

A CSALÓK GYAKRAN HIVATALOS MEGKERESÉSNEK ÁLCÁZVA PRÓBÁLJÁK MEGSZEREZNI A BANKI JELSZAVAINKA ÉS KÁRTYAADATAINKAT.

1. A “NIGÉRIAI” CSALÁS

A „nigériai típusú” csalás a megtévesztés egyik legrégebbi, 19. század végén elterjedt formája.

A hamis levelekben, megkeresésekben jellemzően segítséget kérnek az elkövetők: menekültek vagyonának visszaszerzéséhez, jogtalanul elvett örökség, valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez stb.

Közösségimédia-oldalakon, online társskereső portálokon terjed a nigériai csalás azon változata, melynél az elkövető romantikus kapcsolatot épít fel leendő áldozatával, mielőtt valamilyen megható történettel pénzt kér tőle.

A megtévesztő történetet valódinak látszó, de hamis közösségimédia-profillal és eredetinek tűnő, de szintén fiktív iratokkal igyekeznek alátámasztani.

Annak érdekében, hogy a történet hihetőbb legyen, előfordulhat, hogy a csalók nemzetközi átutalást kezdeményeznek, amit aztán visszavonnak, így mutatva, hogy az összeg valójában rendelkezésre áll, csak a levélben jelzett adminisztratív nehézség áll a kifizetés útjában.

A levélben kért segítség kizárólag egy bizonyos pénzösszeg átutalását jelenti.

Mindezért későbbi busás jutalmat ígérnek, amit azonban a károsultak végül nem kapnak meg, de a befizetett összeget elveszítik.

Az is egy bevett forma, hogy a vagyon kimenekítéséhez a címzettnek meg kell adnia a bankszámlaadatát, aminek az eredménye természetesen nem az, hogy pénzösszeg érkezik rá, ellenkezőleg: az elkövetők immár hozzáférnek a bankszámlához, így akár le is nullázhatják azt.

Mit tegyen, hogy megelőzze a bajt?

- Semmilyen körülmények között ne adjon meg bizalmas információkat, banki adatokat vagy azonosítókat e-mailben érkező felkérésre!
 - Ne kezdeményezzen fizetést levélben kapott felszólításra!
 - Kéretlen levél esetén figyelje a nyelvezetet: a nigériai levelekre jellemző a pongyola megfogalmazás, a számtalan nyelvtani és stilisztikai hiba. Ám sok esetben épp ez támasztja alá a történetet: a „tört magyarság”, a megtévesztő történetben szereplő külföldi levélíró kísérlete, hogy magyarul próbáljon meg segítséget kérni. Ha ilyen levelet kap, legyen megfontolt és gyanakvó!
 - Ne legyen hiszékeny: ne higgyen e-mailben érkező, már-már romantikus történeteknek!
 - Nem reális, hogy ismeretlenek a könnyű meggazdagodás lehetőségét ajánlják fel másoknak.
- Ha ilyen tartalmú levelet kap, gyanakodjon!**

2. PHISHING: ADATHALÁSZ BANKI E-MAILEK

Phishing:

egy gyűjtőfogalom a csalárd adatszerzésekre (főként az e-mailes és hamis weboldalas megoldásokra utal, de ide érthető minden fajta adatszerzés).

Banki ügyfeleket célzó, csaló szándékú adathalász e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására veszi rá a címzettet. Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a bankok valójában küldeni szoktak: tartalmazzák a valódi e-mailek hivatalos céglogóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is.

Általában sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha a címzett nem válaszol, de arra is kérhetik, hogy töltsön le egy mellékletet, vagy kattintson egy hivatkozásra. A kiberbűnözők arra építenek, hogy az emberek elfoglaltak és felületes áttekintésre, futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik a leírtak szerint.

Mit tehet?

- Legyen különösen éber, ha egy „banki” e-mail bizalmas információkat kér, például az online banki jelszavát! A bankok kizárólag biztonságos módon, az online banki felületen kommunikálnak az ügyfelekkel, sosem kérnek bizalmas adatokat ilyen formában!
- Ne kattintson az üzenetben lévő hivatkozásokra, és ne nyissa meg a mellékleteket, a webes bejelentkezések címeit inkább manuálisan gépelje be, vagy használja a hivatalos banki oldalt!
- Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvételekkel szemben, amikor nem tud minden kétséget kizáróan megbizonyosodni a másik fél identitásáról! Különösen igaz ez az elektronikus kommunikációra: ne válaszoljon a gyanús e-mailekre!
- Vizsgálja meg alaposan az e-mailt! Keressen következetlenségeket és értelmetlennek tűnő dolgokat, például furcsa nyelvezet, helyesírási hibák, sürgető hangnem, szokatlan formátumú csatolmány (.zip stb.).

- **Keressen nehezen észrevehető különbségeket a feladó címében: a nulla például „o” betűnek tűnhet! Vesse össze a küldő e-mail címét a bank korábbi üzeneteivel!**
- **Legyen különösen körültekintő a mobileszközök használatakor! Telefonon vagy táblagépen nehezebb lehet észrevenni az adathalász kísérleteket.**
- **Nem lehet a gyanús hivatkozások fölé vinni az egérmutatót, és a kisebb kijelző miatt a nyilvánvaló hibákat is nehezebb észrevenni.**
- **A gyanús e-maileket jelentse bankjának: minden vállalat szívesen veszi az ilyen típusú támadásokról szóló információkat. Ha kétségei vannak, hívja fel a bankját!**
- **Mindig tartsa naprakész állapotban szoftvereit, beleértve a böngészőt, a vírusirtó programokat és az operációs rendszert!**

A phishing ismert fajtái:

- Email phishing:** hivatalosnak tűnő e-mail, amelynek célja, hogy rávegye a címzettet pl. a jelszómódosításra, vagy egy olyan webhelyre átnavigálásra, amelyen megszerezhetik a személyes vagy banki adatait.
- HTTPS phishing:** hasonló email phishing-hez. Ebben az esetben is hivatalosnak tűnő e-mailek küldenek az áldozatnak, melyben egy konkrét hamis webhelyre mutató hivatkozás található.
- Website spoofing:** a fentiekhez kapcsolódik. Ebben az esetben egy, a hivatalos/valid weboldalra megtévesztésig hasonlító hamis weboldalt hoznak létre a csalók (erre van egy másik forma is, az a domain spoofing, ahol egy ismert vállalat domain nevét utánozzák).

3. VISHING: HAMIS BANKI HÍVÁSOK

Vishing: csalárd telefonhívások, amelyek érzékeny (személyes, banki, stb) adatok megszerzését célozzák.

A vishing (az angol „voice” és „phishing”, vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására, vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek.

Tipikus formája a vishingnek, 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.

Mit tegyen hamis banki hívás esetén?

- Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!
- Minél sürgetőbb a hívás és az üzenet, 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!
- Ha a kijelzett telefonszám valóban a bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik.
- Annak az ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát (a weboldalukon vagy online kereséssel), és lépjen velük kapcsolatba közvetlenül!
- Ne használja az ellenőrzéshez a hívó által megadott telefonszámot!
- A szám hamis lehet, vagy kifejezetten a csaláshoz hozhatták létre.

- **A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatáról, amelynek dolgozik, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.**
- **Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV kódját, vagy az online banki jelszavát! A bankok/banki ügyintézők sosem kérik el ezeket az információkat!**
- **Soha ne telepítsen mások kérésére olyan programot számítógépére vagy telefonjára, amit nem ismer!**
- **Soha ne utaljon pénzt telefonon érkező kérésre! Egy bank sosem kér ilyet.**
- **A csalási szándékú hívásokat jelentse a bankjának!**

4. SMISHING: HAMIS BANKI SMS-EK

Smishing: csalárd szöveges (főként SMS) üzenetek, amelyek célja személyes, érzékeny adatok megszerzése. Sokszor egy beágyazott link van az üzenetben (pl. csomagod érkezett).

A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadó SMS segítségével próbál megszerezni személyes, pénzügyi vagy biztonsági információkat. A küldő megbízható forrásnak álcázza magát, úgy tesz, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviselőjeként jelentkezne.

Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot 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.

Célja olyan információk megszerzése, amelyek segítségével aztán ellophatják az áldozat pénzét.

Mit tegyen, ha hamis banki SMS-t kapott?

- Ne kattintson kéretlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre a küldő személyazonosságának ellenőrzése nélkül! Az ellenőrzéshez keressen rá a számra az interneten (ha csalásról van szó, valószínűleg nem Ön lesz az első), vagy hasonlítsa össze a számot az érintett szervezet hivatalos telefonszámával!
- Ne hagyja, hogy siettessék! Végezze el a megfelelő ellenőrzést, bármennyi időbe is kerüljön!
- Ha ismerős számról érkezik az SMS, az sem garancia arra, hogy megbízható. Lehetséges, hogy egy ismerőse már áldozatul esett a csalóknak, így fel tudják használni az ő telefonszámát és adatait.
- Soha ne válaszoljon olyan SMS-re, amely a PIN-kódját, az online banki jelszavát vagy bármilyen más biztonsági azonosító adatát kéri!
- Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy egy smishing üzenetre válaszolt és megadta banki adatait!

5. MEGHAMISÍTOTT BANKI OLDALAK

Az adathalász banki e-mailekben (phishing) található hivatkozások gyakran egy meghamisított banki weboldalra vezetnek, ahol a célszemélyt a pénzügyi és személyes adatai megadására kérik.

Ezek a webhelyek szinte teljesen ugyanolyanok, mint a mintának használt valódi (hivatalos, céges) honlap.

Általában tartalmazznak azonban egy felugró ablakot, amelyik a banki hitelesítő adatok megadását kéri.

Gyanús lehet továbbá a gyenge minőségű grafika, valamint a sürgető hangvételű üzenetek, tartalmak.

A valódi bankok nem használnak ilyen ablakokat, tartalmakat.

Mit tegyen, ha adathalász banki e-mailt kapott?

Soha ne nyissa meg a bank webhelyét e-mailben található hivatkozásra kattintva!

Mindig gépelje be a hivatkozást, vagy használja a „Kedvencek” közé elmentett linket!

Használjon olyan böngészőt, amely lehetővé teszi a felugró ablakok blokkolását!

Előugró ablakok általában bizalmas adatokat kérnek Önről. Ne kattintson rájuk és ne adjon meg személyes adatot az ilyen oldalakon!

Amennyiben a bank szeretné felhívni a figyelmet valamilyen fontos dologra, a figyelmeztetést az online banki felületen jeleníti meg.

6. HAMIS TRANZAKCIÓK JÓVÁHAGYÁSA

A bankok az online belépéshez és a tranzakciók jóváhagyásához kétlépcsős hitelesítést követelnek meg, az ügyfélnek a jelszón kívül egy másik módon is azonosítani kell magát.

Ez az azonosítás történhet az ügyfél birtokában lévő kódgenerátorral, az ún. tokenel, amely a sorozatszámától és a használat időpontjától függően egy egyszer felhasználható, rövid ideig (1-2 perc) érvényes kódot szolgáltat, vagy az ügyfél által megadott telefonszámra érkező SMS-ben szereplő szám megadásával.

Előfordulhat azonban olyan eset is, amikor a másodlagos hitelesítéshez elégséges csak a telefonon megjelenő felugró gombot megnyomni, vagy az ujjlenyomat-olvasóhoz hozzáilleszteni az ujjat.

Ezek a jóváhagyási kérelmek megjelenhetnek az ügyfél telefonján akkor is, ha nem személyesen maga az ügyfél, hanem a bankszámlája felett rendelkező más személy kezdeményezte a belépést vagy a tranzakciót.

Ha egy csaló próbál belépni vagy hamis tranzakciót indítani, az ügyfélnek ugyanúgy meg kell adnia a másodlagos hitelesítési adatokat ahhoz, hogy a belépés vagy a tranzakció sikeres legyen

Mit tegyen, ha hamis azonosítási folyamatot észlel?

- Mindig ellenőrizze, hogy a belépési kísérletet vagy a tranzakciót, melyet jóvá akar hagyni, valóban Ön, vagy az Ön által megbízott személy kezdeményezte! Sose hagyjon jóvá ismertlen kérést!
- A kapott jóváhagyó SMS-ben ellenőrizze a jóváhagyásra váró műveletet, az összeget és a címzettet, ha szerepel benne!
- A banki műveletek jóváhagyásához használt tokent sose hagyja felügyelet nélkül!
- Használjon a mobiltelefonján képernyőzárát!
- Csak saját ujjlenyomatait regisztrálja a telefonjába!
- Állítsa be úgy a mobiltelefonját, hogy az SMS-ben kapott üzenetek tartalma csak a képernyőzár feloldása után legyen látható!

7. HAMIS BEFEKTETÉSI LEHETŐSÉGEK

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

Ezeket a befektetési lehetőségeket gyakran – a tudtukon és beleegyezésükön kívül – közismert emberek, sportolók, modellek képeivel és ajánlásával hirdetik.

Mit tegyen, ha ilyen ajánlatot kapott?

Mindig gyanakodjon, ha folyamatosan kapja a kéretlen telefonhívásokat; ha gyors megtérülést ígérnek és biztosítják arról, hogy a befektetés biztonságos; ha az ajánlat csak korlátozott ideig él; ha az ajánlat csak Önnek érhető el, és megkérik, hogy senkinek se szóljon róla!

Pénz átadása vagy befektetése előtt mindig kérjen pénzügyi tanácsot egy pártatlan féltől, szakértőtől!

Utasítsa el a befektetési lehetőségekkel kapcsolatos kéretlen telefonhívásokat!

Ha egyszer már befektetési csalás áldozatává vált, a csalók valószínűleg újra megkeresik, vagy eladják adatait más bűnözőknek!

Értesítse a rendőrséget, ha gyanakszik!

Befektetések kockázatairól, előnyeiről és hátrányairól szóló bővebb tudnivalókért olvassa el a Jogosulatlan szolgáltatók és a Tájékoztató az online befektetési lehetőségek kockázatairól c. cikket, vagy lapozza fel a Befektetések c. Pénzügyi Navigátor füzetet!

8. NEM BANKI SZOLGÁLTATÓK NEVÉVEL TÖRTÉNŐ VISSZAÉLÉS

Ennél a csalástípusnál az elkövetők hasonló módon próbálják megkárosítani áldozataikat, mint a phishing, vishing vagy a smishing esetén: hivatalosnak tűnő adathalász e-mailekkel, hívásokkal vagy sms-ekkel próbálják személyes vagy bankszámlaadatok megadására, illetve fizetésre, pénz utalására rávenni célpontjaikat.

Ezekben az esetekben azonban nem banknak vagy pénzügyi szolgáltatónak álcázva, hanem valamilyen nagy ügyfélkörrel rendelkező szolgáltató – pl. közmű-, telekommunikációs vagy kábelszolgáltató – nevében keresik fel áldozataikat.

A futárcégek üzenetei is szolgálhatnak visszaélés alapjául.

Ezekben jellemzően adategyeztetésre, vagy fizetési késedelemre, hátralék befizetésével kapcsolatos felszólításra hivatkozva a bankszámlaadatok megadására, illetve pénz befizetésére szólítják fel a megcélzott ügyfeleket.

A hivatalosnak látszó üzenetekben olyan linkeket is elrejthetnek a támadók, amelyek segítségével rosszindulatú szoftvert telepíthetnek az eszközre.

Mit tegyen annak érdekében, hogy ne váljon ilyen csalás áldozatává?

Mivel a csalásoknak ez a formája nagyban hasonlít a smishingre, vishingre és phishingre, ugyanúgy lehet megelőzni őket, és ugyanazok a teendők is, mint a banki adathalász e-mailek, telefonhívások és sms-ek esetén:

Legyen különösen éber, ha egy szolgáltató e-mailben, telefonon vagy sms-ben bizalmas információkat, banki adatokat, azonosítókat kér, vagy azonnali fizetésre szólít fel!

Soha ne adja meg ezeket az információkat, ha e-mailben, telefonhívásban vagy sms-ben kérik őket!

Egy szolgáltatótól érkező e-mail tartalmazhat fizetési késedelemmel kapcsolatos figyelemfelhívást, de ilyen esetben is legyen megfontolt: ne kattintson megdöbbenve a levélben található linkekre és az esetleges sürgető hangvétel ellenére se kezdeményezzen fizetést a hátralék mihamarabbi rendezése érdekében!

Bankszámlaadatait, banki azonosítóit se adja meg automatikusan!

Ellenőrizze a szolgáltatóhivatalos csatornáin, hogy valóban ők küldték-e a levelet, a felszólítást, és annak tartalma valós-e!

Ne telepítsen az e-mailben, sms-ben kapott linkekről szoftvert! Mindig a szolgáltató hivatalos oldalán megadott linket vagy a hivatalos alkalmazásboltokat (pl. Google Play, App Store) használja szoftvertelepítéskor!

Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat! Minél sürgetőbb a hívás és az üzenet, annál gyanúsabb!

Gyanús telefonhívás esetén ne adjon meg személyes adatokat és szakítsa meg a beszélgetést!

A hívó telefonszámát jegyezze fel, majd keresse a szolgáltatót valamelyik hivatalos csatornán, és jelezze neki a gyanús megkeresést!

Ne használja az ellenőrzéshez a hívó által megadott telefonszámot!

A szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták.

Soha ne utaljon pénzt telefonon érkező kérésre! Egy szolgáltató sosem kér ilyet.

A csalási szándékú hívásokat jelentse a szolgáltatónak!

9. WANGIRI: VISSZAHÍVÁSOS TELEFONOS CSALÁS

A Japánból származó wangiri a mobiltelefonoknak köszönhetően vált az egyik legelterjedtebb csalástípussá.

Lényege, hogy a csalók tömegesen generált számítógépes hívások részeként ismeretlen, általában külföldi – jellemzően 2-essel kezdődő országhívóval rendelkező afrikai, vagy 5-össel kezdődő országhívóval rendelkező közép-amerikai – számról hívják fel áldozataikat, ám a hívást egy-két csöngés után bontják a visszahívás reményében.

A visszahívás azonban a belföldinél magasabb tarifán zajlik, és a csalás akkor is eredményes, ha a hívás látszólag sikertelen: például folyamatosan kicsöng, vagy épp nem csöng ki, hanem vonalszakadást vagy folyamatosan foglaltat jelez.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

Ne vegye fel a telefont, ha híváskor ismeretlen külföldi hívószámot jelez ki a telefonja, és ne is hívja vissza rögtön – először ellenőrizze azt!

Különösen legyen óvatos akkor, ha olyan külföldi számról hívják, ahol nem él ismerőse vagy ahonnan nem vár hívást, illetve, ha az országghívó 2-essel vagy 5-össel kezdődik (ld. fentebb: afrikai és közép-amerikai azonosítók)!

Egy internetes kereséssel utánajárhat annak, hogy az adott telefonszámmal kapcsolatban korábban felmerül-e a csalás gyanúja: ha igen, nagy valószínűséggel talál ezzel kapcsolatos információt a világhálón.

Az ismeretlen előhívószámokról érkező külföldi hívások egyedileg és csoportosan is letilthatók. Az egyedi hívószámokat a készülék beállításában lehet letiltotta

10. HAMIS ONLINE AJÁNLATOK

A fogyasztók és a vállalkozások egyre többet vásárolnak és adnak el az interneten.

Az online ajánlatok sokszor valóban kedvezők, de óvakodjon a csalóktól!

Mit tegyen, hogy elkerülje a hamis online ajánlatokat?

- Ha lehet, belföldi kiskereskedelmi webhelyeken vásároljon, így nagyobb valószínűséggel kerülheti el, oldhatja meg az esetleges problémákat!
- Nézzon utána a dolgoknak: vásárlás előtt olvasson értékeléseket, ismertetőket az adott termékről!
- Kizárólag biztonságos fizetési szolgáltatásokkal fizessen!
- Gyanakodjon, ha pénzküldési szolgáltatás használatát kérik!

Csak biztonságos internetkapcsolat használatakor fizessen, ne használjon ingyenes vagy nyilvános wifi 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! Valószínűleg hamis, ha túl szépnek tűnik ahhoz, hogy igaz legyen.

Ha olyan felugró ablak jelenik meg a képernyőn, amely nem várt nyereményről tájékoztatja Önt, jusson eszébe, hogy ez nagy valószínűséggel egy rosszindulatú program!

Ha nem érkezik meg a termék, vegye fel a kapcsolatot az eladóval!

Ha nem válaszol, vegye fel a kapcsolatot bankjával és az online piactér üzemeltetőjével!

11. SZEMÉLYESADAT-LOPÁS A KÖZÖSSÉGI MÉDIÁBAN

A csalók különböző módszerek alkalmazásával megpróbálják elérni, hogy Ön megadja személyes adatait (név, e-mail cím, jelszó, hitelkártyaszám stb.).

Ezt annak ellenére is megtehetik, hogy Ön megfelelő védelmet alkalmaz, közösségimédia-fiókjainak tartalmát nem láthatja mindenki, vagy ha óvatosságból nem oszt meg túl sok információt a profiljában (olyanokat, amelyekkel ellophatják a személyazonosságát).

Az adatok birtokában aztán jóvá nem hagyott vásárlásokat hajthatnak végre az Ön hitelkártyájával, bankszámlát nyithatnak; telefon-előfizetést vásárolhatnak; hitelt vehetnek fel; illegális üzleti tranzakciókat hajthatnak végre; eladhatják adatait más csalóknak.

Mit tegyen személyes adatai védelme érdekében?

- Rendszeresen tekintse át közösségimédia-fiókjai adatvédelmi és biztonsági beállításait!
- Áldozzon némi időt annak a megismerésére, hogy mit mutat a profilja Önről a külvilág számára!
- Gondolja át alaposan, hogy mennyi információt és fényképet oszt meg a közösségimédia-oldalakon!
- Felhasználásukkal a csalók hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.
- Végezzen online kutatást!
- Keressen rá az adott termék nevére vagy a munkaaajánlatra, és nézze meg, mit mondanak a többiek!

Használjon olyan szavakat a keresőkifejezésben, mint „felülvizsgálat”, „panasz” és „csalás”!

Jelentse a közösségimédia-platform üzemeltetőinek azokat a profilokat, amelyekről azt gyanítja, hogy csaláshoz hozták létre őket!

Tiltsa le őket, ha az ismerősei vagy a követői, és szakítson meg velük minden kapcsolatot!

Ha valódi ismerőseitől kap szokatlan vagy gyanús üzenetet, illetve lát általuk közzétéve furcsa posztot, gyanakodjon és jelentse a közösségimédia-platform üzemeltetőjének!

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!

Egyéb, a fentiekben nem részletezett csalási formák:

Pharming: a támadás során az áldozat eszközére rosszindulatú kódot telepítenek, ami figyeli és gyűjti a bejelentkezési adatokat (ilyennel lehet találkozni egy validnak tűnő alkalmazás (pl. játék) telepítése során is)

Evil twin phishing: hamis Wi-Fi hálózat létrehozása, amely valódinak tűnik (ha valaki bejelentkezik, és bizalmas adatokat ad meg, a hacker rögzíti az adatait)

Angler phishing: hamis közösségi média bejegyzések / hirdetések használata adatszerzésre (legtöbbször ráveszik az áldozatot arra, hogy töltsön le valamit, vagy kattintson egy linkre)

Social engineering: ez a klasszikus átverős, megtévesztős, manipulálós dolgok gyűjtőneve (sok a fentiek közül ide is tartozik)

MUNKAHELYI CSALÁSOK

1. HAMIS ÜGYFÉL VAGY BESZÁLLÍTÓ

Ebben az esetben valaki megkeresi a vállalatot, aki egy ügyfél, beszállító vagy hitelező képviselőjeként azonosítja magát. A megkeresés érkezhethet telefonon, levélben, faxon vagy e-mailben.

A csaló azt kéri, hogy az egyik partner jövőbeli számláinál módosítsák valamelyik banki adatot, például a kedvezményezett bankszámlaszámát vagy másodlagos számlaazonosítóját.

Az így megadott bankszámla felett a csaló rendelkezik.

Mit tegyen, ha hamis ügyféllel vagy beszállítóval áll szemben?

- Ellenőrizzen minden, állítólagosan a hitelezőktől érkező kérelmet – főleg akkor, ha azt kéri, hogy a jövőbeli számláknál módosítsák valamelyik banki adatot!
- Ne használja a módosítást vagy ellenőrzést kérő levélben, e-mailben szereplő kapcsolattartási adatokat!

Keressen egy korábbi üzenetet, és annak a kapcsolattartási adatait használja!

Jelöljön ki egy megbízott kapcsolattartót azoknak a vállalatoknak az esetében, amelyek számára rendszeresen indít kifizetéseket!

Vezessen be egy rendszert adott összeghatár feletti kifizetések esetében, amelynek kifejezetten a helyes bankszámlaszám és kedvezményezett ellenőrzése a célja! Ez lehet például egy megbeszélés az érintett vállalattal.

A számla kifizetésekor egy ellenőrzött e-mail címre küldjön tájékoztatást a kedvezményezettnek!

A biztonság szavatolása érdekében szerepeltesse a fogadó bank nevét és a bankszámlaszám utolsó négy számjegyét, illetve a másodlagos számlaazonosítójának jellemző részletét (pl. adóazonosító utolsó négy karakterét)!

Korlátozza azokat az adatokat, amelyeket megoszt az alkalmazottakról a közösségi médiában!

Jelentse a vezetőségnek vagy a megfelelő osztálynak (IT, biztonsági stb.) a csalási kísérleteket!

2. HAMIS VEZETŐI UTASÍTÁS E-MAILBEN VAGY TELEFONON

Ezzel a módszerrel általában kifizetési jogkörrel rendelkező alkalmazottat támadnak az elkövetők, akit hamis számla kifizetésére, vagy jóvá nem hagyott átutalás indítására próbálnak rávenni.

Arra építenek, hogy az alkalmazottak igyekeznek gyorsan teljesíteni azokat a feladatokat, amelyek közvetlenül a felső vezetéstől érkeznek.

A csalók általában részletes információkkal rendelkeznek a szervezetről, és az e-mail rendkívül meggyőzőnek látszik.

Ez a fajta megkeresés kéretlen e-mail vagy telefonhívás formájában érkezik, látszatra a megfelelő felsővezetőtől.

Rendszerint a téma bizalmas kezelését kéri, de sürgeti az ügyintézését, ugyanakkor szokatlan, a belső előírásoknak ellentmondó kéréseket tartalmazhat.

Mit tegyen, ha gyanús feladatot kap?

Tartsa be szigorúan a kifizetésekre és beszerzésre vonatkozó biztonsági eljárásokat! Ne hagyjon ki eljárási lépéseket, és ne engedjen a nyomásgyakorlásnak!

Mindig gondosan ellenőrizze az e-mail-címeket a bizalmas információk, pénzáttalások esetében!

A csalók gyakran használják a valódihoz nagyon hasonló e-mail címeket, amelyek csak egy karakterben térnek el az eredetitől.

Ne az e-mailre válaszolva próbálja meggyőződni annak valódiságáról, hanem inkább telefonáljon vagy más csatornán ellenőrizze a feladatot!

Ha van rá mód, hívja fel a felsővezetőt, vagy asszisztensét/titkárságát!

Amennyiben kétségei vannak egy áttalási 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-fiókját!

Korlátozottan terjessze az információkat, és kezelje óvatosan a közösségi médiát!

A munkahelyi számítógépén, laptopján ne nyisson meg privát közösségi oldalt, és ne tegyen közzé semmilyen, a munkájával vagy a munkahelyével kapcsolatos tartalmat, információt!

Ne osszon meg a vállalati hierarchiára, biztonságra és eljárásokra vonatkozó információkat!

Minden esetben értesítse az IT-osztályt, ha gyanús e-mailt vagy telefonhívást kap!

A munkahelyi csalások a fentiekben nem részletezett egyéb formái:

• **Spear phishing:** egy adott személy megcélzása egy szervezetben, hogy megpróbálják ellopni a bejelentkezési adataikat (a támadók itt gyakran először információkat gyűjtenek a személyről a támadás megkezdése előtt, hogy kellően elő legyen készítve a megkeresés).

• **Whaling (CEO fraud):** a fenti egy formája, amikor egy felsővezető a célzott személy.

• **BEC (avagy business email compromise):** szorosan kötődik az előző kettőhöz, itt a lényeg, hogy a csaló úgy tesz, mintha egy szervezet vezetője lenne, annak nevében küld utasításokat az alkalmazottaknak e-mailen keresztül (ehhez általában kell, hogy hozzáférjenek egy felső vezető email fiókjához).

• **Ransomware:** ez a zsarolóvírus (általában cégeket találják be, a lényege, hogy tartalmakat blokkolnak és váltságdíjat kérnek a feloldásért, illetve újabban már csak fenyegetnek azzal, hogy küldenek egy zsaroló vírust, ha nem fizetsz előre)

• **DDoS (avagy distributed denial-of-service):** túlterheléses támadás, hogy átmenetileg elérhetetlenek legyenek weboldalak (sokszor ezért is kvázi váltságdíjat kérnek, hogy abbahagyják, de egyre inkább kombinálják a fentivel, és azért terhelnek túl, hogy bejuttassanak egy zsaroló vagy trójai vírust egy rendszerbe)