PODVODY S KRYPTOAKTÍVAMI

BUĎTE OSTRAŽITÍ A CHRÁŇTE SA

Rýchly rast kryptoaktív a ich špecifické vlastnosti – celosvetová dostupnosť, rýchlosť, anonymita a často nezvratnosť transakcií – z vás robia hlavný cieľ pre páchateľov počítačovej kriminality. Podvodníci používajú sofistikované taktiky na to, aby vás oklamali, ako sú „Ponziho schémy“, falošné investičné príležitosti, bezplatné ponuky na sociálnych médiách a falošné správy. Používajú tiež romantické podvody alebo falošné adresy, aby otrávili vašu peňaženku. Často sa k Vám dostanú prostredníctvom sociálnych médií, aplikácii na odosielanie správ, e-mailov a neočakávaných hovorov, ktoré znejú dôveryhodne. Môžete čeliť rizikám, ako je finančná strata, krádež identity a emocionálna ujma.

Buďte opatrní a postupujte podľa týchto kľúčových tipov, aby zostali v bezpečí:

Buďte ostražití vo vzťahu k možným podvodom s kryptoaktívami:
ak sa chcete dozvedieť viac o rôznych druhoch podvodov (viď str. 5- 8).

Všimnite si varovné signály:
naučte sa rozpoznať podozrivé správanie, správy alebo ponuky (viď str. 2).

Chráňte seba a svoj majetok:
zabezpeč svoje osobné údaje (viď str. 3).

Zistite si čo robiť, ak sa stanete obeťou podvodu
(viď str.4).

Varovné signály

Sľub, ktorý sa zdá byť príliš dobrý na to, aby bol pravdivý.

Nevyžiadaná ponuka.

Zaručená rýchla a vysoká návratnosť.

Naliehavosť konať (napr. časovo obmedzené ponuky, ktoré vás nútia okamžite konať).

Žiadosť o platbu nevystopovateľnými spôsobmi (napr. kryptoaktívami, darčekovými kartami, bankovými prevodmi alebo predplatenými debetnými kartami).

Pozvánka na kliknutie na odkaz, naskenovanie QR kódu alebo stiahnutie aplikácie.

Žiadosť o odoslanie alebo zdieľanie súkromných kľúčov a “seed” fráz (zoznam slov na prístup a obnovenie vašej krypto peňaženky).

Podozrivá alebo nesprávna URL

Logo s miernymi deformáciami, webové sídlo, ktoré kopíruje vzhľad webového sídla skutočnej spoločnosti alebo vyzerá profesionálne, ale chýbajú mu overené kontaktné údaje, registračné informácie spoločnosti, záznamy alebo overiteľné sídlo.

Neznáma burza.

Podozrivá príloha, najmä .exe, .scr, .zip alebo súbor balíka Office s podporou makra (.docm, .xlsm).

Kroky, ako sa chrániť:

1 Zastavte sa a zamyslite sa skôr, ako začnete konať:

Neponáhľajte sa investovať, poskytnúť svoje osobné informácie alebo kliknúť na odkazy – podvodníci zámerne vytvárajú pocit naliehavosti. V prípade akýchkoľvek pochybností, dokonca aj menších, nekonajte alebo neinvestujte a overujte zdroj starostlivo.

2 Starostlivo skontrolujte zdroj:

- Vždy overte, odkiaľ prichádzajú správy, hovory, e-maily a odkazy, aj keď vyzerajú oficiálne, prípadne sa zdá, že pochádzajú od priateľa alebo vašej rodiny, alebo dokonca od verejnej osobnosti. Všímajte si pravopisné chyby, podivné adresy URL alebo chýbajúce bezpečnostné indikátory, napr. overte, či odkaz na webové sídlo obsahuje „s“ v „HTTPS“, aby ste sa uistili, že webové sídlo je bezpečné, a všimnite si prípadné pridané alebo chýbajúce písmená v názve spoločnosti.
- Neotvárajte odkazy z nevyžiadaných správ, inštalujte iba oficiálne aplikácie prostredníctvom dôveryhodných obchodov s aplikáciami a neskenujte neznáme QR kódy.
- Aj keď ponuka vyzerá oficiálne, vždy ju overte porovnaním s webovým sídlom spoločnosti alebo overte, či je účet na sociálnych médiách overený (napr. oficiálnymi kontrolnými značkami).
- Použite overené kontaktné údaje na priame oslovenie spoločnosti alebo jednotlivca a nikdy sa nespoliehajte na kontaktné informácie poskytnuté podozrivým podvodníkom (napr. vyhľadajte názov spoločnosti nezávisle, použite overené obchodné adresáre). Podvodníci môžu tvrdiť, že sú autorizovaní alebo napodobňujú webové sídlo autorizovanej spoločnosti. Overiť, či má poskytovateľ služieb kryptoaktív povolenie v EÚ, môžete tak, že skontrolujete register orgánu ESMA (). Takisto si môžete pozrieť web vnútroštátneho orgánu dohľadu nad finančným trhom () aby ste zistili, či boli vydané nejaké varovania alebo čiernu listinu, alebo zoznam IOSCO I-SCAN (iosco.org/i-scan/).

3 Nikdy nezdieľajte heslá, súkromné kľúče alebo “seed” frázy:

Ktokoľvek s prístupom k nim môže prevziať kontrolu nad vašimi aktívami. Legitímne spoločnosti nikdy nebudú žiadať o vaše heslá alebo bezpečnostné kódy prostredníctvom e-mailu, textu alebo telefónu.

4 Zabezpečte zariadenia a súkromné kľúče:

Používajte silné a jedinečné heslá pre každý z vašich krypto účtov, udržujte svoje heslo v tajnosti a vyhnite sa opätovnému používaniu rovnakých prístupových údajov na rôznych platformách. Ak je to možné, povoľte viacfaktorovú autentifikáciu. Pozrite si niekoľko tipov na heslá Aktualizujte a aktivujte svoj softvér a antivírusovú ochranu.

5 Buďte opatrní pri neočakávaných investičných ponukách:

Dávajte si pozor na investície, ktoré sľubujú obrovské výnosy. Ak ponuka znie príliš dobre na to, aby to bola pravda, pravdepodobne ide o podvod.

6 Premýšľajte predtým, ako budete zdieľať informácie na sociálnych médiách:

Chatové skupiny, fóra, príspevky na sociálnych médiách a fotografie môžu byť cenným zdrojom vedomostí pre podvodníkov. Odhalenie príliš veľa o sebe alebo vašich investíciách z vás môže urobiť ľahký cieľ.

Čo robiť, keď ste sa stali obeťou podvodu alebo podvodu

Okamžite zastaviť transakcie

S cieľom zablokovať akékoľvek ďalšie prevody na podozrivé účty a zabrániť ďalším stratám. Zastavte akýkoľvek kontakt s podvodníkmi – ignorujte ich hovory a e-maily a zablokujte odosielateľa.

Zmeňte svoje heslá na všetkých svojich zariadeniach a aplikáciách/webových stránkach.

Podvodníci kupujú uniknuté heslá online a skúšajú ich na viacerých účtoch. Zmeniť len jedno heslo nestačí. Uistite sa, že ich všetky zmeníte, aby ich podvodníci nemohli opätovne použiť.

Odpojiť a zrušiť prístup:

Zrušte podozrivé povolenia, ktoré sa automaticky spúšťajú na blockchaine (inteligentná zmluva), aby ste zabránili podvodníkom míňať vaše tokeny bez vášho súhlasu. Mnohé peňaženky a prehliadače blockchainu ponúkajú nástroje, ktoré vám umožnia zistiť, ktoré inteligentné zmluvy majú v súčasnosti prístup k míňaniu vašich tokenov. Na tento účel môžete:

- používať dôveryhodnú „kontrolu povolení“, ktorou sa overuje, či má používateľ alebo adresa blockchainu povolenie na vykonanie operácie.
- preskúmať zoznam schválení a
- použite tlačidlo „zrušiť“ priamo z platformy.

Presuňte svoje finančné prostriedky:

Ak je vaša peňaženka ohrozená, okamžite preneste zostávajúce aktíva do novej zabezpečenej peňaženky.

Obráťte sa na svojho poskytovateľa služieb kryptoaktív:

Čo najskôr informujte svojho poskytovateľa služieb kryptoaktív prostredníctvom oficiálnych kontaktných kanálov, aby ste preskúmali potenciálne možnosti. Aj keď vo väčšine prípadov nebude možné zvrátiť transakciu blockchainu, poskytovateľ môže stále zmraziť účet podvodníka (ak je na jeho platforme) a zapísať adresu peňaženky na čiernu listinu.

Správa a upozornenie:

Nahláste incident polícii alebo vášmu vnútroštátnemu orgánu dohľadu nad finančným trhom (https://podanie.nbs.sk/) a informujte svojich blízkych (priateľov a rodinu) s cieľom zvýšiť informovanosť. Tieto opatrenia sú najlepším spôsobom, ako chrániť seba a ostatných.

Pozor na „vymáhacie“ podvody:

Podvodník vás môže kontaktovať po tom, ako ste sa stali obeťou podvodu, pričom môže tvrdiť, že je orgánom verejnej moci (napr. políciou, daňovým alebo finančným orgánom atď.) a ponúknuť vám náhradu vašich stratených peňazí za poplatok. To je často ďalší pokus o podvod. Pamätajte si: byť raz podvedený nezabráni tomu, aby ste boli opäť podvedený.

Viac informácií o rizikách súvisiacich s kryptoaktívami nájdete v Upozornení na kryptoaktíva (↖) a v informačnom prehľade „Vysvetlenie kryptoaktív: Čo MiCA znamená pre vás ako spotrebiteľa” (↖)

Európsky orgán pre bankovníctvo, Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov, Európsky orgán pre cenné papiere a trhy, 2025

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2025

Reprodukcia je povolená len s uvedením zdroja.
Illustrations: © Nadezhda Buravleva / madedee / Orapun- StockAdobe.com.

PDF ISBN 978-92-9407-238-2 doi:10.2853/4778216 DZ-01-25-126-SK-N

TYPY PODVODOV S KRPTOAKTÍVAMI

Schéma „Pump-and-dump" alebo „Rug pull"

Na sociálnych médiách alebo na webovom sídle vidíte reklamu propagujúcu „investičnú príležitosť na obmedzený čas" v oblasti kryptoaktív, v ktorej sa odporúča investovať do nového tokenu alebo projektu. Po prejavení záujmu vás kontaktujú a presmerujú na platformu na výmenu kryptoaktív alebo na komunikačný kanál (napr. Telegram, Viber alebo Whatsapp). Zdanlivo dôveryhodný kontakt sľubuje rýchle zisky alebo vysoké výnosy, ak investujete rýchlo. Povzbudzuje vás, aby ste najskôr investovali malú sumu a potom na vás vyvíja tlak, aby ste investovali viac.

Čo sa môže stať:

Zistíte, že token je bezcenný a kontakt, s ktorým ste komunikovali prestal reagovať. Keď sa pokúsite vybrať svoje peniaze, webová stránka už neexistuje a spoločnosť je nedosiahnuteľná. Podvodníci umelo nafúkli alebo nadhodnotili kryptoaktívum („pump"), potom predali svoje aktíva („dump"), čo spôsobilo krach ceny a investorom zanechalo straty. Prípadne by mohli ukončiť projekt a zmiznúť s finančnými prostriedkami („rug pull").

Podvod s identitou

Po odoslaní otázky na platforme sociálnych médií alebo webovej stránke o probléme s krypto peňaženkou dostanete neočakávanú priamu správu (DM) alebo e-mail od niekoho, kto predstiera, že je dôveryhodným kontaktom (napr. kryptoburza, poskytovateľ peňaženky, IT podpora alebo dokonca priateľ). Osoba požiada o vašu "seed" frázu (t. j. sekvenciu slov, ktorá slúži ako centrálna záloha na prístup k vašej digitálnej peňaženke), heslá alebo súkromné kľúče (automaticky generovaný kryptografický kód, ktorý dokazuje vlastníctvo digitálnych aktív).

Čo sa môže stať:

Akonáhle zdieľate svoju "seed" frázu, heslo alebo súkromné kľúče, podvodník ich používa na ukradnutie vašich kryptomien alebo iných finančných prostriedkov. Majte na pamäti, že strata súkromných kľúčov má za následok trvalú a nezvratnú stratu prístupu a vlastníctva vašich kryptoaktív. Na rozdiel od bankových transakcií, v prípade prevodov kryptomaktív, akonáhle sú vaše finančné prostriedky preč, zotavenie je takmer nemožné.

Phishing

Dostanete neočakávanú správu prostredníctvom e-mailu, telefónu, kontextového okna alebo sociálnych médií, v ktorej sa uvádza, že je od známeho poskytovateľa služieb kryptoaktív. Správa vás vyzve, aby ste sa prihlásili alebo si stiahli novú aplikáciu. Môžete tiež dostať e-mail, ktorý sa zdá byť z vašej aplikácie krypto peňaženky, a vyzýva vás, aby ste vyriešili problém so zabezpečením kliknutím na odkaz poskytnutý neoficiálnym zdrojom alebo aktualizáciou aplikácie.

Čo sa môže stať:

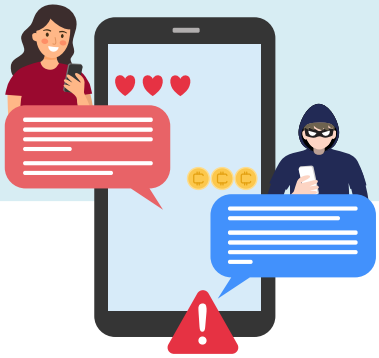
Kliknutím na odkaz, stiahnutím aplikácie alebo skenovaním QR kódu nainštalujete malvér, ktorý umožňuje podvodníkovi prístup k informáciám a ich použitie na krádež vašich kryptoaktív alebo finančných prostriedkov.

Giveaway podvod (Falošné rozdávanie)

Stretnete sa s oznámením na sociálnych médiách, ktoré tvrdí, že spoločnosti rozdávajú kryptoaktíva po malej investícii do kryptomien. Zahŕňajú video alebo príspevok s fotografiami celebrity alebo značky – zvyčajne falošnej alebo získanej bez povolenia – ktoré sľubujú „zdvojnásobenie vašich kryptoaktív“, ak im najprv pošlete peniaze. Logo, rozloženie, recenzie a použitý jazyk vyzerajú profesionálne a oficiálne, rovnako ako webová stránka, na ktorú ste presmerovaní.

Čo sa môže stať:

Po odoslaní vášho kryptoaktíva nedostanete nič na oplátku a stratíte odoslané peniaze. Giveaway bola falošná a príspevok alebo livestream, ktorý sa vydával za celebrity alebo spoločnosti, bol navrhnutý tak, aby vás oklamal.



Romantický investičný podvod

Boli ste kontaktovaní na sociálnych médiách, zoznamovacích aplikáciách alebo telefóne / SMS niekým, koho ste v reálnom živote nestretli. Táto osoba sa chce s vami zapojiť do častých, osobných a romantických rozhovorov a získava si vašu dôveru pomocou falošného profilu. Postupne vedie konverzáciu smerom k finančným príležitostiam, nárokuj si obrovské zisky z investícií do kryptoaktív a povzbudzuj vás, aby ste investovali s prísľubmi vysokých výnosov a nízkeho rizika. Sprevádza vás zriadením účtu a vykonaním malého počiatočného vkladu, aby sa systém zdal legitímny.

Podvodníci vytvárajú falošné online profily a používajú ukradnuté obrázky alebo obrázky vytvorené umelou inteligenciou, aby sa k vám priblížili.

Čo sa môže stať:

Podvodník vás oberie o čo najviac peňazí, potom preruší všetku komunikáciu a zmizne. Podvodné investičné webové stránky alebo aplikácie sú zrazu offline, takže nemáte prístup k údajným investíciám. V niektorých prípadoch môžu podvodníci použiť informácie získané počas podvodu na to, aby sa zamerali na vašich priateľov a rodinu a spáchali krádež totožnosti, ktorá môže mať pre vás finančné alebo právne dôsledky (napr. podvodník môže overiť ukradnuté peňaženky vo vašom mene a môžete byť zodpovedný za dlhy alebo trestné činy spáchané pod vaším menom, kým sa nepreukáže opak).

Ponziho schéma

Ste pozvaní zúčastniť sa na projekte, ktorý sľubuje konzistentne vysoké výnosy z investícií do kryptoaktív, často podložené svedectvami alebo falošnými úspešnými príbehmi. Schéma môže byť prezentovaná ako viacúrovňová marketingová príležitosť, kde získavate odmeny nielen z vlastnej investície, ale aj náborom iných. Skorší investori dostávajú výplácané prostriedky, čo povzbudzuje viac ľudí, aby sa pripojili a propagovali systém.

V skutočnosti neexistuje žiadny skutočný obchod alebo zisk, ktorý by sa vytváral. Peniaze namiesto toho pochádzajú výlučne z príspevku novších investorov, ktorý sa používa na vyplácanie výnosov organizátorom systému a prvým účastníkom.

Čo sa môže stať:

Akonáhle sa nové investície spomalia, schéma sa zrúti a vy, ako aj väčšina účastníkov, stratíte svoje peniaze. Organizátori zmiznú a nenechajú žiadny spôsob, ako získať späť finančné prostriedky. Viacúrovňová štruktúra pomáha, aby sa podvod šíril rýchlo a obete sa nevedomky stali propagátormi.

Podvrhnutie adresy

Po vykonaní transakcie s kryptoaktívami si všimnete, že sa vo vašej histórii peňaženky objavila nová adresa. Táto adresa vyzerá podobne ako adresa, s ktorou ste predtým komunikovali. Podvodníci môžu spôsobiť, že podvrhnuté adresy peňaženky sa zobrazia v histórii transakcií odoslaním malého množstva kryptoaktív z podobnej adresy do vašej peňaženky. Výsledkom je, že v zozname nedávnych aktivít alebo v automatických návrhoch vašej peňaženky zostane uložená falošná adresa podvodníka. Podvodníci zámerne vytvárajú podobné adresy zmenou len niekoľkých znakov, často uprostred adresy, aby sa vyhli detekcii.

Čo sa môže stať:

Keď sa pokúšate odoslať kryptoaktíva a skopírujete nesprávnu adresu z histórie peňaženky, nevedomky posielate finančné prostriedky do peňaženky podvodníka. Pretože transakcie s kryptoaktívami sú často nezvratné, vaše finančné prostriedky sú vo väčšine prípadov stratené natrvalo. Tento podvod sa opiera o vizuálny podvod a chybu používateľa, pričom využíva zvyk kopírovania a vkladania adries peňaženky bez dôkladnej kontroly.