak megszerezni, mely adatok birtokában kiürítik az áldozatok bankszámláit.

Hogyan történik?

A leggyakoribb adathalász technika egy bank vagy szolgáltató (telefon, áram, tv, stb.) megszemélyesítése email-ben**,** rávéve a felhasználót arra, hogy egy hamis – az emailben található vagy mellékletként küldött – adatlapot töltsön ki, vagy látogasson meg egy weboldalt, ami a belépéshez kéri a fiókjának adatait vagy a belépéshez szükséges hitelesítő adatokat. Ha ezt megteszi, ott a szükséges adatok beírásával gyakorlatilag hozzáférhetővé teszi a bankszámláját a csaló számára. Hasonló támadások végezhetők telefonhívásokkal és SMS üzenetekkel.

Hogyan előzhető meg?

Számos különféle verziója van ezeknek az üzeneteknek, ezért a legfontosabb, hogy mindig alaposan vizsgáljuk meg. Néhányat rögtön ki lehet szűrni, pl. ha nincsen Netflix előfizetésünk, akkor nem kaphatunk felszólítást elmaradt befizetésről. Sok esetben szokatlan, magyartalan a szövegezés, rossz a helyesírás, általános a megszólítás, nem közölnek ügyfélszámot.

- Mindig azonosítsuk a feladót, ellenőrizzük a küldő címét, telefonszámát. Hasonlítsuk össze a szolgáltató egy korábbi levelével, SMS-ével, nézzük meg, egyezik-e.
- Ne adjuk meg személyes adatainkat: Mindig legyünk óvatosak, ha egy látszólag megbízható helyről származó elektronikus üzenet a hitelesítő adataink vagy más érzékeny adataink felől érdeklődik. Ha szükséges, ellenőriztessük le az üzenet tartalmát azzal a feladóval vagy szervezettel, akitől az üzenet látszólag érkezett.
- Telefonhívás esetén se adjuk ki banki adatainkat, ha bizonytalanok vagyunk, bontsuk a vonalat, majd hívjuk fel az általunk ismert számon azt a bankot, szolgáltatót, akitől látszólag a hívás érkezett.
- Amennyiben üzenetet kapunk, mindig gondoljuk meg kétszer, hogy a kapott linkre kattintunk-e, soha ne legyen ez automatikus.
- Ha mégis rákattintunk, és banki illetve egyéb személyes adatokat kér, soha ne adjuk meg azokat!! Azonnal töröljük az üzenetet!! SMS-nél tiltsuk le a számot!
- A bankunk, szolgáltatónk weboldalát mentsük a kedvencek közé, és azt mindig onnan nyissuk meg! Ne kattintsunk rá az első hasonló oldalra!
- Figyelmeztessünk másokat is, jelezzük az eseteket a közösségi oldalunkon ismerőseink felé!
- Legyünk tisztában az új adathalász technikákkal, kövessük a médiában az adathalász támadásokkal kapcsolatos beszámolókat, mivel a támadók újabb és újabb technikákat dolgoznak ki a felhasználók megtévesztésére.

Mi az a romantikus csalás?

A csalók általában özvegy, egyedülálló külföldi orvosnak, katonának, mérnöknek kiadva magukat ismerkednek gyanútlan, általában már idősebb korosztályba tartozó hölgyekkel, akivel rövid idő alatt elhitetik, hogy szoros érzelmi kapcsolatba kerültek, és közös jövőt tervezhetnek. Akár hónapokig tartó levelezés, csetelés után valamilyen ürüggyel pénzt csalnak ki az áldozattól, sok esetben jelentős összegeket. Természetesen férfiak is lehetnek célpontok.

Honnan lehet felismerni a csalási szándékot? Hogyan előzzük meg?

A kívülálló tipikus reakciója: Túl szép, hogy igaz legyen. A sértettek mégis elhiszik.
Rendszerint közösségi, társkereső oldalakon jelentkezik a csaló, nagyon gyorsan tájékozódik a potenciális sértett személyes körülményeiről, nagyon gyorsan alakít ki szoros érzelmi kapcsolatot, viszont a képek küldésén túl nem kerül sor telefon- vagy video-beszélgetésre, nincs személyes találkozó. Végül mindig pénzt próbál kicsikarni az illető valamilyen hihető ürüggyel, azonban, ha ez nem sikerül sok esetben a zsarolástól sem riad vissza!

- Mindig vegyük figyelembe, hogy nem tudhatjuk biztosan, hogy ki van a profil mögött!
- A közösségi oldalon ne írjuk ki családi állapotunkat! Legyünk nagyon óvatosak, hogy mennyi személyes információt osztunk meg magunkról.
- Gyanakodjunk, ha az új online ismerős nem szeretne személyes találkozót vagy tartózkodik attól, hogy telefonon vagy webkamerán keresztül beszéljünk.
- Akit nem ismerünk személyesen, annak ne küldjünk pénzt, ne adjunk ki információt anyagi helyzetünkről.
- Ne adjuk meg bankkártya vagy online banki adatainkat és ne küldjünk másolatot okmányainkról.
- Lehetőleg ne osszunk meg olyan információkat és ne küldjünk olyan fotókat magunkról, amivel később megzsarolhatnak.
- Mindig legyen gyanús, ha valaki arra kér minket, hogy ne beszéljünk másnak a kapcsolatról!

Hogyan működnek az online vásárlással elkövetett csalások?

Mivel manapság már rendszeresen vásárolunk online, sokszor elmulasztjuk az óvatosságot. A csaló meghirdet egy árut egy online oldalon, előre kéri átutalni a vételárat, de ha ez megtörtént, nem küld semmit a vevőnek, vagy valamilyen használhatatlan, vagy jóval olcsóbb holmit küld.
Az utalásokat követően az eladó egyszerűen eltűnik, majd profilváltás után visszatér és más néven folytatja a tevékenységét.

Hogyan előzhetjük meg? Mi a teendő, ha már becsaptak?

- Ha tehetjük, online piacterek helyett inkább webshopokban vásároljunk, mert ebben az esetben vevőként jogszabály is védi az érdekeinket, mint például a fogyasztóvédelmi törvény. Külföldi oldalakról is csak előzetes tájékozódás után rendeljünk!
- Biztonságot nyújtanak azok az oldalak, ahol kiválasztható a fizetéshez valamilyen pénztranszferrel foglalkozó köztes szolgáltató, pl. Paypal, rajtuk keresztül visszaigényelhető az elutalt összeg.
- Ha valamit aránytalanul olcsón árulnak, akkor mindig gyanakodnunk kell!
- Mindig megfelelő gondossággal ellenőrizzük le azt az eladót, akitől vásárolni szeretnénk. Próbáljunk meg rákeresni korábbi vásárlók véleményeire, értékeléseire is.
- Ha egy eladó túl sok személyes információ megadását kéri, az legyen azonnali intő jel! A legjobb és legbiztonságosabb az, ha csak olyan megbízható, ismert webshopokból vásárolunk, amelyek igazolt korábbi eladásokkal rendelkeznek.
- Kezdjünk gyanakodni, ha nem kapunk néhány percen belül megerősítést a vásárlásunkról. Elsőként az eladóknál kezdjünk érdeklődni. De ha onnan sem jön válasz, akkor forduljunk azonnal a bankhoz, hiszen ekkor már nagyon valószínű, hogy internetes csalás áldozatai lettünk.
- A bankok fel vannak készülve az ilyen esetek kezelésére, mindenképp forduljunk hozzájuk, ha bajba kerültünk, mert arra is van esély, hogy a bank vissza tudja hívni a leemelt összeget.

Itt kell megjegyezni, hogy legújabb elkövetési mód, hogy az interneten megjelentek azok a magyar nyelven elérhető weboldalak, melyek a piaci ár alatt jelentősen olcsóbban árulnak márkás termékeket (cipőket, Samsung vagy iPhone telefonokat, stb.), melyek megrendelése esetén utánvétes fizetést lehet választani.

Az ár miatt mindenképpen aggályos az ilyen oldalakról vásárolni, de az óvatosságot figyelmen kívül hagyva az emberek még is vásárolnak, hisz azt gondolják, hogy utánvét esetén nem válhatnak áldozattá. A csomagokat rövid időn belül a posta vagy a GLS futár szállítja ki. A vételár megfizetését követően a vásárlók azzal szembesülnek, hogy nem az általuk megrendelt árut kapják meg, hanem pl. egy Tetrisz játékot.

- Amennyiben ilyen típusú csalás áldozatává vált valaki, a csomag átvételét követően a lehető legrövidebb időn belül tegyen rendőrségi feljelentést!

Hogyan működnek a netes befektetési csalások?

A kiberbűnözők az esetek többségében online hirdetési felületeken kecsegtetnek nagy hozamokat ígérő, biztosan és gyorsan megtérülő befektetési tippekkel. Szembetűnő jellegzetessége a befektetési átveréseknek, hogy a korábbi – soha nem is létező – hozamokra támaszkodva szeretnének minél több felhasználót rávenni az ügyletre. Nagy hangsúlyt fektetnek a hitelességre és használják fel közéleti személyiségek (sok esetben pénzemberek) arcát.

A befektetési csalók magas nyereséget és gyors megtérülést ígérnek. Az ajánlatok eltérőek, de a lényeg minden esetben ugyanaz - gyorsan és egyszerűen megsokszorozhatjuk befektetésünket.

Mit kell tudni ahhoz, hogy megelőzhessük a sértetté válást?

A csaló általában bemutat egy jónak tűnő üzleti lehetőséget, mellyel megtízszerezhetjük befektetésünket. Előfordulhat, hogy az illető egy valódi befektetési társaság képviselőjének adja ki magát, és az is elképzelhető, hogy az általa említett befektetés valós, de a pénzünk a címzetthez sosem fog eljutni, csak a bűnözők lesznek vele gazdagabbak.

- Legyünk mindig körültekintőek, tudni kell, hogy nincs olyan garantált befektetés vagy módszer, amely könnyen pénzt hoz.
- Ha egy ajánlat mégis felkelti az érdeklődésünket, feltétlenül alaposan nézzünk utána az ajánlatnak, illetve a mögötte álló cégnek.
- Ha a befektetés és a vállalat egyaránt valósnak bizonyul, ellenőrizzük le annak a személynek a személyazonosságát is, aki az üzletet kínálja nekünk, mert lehet, hogy a saját zsebére dolgozik.

Mit kell tudni az un. távoli elérést biztosító programok telepítésével elkövetett csalásokról?

A távoli elérést biztosító program - pl. az AnyDesk - telepítésére gyanútlan „ügyfeleket” vesznek rá a csalók, ez a program hozzáférést biztosít az áldozat számítógépéhez és telefonjához, ha telepíti, és engedélyt ad másnak a használatára.

Hogyan működik ez a fajta csalás, hogyan lehet ellene védekezni?

A csalók telefonon jelentkeznek, nagyon meggyőzően tudják alakítani a banki ügyintézőt, a bankbiztonsági szakembert, ezért általában sikerrel járnak. Meggyőző kommunikációval, valóban meglévő szakértelemmel ráveszik az áldozatokat, hogy a telefonjukra az AnyDesk elnevezésű alkalmazást telepítsék, mert ezzel megvédhetik számítógépüket, és így nagyobb biztonságban lesz a bankszámlájuk.

A csalók a program segítségével átveszik az irányítást az eszköz felett, és hozzáférnek a jelszavakhoz, bankkártya adatokhoz, bankszámlához, tehát a bankszámlánkról elvehetik a pénzünket, de minden más adathoz is hozzáférnek a gépünkön. Tehát számos visszaélésre nyílik lehetőségük.

Tudni kell, hogy

- A bank sosem javasolja különböző programok telepítését, az ilyen hívások minden esetben csalóktól származnak!
- Soha ne telepítsünk programot a gépeinkre ismeretlenek javaslatára, főként, ha készségesen felajánlják, hogy lépésről-lépésre segítenek a telepítésben!
- Tájékozódjunk a hasonló programok működéséről, ne hagyjuk magunkat becsapni!

A legfontosabb a TUDATOS INTERNETHASZNÁLAT!

Mindig kellő figyelemmel olvassuk az érkező küldeményeket, tájékozódjunk a veszélyekről, ne higgyünk el mindent!!!

Ha megtörtént a baj, azonnal forduljunk a bankhoz és a rendőrséghez!

NE LÉGY BALEK!!

Ismeretlenben sose bízz!!!

- **Külföldi katona, orvos udvarolgat neked a neten? Vagy egy kedves csinos hölggyel hozott össze a világháló?**
- **Túl szép, hogy igaz legyen?**
- **Még csak fényképen láttad?**
- **Sosem jön össze a videochat?**
- **Egy kis kölcsönre lenne szüksége, hogy meglátogathasson?**

Profi külföldi csalók áldozata lehetsz, és sosem kapod vissza a pénzedet! Visszaélnek az érzéseiddel, kihasználnak, sőt meg is zsarolhatnak!

Keresd a Facebookon a ROMANTIKUS CSALÓK oldalt, és

GONDOLKODJ!!!

NE LÉGY BALEK!!

Ne engedd át az irányítást!!!

- **Bank vagy szolgáltató „ügyintézője” telefonon arra buzdít, hogy telepíts a számítógépedre vírusirtó alkalmazást?**
- **Készségesen, lépésről lépésre segít a szoftver telepítésében?**
- **Biztos, hogy az, akinek mondja magát?**
- **Biztos vagy benne, hogy az alkalmazás biztonságos?**

A csalók az AnyDesk-en keresztül támadnak!!!

A csalók a szoftveren keresztül átveszik az irányítást a számítógéped felett, ellopják az adataidat, jelszavaidat, elveszik a pénzedet, a nevedben használják az internetet! Mindig ellenőrizd, kivel beszélsz! Ne dőlj be!

Ne kockáztass!

GONDOLKODJ!!!

NE LÉGY BALEK!!

Vigyázz a befektetésekkel!!!

- **Biztonságosnak gondolsz egy reklámban talált külföldi befektetési oldalt?**
- **Biztos lehetsz a holtbiztosnak feltüntetett hozamban?**
- **Biztosan kockáztatni akarod hosszú évek munkájával gyűjtött megtakarításodat?**

A kezdeti kis nyereségek után „elolvad” a befektetésed és nem tudod visszaszerezni! Legálisnak tűnő befektetési oldalakon a végeredmény a biztos veszteség!

Ne kockáztass!

GONDOLKODJ!!!

NE LÉGY BALEK!!

Online is vásárolj körültekintően!!!

- **Túl olcsónak tűnik? Nem gyanús?**
- **Előre átutalnád a vételárat? Jó ötlet ez?**
- **Tájékozódtál az eladóról? Kerestél visszajelzéseket korábbi vevőktől?**

Még akkor is megkárosíthatnak, ha <u>UTÁNVÉTTEL</u> vásárolsz! Mielőbb ellenőrizd a küldeményt, és <u>AZONNAL</u> jelezd a futárszolgálatnak a csalást, de inkább előre

GONDOLKODJ!!!

VIGYÁZZON ADATAIRA!

FELADÓ ELLENŐRZÉSE

Mindig ellenőrizze, hogy valóban a feladónak tűnő személy, szervezet küldte az e-mailt! Pl: az e-mail cím @ utáni része helyesen tartalmazza a cégnevet.

BANKKÁRTYAADATOK

A bankok nem kérnek e-mailben bankkártya adatokat, más szervezeteknek, személyeknek pedig ne adja meg azokat! A kártyaadatok birtokában visszaélhetnek bankkártyájával!

FIZETÉS ONLINE

Online történő bankkártyás fizetésnél mindig győződjön meg arról, hogy valódi banki oldalon adja meg az adatokat, más oldalon (pl. kereskedő oldalán) ne adja meg azokat!

HTTPS ELLENŐRZÉSE

Amikor belép egy banki vagy bármilyen más oldalra, ellenőrizze, hogy valóban ahhoz a szervezethez tartozik! Felhasználói nevet és jelszót csak tanúsítvánnyal rendelkező (https előtaggal rendelkező) oldalon adjon meg!

KÉPET SE!

Idegennek ne adjon meg semilyen személyes adatot. Ne küldjön képet igazolványairól, bankkártyájáról vagy képernyőmentést monitorjáról, telefonjáról!

FIGYELMEZTESSE CSALÁDJÁT!

Adja tovább a tanácsokat családtagjainak! Figyelmeztesse gyermekét, hogy ő se adjon meg sem magáról, sem családtagjairól semmilyen információt! Ha ilyet kérnek tőle, azonnal szóljon Önnek!

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság