ONLINE PÉNZÜGYI CSALÁSOK ÉS ÁTVERÉSEK A MESTERSÉGES INTELLIGENCIA VILÁGÁBAN

MARADJON ÉBER ÉS VÉDJE MEG MAGÁT!

Az online pénzügyi csalások és átverések nem új keletűek, de a mesterséges intelligencia (MI, AI) kifinomultabbá és nehezebben észrevehetővé tette ezeket. A bűnözők hamis üzeneteket és weboldalakat, hamis hírességprofilokat, sőt mesterséges intelligencia által generált hangokat vagy videókat használnak, amelyeken a megjelenő személyek úgy néznek ki, mint a bankára, a barátai vagy a családtagjai.

Gyakran a közösségi médián, üzenetküldő alkalmazásokon, e-mail-eken és valósnak tűnő váratlan telefonhívásokon keresztül érik el Önt.

Előfordulhat, hogy olyan kockázatokkal szembesül, mint a pénzügyi veszteség, a személyazonosság-lopás és az érzelmi stressz. Legyen óvatos, és biztonsága érdekében kövesse az alábbi kulcsfontosságú javaslatokat:

Legyen óvatos az online pénzügyi csalásokkal és a mesterséges intelligenciával működő csalásokkal, például a megszemélyesítéssel, az adathalászattal, a befektetési és biztosítási csalásokkal, valamint a romantikus csalásokkal és átverésekkel kapcsolatban. A különböző típusú csalásokról és átverésekről további részleteket az 5-7. oldalon talál.

Vegye észre a figyelmeztető jeleket: tanulja meg felismerni a gyanús magatartásokat, üzeneteket vagy ajánlatokat (részletek az 2. oldalon).

Védje meg magát: tartsa biztonságban személyes adatait (részletek a 3. oldalon) és

Tudja meg, mi a teendő, ha csalás vagy átverés áldozatává válik (részletek a 4. oldalon)

Figyelmeztető jelek

Egy ígéret, ami túl szép ahhoz, hogy igaz legyen.

Váratlan hívás ismeretlen számról.

Pénzre vagy személyes adatok megküldésére vonatkozó sürgős kérés, beleértve azt is, ha valaki családtagnak, barátnak vagy akár közszereplőnek adja ki magát.

Kérés az eszköze (pl. számítógép, telefon) irányításának átvételére, egy alkalmazás letöltésére, egy QR-kód beolvasására vagy egy linkre való kattintásra.

Személyes adatok vagy banki adatok (pl. jelszavak, bankkártya információk, internetes banki hitelesítő adatok vagy biztonsági kódok) kérése.

Fizetési kérelem nem nyomon követhető fizetési módok alkalmazásával (pl. kripto-eszközök, ajándékkártyák, nem bankon keresztüli elektronikus pénzküldések).

Gyanús vagy helytelen e-mail cím vagy hivatkozás (pl. helyesírási hibák az URL-ben vagy szokatlan webcímek).

Ismeretlen forrásból származó melléklet, különösen .exe, .scr, .zip vagy makróbarát Office-fájl (.docm, .xlsm).

Pontatlan helyesírás vagy formázás egy hivatalosnak tűnő dokumentumban, bár a mesterséges intelligencia lehetővé teheti a csalók számára, hogy hatékonyabban elrejtsék ezeket a hibákat.

Olyan weboldal, amely ugyan professzionálisnak tűnik, de nem rendelkezik ellenőrzött kapcsolattartási adatokkal vagy cégnyilvántartási információkkal.

Olyan hanghordozás, amely természetellenesen hangzik, nem alkalmaz szüneteket, és túlságosan egysíkúnak vagy robotikusnak tűnik. Ügyeljen a „hangklónozásra”, bár a mesterséges intelligencia által generált beszéd nagyon természetesnek tűnhet.

Azok a videók, ahol a hang robotikus vagy természetellenes, az ajakmozgások és az arckifejezések nem igazodnak a beszédhez, vagy a háttér, a világítás és az árnyékok szokatlanok lehetnek. Ezek gyakran mesterséges intelligencia által generált videók („deepfake”).

Lépések az Ön védelme érdekében

1 **Soha ne osszon meg személyes vagy banki információkat:**

A törvényesen működő vállalatok soha nem fogják kérni a PIN-kódokat, jelszavakat, internetes banki hitelesítő adatokat vagy biztonsági kódokat e-mailben, szöveges üzenetben, közösségi médiában vagy telefonon.

2 **Álljon meg és gondolkodjon, mielőtt cselekszik:**

Ne siessen a pénzküldéssel, az információmegosztással vagy a linkekre kattintással – a csalók szándékosan a sürgősség érzetét keltik (pl. informatikai problémák a bankjával, vészhelyzeti hívások a barátaival és családtagjaival kapcsolatban, fenyegető nyelvezet stb.). Bármilyen kétség esetén, még ha kisebb is, ne cselekedjen. Fejezze be a hívást, és ellenőrizze a forrás vagy a személyazonosság hitelességét.

3 **Gondosan ellenőrizze a forrást/személyazonosságot:**

- Mindig ellenőrizze, hogy az üzenetek, hívások, e-mailek és linkek honnan származnak- még akkor is, ha hivatalosnak tűnnek, vagy úgy tűnik, hogy egy baráttól, családtagjától, vagy akár egy közszereplőtől származnak. Például a csaló felhívhatja családtagjait és barátait (vagy SMS-t küldhet) egy ismert szám használatával egy megbízható csatornán keresztül. Keressen helyesírási hibákat, furcsa URL-eket vagy hiányzó biztonsági jelzéseket: (pl. ellenőrizze, hogy a weboldal linkje tartalmaz-e „s”-t a „HTTPS”-ben, hogy megbizonyosodjon arról, hogy a weboldal biztonságos-e, és ellenőrizze, hogy vannak-e hozzáadott vagy hiányzó betűk a vállalat nevében).

- Ne nyisson meg kéretlen üzenetekből származó linkeket, csak hivatalos alkalmazásokat telepítsen megbízható alkalmazás-áruházakon keresztül, és ne szkenneljen ismeretlen QR-kódokat.

- Állapodjon meg családjával egy “biztonságos szóról”- egy titkos kifejezésről, amelyet a személyazonosság megerősítésére használhat, ha valaki ismerős hanggal felhívja Önt egy sürgős pénzkéréssel, és azt állítja, hogy családtag (pl. szülő, testvér, gyermek).

- Használjon ellenőrzött kapcsolattartási adatokat, hogy közvetlenül elérje a vállalatot vagy az egyént, és soha ne támaszkodjon a feltételezett csaló által megadott kapcsolattartási adatokra (pl. önállóan keresse meg a vállalat nevét, használjon ellenőrzött üzleti címjegyzékeket, korábban megerősített kapcsolattartási módszereket). A csalók azt állíthatják, hogy engedéllyel rendelkeznek, vagy lemásolhatják egy engedélyezett vállalat weboldalát. Ellenőrizze, hogy a nemzeti pénzügyi hatóság adott-e ki figyelmeztetést, vagy az szerepel-e az IOSCO I-SCAN listáján (iosco.org/i-scan/). A kriptoeszköz-szolgáltatók esetében ellenőrizze, hogy rendelkeznek-e engedéllyel az EU-ban (pl. tekintse meg az ESMA nyilvántartását ( ).

4 **Ügyeljen a lehetséges mesterséges intelligencia-trükkökre:**

Ahogy az AI technológia fejlődik, a csalások egyre meggyőzőbbek- még a legjobb biztonsági tippek betartása mellett is. Ha valami szokatlannak tűnik, vagy a fent vázolt figyelmeztető jelek bármelyikét észleli, álljon meg és értékelje újra a helyzetet.

5 **Soha ne telepítsen távelérési szoftvert, és ne ossza meg a képernyőjét:**

A bankok és a pénzügyi intézmények soha nem fogják ezt kérni Öntől.

6 **Tartsa biztonságban az eszközeit és fiókjait:**

Használjon erős és egyedi jelszavakat, tartsa titokban őket, és ne használja újra ugyanazokat a hitelesítő adatokat különböző platformokon. Lehetőség szerint engedélyezze a többfaktoros hitelesítést. Néhány jelszóval kapcsolatos tippet itt talál (https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszo-ellenorzo/). Tartsa naprakészen és aktiválva szoftvereit és vírusvédelmét.

7 **Legyen óvatos a váratlan és korlátozott idejű befektetési lehetőségekkel:**

Ha túl jól hangzik ahhoz, hogy igaz legyen, akkor valószínűleg nem is az.

8 **Gondolkodjon, mielőtt információkat oszt meg a közösségi médiában:**

A csevegőcsoportok, fórumok, közösségimédia-bejegyzések és fényképek értékes információforrások lehetnek a csalók számára. Ha túl sokat árul el magáról vagy befektetéseiről, könnyű célponttá válhat.

Mi a teendő, ha csalás vagy átverés áldozatává vált?

Azonnal állítsa le a tranzakciókat,

Hogy blokkolja a gyanús számlákra történő további átutalásokat, és elkerülje a további veszteségeket. Szüntessen meg minden kapcsolatot a csalókkal – hagyja figyelmen kívül hívásaikat és e-mailjeiket, valamint blokkolja a feladót.

Vegye fel a kapcsolatot bankjával vagy pénzügyi szolgáltatójával.

Azonnal tájékoztassa bankját vagy pénzügyi szolgáltatóját a hivatalos kapcsolattartási csatornákon keresztül, hogy feltárja a tranzakciók befagyasztásának vagy visszafordításának lehetőségeit.

Módosítsa jelszavát az összes eszközén és alkalmazásában/weboldalán.

A csalók online vásárolnak kiszivárgott jelszavakat, és több fiókon próbálják ki őket. Csak egy jelszó megváltoztatása nem elegendő; győződjön meg róla, hogy mindegyiket megváltoztatta, hogy a csalók ne használhassák újra őket.

Jelentés és riasztás:

Jelentse az eseményt a rendőrségnek és tájékoztassa a kapcsolatait (pl. barátok és családtagok) a figyelemfelkeltés érdekében. Ezek az intézkedések segíthetnek megvédeni önmagát és másokat.

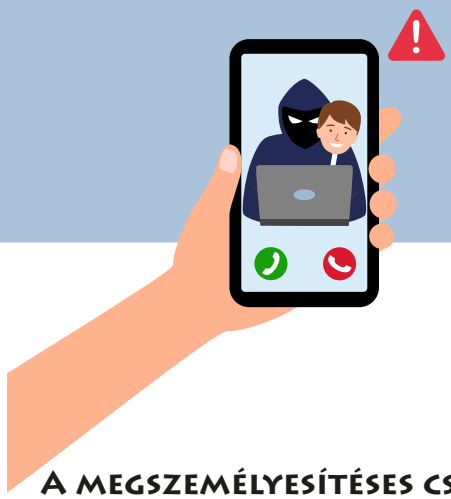
Óvakodjon a „recovery room” (pénz visszaszerzést ígérő) csalásoktól:

A csaló felveheti Önnel a kapcsolatot, tudva, hogy Ön egy korábbi csalás áldozata, azt állítva, hogy egy hatóság (pl. rendőrség, adó- vagy pénzügyi hatóság stb.) tagja, és felajánlja, hogy díj ellenében visszaszerzi az elveszett pénzét. Ez gyakran egy újabb kísérlet arra, hogy átverjék. Ne feledje: az, hogy egyszer átverték, nem zárja ki, hogy újra megtegyék.

Európai Bankhatóság, Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság, Európai Értékpapír-piaci Hatóság, 2025
Luxembourg: Az Európai Unió Kiadóhivatala, 2025

PDF ISBN 978-92-9407-221-4 doi:10.2853/0688542 DZ-01-25-109-HU-N

AZ MI ÁLTAL LÉTREHOZOTT ONLINE PÉNZÜGYI CSALÁSOK ÉS ÁTVERÉSEK TÍPUSAI



A megszemélyesítéses csalás („Impersonation scam”) és a „mély hamisítás” („deepfake”) használata

Váratlan hívást kap valakitől, aki azt állítja, hogy az Ön bankja, egy hatóság (pl. rendőrség, adó- vagy pénzügyi hatóság stb.) tagja, egy biztosítás közvetítő, egy informatikai vállalat vagy akár egy családtag. A hívó fél arra ösztönözheti Önt, hogy pénzt utaljon át annak biztonsága érdekében, gyanús tevékenységre hivatkozva a számláján vagy a biztosításához kapcsolódóan. Azt is kérhetik, hogy adja meg banki adatait (pl. fizetési kártya száma, internetes banki hitelesítő adatok vagy jelszavak), kattintson egy linkre, vagy telepítsen egy szoftvert, úgy téve, mintha ez gyorsan megoldaná a problémát. A hívó fél hamisított számot használhat, amely gyakran megegyezik a bank telefonszámával annak érdekében, hogy jogszerűnek tűnjön (hamisítás – „spoofing”).

A csalók mesterséges intelligenciát használhatnak olyan hamis videók, képek vagy hangok létrehozására, amelyek utánozzák valaki hangját (pl. bankár vagy családtag), arcát (pl. híresség) vagy mozgását. **Ez az úgynevezett „Deepfake”.**

Mi történhet?

A személyes adatok megemlítésével és a sürgősség érzésének megteremtésével a csaló ráveheti Önt olyan tevékenységekre, amelyeket nem szándékozott megtenni – például pénzt küldeni a számlájukra, rosszindulatú linkre kattintani, vagy rosszindulatú programot telepíteni az eszközére. Ez közvetlen hozzáférést biztosíthat a csalónak a banki hitelesítő adataihoz. Ezzel az információval megváltoztathatják a jelszavát, hozzáférhetnek a bankszámlájához, és ellophatják a pénzét. Ne feledje: csak azért, mert a hívó ismeri az Ön személyes adatait, még nem jelenti azt, hogy megbízható.

Adathalászat és pszichológiai manipuláció („Phishing and social engineering”)

Olyan e-mailt vagy üzenetet kap, amely úgy tűnik, hogy a bankjától vagy egy pénzügyi szolgáltatótól érkezik, és figyelmezteti Önt a számláján végzett „gyanús tevékenységre”. A logó, az elrendezés és a nyelv professzionálisnak tűnik, és az üzenet ugyanazon a csatornán jelenhet meg, mint a bankkal folytatott többi beszélgetése. Az üzenet arra ösztönzi, hogy kattintson egy linkre a fiókja hitelesítéséhez vagy a jelszavának visszaállításához. A link egy hamis weboldalhoz vezet, amely megegyezik az internet banki felületével. Anélkül, hogy észrevenné, beírja adatait egy olyan webhelyre, amelynek célja személyes adatainak ellopása.

A csalók mesterséges intelligenciát használnak arra, hogy meggyőző adathalász üzeneteket készítsenek azáltal, hogy elemzik a közösségi média adatait az áldozatok azonosítása és az üzenet tartalmának az egyes célpontokhoz történő testre szabása érdekében.

Mi történhet?

A csaló hozzáfér a bankszámlájához, és ellopja a pénzét, vagy hamis profilt hoz létre a személyes adataival, hogy csalást kövessen el.

Befektetési vagy biztosítási csalás („Investment or insurance scam")

A közösségi médiában vagy egy weboldalon olyan hirdetés jelenik meg, amely egy jól ismert vállalat biztosítására vonatkozó „korlátozott idejű, alacsony kockázatú befektetési lehetőséget" vagy „korlátozott idejű kedvezményt" népszerűsít. A hirdetés egy híresség fényképét és gyakran hamis ajánlásokat tartalmaz. Miután egy linkre kattintva vagy egy űrlap kitöltésével kifejezte érdeklődését, kapcsolatba lépnek Önnel, és átirányítják egy platformra vagy üzenetküldő csatornára, ahol professzionálisnak tűnő tanácsokat és dokumentumokat kap. Javasolják továbbá, hogy fektessen be egy kis összeget, majd egyre nagyobb összegeket, vagy fizesse be a hozamot egy biztonságosnak tűnő számlára.

A csalók mesterséges intelligencia-eszközöket használnak arra, hogy ezeket a hamis javaslatokat vagy e-maileket rendkívül meggyőzővé és nehezen felismerhetővé tegyék. AI-alapú közösségi média-botokat is használnak, hogy hamis fiókokat hozzanak létre, amelyek kapcsolatba lépnek Önnel, téves információkat terjesztenek, és valódi viselkedést szimulálnak annak érdekében, hogy elnyerjék a bizalmát és befolyásolják döntéseit.

Mi történhet?

Miután megpróbálja visszahívni a pénzét vagy követelését benyújtani, a kapcsolattartó nem válaszol. Felfedezi, hogy a vállalat nem létezik, vagy hogy a biztosított kockázatot nem fedezik. Ezután rájön, hogy pénzt küldött közvetlenül egy csalónak egy csalárd rendszer részeként. Sajnos nem kaphatja vissza a pénzét, valamint személyes és pénzügyi adatait további csalások elkövetésére használhatják fel (pl. szerződések aláírása az Ön nevében, ami még több pénz elvesztéséhez vezethet).

Romantikus csalás és átverés („Romance fraud and scam")

Olyan személy vette fel Önnel a kapcsolatot szociális média, társkereső alkalmazás, vagy telefon / SMS útján, akivel még nem találkozott a valós életben. Ez a személy gyakori, személyes és romantikus beszélgetéseket folytat, hamis profilok segítségével bizalmat épít. Idővel a beszélgetés a pénz vagy a pénzügyi lehetőségek felé tolódik el, mint például a kripto-befektetések, amelyek magas megtérülést és alacsony kockázatot ígérnek. A személy arra kéri Önt, hogy utaljon pénzt egy számlára, vagy segítséget nyújt egy számla létrehozásához és egy kisebb összegű kezdeti befizetés teljesítéséhez annak érdekében, hogy a rendszer jogszerűnek tűnjön, mielőtt arra ösztönözné Önt, hogy többet fektessen be.

A csalók mesterséges intelligenciát használnak hamis profilok létrehozására, áldozataik azonosítására a közösségi médiában/randevú alkalmazásokban az Ön által rendelkezésre bocsátott adatok felhasználásával, vagy chatbotokat használnak üzenetek generálására.

Mi történhet?

A csaló a lehető legtöbb pénzt szerzi meg Öntől, majd megszakítja az összes kommunikációt és eltűnik. A csalárd befektetési weboldal vagy alkalmazás offline állapotba kerül, így Ön nem férhet hozzá az állítólagos befektetésekhez. A pénzügyi veszteség mellett az Ön által megosztott személyes adatok felhasználhatóak barátai és családtagjai megcélzására vagy személyazonosság-lopásra, ami pénzügyi és/ jogi következményekkel járhat az Ön számára (pl. a csaló vásárolhat, hitelt vehet fel az Ön nevében, vagy az ellenkező bizonyításáig Ön felelősségre vonható az Ön nevében felhalmozott adósságokért vagy elkövetett bűncselekményekért).

Vásárlással kapcsolatos átverés („Purchase scam”)

Vonzó ajánlatot talál egy online piactéren. Az ajánlatot adó vállalat fizetési művelet teljesítését kéri a hivatalos platformon kívül, azt állítva, hogy „biztonságos fizetési rendszert” használ, és elküldi Önnek a vásárlás befejezéséhez szükséges linket. A link átirányítja Önt egy hamis banki hitelesítési oldalra, amely a bank hivatalos weboldalát utánozza, annak logóját és kialakítását alkalmazza, így Ön megadja az online banki adatait a fizetési művelet teljesítése érdekében.

A csalók mesterséges intelligenciát használnak annak érdekében, hogy rendkívül meggyőző hamis banki weboldalakat, megrendelés-visszaigazolásokat és számlákat hozzanak létre. Az AI segít nekik utánozni a valódi vállalatok hangvételét, márkáját és stílusát. Bizonyos esetekben AI chatbotokat használnak a kérdések megválaszolására és az üzlet hihetőbbé tételére.

Mi történhet?

A harmadik féltől származó linken keresztül történő fizetés megkerüli a piactér által kínált védelmet. A csaló megkapja a bankszámlájához kapcsolódó bejelentkezési adatait, és ellopja a pénzét.