KRIPTOESZKÖZÖKKEL KAPCSOLATOS CSALÁSOK ÉS ÁTVERÉSEK

MARADJON ÉBER ÉS VÉDJE MEG MAGÁT

A kriptoeszközök számának/mennyiségének gyors növekedése és sajátos jellemzőik – globális hozzáférhetőség, gyorsaság, anonimitás és gyakran a tranzakciók visszafordíthatatlansága – a kiberbűnözők elsődleges célpontjává teszik Önt. A csalók kifinomult taktikákat alkalmaznak az Ön átverésére, például „Ponzi-rendszereket", hamis befektetési lehetőségeket, ingyenes ajánlatokat a közösségi médiában és hamis üzeneteket. Romantikus befektetési csalásokat vagy hasonmás címeket is használnak a pénztárcája feltörésére. Elérhetik Önt a közösségi médián, üzenetküldő alkalmazásokon, e-mail-eken és valósnak tűnő váratlan telefonhívásokon keresztül. 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 esetleges kripto-csalásokkal és átverésekkel kapcsolatban:
a csalások és átverések különböző típusairól további (részleteket az 5-8. oldalon talál).

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

Védje meg magát és vagyonát:
biztosítsa személyes adatait (részletek a 3. oldalon).

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.

Kéretlen ajánlat.

Garantáltan gyors és magas megtérülés.

Cselekvésre sürget (pl. korlátozott idejű ajánlatok, amelyek azonnali cselekvésre kényszerítik Önt).

Fizetési kérelem nyomon követhetetlen fizetési módok alkalmazásával (pl. kriptovaluták, ajándékkártyák, nem banki pénzküldések vagy előre feltöltött fizetési kártyák).

Egy linkre való kattintásra, QR-kód beolvasására vagy egy alkalmazás letöltésére történő felhívás.

Kérés privát kulcsok és helyreállító kifejezések küldésére vagy megosztására (szavak listája a kriptotárca eléréséhez és helyreállításához).

Gyanús vagy helytelen URL.

Kisebb torzulásokat mutató logó: olyan weboldal, amely egy valódi vállalat weboldalának kinézetét másolja, ami bár professzionálisnak tűnik, de nem rendelkezik ellenőrzött elérhetőségekkel, cégnyilvántartási információkkal, nyilvántartási adatokkal vagy ellenőrizhető jelenléttel.

Ismeretlen csereplatform.

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

Lépések az Ön védelme érdekében:

1 Álljon meg és gondolkodjon, mielőtt cselekszik!

Ne siessen a befektetéssel, az információk megosztásával vagy a linkekre való kattintással – a csalók szándékosan a sürgősség érzetét keltik. Bármilyen kétség esetén, még ha kisebb is, ne cselekedjen vagy fektessen be.

2 Gondosan ellenőrizze a forrást!

- Mindig ellenőrizze, hogy az üzenetek, hívások, e-mailek és linkek honnan származnak, még akkor is, ha hivatalosnak tűnnek, vagy úgy tűnik, hogy egy baráttól vagy családtagjától, vagy akár egy közszereplőtől származnak. Keresse meg a helyesírási hibákat, a furcsa URL-eket vagy a hiányzó biztonsági jelzéseket: például 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.
- Még akkor is, ha az ajánlat hivatalosnak tűnik, mindig ellenőrizze azt a vállalat honlapján, vagy ellenőrizze, hogy a közösségimédia-fiók hitelesített-e (pl. hivatalos jelölőnégyzetekkel).
- 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). A csalók azt állíthatják, hogy engedéllyel rendelkeznek, vagy utánozhatják egy engedélyezett vállalat weboldalát. Ellenőrizheti, hogy a kriptoeszköz-szolgáltató rendelkezik-e engedéllyel az EU-ban, ha megtekinti az ESMA nyilvántartását (↖). A nemzeti pénzügyi hatóság honlapján (https://www.mnb.hu/felugyelet/piacfelugyelet/befektetoi-figyelmeztetesek) is tájékozódhat arról, hogy kiadtak-e figyelmeztetéseket vagy feketelistákat, illetve az IOSCO I-SCAN listáján (iosco.org/i-scan/).

3 Soha ne osszon meg jelszavakat, privát kulcsokat vagy helyreállító kifejezéseket:

Bárki, aki hozzáfér ezekhez, átveheti az irányítást a vagyona felett. A törvényes vállalatok soha nem fogják kérni jelszavait vagy biztonsági kódjait e-mailben, szöveges üzenetben vagy telefonon.

4 Tartsa az eszközöket és a privát kulcsokat biztonságban:

Használjon erős és egyedi jelszavakat minden egyes kriptoszámlájához, tartsa titokban jelszavát, és kerülje ugyanazon hitelesítő adatok újrafelhasználását különböző platformokon. Lehetőség szerint engedélyezze a többtényezős hitelesítést. Tartsa naprakészen és aktiválva szoftverét és vírusvédelmét.

5 Legyen óvatos a lehengerlő befektetési ajánlatokkal:

Óvakodjon azoktól a befektetésektől, amelyek hatalmas megtérülést ígérnek. Ha túl jól hangzik ahhoz, hogy igaz legyen, akkor valószínűleg nem is az.

6 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, és blokkolja a feladót.

Módosítsa a jelszavakat az összes eszközén és alkalmazásában / webhelyen:

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 fel újra őket.

A hozzáférés leválasztása és visszavonása:

Vonja vissza a gyanús engedélyeket a digitális megállapodásban, amelyek automatikusan futnak a blokkláncon (intelligens szerződés), annak érdekében, hogy megakadályozza a csalókat abban, hogy a beleegyezése nélkül költsék el a tokeneket. Számos pénztárca és blokklánc felfedező kínál olyan eszközöket, amelyek lehetővé teszik, hogy megtekintse, mely intelligens szerződések rendelkeznek jelenleg hozzáféréssel tokenjei elköltéséhez. Ennek érdekében a következőket teheti:

- megbízható „engedélyellenőrzőt” használ, amely ellenőrzi, hogy a felhasználó vagy a blokkláncím jogosult-e egy művelet végrehajtására,
- felülvizsgálja a jóváhagyások jegyzékét, és
- közvetlenül a platformról használja a „visszavonás” gombot.

Mozgassa át az eszközeit:

Ha a pénztárcája veszélybe kerül, azonnal helyezze át a fennmaradó eszközeit egy új, biztonságos pénztárcába.

Vegye fel a kapcsolatot kriptoszolgáltatójával:

Tájékoztassa kriptoszolgáltatóját a lehető leghamarabb a hivatalos kapcsolattartási csatornákon keresztül, hogy feltárja a lehetőségeket. Még akkor is, ha a legtöbb esetben a blokklánc-tranzakció visszafordítása nem lehetséges, a szolgáltató befagyaszthatja a csaló fiókját (ha az a szolgáltató platformján van), és feketelistára teheti a tárca címét.

Jelentés és riasztás:

Jelentse az eseményt a rendőrségnek és tájékoztassa kapcsolatait (pl. barátok és családtagok) a figyelemfelkeltés érdekében. Ezek az intézkedések a legjobb módjai annak, hogy megvédje önmagát és másokat.

Óvakodjon a pénz visszaszerzését ígérő, „recovery room” típusú csalástól:

A csaló kapcsolatba léphet Önnel, mint egy korábbi csalás áldozatával, 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: ha egyszer átverték, az nem zárja ki, hogy újra megtegyék.

Tekintse meg az európai felügyeleti hatóságok közös figyelmeztetését a kriptoeszközökkel kapcsolatos kockázatokról (https://www.mnb.hu/letoltes/updated-joint-esas-revised-warning-on-crypto-assets-hu.pdf) és a „Kriptoeszközök magyarázata: Mit jelent Önnek mint fogyasztónak a MiCA?” (https://www.mnb.hu/letoltes/updated-joint-esas-factsheet-on-crypto-assets-hu.pdf) című információs dokumentumot.

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

PDF ISBN 978-92-9407-255-9 doi:10.2853/5974794 DZ-01-25-143-HU-N

A KRIPTO-CSALÁSOK TÍPUSAI

„Pump-and-dump” rendszer vagy „rug pull” rendszer

Hirdetést lát a közösségi médiában vagy egy olyan weboldalon, amely „korlátozott idejű befektetési lehetőséget” kínál a kriptovaluták terén, és új kriptotokenbe vagy projektbe való befektetést javasol. Érdeklődésének kifejezése után kapcsolatba lépnek Önnel, és átirányítják egy kripto-csere platformra vagy üzenetküldő csatornára (például Telegram, Viber vagy WhatsApp). A látszólag hiteles kapcsolat gyors nyereséget vagy magas hozamot ígér, ha azonnal befektet. Arra ösztönzik, hogy fektessen be egy kis összeget, majd nyomást gyakorolnak Önre annak érdekében, hogy többet fektessen be.

Mi történhet?

Rájön, hogy a befektetett token értéktelen, és a kapcsolati partner nem válaszol. Amikor megpróbálja visszahívni a pénzét, a weboldal már nem létezik, és a vállalat elérhetetlen. A csalók mesterségesen felfújták vagy túlbecsülték egy alacsony értékű kriptoeszköz forgalmát és/vagy árát, hogy növeljék annak értékét („pump”), majd eladták az eszközeiket („dump”), ami az érték összeomlásához vezetett, és veszteségeket okozott a befektetőknek. Alternatív megoldásként leállíthatják a projektet, és az eszközökkel együtt eltűnhetnek („rug pull”).

Megszemélyesítéses csalás („Impersonation scam”)

Miután feltett egy kérdést egy közösségimédia-platformon vagy egy weboldalon egy kriptotárca-problémával kapcsolatban, váratlanul közvetlen üzenetet (DM) vagy e-mailt kap valakitől, aki úgy tesz, mintha megbízható kapcsolati partner lenne (pl. kriptotőzsde, pénztárca-szolgáltató, informatikai támogatás vagy akár egy barát). A személy kéri a helyreállító kifejezést (seed phrase), azaz a szavak sorozatát, amely központi biztonsági mentésként szolgál a digitális pénztárcájához való hozzáféréshez, jelszavakat vagy privát kulcsokat (automatikusan generált kriptográfiai kód, amely bizonyítja a digitális eszközök tulajdonjogát).

Mi történhet?

Miután megosztotta a helyreállító kifejezést, jelszavakat vagy privát kulcsokat, a csaló arra használja ezeket, hogy ellopja a kripto- vagy más pénzeszközeit. Ne feledje, hogy a privát kulcsok elvesztése a kriptoeszközökhöz való hozzáférés és tulajdonjog végleges és visszafordíthatatlan elvesztését eredményezi. Ellentétben a banki tranzakciókkal, a kripto átutalások esetében ha az eszközök elvesztek, a helyreállítás szinte lehetetlen.

Adathalászat („Phishing”)

Váratlan üzenetet kap e-mailben, telefonon, felugró ablakban vagy a közösségi médiában, azt állítva, hogy az egy jól ismert kriptoeszköz-szolgáltatótól származik. Az üzenetben arra kérik, hogy jelentkezzen be vagy töltsön le egy új alkalmazást. Előfordulhat, hogy egy e-mailt is kap, amely úgy tűnik, hogy a kripto-pénztárca alkalmazásából származik, és arra ösztönzi Önt, hogy megoldja a biztonsági problémát egy nem hivatalos forrás által biztosított linkre kattintva, vagy az alkalmazás frissítésével.

Mi történhet?

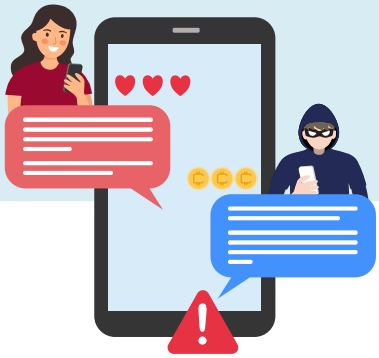
A linkre kattintva, az alkalmazás letöltésével vagy a QR-kód beolvasásával olyan rosszindulatú programot telepít, amely lehetővé teszi a csaló számára, hogy hozzáférjen és felhasználja az információkat a kriptoeszközeinek vagy a pénzeszközeinek ellopásához.

Nyereményjáték-átverés („Giveaway scam”)

Találkozik egy bejelentéssel a közösségi médiában, amely azt állítja, hogy a vállalatok egy, az Ön részéről történt kisösszegű kriptoeszköz-befektetést követően ajándékoznak kriptoeszközöket. Ezekbe beillesztenek egy olyan videót vagy posztot, amely egy – általában hamisan vagy engedély nélkül megszerzett – hírességről vagy márkáról készült fényképeket tartalmaz, és ígéretet tesz arra, hogy „megduplázza a kriptopénzét”, ha először pénzt küld. A logó, az elrendezés, a beszámolók és a használt nyelv professzionálisnak és hivatalosnak tűnnek, csakúgy, mint az a webhely, amelyre Önt átirányították.

Mi történhet?

Miután elküldte a pénzét, akkor nem kap semmit cserébe, és elvesztette a küldött pénzt. A nyereményjáték hamis volt, és a híresség eket vagy cégeket megszemélyesítő poszt vagy élő közvetítés célja az volt, hogy megtévessze Önt.



Romantikus befektetési csalás („Romance investment scam")

Olyan személy vette fel Önnel a kapcsolatot szociális médiában, társkereső alkalmazáson, vagy telefonon/ SMS-ben, akivel még nem találkozott a valós életben. Ez a személy gyakori, személyes és romantikus beszélgetéseket kezdeményezhet, hamis profilok használatával bizalmat építve. Fokozatosan irányítják a beszélgetést a pénzügyi lehetőségek felé, hatalmas nyereséget ajánlva kripto-befektetések útján, magas hozamok és alacsony kockázatok ígérete mellett befektetésre ösztönözve Önt. Segítenek Önnek létrehozni egy fiókot egy kis kezdeti befizetéssel annak érdekében, hogy a rendszer jogszerűnek tűnjön.

A csalók hamis online profilokat hoznak létre, és lopott vagy mesterséges intelligencia által generált képeket használnak, hogy közel kerülhessenek Önhöz.

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. Bizonyos esetekben a csalók felhasználhatják a csalás során szerzett információkat arra, hogy megcélozzák barátait, családját és személyazonosság-lopást kövessenek el, ami pénzügyi vagy jogi következményekkel járhat az Ön számára (pl. a csaló lopott pénztárcákat hitelesíthet az Ön nevében, és az ellenkező bizonyításáig Ön felelősségre vonható a neve alatt felhalmozott adósságokért vagy elkövetett bűncselekményekért).

Ponzi-rendszer

Felkérést kap arra, hogy vegyen részt egy olyan projektben, amely következetesen magas megtérülést ígér a kriptoeszköz-befektetésekből, gyakran beszámolókkal vagy hamis sikertörténetekkel alátámasztva. A rendszer többszintű marketing lehetőségként (MLM) is bemutatható, ahol nemcsak a saját befektetéséből, hanem mások toborzásával is pénzt keres. Úgy tűnik, hogy a korai befektetők kifizetéseket kapnak, ami több embert ösztönöz a rendszerhez való csatlakozásra és a rendszer népszerűsítésére.

A valóságban nem jön létre valódi üzlet vagy nyereség. Ehelyett a pénz kizárólag az újabb befektetők hozzájárulásából származik, amit a rendszer szervezőinek és első résztvevőinek történő hozamfizetésre használnak fel.

Mi történhet?

Amint az új befektetések lelassulnak, a rendszer összeomlik, és Ön, mint a legtöbb résztvevő, elveszíti a pénzét. A szervezők eltűnnek, így nincs mód az eszközök visszaszerzésére. A többszintű struktúra segíti az átverés gyors terjedését, mivel az áldozatok tudtukon kívül promóterekké válnak.

Egy hasonmás cím, ami megtéveszti a pénztárcádat

Miután végrehajtott egy kriptotranzakciót, észrevesz egy, a pénztárca előzményeiben megjelenő új címet. Ez a cím hasonlít ahhoz, amellyel korábban kapcsolatba lépett. A csalók hamis pénztárca címeket jeleníthetnek meg a tranzakciós előzményeiben, ha egy kis mennyiségű kriptovalutát küldenek egy hasonló címről a pénztárcájába. Végül a pénztárca legutóbbi tevékenységében tárolja, vagy automatikusan javasolja a csaló által létrehozott hamis címet. A csalók szándékosan hasonló címeket hoznak létre azáltal, hogy csak néhány karaktert módosítanak, gyakran a cím közepén, hogy elkerüljék az észlelést.

Mi történhet?

Amikor megpróbál kriptovalutát küldeni, és rossz címet másol a pénztárcája előzményeiből, tudtán kívül pénzt küld a csaló pénztárcájába. Mivel a kriptotranzakciók gyakran visszafordíthatatlanok, a pénze a legtöbb esetben végleg elvész. Ez a csalás a vizuális megtévesztésen és a felhasználói hibán alapul, kihasználva a pénztárca címek érdemi ellenőrzés nélküli másolásának és beillesztésének szokását.