KRYPTOMĚNOVÉ PODVODY

ZŮSTAŇTE VE STŘEHU A CHRAŇTE SE

Rychlý nárůst oblíbenosti kryptoaktiv a jejich specifické vlastnosti – celosvětová dostupnost, rychlost, anonymita a často nezvratnost transakcí – z Vás činí hlavní cíl pro pachatele kyberkriminality. Podvodníci používají sofistikované metody, aby Vás oklamali, jakými jsou např. tzv. „Ponziho schémata“, falešné investiční příležitosti, rozdávací akce na sociálních sítích a falešné zprávy. Navazují také falešné romantické vztahy, které zneužívají pro investiční podvody, nebo vytvářejí blízké napodobeniny Vám známých adres, kterými tzv. „otráví“ Vaši krypto-peněženku. Podvodníci s Vámi často naváží kontakt prostřednictvím sociálních sítí, aplikací pro zasílání zpráv, e-mailů a neočekávaných telefonátů, které zní skutečně. Můžete čelit rizikům, jako je finanční ztráta, krádež identity a citová úzkost.

Buďte opatrní a řiďte se těmito klíčovými doporučeními, abyste zůstali v bezpečí:

Mějte se na pozoru před možnými podvody s kryptoměnami:
Více o různých typech podvodů se dozvíte (viz str. 5, 6, 7 a 8);

Všimněte si varovných signálů:
Naučte se rozpoznat podezřelé chování, zprávy nebo nabídky (viz str. 2);

Chraňte sebe a svůj majetek:
zabezpečte si své osobní údaje (viz str. 3);

Vězte, co dělat, pokud se stanete obětí podvodu
(viz str. 4).

Varovné signály

Příslib, který se zdá být příliš dobrý na to, aby byl pravdivý.

Nevyžádaná nabídka.

Zaručená rychlá a vysoká návratnost.

Naléhavost jednání (např. časově omezené nabídky, které Vás nutí jednat okamžitě).

Žádost o platbu prostřednictvím nevysledovatelných metod (např. kryptoměnami, dárkovou kartou, bezhotovostním převodem nebo předplacenou debetní kartou).

Pozvánka ke kliknutí na odkaz, naskenování QR kódu nebo stažení aplikace.

Žádost o odeslání nebo sdílení soukromých klíčů a obnovovacích frází (posloupnost slov, která umožňuje obnovit přístup do Vaší krypto-peněženky).

Podezřelá nebo nesprávná URL adresa.

Mírně zkreslené logo, internetová stránka, která napodobuje vzhled webových stránek skutečné společnosti nebo vypadá profesionálně, ale postrádá ověřené kontaktní údaje, informace o registraci společnosti, záznamy o činnosti nebo ověřitelnou existenci.

Neznámá směnárenská platforma.

Podezřelá příloha, zejména soubor .exe, .scr, .zip nebo soubor Office s podporou maker (.docm, .xlsm).

Jak se chránit:

1 Zastavte se a zamyslete se, než začnete jednat:

Nespěchejte s investováním, sdílením informací nebo kliknutím na odkazy- podvodníci záměrně vytvářejí pocit naléhavosti. V případě jakýchkoli, i malých, pochybností, nejednejte ani neinvestujte a pečlivě ověřte daný zdroj.

2 Pečlivě prověřte zdroj:

- Vždy ověřte, odkud pocházejí zprávy, hovory, e-maily a odkazy, které jste obdrželi, a to i pokud vypadají oficiálně nebo se zdají být od přátel či Vaší rodiny, nebo dokonce veřejně známé osoby. Všímejte si pravopisných chyb, zvláštní URL adresy nebo chybějícího bezpečnostního ukazatele, např. ověřte, zda odkaz na internetové stránky obsahuje písmeno „s“ v předponě odkazu „HTTPS“, abyste se ujistili, že internetové stránky jsou zabezpečené. Zkontrolujte také, zda v názvu společnosti nejsou přidána nebo naopak nechybí písmena.
- Neotevírejte odkazy z nevyžádaných zpráv, instalujte si pouze oficiální aplikace prostřednictvím důvěryhodných obchodů s aplikacemi a neskenujte neznámé QR kódy.
- I když nabídka vypadá oficiálně, vždy ji porovnejte s webovými stránkami společnosti nebo zkontrolujte, zda je účet, který nabídku činí, ověřen na sociálních médiích (např. pomocí oficiálních značek u názvu profilu).
- Použijte ověřené kontaktní údaje k přímému oslovení společnosti nebo jednotlivce a nikdy se nespoléhejte na kontaktní údaje poskytnuté osobou, u které podezříváte, že by mohla být podvodníkem (např. nezávisle vyhledejte název společnosti, použijte ověřené obchodní adresáře). Podvodníci mohou tvrdit, že mají příslušnou licenci nebo mohou napodobovat webové stránky licencované společnosti. Zda je poskytovatel služeb souvisejících s kryptoaktivy povolen v EU, si můžete ověřit v rejstříku orgánu ESMA (). Můžete se také podívat na internetové stránky České národní banky () a zjistit, zda nebyla k dané osobě vydána nějaká varování, nebo se můžete podívat na seznam I-SCAN organizace IOSCO (iosco.org/i-scan/).

3 Nikdy nesdílejte svá hesla, soukromé klíče nebo obnovovací fráze:

Každý, kdo k nim má přístup, může převzít kontrolu nad Vaším majetkem. Licencované společnosti Vás nikdy nepožádají o Vaše hesla nebo bezpečnostní kódy e-mailem, zprávou nebo telefonicky.

4 Udržujte svá zařízení a soukromé klíče v bezpečí:

Používejte silná a jedinečná hesla pro každý z Vašich účtů s kryptoaktivy, udržujte své heslo v tajnosti a vyvarujte se opakovanému používání stejných přihlašovacích údajů na různých platformách. Pokud je to možné, povolte vícefaktorové ověřování. Zde naleznete několik tipů ohledně hesel (). Udržujte svůj software a antivirovou ochranu aktuální a aktivovanou.

5 Buďte opatrní při neočekávaných investičních nabídkách:

Dávejte si pozor na investice slibující vysoké výnosy. Pokud to zní příliš dobře na to, aby to byla pravda, pravděpodobně to pravda není.

6 Zamyslete se předtím, než budete sdílet informace na sociálních médiích:

Chatové skupiny, fóra, příspěvky na sociálních sítích a fotografie mohou být cenným zdrojem informací pro podvodníky. Pokud o sobě nebo svých investicích odhalíte příliš mnoho, můžete se stát snadným cílem pro podvodníky.

Co dělat, pokud jste se stali obětí podvodu

Okamžitě zastavte transakce,

abyste zablokovali další převody na podezřelé účty a vyhnuli se dalším ztrátám. Zastavte veškerý kontakt s podvodníky – ignorujte jejich hovory a e-maily a zablokujte si je jako odesílatele.

Změňte si hesla na všech svých zařízeních a aplikacích/webových stránkách.

Podvodníci nakupují uniklá hesla online a zkouší je na více účtech. Změnit pouze jedno heslo nestačí. Ujistěte se, že změníte všechna hesla, aby je podvodníci nemohli znovu použít.

Odpojte se a zrušte přístup.

Zrušte podezřelá oprávnění ve Vaší digitální smlouvě, která běží automaticky na blockchainu (tzv. chytré kontrakty – smart contracts), abyste zabránili podvodníkům v utrácení Vašich tokenů bez Vašeho souhlasu. Mnoho peněženek a průzkumníků blockchainu nabízí nástroje, které Vám umožní zjistit, které chytré kontrakty mají v současné době přístup k utrácení Vašich tokenů. Chcete-li tak učinit, můžete:

- používat důvěryhodnou „kontrolu oprávnění“, která ověřuje, zda je uživatel nebo adresa blockchainu oprávněná provádět operaci.
- přezkoumat seznam schválení a
- použít tlačítko „odvolat“ přímo na platformě.

Přesuňte své finanční prostředky.

Pokud je Vaše peněženka ohrožena, okamžitě převeďte svůj zbývající majetek do nové zabezpečené peněženky.

Obraťte se na svého poskytovatele služeb souvisejících s kryptoaktivy.

Co nejdříve informujte svého poskytovatele služeb souvisejících s kryptoaktivy prostřednictvím oficiálních kontaktních kanálů, abyste prozkoumali Vaše možnosti. I když ve většině případů nebude možné transakci na blockchainu zvrátit, poskytovatel může účet podvodníka (pokud je na jeho platformě) zmrazit a zařadit adresu jeho peněženky na černou listinu.

Nahlaste podvod a varujte své okolí.

Nahlaste incident policii a České národní bance (↖) a informujte své okolí (např. přátele a rodinu), abyste zvýšili i jejich povědomí o podvodu. Tím nejlépe ochráníte sebe i ostatní.

Pozor na tzv. „recovery room“ podvod.

Podvodník Vás může kontaktovat jako oběť předchozího podvodu, prohlašovat, že je orgánem veřejné moci (např. policie, daňový nebo finanční orgán atd.), a nabízet vrácení ztracených peněz za poplatek. To je často další pokus o to Vás podvést. Nezapomeňte: To, že jste byli jednou podvedeni, neznamená, že nemůžete být podvedeni znovu.

Podívejte se také na společné varování evropských orgánů dohledu, kde se dozvíte více o rizicích souvisejících s kryptoaktivy (↖). a informativní přehled „Kryptoaktiva srozumitelně: Co pro vás jako spotřebitele znamená nařízení MiCA“ (↖).

Evropský orgán pro bankovnictví, Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění, Evropský orgán pro cenné papíry a trhy, 2025

Lucemburk: Úřad pro publikace Evropské unie, 2025

PDF ISBN 978-92-9407-223-8 doi:10.2853/9679057 DZ-01-25-111-CS-N

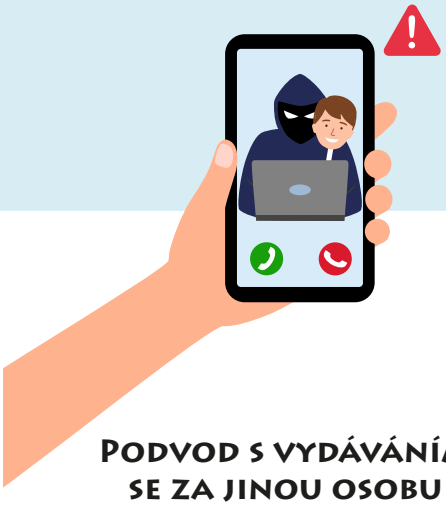
TYPY KRYPTOMĚNOVÝCH PODVODŮ

„PUMP-AND-DUMP" PODVODY NEBO „RUG PULL"

Na sociálních sítích nebo na internetových stránkách vidíte reklamu propagující „investiční příležitost na omezenou dobu" týkající se kryptoměn, která doporučuje investovat do nového tokenu nebo krypto projektu. Po vyjádření zájmu jste kontaktováni a přesměrováni na platformu pro směnu kryptoměn nebo na komunikační kanál (např. Telegram, Viber nebo WhatsApp). Zdánlivě důvěryhodá kontaktní osoba slibuje rychlé zisky nebo vysoké výnosy, pokud zainvestujete rychle. Jste povzbuzováni, abyste investovali malou částku a pak tlačeni investovat více.

Co se může stát:

Zjistíte, že token, do kterého jste investovali, je bezcenný a kontaktní osoba, se kterou jste byli v kontaktu, přestane reagovat. Když se pokusíte vybrat si peníze, webová stránka již neexistuje a společnost je nedostupná. Podvodníci uměle nafoukli cenu tokenu nebo nadhodnotili token nízké hodnoty s cílem zvýšit jeho hodnotu („pump"), poté prodali své tokeny („dump"), což způsobilo pád hodnoty tokenů ostatních a zanechalo investorům ztráty. Případně mohou podvodníci projekt ukončit a s finančními prostředky zmizet (tzv. „rug pull").



PODVOD S VYDÁVÁNÍM SE ZA JINOU OSOBU

Poté, co jste na sociální síť nebo webovou stránku napsali otázky ohledně problému s krypto peněženkou, obdržíte neočekávanou přímou zprávu (DM) nebo e-mail od někoho, kdo předstírá, že je důvěryhodnou kontaktní osobou (např. krypto-směnárna, poskytovatel peněženky, IT podpora nebo dokonce Váš kamarád). Osoba Vás požádá o Vaši obnovovací frázi (tj. posloupnost slov, která slouží jako záloha pro přístup k Vaší digitální peněžence), Vaše hesla nebo Vaše soukromé klíče (automaticky generovaný kryptografický kód, který prokazuje vlastnictví digitálních aktiv).

Co se může stát:

Jakmile se podělíte o svou obnovovací frázi, hesla nebo soukromé klíče, podvodník je použije k tomu, aby ukradl Vaše kryptoaktiva nebo jiné finanční prostředky. Mějte na paměti, že ztráta soukromých klíčů vede k trvalé a nevratné ztrátě přístupu a vlastnictví Vašich kryptoaktiv. Na rozdíl od některých bankovních transakcí, v případě převodů kryptoměn není možné Vám Vaše finanční prostředky vrátit, jakmile jsou převedeny pryč.

Phishing

Obdržíte neočekávanou zprávu prostřednictvím e-mailu, telefonu, vyskakovacího okna nebo sociálních sítí, která tvrdí, že pochází od známého poskytovatele služeb souvisejících s kryptoaktivy. Zpráva vás vyzývá k přihlášení se nebo stažení nové aplikace. Můžete také obdržet e-mail, který se zdá být z aplikace Vaší krypto peněženky a vyzývá Vás k vyřešení bezpečnostního problému kliknutím na odkaz zaslaný neoficiálním kontaktem nebo aktualizací aplikace.

Co se může stát:

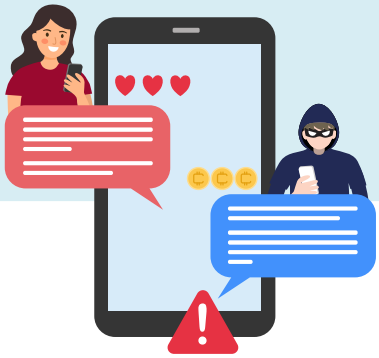
Kliknutím na odkaz, stažením aplikace nebo naskenováním QR kódu nainstalujete malware, který umožňuje podvodníkovi přístup a použití Vašich informací ke krádeži Vašich kryptoaktiv nebo Vašich finančních prostředků.

Rozdávací („giveaway") podvod

Narazíte na oznámení na sociálních sítích, které tvrdí, že jisté společnosti rozdávají kryptoaktiva poté, co učiníte malou investici do kryptoměn. Oznámení zahrnují video nebo příspěvek s fotografiemi celebrity nebo značky – obvykle falešné nebo získané bez povolení – které slibují, že pokud jim pošlete peníze, „zdvojnásobí Vám je v kryptoaktivech". Logo, design, odkazy a použitý jazyk vypadají profesionálně a oficiálně, stejně jako webová stránka, na kterou jste přesměrováni.

Co se může stát:

Po odeslání kryptoměny neobdržíte nic na oplátku a o zaslané peníze přijdete. Rozdávací kampaň byla falešná a příspěvek nebo živý přenos, který se vydával za celebrity nebo společnosti, byl navržen tak, aby Vás oklamal.



Romantické podvody

Byli jste kontaktováni na sociálních sítích, seznamovacích aplikacích nebo přes telefon či textovou zprávu někým, koho jste fyzicky nikdy nepotkali. Tato osoba se může zapojit do častých, osobních a romantických rozhovorů a budování důvěry pomocí falešných profilů. Postupně vede konverzaci směrem k finančním příležitostem, tvrdí Vám o svých vysokých ziscích z investic do kryptoaktiv a povzbuzuje Vás, abyste investovali s příslibem vysokých výnosů a nízkého rizika. Provede Vás zřízením účtu a provedením malého počátečního vkladu, aby se systém zdál legitimní.

Podvodníci vytvářejí falešné online profily a používají ukradené obrázky nebo obrázky vytvořené umělou inteligencí, aby Vás oslovili.

Co se může stát:

Podvodník z Vás vyláká co nejvíce peněz, pak přeruší veškerou komunikaci a zmizí. Podvodné investiční webové stránky nebo aplikace jsou offline, takže nemáte přístup k Vašim domnělým investicím. V některých případech mohou podvodníci použít informace získané během podvodu k tomu, aby se zaměřili na Vaše přátele a rodinu a dopustili se krádeže identity, která pro Vás může mít finanční nebo právní důsledky (např. podvodník může ověřit ukradené peněženky vaším jménem a Vy můžete být činěni odpovědnými za dluhy nebo trestné činy spáchané pod Vaším jménem, dokud se neprokáže opak).

Ponziho schéma

Jste přizváni k účasti na projektu, který slibuje konzistentní vysoké výnosy z investic do kryptoaktiv, často podpořené svědectvími nebo falešnými příběhy o úspěchu. Schéma může být prezentováno jako víceúrovňová marketingová příležitost, kde získáte odměny nejen z vlastní investice, ale také náborem dalších. Zdá se, že počátečním investorům jsou vypláceny výnosy, což povzbuzuje více lidí, aby se do systému zapojili a propagovali jej.

Ve skutečnosti neexistuje žádný skutečný projekt nebo zisk. Místo toho pocházejí peníze výhradně z investic novějších investorů, které se používají k výplatě výnosů organizátorům a prvním účastníkům schématu.

Co se může stát:

Jakmile se příliv nových investic zpomalí, schéma se zhroutí a Vy, stejně jako většina účastníků, přijdete o své peníze. Pořadatelé zmizí a nezanechají žádný způsob, jak získat finanční prostředky zpět. Víceúrovňová struktura pomáhá podvod rychle šířit, protože se oběti nevědomky stávají jeho propagátory.

Napodobeniny Vám známých adres, které „otráví" Vaši peněženku

Po provedení transakce s kryptoaktivy si všimnete nové adresy, která se objeví v historii Vaší peněženky. Tato adresa vypadá podobně jako adresa, se kterou jste dříve komunikovali. Podvodníci mohou způsobit, že se falešné adresy peněženky objeví ve Vaší historii transakcí tím, že pošlou malé množství kryptoměny z adresy podobné Vaší peněžence. Nakonec uložíte do své peněženky nedávnou aktivitu nebo se Vám automaticky navrhne falešná adresa vytvořená podvodníkem. Podvodníci záměrně vytvářejí podobné adresy změnou pouze několika znaků, často uprostřed adresy, aby se zabránilo jejich odhalení.

Co se může stát:

Když se pokusíte odeslat kryptoaktiva, zkopírujete nesprávnou adresu z historie Vaší peněženky a nevědomky pošlete finanční prostředky do peněženky podvodníka. Vzhledem k tomu, že transakce s kryptoaktivy jsou často nevratné, ztratíte ve většině případů Vaše finanční prostředky trvale. Tento podvod staví na vizuálním podvodu a chybě uživatele, přičemž využívá zvyk kopírovat a vkládat adresy peněženky bez důkladné kontroly.