A 7 leggyakoribb online pénzügyi csalás és az elkerülésük módja

A kiberbűnözők folyamatosan keresik a módját annak, hogy pénzt kereshessenek a megkárosításunkkal. Ezekben az esetekben az információkat egy adott személytől csalják ki, és nem a rendszereket törik fel.

Általános tippek:

- Ellenőrizze rendszeresen az online fiókjait.
- Ellenőrizze rendszeresen a bankszámláját, és a gyanús tevékenységekről tegyen bejelentést a bankjának.
- Az interneten csak biztonságos webhelyeken fizessen (ellenőrizze, hogy a webhely címének beírására szolgáló mezőben látható-e a lakat, illetve figyeljen arra, hogy a cím eleje http**s** legyen), és csak biztonságos kapcsolatot használjon (nyilvános Wi-Fi helyett használja a mobilinternetet).
- A bankja soha nem kérdez olyan bizalmas információkat telefonon vagy e-mailben, mint az online fiókja hitelesítő adatai.
- Ha egy ajánlat túl jónak tűnik ahhoz, hogy igaz legyen, szinte minden esetben csalás.
- Mindig ügyeljen a személyes adatai biztonságára, valamint a biztonságos tárolásukra.
- Gondolja át nagyon alaposan, hogy mennyi személyes információt oszt meg a közösségimédia-oldalakon. A csalók az adatai és fényképei felhasználásával hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.
- Ha megadta a fiókja adatait egy csalónak, azonnal vegye fel a kapcsolatot a bankjával.
- Ha megpróbálták megkárosítani, minden esetben tegyen bejelentést a rendőrségen, még akkor is, ha nem vált a csalási kísérlet áldozatává.

Az alábbi csalások tipikus példák arra, hogy a kibertámadók milyen módon tudják egyszerűen kihasználni az embereket. A következő tippek ahhoz nyújtanak segítséget, hogyan védekezzünk a támadások ellen.

1. Az ügyvezetőnek adják ki magukat

Az ügyvezető/üzleti e-mailes csalás esetében egy kifizetési jogkörrel rendelkező alkalmazottat vesznek rá arra, hogy kifizessen egy hamis számlát, vagy jóvá nem hagyott átutalást indítson az üzleti bankszámláról.

Hogy működik?

Ez a módszer arra épít, hogy az alkalmazottak általában igyekeznek gyorsan teljesíteni azokat a feladatokat, amelyek közvetlenül a felső vezetéstől érkeznek. Általában úgy tűnik, hogy a csalók részletes információkkal rendelkeznek a szervezetről, és az e-mail rendkívül meggyőzőnek látszik.

Melyek a figyelmeztető jelek?

- Közvetlen megkeresés egy felsővezetőtől kéretlen e-mail, vagy telefonhívás formájában.
- A kérés bizalmas jellegének hangsúlyozása.
- Nyomásgyakorlás, sürgetés.
- Szokatlan, a belső előírásoknak ellentmondó kérés.
- Fenyegetések, szokatlan szívélyesség és/vagy jutalom kilátásba helyezése.

Mit tehetünk?

CÉGKÉNT:

- Legyen tisztában a kockázatokkal, és gondoskodjon arról, hogy az alkalmazottak megkapják a megfelelő tájékoztatást, és ők is tisztában legyenek a veszéllyel.
- Figyelmeztesse a munkavállalókat arra, hogy körültekintően kezeljék a kifizetési kérelmeket.
- Vezessen be belső protokollokat a kifizetésekre.
- Vezessen be egy eljárást, amelyik ellenőrzi az e-mailben érkezett kifizetési kérelmek valódiságát.
- Vezessen be jelentési rutinokat a csalás kezelésére.
- Vizsgálja felül a cég webhelyén közzétett adatokat, korlátozza az információkat, és kezelje óvatosan a közösségi médiát.
- Frissítse és korszerűsítse a biztonsággal kapcsolatos műszaki megoldásokat.
- Minden esetben tegyen bejelentést a rendőrségen a csalási kísérletekről, még akkor is, ha nem vált áldozattá.

ALKALMAZOTTKÉNT:

- Tartsa be szigorúan a kifizetésekre és beszerzésre vonatkozó biztonsági eljárásokat. Ne hagyjon ki eljárási lépéseket, és ne engedjen a nyomásgyakorlásnak.
- A bizalmas információk/pénzátutalások esetében mindig gondosan ellenőrizze az e-mail-címeket. A csalók gyakran használnak nagyon hasonló e-mail-címeket, amelyek csak egy karakterben térnek el az eredetitől.
- Amennyiben kétségei vannak egy átutalási utasítással kapcsolatban, mindig kérdezzen meg egy kompetens munkatársat, még akkor is, ha a feladat diszkrét kezelésére kérték.
- Soha ne nyisson meg e-mailben kapott gyanús hivatkozásokat vagy mellékleteket. Különös körültekintéssel járjon el, ha a vállalati számítógépeken nyitja meg személyes e-mail-postafiókját.
- Korlátozottan terjessze az információkat, és kezelje óvatosan a közösségi médiát.
- Ne osszon meg a vállalati hierarchiára, biztonságra és eljárásokra vonatkozó információkat.
- Ha gyanús e-mailt vagy telefonhívást kap, minden esetben értesítse az IT osztályt.

2. A csalók ügyfélnek/beszállítónak adják ki magukat

Hogy működik?

A vállalatot megkeresi valaki, aki egy ügyfél, beszállító vagy hitelező képviselőjeként azonosítja magát. A megkeresés érkezhet telefonon, levélben, faxon vagy e-mailben. A csaló azt kéri, hogy valamelyik partner jövőbeli számláinál módosítsák valamelyik banki adatot (például a kedvezményezett bankszámlaszámát). Az így megadott bankszámla felett a csaló rendelkezik.

Mit tehetünk?

CÉGKÉNT:

- Gondoskodjon arról, hogy az alkalmazottak ismerjék ezt a csalástípust, és azt is, hogy hogyan lehet védekezni ellene.
- Vezessen be egy eljárást, amelyik ellenőrzi a kifizetési kérelmek valódiságát.
- Adja utasításba a számlák kifizetéséért felelős munkatársak számára, hogy mindig vessék össze a rendszerben levő adatokat a számla adataival.
- Vizsgálja felül a vállalat webhelyén közzétett adatokat, különös tekintettel a szerződésekre és a beszállítókra. Kifejezetten javasolt, hogy a munkatársak korlátozzák azokat az információkat, amelyeket személyes közösségimédia-fiókjaiban osztanak meg a vállalatról és a munkahelyükről.

- Minden esetben tegyen bejelentést a rendőrségen a csalási kísérletekről, még akkor is, ha nem vált áldozattá.

ALKALMAZOTTKÉNT:

- Ellenőrizzen minden, állítólagosan a hitelezőktől érkező kérelmet, főleg akkor, ha azt kérik, hogy a jövőbeli számláknál módosítsák valamelyik banki adatot.
- Ne használja a módosítást vagy ellenőrzést kérő levélben/faxon/e-mailben szereplő kapcsolattartási adatokat. Keressen egy korábbi üzenetet, és annak a kapcsolattartási adatait használja.
- Azoknak a vállalatoknak az esetében, amelyek számára rendszeresen indít kifizetéseket, jelöljön ki egy megbízott kapcsolattartót.
- Adott összeghatár feletti kifizetések esetében vezessen be egy rendszert, amelynek kifejezetten a helyes bankszámlaszám és kedvezményezett ellenőrzése a célja (például megbeszélés az érintett vállalattal).
- A számla kifizetésekor küldjön e-mailes tájékoztatást a kedvezményezettnek. A biztonság szavatolása érdekében szerepeltesse a fogadó bank nevét és a bankszámlaszám utolsó négy számjegyét.
- Korlátozza azokat az adatokat, amelyeket megoszt az alkalmazottakról a közösségi médiában.
- A csalási kísérleteket jelentse a vezetőségnek vagy a megfelelő osztálynak.

3. Felhívják, szöveges üzenetet vagy e-mailt küldenek

A banki ügyfeleket célzó, pszichológiai manipulációra építő támadások leggyakoribb formái a phishing (adathalászat e-mail használatával), a smishing (adathalászat SMS használatával) és a vishing (adathalászat hanghívással).

Banki phishing e-mailek

A phishing olyan csaló szándékú e-mailt jelent, amely személyes, pénzügyi vagy biztonsági információi megosztására veszi rá a címzettjét.

Hogy működik?

Ezek az e-mailek:

- Azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a bankok küldenek: lemásolják a valódi e-mailek logóit, kinézetet és stílusát.
- Sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha nem válaszol.
- Arra is megkérhetnek, hogy töltsünk le egy mellékletet vagy kattintsunk egy hivatkozásra.

A bűnözők arra építenek, hogy az emberek elfoglaltak: futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik a leírtak szerint.

Mit tehetünk?

- Mindig tartsuk naprakész állapotban a szoftvert, beleértve a böngészőt, a vírusellenes programokat és az operációs rendszert.
- Legyünk különösen éberek, ha egy „banki” e-mail bizalmas információkat kér (például az online banki jelszavunkat). A bankok kizárólag biztonságos módon, az online banki felületen kommunikálnak az ügyfelekkel.

- Vizsgáljuk meg alaposan az e-mailt. Keresünk következetlenségeket és értelmetlennek tűnő dolgokat:
  - Keresünk nehezen észrevehető különbségeket a feladó címében: a nulla például „o”-nak tűnhet.
  - Vigyük az egérmutatót a küldő címére, és vizsgáljuk meg alaposan: amennyiben lehetséges, vessük össze a küldő e-mail-címét a banktól érkezett korábbi üzenetekével.
  - Ellenőrizzük, hogy vannak-e elgépelések és nyelvtani hibák.
- A gyanús e-mailekre ne válaszoljunk, hanem továbbítsuk a bankunknak úgy, hogy saját kezűleg gépeljük be a címet.
- Ne kattintsunk a hivatkozásokra, és ne töltsük le a mellékleteket; ehelyett gépeljük be a címet a böngészőbe.
- Mobileszközök használatakor legyünk különösen körültekintőek. Telefonon vagy táblagépen nehezebb lehet észrevenni a phishing kísérleteket. Nem lehet a gyanús hivatkozások fölé vinni az egérmutatót, és a kisebb kijelző miatt a nyilvánvaló hibákat is nehezebb észrevenni. A csaló e-maileket jelentsük a bankunknak: minden vállalat szívesen veszi az ilyen típusú támadásokról szóló információkat. Ha kétségei vannak, hívja fel a bankját.

Banki vishing hívások

A vishing (az angol „voice” és „phishing”, vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynek az esetében a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására, vagy pénz átutalására rávenni az áldozatot.

Mit tehetünk?

- Kezeljük óvatosan a kéretlen telefonhívásokat.
- Jegyezzük fel a hívó telefonszámát, és mondjuk meg neki, hogy visszahívjuk.
- Annak az ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keressük meg a szervezet telefonszámát (a weboldalukon vagy online kereséssel), és keressük meg őket közvetlenül.
- Az ellenőrzéshez ne használjuk a hívó által megadott telefonszámot (a szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták).
- A csalók az interneten könnyen megszerezhetik az alapvető információkat rólunk vagy a vállalatunkról (például a közösségimédia-profilok felhasználásával). Nem bízhatunk meg a hívóban csak azért, mert ismeri ezeket az adatokat.
- Soha ne adjuk meg a betéti vagy hitelkártyánk PIN-kódját, vagy az online banki jelszavakat. A bankok sosem kérik el ezeket az információkat.
- Soha ne utaljunk pénzt egy számlára, telefonon érkező kérése. Egy bank sosem kér ilyet.
- A csalási szándékú hívásokat jelentsük a bankunknak.

Banki smishing SMS-ek

A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynek az esetében a támadó SMS segítségével próbálja megszerezni személyes, pénzügyi vagy biztonsági információinkat. Megbízható forrásnak álcázzák magukat, úgy tesznek, mintha egy bank, kártyakibocsájtó vagy közműszolgáltató/egyéb szolgáltató képviseletében jelentkeznének.

Hogy működik?

Az üzenet az esetek nagy részében arra kéri a címzettet (általában sürgető módon), hogy nyisson meg egy weboldalra vezető hivatkozást vagy hívjon fel egy telefonszámot a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás egy csaló weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja

ki magát. A cél olyan információk megszerzése, amelyeknek a segítségével aztán ellophatják a pénzünket.

Mit tehetünk?

- A küldő személyazonosságának ellenőrzése nélkül ne kattintsunk kéretlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre. Az ellenőrzéshez keressünk rá a számra az interneten (ha csalásról van szó, valószínűleg nem mi leszünk az elsők), vagy hasonlítsuk össze a számot az érintett szervezet hivatalos telefonszámával.
- Ne hagyjuk, hogy siettessenek. Végezzük el a megfelelő ellenőrzést, bármennyi időbe is kerüljön.
- Soha ne válaszoljon olyan SMS-re, amelyik a PIN-kódját, az online banki jelszavát vagy bármilyen más biztonsági azonosító adatát kéri.
- Ha azt gyanítja, hogy válaszolt egy smishing szöveges üzenetre és megadta a banki adatait, azonnal vegye fel a kapcsolatot a bankjával.

4. Meghamisított banki oldalakat készítenek

A banki phishing e-mailekben található hivatkozások általában egy meghamisított banki weboldalra vezetnek, ahol a célszemélyt a pénzügyi és személyes adatai megadására kérik.

Mik a jelek?

A meghamisított banki webhelyek szinte teljesen ugyanolyanok, mint a mintának használt valódi oldal. Általában tartalmaznak egy felugró ablakot, amelyik a banki hitelesítő adatok megadását kéri. A valódi bankok nem használnak ilyen ablakokat.

A hamis banki webhelyeket általában a következők jellemzik:

- Sürgetés: a valódi webhelyeken nem találhatók ilyen üzenetek.
- Gyenge minőségű design: legyünk óvatosak az olyan webhelyekkel, amelyek tervezési hibákat, vagy nyelvtani és helyesírási hibákat tartalmaznak.
- Felugró ablakok: rendszerint bizalmas információk megszerzésére használják őket. Ne kattintson rájuk, és ne adjon meg személyes adatokat az ilyen ablakokban.

Mit tehetünk?

- A bank webhelyét soha ne nyissuk meg e-mailben található hivatkozásra kattintva.
- A hivatkozást mindig gépeljük be, vagy használjuk a „Kedvencek” közé elmentett hivatkozást.
- Használjunk olyan böngészőt, amelyik lehetővé teszi a felugró ablakok blokkolását.
- Amennyiben a bank fel szeretné hívni a figyelmünket valamilyen fontos dologra, az online banki felületen jeleníti meg a figyelmeztetést.
- Ha kétségei vannak, hívja fel a bankját.

5. Úgy tesznek, mintha romantikus kapcsolatot keresnének a kiszemelt áldozattal

A romantikus kapcsolattal operáló csalások tipikus helyszínét az online társkereső oldalak jelentik, de a csalók gyakran használják a közösségi médiát vagy az e-mailt a kapcsolatfelvétel eszközeként.

Mik a jelek?

- Valaki, akit a közelmúltban ismertünk meg az interneten, erős érzelmeket mutat irántunk, és chatelni szeretne.
- Az illető üzenetei gyakran tele vannak helyesírási hibákkal és elnagyoltak.
- Az online profilja nincs összhangban azzal, amit mond.
- Előfordulhat, hogy intim képek vagy videók küldését kéri.
- A csalók türelmesen várnak arra, hogy megszerezzék a bizalmunkat: akár heteket vagy hónapokat is. Ezután jön az a fázis, amikor valamilyen jól kidolgozott mesével pénzt, ajándékokat vagy a bankszámlánk/hitelkártyánk adatait kérik.
- Ha nem kapnak pénzt, előfordulhat, hogy megpróbálnak megzsarolni. Ha megkapják a kért összeget, újra és újra pénzt kérnek.
- Mindig lesz valamilyen kifogásuk arra, hogy miért nem működik a webkamera, miért nem tudnak elutazni, hogy találkozzanak az áldozattal, és hogy miért van mindig szükségük pénzre.

Mit tehetünk?

- Gondoljuk át nagyon alaposan, hogy mennyi személyes információt oszt meg a közösségimédia- és a társkereső oldalakon.
- Mindig legyünk tisztában a kockázattal. A csalók a legjobb hírű oldalakon is ott vannak.
- Ne siessünk el semmit, és tegyünk fel kérdéseket.
- Keressünk rá az illető fényképére és profiljára online keresőeszközökkel hogy kiderüljön, nem máshonnan használták-e fel őket.
- Kezdjünk el gyanakodni, ha sok helyesírási és nyelvtani hibával találkozunk, ha az illető története tele van logikai ellentmondásokkal, és ha soha nem működik a kamerája.
- Ne osszunk meg személyes képeket, videókat vagy olyan kompromittáló anyagokat, amelyekkel később megzsarolhatnak.
- Ha személyes találkozóra indul, mondja el a családtagjainak és a barátainak, hogy hová megy.
- Legyünk óvatosak, ha valaki pénzt akar kérni. Soha ne küldjünk pénzt, ne adjuk ki a hitelkártyánk vagy az online banki hozzáférésünk adatait, illetve senkinek se küldjük el a fontos személyazonosító okmányaink másolatát.
- Szakítsuk meg a kapcsolatot az olyan idegenekkel, akik előre fizetést kérnek pénzutalvány, banki átutalás, nemzetközi átutalás, előre feltöltött kártyák vagy kriptovaluta formájában. Az ilyen módon küldött pénzt szinte lehetetlen visszaszerezni.
- Senkinek se küldjön pénzt: a pénzmosás bűncselekmény.

Ha romantikus kapcsolattal operáló csalás áldozata lett:

- Ne érezze úgy, hogy szégyellnie kell magát: kevesen tudják, mennyire gyakori ez a csalás.
- Azonnal szakítson meg minden kapcsolatot.
- Ha lehetséges, őrizze meg minden információcsere adatait (például a csevegőüzeneteket), illetve bármilyen bizonyítékot, amely segíthet azonosítani a csalót.
- Tegyen rendőrségi feljelentést.

- Tegyen bejelentést azon a webhelyen, ahol a csalók először felvették önnel a kapcsolatot. Küldje el a csaló profilnevét és minden egyéb adatot, amely segíthet annak a megakadályozásában, hogy mások is áldozattá váljanak.
- Ha megadta a számlaadatait egy csalónak, azonnal vegye fel a kapcsolatot a bankjával vagy pénzintézetével.

6. Ellopják a személyes adatait a közösségi médián keresztül

A személyes adatok értékesek a bűnözők számára. A védekezés a csalók ellen egyben azt is jelenti, hogy ügyelünk személyes adataink biztonságára, valamint biztonságos tárolására.

Hogy működik?

Még ha nem is teszi mindenki által megtekinthetővé az ember a közösségi médiában és megfelelő védelmet alkalmaz, vagy ha óvatosságból nem oszt meg túl sok információt a profiljában (képek, videók, állapotfrissítések stb.), a csalók különböző módszerek alkalmazásával el tudják érni, hogy beírjuk a személyes adatainkat (név, e-mail-cím, jelszó, hitelkártyaszám stb.): olyan információkat, amelyekkel ellophatják a személyazonosságunkat.

A személyes adatok birtokában a csalók a következőket tehetik:

- Jóvá nem hagyott vásárlásokat hajthatnak végre a hitelkártyánkkal, bankszámlát nyithatnak vagy telefon-előfizetést vásárolhatnak.
- Hitelt vehetnek fel.
- Eladhatják a személyes adatokat más csalóknak.
- Illegális üzleti tranzakciókat hajthatnak végre az áldozat személyes adataival.

A támadások általában tipikus mintázatokat követnek, íme néhány klasszikus példa:

- **Twishing** (a „Twitter” és az angol „phishing” szavak kombinációja, vagyis Twitteres adathalászat): üzenet küldése egy Twitter-felhasználónak, arra kérve, hogy látogasson el egy webhelyre. Amikor a felhasználó bejelentkezik a csaló webhelyre, a támadó megszerzi a fiókinformációit (név és jelszó).

- **Ki nézte meg a profilomat, vagy a közösségimédia-oldalamat?** Az ide tartozó szolgáltatások hozzáférési engedélyt kérnek a profilunkhoz. Ezután megnyílik egy csaló felmérés, amelyben meg kell adnunk a személyes adatainkat. A csaló minden egyes alkalommal jutalékot kap, amikor valaki kitölti a felmérést. Soha nem fog kiderülni, hogy ki nézte meg a profilját.
- **„Ezen a videón te szerepelsz?”** Az ilyen videókra kattintva végül mindig egy felmérés jelenik meg, amelynek a kitöltése után a csaló jutalékot kap. Ráadásul a készülékünk rosszindulatú programokkal is megfertőződhet.
- **„A fiókját zároltuk”, „igazolja e-mail-fiókját”.** Ezeknek a csalásoknak az a célja, hogy megszerezzék a személyes információit, és a fiókja hozzáférési adatait.
- **Csalás ajándékkártyákkal, illetve hamis ajánlatok népszerű, ismert üzletektől vagy értékes márkáktól.** Ezek a csalások arra próbálják meg rávenni a felhasználót, hogy adja meg személyes adatait, vagy regisztráljon drága szolgáltatásokra. Minden hónapban új formában jelennek meg, és az ajánlat túl szép ahhoz, hogy igaz legyen – a kért termék vagy szolgáltatás soha nem érkezik meg.
- **Csodatevő termék, ingyenes kipróbálás!** Ez az online csalási módszer ingyenes kipróbálást ígér, hogy aztán trükkös módszerrel kérjen beleegyezést

vagy felmérésekkel érje el, hogy úgy regisztráljunk termékekre vagy előfizetésekre, hogy észre sem vesszük (például rendszeres, kötelező szállítási költség).

- **„Keressen rengeteg pénzt otthonról dolgozva”.** Ha egy munka elkezdéséhez előre fizetendő regisztrációs díjat kérnek, valószínűleg csalásról van szó. Az ilyen hirdetések a közösségimédia-oldalakon bukkannak fel: az ajánlat szerint egy kezdőkészlet megvásárlása után több ezer eurót kereshetünk. Rengeteg személyes adatot kérhetnek el, például az adószámunkat, vagy az útlevelünk és a jogosítványunk fénymásolatát. A munkaajánlatok egy része pénzmosáshoz kötődik: ilyenkor pénzt utalnak a számlánkra, és az összeget némi jutalék levonása után tovább kell utalnunk egy külföldi cégnek. Az áldozat ilyenkor gyakorlatilag orgazdaként működik, és bűncselekményt követ el.

- **Segítség bajban vagyok!** A csaló úgy tesz, mintha a rokonunk lenne, és a közösségi médiában azt üzeni, hogy sürgősen pénzre van szüksége. A csaló azt mondja, komoly bajban van, és arra kér, hogy utaljunk át neki pénzt. A megkeresés érkezhet telefonon, e-mailben vagy SMS-ben is.

Mit tehetünk?

- Ha ellenőrizni akarja egy közösségimédia-oldalról származó információk igazságtartalmát, mindig írja be az adott oldal címét, és ne bízzon meg azokban a hivatkozásokban, amelyek azt állítják, hogy oda viszik.
- Gondolja át alaposan, hogy mennyi információt és fényképet oszt meg a közösségimédia-oldalakon. A csalók a felhasználásukkal hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.
- Tekintse át a közösségimédia-fiókjai adatvédelmi és biztonsági beállításait. Áldozzon némi időt annak a pontos megismerésére, hogy mit mutat a profilja önről a külvilágnak.
- Végezzen online kutatást. Keressen rá az adott termék nevére vagy a munkaajánlatra, és nézze meg, hogy mit mondanak a többiek. A keresőkifejezésben használjon olyan szavakat, mint a „felülvizsgálat”, a „panasz” és a „csalás”.
- Jelentse a közösségimédia-platform üzemeltetőinek azokat a profilokat, amelyekről azt gyanítja, hogy csaláshoz hozták létre őket. Ha az ismerősei vagy a követői, tiltsa le őket, és szakítson meg minden kapcsolatot.
- Ellenőrizze rendszeresen a hitelkártyája és a betéti kártyája kivonatait. Ha olyan dologért terhelték meg a számláját, amelyet nem ön rendelt meg, vegye fel a kapcsolatot a bankkal és a kártyatársasággal.

7. Elhitetik, hogy okos befektetési lehetőséget találtunk...

A befektetésekkel kapcsolatos legelterjedtebb csalásoknál olyan területeken kínálnak vonzó befektetési lehetőségeket, mint például a részvények, a kötvények, a kriptovaluták, a ritka fémek, a tengerentúli ingatlanok vagy az alternatív energia.

Mik a jelek?

- Folyamatosan kapja a kéretlen telefonhívásokat.
- Gyors megtérülést ígérnek, és biztosítják arról, hogy a befektetés biztonságos.
- Az ajánlat csak korlátozott ideig él.
- Az ajánlat csak önnek érhető el, és megkérik, hogy senkinek se szóljon róla.

Mit tehetünk?

- Pénz átadása vagy befektetése előtt mindig kérjen pénzügyi tanácsot egy pártatlan féltől.
- Utasítsa el a befektetési lehetőségekkel kapcsolatos kéretlen telefonhívásokat.
- Kezelje gyanakvással a biztonságos befektetést, garantált megtérülést és nagy profitot ígérő ajánlatokat.
- Óvakodjon a jövőbeli csalásoktól. Ha egyszer már egy befektetési csalás áldozatává vált, a csalók valószínűleg újra megkeresik, vagy eladják az adatait más bűnözőknek.
- Ha gyanakszik, értesítse a rendőrséget.

...vagy nagyszerű online ajánlattal keresnek meg!

A fogyasztók és a vállalkozások egyre többet vásárolnak és adnak el az interneten. Az online ajánlatok sokszor valóban kedvezők, de óvakodjon a csalóktól.

Mit tehetünk?

- Ha lehet, belföldi kiskereskedelmi webhelyeken vásároljon – így nagyobb valószínűséggel oldhatja meg az esetleges problémákat.
- Nézzen utána a dolgoknak – olvasson értékeléseket, ismertetőket az adott termékről a vásárlás előtt.
- Használjon hitelkártyát – így nagyobb eséllyel kaphatja vissza a pénzét.
- Kizárólag biztonságos fizetési szolgáltatásokkal fizessen. Pénzküldési szolgáltatás vagy a banki átutalást használatát kérik? Jól fontolja meg!
- Csak biztonságos internetkapcsolat használatakor fizessen – ne használjon ingyenes vagy nyilvános Wi-Fi-hálózatokat.
- Csak biztonságos készülékről fizessen. Gondoskodjon az operációs rendszer és a biztonsági szoftverek folyamatos frissítéséről.
- Óvakodjon a hihetetlenül jó ajánlatokat kínáló reklámoktól vagy a csodát ígérő termékektől. Ha túl szépnek tűnik ahhoz, hogy igaz legyen, valószínűleg az is!
- Felugró ablak, amelyik közli, hogy megnyert valamilyen díjat? Gondolja meg kétszer: lehet, hogy a nyeremény valamilyen rosszindulatú program lesz.
- Ha nem érkezik meg a termék, vegye fel a kapcsolatot az eladóval. Ha nem válaszol, vegye fel a kapcsolatot bankjával.
- Ha azt gyanítja, hogy megpróbálták megkárosítani, minden esetben tegyen bejelentést a rendőrségen, még akkor is, ha nem vált a csalási kísérlet áldozatává.

A biztonságos online vásárlásról ide kattintva találhat további információkat.