FRAUDE & ESCROCHERII CU CRIPTO

FIȚI VIGILENȚI ȘI PROTEJAȚI-VĂ

Răspândirea rapidă a criptoactivelor și caracteristicile lor specifice – accesibilitatea la nivel mondial, viteza, anonimatul și, adesea, ireversibilitatea tranzacțiilor – vă transformă într-o țintă principală pentru infractorii cibernetici. Impostorii și escrocii utilizează tactici sofisticate pentru a vă păcăli, cum ar fi „schemele Ponzi", oportunitățile de investiții false, ofertele gratuite pe platformele de comunicare socială și mesajele false. Ei folosesc, de asemenea, escrocherii cu investiții romantice sau adrese asemănătoare pentru a vă goli portofelul. Ele ajung adesea la dvs. prin intermediul social media, aplicații de mesagerie, e-mailuri și apeluri telefonice neașteptate care sună real. S-ar putea să vă confruntați cu riscuri cum ar fi pierderea financiară, furtul de identitate și suferința emoțională.

Fiți precauți și urmați aceste sfaturi cheie pentru a rămâne în siguranță:

Fiți atenți la posibilele fraude și înșelătorii cu criptomonede:
Învățați mai multe despre diferitele tipuri de fraude și escrocherii (vedeți paginile 5, 6, 7 și 8).

Identificați semnalele de alarmă:
învățați să recunoașteți comportamentele, mesajele sau ofertele suspecte (vedeți pagina 2).

Protejați-vă pe dumneavoastră și bunurile dumneavoastră:
securizați-vă informațiile dumneavoastră cu caracter personal (vedeți pagina 3).

Aflați ce trebuie să faceți dacă sunteți victima unei fraude sau a unor escrocherii
(vedeți pagina 4).

Semne de avertizare

O promisiune care pare prea bună pentru a fi adevărată.

O ofertă nesolicitată.

Un randament rapid și ridicat despre care se spune că este garantat.

Urgența de a acționa (de exemplu, oferte limitate în timp care vă presează să acționați imediat).

O cerere de plată prin metode ce nu pot fi urmărite (de exemplu, criptomonede, carduri cadou, transferuri bancare sau carduri de debit preplătite).

O invitație de a face clic pe un link, de a scana un cod QR sau de a descărca o aplicație.

O cerere de a trimite sau partaja chei private și fraze de recuperare (lista de cuvinte pentru a accesa și recupera portofelul dvs. cripto).

URL suspect sau incorect.

Logo cu mici distorsiuni, un site de internet care copiază aspectul site-ului de internet al unei societăți reale sau care arată credibil, dar nu dispune de date de contact verificate, de informații privind înregistrarea societății, de un istoric sau de o prezență verificabilă.

Platformă de schimb necunoscută.

Un atașament suspect, în special fișierul Office .exe, .scr, .zip sau cu macro-activat (.docm, .xlsm).

Pași pentru a vă proteja:

1 Opriți-vă și gândiți-vă înainte de a acționa:

Nu vă grăbiți să investiți, să faceți schimb de informații sau să faceți clic pe linkuri – escrocii creează în mod deliberat un sentiment de urgență. În caz de îndoieli, chiar minore, nu acționați sau investiți și verificați cu atenție sursa.

2 Verificați cu atenție sursa:

- Verificați întotdeauna de unde provin mesajele, apelurile, e-mailurile și link-urile, chiar dacă par oficiale, par să provină de la un prieten sau de la familia dvs. sau chiar de la o persoană publică. Căutați erori de ortografie, adrese URL ciudate sau indicatori de securitate care lipsesc, de exemplu, verificați dacă link-ul site-ului web include un „s” în „HTTPS” pentru a vă asigura că site-ul web este securizat și verificați dacă există litere adăugate sau lipsă în numele societății.
- Nu deschideți link-uri din mesaje nesolicitate, instalați numai aplicații oficiale prin intermediul magazinelor de aplicații de încredere și nu scanați coduri QR necunoscute.
- Chiar dacă o ofertă pare oficială, verificați-o întotdeauna prin comparație cu site-ul web al societății sau verificați dacă contul de pe platformele de comunicare socială este verificat (”verified”) (de exemplu, cu marcaje oficiale).
- Utilizați datele de contact verificate pentru a ajunge direct la societate sau la persoana fizică și nu vă bazați niciodată pe informațiile de contact furnizate de persoana suspectată de fraudă (de exemplu, căutați numele societății în mod independent, utilizați anuare profesionale verificate). Este posibil ca escrocii să pretindă că sunt autorizați sau să imite site-ul web al unei companii autorizate. Puteți verifica dacă furnizorul de criptomonede este autorizat în UE verificând registrul ESMA (↖). De asemenea, puteți consulta site-ul autorității financiare naționale din țara dumneavoastră pentru a vedea dacă au fost emise avertismente sau liste negre sau lista I-SCAN a IOSCO (iosco.org/i-scan/).

3 Nu partajați niciodată parole, chei private sau fraze de recuperare:

Oricine are acces la ele poate prelua controlul asupra activelor dvs. Companiile legitime nu vă vor solicita niciodată parolele sau codurile de securitate prin e-mail, text sau telefon.

4 Păstrați dispozitivele și cheile private în siguranță:

Utilizați parole puternice și unice pentru fiecare dintre conturile dvs. cripto, păstrați-vă parola secretă și evitați reutilizarea acelorași date de autentificare pe platforme diferite. Activați autentificarea multi-factor acolo unde este posibil. A se vedea câteva sfaturi privind parolele aici (↖). Păstrați software-ul și protecția antivirus actualizate și activate.

5 Fiți precauți cu privire la ofertele de investiții neașteptate:

Fiți atenți la investițiile care promit profituri uriașe. Dacă sună prea bine ca să fie adevărat, probabil că este.

6 Gândiți-vă înainte de a partaja informații pe platformele de comunicare socială:

Grupurile de chat, forumurile, postările de pe platformele de comunicare socială și fotografiile pot fi surse valoroase de cunoștințe pentru autorii fraudelor. Dezvăluirea prea multor lucruri despre dvs. sau despre investițiile dvs. vă pot face o țintă ușoară.

Ce trebuie să faceți atunci când ați devenit victima unei fraude sau a unei înșelătorii

Opriți imediat tranzacțiile

Pentru a bloca orice transferuri ulterioare către conturi suspecte și pentru a evita pierderi suplimentare. Opriți orice contact cu escrocii – ignorați apelurile și e-mailurile acestora și blocați expeditorul.

Schimbați-vă parolele pe toate dispozitivele și aplicațiile/site-urile web:

Escrocii cumpără parole compromise online și le încearcă pe mai multe conturi. Schimbarea unei singure parole nu este suficientă; asigurați-vă că le schimbați pe toate, astfel încât autorii fraudelor să nu le poată reutiliza.

Deconectarea și revocarea accesului:

Revocați permisiunile suspecte din acordul dvs. digital care rulează automat pe blockchain (contract inteligent) pentru a opri escrocii să vă cheltuiască token-urile fără consimțământul dvs. Multe portofele și exploratori blockchain oferă instrumente care vă permit să vedeți care contracte inteligente au acces în prezent pentru a cheltui token-urile. Pentru a face acest lucru, puteți:

- să utilizați un „verificator de permisiune” de încredere, care verifică dacă un utilizator sau o adresă blockchain este autorizată să execute o operațiune,
- revizuiți lista aprobărilor și
- să utilizați butonul „revocă” direct de pe platformă.

Mutați-vă fondurile:

Dacă portofelul dvs. este compromis, transferați imediat activele rămase într-un nou portofel securizat.

Contactați furnizorul dvs. de criptomonede:

Să vă informați furnizorul de criptomonede cât mai curând posibil, utilizând canalele oficiale de contact, pentru a explora opțiunile potențiale. Chiar dacă, în majoritatea cazurilor, inversarea tranzacției blockchain nu va fi posibilă, furnizorul ar putea totuși să înghețe contul escrocului (dacă acesta se află pe platforma sa) și să includă pe lista neagră adresa portofelului.

Raport și alertă:

Raportați incidentul poliției sau autorității naționale de supraveghere financiară din țara dumneavoastră și informați rețeaua dumneavoastră (de exemplu, prietenii și familia) pentru a crește gradul de conștientizare. Aceste acțiuni sunt cel mai bun mod de a vă proteja pe dvs. și pe ceilalți.

Atenție la frauda legată de „camera de recuperare”:

Escrocul vă poate contacta ținând cont de calitatea dvs. de victimă a unei înșelătorii anterioare, pretinzând că este o autoritate publică (de exemplu, poliție, autoritate fiscală sau financiară etc.) și oferindu-se să vă ajute să recuperați banii pierduți în schimbul unei taxe. Aceasta este adesea o altă încercare de a vă înșela. Nu uitați: a fi înșelat o dată nu vă împiedică să fiți înșelat din nou.

A se vedea avertismentul autorităților europene comune de supraveghere pentru a afla mai multe despre riscurile legate de criptoactive „Avertisment privind Criptoactivele” (↖) și fișa informativă „Criptoactivele explicate: Ce înseamnă MiCA pentru dumneavoastră în calitate de consumator” (↖).

Autoritatea Bancară Europeană, Autoritatea Europeană de Asigurări și Pensii Ocupaționale, Autoritatea Europeană pentru Valori Mobiliare și Piețe, 2025

Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2025

PDF ISBN 978-92-9407-268-9 doi:10.2853/9066058 DZ-01-25-157-RO-N

TIPURI DE ESCROCHERII CU CRIPTO

Schema „ umflă prețul, apoi vinde" sau „rug pull"

Veți vedea o reclamă (un anunț) pe platformele de comunicare socială sau pe un site web care promovează o „oportunitate de investiții pe termen limitat" în criptomonede, recomandând să investiți într-un nou token cripto sau într-un nou proiect cripto. După exprimarea interesului, sunteți contactat și redirecționat către o platformă de schimb cripto sau un canal de mesagerie (de exemplu, Telegram, Viber sau WhatsApp). Un contact aparent credibil promite profituri rapide sau randamente ridicate dacă investiți rapid. Sunteți încurajat să investiți o sumă mică și apoi presat să investiți mai mult.

Ce s-ar putea întâmpla:

Descoperiți că token-ul investit este lipsit de valoare și contactul cu care ați fost în legătură nu mai răspunde. Când încercați să vă retrageți banii, site-ul nu mai există, iar compania este de negăsit. Înșelătorii au umflat sau au supraestimat în mod artificial un criptoactiv cu valoare scăzută pentru a-i crește valoarea („pump"), apoi și-au vândut activele („dump"), cauzând prăbușirea valorii și lăsând investitorii cu pierderi. Alternativ, aceștia ar putea să închidă proiectul și să dispară odată cu fondurile („rug pull").

Înșelătorie prin uzurparea identității

După ce ați postat o întrebare pe o platformă de social media sau pe un site web despre o problemă de portofel cripto, primiți un mesaj direct neașteptat (DM) sau un e-mail de la cineva care pretinde a fi un contact de încredere (de exemplu, un schimb de criptomonede, un furnizor de portofel, suport IT sau chiar un prieten). Persoana solicită fraza dvs. de recuperare (adică secvența de cuvinte care servește drept copie de rezervă centrală pentru accesarea portofelului dvs. digital), parole sau chei private (un cod criptografic generat automat care dovedește proprietatea asupra activelor digitale).

Ce s-ar putea întâmpla:

Odată ce partajați fraza de recuperare, parolele sau cheile private, escrocul le folosește pentru a vă fura criptoactivele sau alte fonduri. Rețineți că pierderea cheilor private duce la pierderea permanentă și ireversibilă a accesului și a dreptului de proprietate asupra criptoactivelor dumneavoastră. Spre deosebire de tranzacțiile bancare, în cazul transferurilor criptografice, odată ce fondurile dvs. au dispărut, recuperarea este aproape imposibilă.

Phishing

Primiți un mesaj neașteptat prin e-mail, telefon, pop-up sau social media, pretinzând că este de la un furnizor de criptoactive bine-cunoscut. Mesajul vă invită să vă conectați sau să descărcați o nouă aplicație. De asemenea, este posibil să primiți un e-mail care pare să provină din aplicația dvs. de portofel cripto, care vă îndeamnă să rezolvați o problemă de securitate făcând clic pe un link furnizat de o sursă neoficială sau actualizând aplicația.

Ce s-ar putea întâmpla:

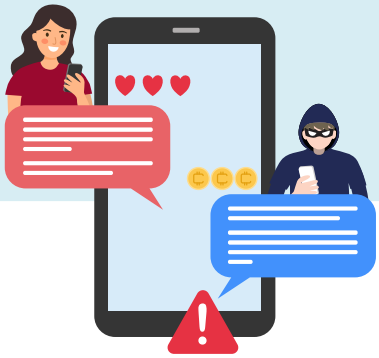
Făcând clic pe link, descărcând aplicația sau scanând un cod QR, instalați un malware care permite escrocului să acceseze și să utilizeze informațiile pentru a vă fura criptoactivele sau fondurile.

Înșelătorie prin cadouri

Ați dat peste un anunț pe social media care susține că companiile oferă criptoactive suplimentare după o mică investiție în respectivele criptoactive. Acestea includ un videoclip sau o postare cu fotografii ale unei celebrități sau ale unei mărci – de obicei false sau obținute fără autorizație – care promite să vă „dubleze deținerile de criptoactive” dacă trimiteți bani mai întâi. Logo-ul, aspectul, mărturiile și limba utilizată arată profesional și oficial, la fel ca și site-ul web către care sunteți redirecționat.

Ce s-ar putea întâmpla:

După ce trimiteți cripto, nu primiți nimic în schimb și ați pierdut banii trimiși. Cadoul era fals, iar postarea sau transmisia în direct care imita celebrități sau companii au fost concepute pentru a vă înșela.



Înșelătorie romantică cu investiții

Ați fost contactat pe social media, prin aplicații de cunoaștere a unor potențiali parteneri sau telefon / text de către cineva pe care nu l-ați întâlnit în viața reală. Această persoană poate iniția conversații frecvente, personale și romantice, construind încredere folosind profiluri false. Treptat, ei orientează conversația spre oportunități financiare, pretinzând profituri uriașe din investiții în cripto și încurajându-vă să investiți cu promisiuni de randament ridicat și risc scăzut. Acestea vă ghidează prin crearea unui cont și efectuarea unui mic depozit inițial pentru a face schema să pară legitimă.

Escrocii creează profiluri online false și folosesc imagini furate sau generate de inteligența artificială pentru a vă aborda.

Ce s-ar putea întâmpla:

Escrocul extrage cât mai mulți bani posibil, apoi întrerupe orice comunicare și dispare. Site-ul sau aplicația de investiții frauduloase devine offline, lăsându-vă fără acces la presupusele investiții. În unele cazuri, escrocii pot utiliza informațiile obținute în timpul înșelăciunii pentru a vă viza prietenii și familia și pentru a comite furt de identitate care poate avea consecințe financiare sau juridice pentru dumneavoastră (de exemplu, autorul fraudei poate verifica portofelele furate în numele dumneavoastră și ați putea fi tras la răspundere pentru datorii sau infracțiuni comise sub numele dumneavoastră până la proba contrarie).

Schema Ponzi

Sunteți invitat să participați la un proiect care promite randamente consistente ridicate ale investițiilor în criptoactive, adesea susținute de mărturii sau de povești de succes false. Schema poate fi prezentată ca o oportunitate de marketing pe mai multe niveluri, în care câștigați recompense nu numai din propria investiție, ci și prin recrutarea altora. Investitorii timpurii par să primească plăți, încurajând mai multe persoane să se alăture și să promoveze schema.

În realitate, nu există nicio afacere reală sau profit generat. În schimb, banii provin exclusiv din contribuția investitorilor mai noi, care este utilizată pentru a plăti venituri organizatorilor și primilor participanți la sistem.

Ce s-ar putea întâmpla:

Odată ce noile investiții încetinesc, schema se prăbușește și, la fel ca majoritatea participanților, vă pierdeți banii. Organizatorii dispar, nelăsând nicio modalitate de recuperare a fondurilor. Structura pe mai multe niveluri ajută înșelătoria să se răspândească rapid, pe măsură ce victimele devin promotori în necunoștință de cauză.

O ADRESĂ ASEMĂNĂTOARE CARE VĂ GOLEȘTE PORTOFELUL

După efectuarea unei tranzacții cu cripto, observați o nouă adresă care apare în istoricul portofelului dvs. Această adresă arată similar cu cea cu care ați interacționat anterior. Escrocii pot face ca adresele portofelului fals să apară în istoricul tranzacțiilor dvs. prin trimiterea unei cantități mici de criptomonede de la o adresă asemănătoare către portofelul dvs. Veți ajunge să stocați în activitatea recentă a portofelului dvs. sau în autosugestii adresa falsă creată de escroc. Escrocii creează în mod deliberat adrese asemănătoare, schimbând doar câteva caractere, adesea în mijlocul adresei, pentru a evita detectarea.

Ce s-ar putea întâmpla:

Atunci când încercați să trimiteți criptomonede și să copiați adresa greșită din istoricul portofelului, trimiteți în necunoștință de cauză fonduri în portofelul escrocului. Deoarece tranzacțiile cripto sunt adesea ireversibile, în majoritatea cazurilor fondurile dvs. sunt pierdute permanent. Această înșelătorie se bazează pe înșelăciunea vizuală și pe eroarea utilizatorului, exploatând obiceiul de a copia și lipi adresele portofelului fără o inspecție atentă.