CRYPTOFRAUDE & OPLICHTING

BLIJF ALERT EN BESCHERM UZELF

De snelle groei van cryptoactiva en de specifieke kenmerken ervan – wereldwijde toegankelijkheid, snelheid, anonimiteit en vaak onomkeerbaarheid van transacties – maken gebruikers tot een aantrekkelijk doelwit voor cybercriminelen. Fraudeurs en oplichters gebruiken geavanceerde strategieën van fraude en oplichting, zoals “Ponzifraude”, valse investeringsmogelijkheden, gratis aanbiedingen op sociale media, valse berichten, datingfraude en ”address poisoning”. Ze bereiken u vaak via sociale media, e-mail, onverwachte telefoontjes en berichten die echt lijken. U loopt risico op financieel verlies, identiteitsdiefstal en emotionele schade.

Wees voorzichtig en volg deze tips om veilig te blijven:

Blijf alert voor mogelijke cryptofraude en oplichting:
Voor meer informatie over verschillende soorten fraude en oplichting (blz. 5, 6, 7 en 8)

Let op waarschuwingssignalen:
leer verdacht gedrag, verdachte berichten en verdachte aanbiedingen te herkennen (blz. 2)

Bescherm uzelf en uw bezittingen:
beveilig persoonsgegevens (blz. 3)

Weet wat u moet doen als u het slachtoffer wordt van fraude of oplichting
(blz. 4).

Waarschuwingssignalen

Een belofte die te mooi lijkt om waar te zijn.

Een ongevraagd aanbod.

Een gegarandeerd snel en hoog rendement.

Urgentie voor actie (bijvoorbeeld aanbiedingen voor beperkte tijd die druk geven om onmiddellijk te handelen).

Een betalingsverzoek via niet-traceerbare methoden (bijvoorbeeld crypto's, cadeaubonnen, overschrijvingen of prepaid debetkaarten).

Een uitnodiging om op een link te klikken, een QR-code te scannen of een app te downloaden.

Een verzoek om 'private keys' *en* herstelzinnen te verzenden of te delen (lijst met woorden om toegang te krijgen tot je cryptowallet en deze te herstellen).

Verdachte of onjuiste URL.

Logo met lichte vervormingen, een website die het uiterlijk van een echte website van een echt bedrijf nabootst of er professioneel uitziet, maar geen geverifieerde contactgegevens, bedrijfsregistratie-informatie, trackrecord of verifieerbare aanwezigheid heeft.

Onbekend handelsplatform.

Een verdachte bijlage, met name een.exe, .scr, .zip of Office-bestand (.docm, .xlsm) met macro's.

Stappen om zichzelf te beschermen:

1 Pauzeer en denk na voordat u handelt:

Haast u niet om te investeren, informatie te delen of op links te klikken- oplichters creëren opzettelijk een gevoel van urgentie. Bij twijfel: niet handelen of investeren en verifieer de bron zorgvuldig.

2 Controleer de bron zorgvuldig:

- Controleer altijd waar de berichten, oproepen, e-mails en links vandaan komen, zelfs als ze er officieel uitzien en lijken te komen van een vriend of familie, of zelfs een publiek figuur. Zoek naar spelfouten, vreemde URL's of ontbrekende beveiligingsindicatoren. Controleer bijvoorbeeld of de link op de website een "s" in "HTTPS" bevat om ervoor te zorgen dat de website veilig is, en controleer op toegevoegde of ontbrekende letters in de bedrijfsnaam.
- Open geen links vanuit ongevraagde berichten, installeer alleen officiële applicaties via vertrouwde appstores en scan geen onbekende QR-codes.
- Zelfs als een aanbieding er officieel uitziet, vergelijk deze met de website van het bedrijf of controleer of het socialemedia-account is geverifieerd (bijvoorbeeld met officiële vinkjes).
- Gebruik geverifieerde contactgegevens om het bedrijf of de persoon rechtstreeks te bereiken en vertrouw nooit op de contactgegevens die door de vermoedelijke fraudeur zijn verstrekt (zoek bijvoorbeeld zelf naar de bedrijfsnaam, gebruik geverifieerde registers van bedrijven). Oplichters kunnen beweren dat ze geautoriseerd zijn of de website van een geautoriseerd bedrijf nabootsen. Je kan controleren of de cryptoaanbieder een vergunning heeft in de EU door het ESMA-register te controleren (↖). U kan ook de website van de nationale financiële toezichthoudende autoriteit raadplegen (↖) om te zien of er waarschuwingen of zwarte lijsten zijn afgegeven of de I-SCAN-lijst van IOSCO (iosco.org/i-scan/).

3 Deel nooit wachtwoorden, private keys of herstelzinnen:

Iedereen die toegang hiertoe heeft kan de beschikking over uw activa krijgen. Legitieme bedrijven zullen nooit om wachtwoorden of beveiligingscodes vragen via e-mail, sms of telefoon.

4 Houd apparaten en private keys veilig:

Gebruik sterke en unieke wachtwoorden voor alle crypto-accounts, houd wachtwoorden geheim en vermijd het hergebruik van dezelfde inloggegevens op verschillende platforms. Schakel waar mogelijk multifactorauthenticatie in. Zie enkele tips voor wachtwoorden hier (↖) Houd software en antivirusbeveiliging up-to-date en geactiveerd.

5 Wees voorzichtig met onverwachte investeringsaanbiedingen:

Wees op uw hoede voor investeringen die enorme rendementen beloven. Als het te mooi klinkt om waar te zijn, dan is dat het waarschijnlijk ook.

6 Denk na voordat u informatie deelt op sociale media:

Chatgroepen, forums, posts en foto's op sociale media kunnen waardevolle bronnen zijn voor fraudeurs. Te veel onthullen over zichzelf of uw investeringen kan u een gemakkelijk doelwit maken.

Wat te doen als u slachtoffer bent geworden van fraude of oplichting

Stop transacties onmiddellijk

Om verdere overdrachten naar verdachte accounts te blokkeren en extra verliezen te voorkomen. Stop alle contacten met de oplichters – negeer hun oproepen en e-mails en blokkeer de afzender.

Wijzig wachtwoorden op al je apparaten en apps/websites.

Fraudeurs kopen gelekte wachtwoorden online en proberen ze op meerdere accounts. Het wijzigen van slechts één wachtwoord is niet voldoende: wijzig alle wachtwoorden, zodat fraudeurs ze niet opnieuw kunnen gebruiken.

Ontkoppelen en toegang intrekken.

Herroep verdachte machtigingen in digitale overeenkomsten die automatisch op de blockchain worden uitgevoerd (smart contract) om te voorkomen dat oplichters tokens uitgeven zonder uw toestemming. Veel wallets en blockchain-verkenners bieden tools waarmee u kunt zien welke smart contracts momenteel toegang hebben om uw tokens uit te geven. Om dit te doen, kunt u:

- een vertrouwde “permission checker” gebruiken om te controleren of een gebruiker of blockchain-adres gemachtigd is om een actie uit te voeren.
- de lijst van goedkeuringen herzien, en
- rechtstreeks vanaf het platform de knop “intrekken” gebruiken.

Verplaats uw geld:

Als uw wallet is gecompromitteerd, zet dan resterende activa onmiddellijk over naar een nieuwe beveiligde wallet.

Neem contact op met uw crypto-aanbieder:

Informeer uw crypto-aanbieder zo snel mogelijk via officiële contactkanalen om mogelijke opties te verkennen. Zelfs als het in de meeste gevallen niet mogelijk is om de blockchaintransactie terug te draaien, kan de aanbieder het account van de oplichter nog steeds bevriezen (als het op hetzelfde platform staat) en het adres van de wallet op de zwarte lijst zetten.

Melden en waarschuwen:

Meld het incident aan de politie of nationale financiële toezichthoudende autoriteit (↖) en informeer je netwerk (bijvoorbeeld vrienden en familie) om het bewustzijn te vergroten. Deze acties zijn de beste manier om zichzelf en anderen te beschermen.

Pas op voor recovery scams:

De fraudeur kan contact opnemen met een slachtoffer van een eerdere oplichting, waarbij de fraudeur beweert een overheidsinstantie te zijn (bijvoorbeeld politie, belastingdienst of financiële toezichthouder) en aanbiedt om verloren geld tegen een vergoeding terug te vorderen. Dit is vaak een nieuwe poging tot oplichting. Vergeet niet: als u eenmaal bent opgelicht, voorkomt dit niet dat u opnieuw wordt opgelicht.

Zie de waarschuwing van de gezamenlijke Europese toezichthoudende autoriteiten voor meer informatie over de risico’s in verband met cryptoactiva (↖). en de factsheet “Cryptoactiva uitgelegd: Wat betekent MiCA voor u als consument”(↖).

Europese Bankautoriteit, Europese Autoriteit voor verzekeringen en bedrijfspensioenen, Europese Autoriteit voor effecten en markten, 2025
Luxemburg: Bureau voor publicaties van de Europese Unie, 2025

PDF ISBN 978-92-9407-211-5 doi:10.2853/3311257 DZ-01-25-099-NL-N

Soorten CRYPTO-SCAMS

"Pump-and-dumpfraude" of "rug pull"

U ziet een advertentie op sociale media of een website die een "tijdelijke investeringsmogelijkheid" in crypto promoot, waarin wordt aanbevolen te investeren in een nieuw cryptotoken of -project. Nadat u interesse hebt getoond, wordt u gecontacteerd en doorgestuurd naar een crypto-platform of berichtenapplicatie (bijvoorbeeld Telegram, Viber of WhatsApp). Een schijnbaar geloofwaardig contact belooft snelle winsten of hoge rendementen als u snel investeert. U wordt aangemoedigd om een klein bedrag te investeren en vervolgens onder druk gezet om meer te investeren.

Wat kan er gebeuren:

U ontdekt dat de token waar u in geïnvesteerd hebt, waardeloos is en degene waarmee u contact hebt gehad, reageert niet meer. Wanneer u probeert geld op te nemen, bestaat de website niet meer en is het bedrijf onbereikbaar. Oplichters hebben een crypto met een lage waarde kunstmatig opgeblazen of overschat om de waarde ervan te verhogen ("pump") en vervolgens hun cryptoactiva verkocht ("dump"), waardoor de waarde crasht en beleggers verliezen lijden. Een andere mogelijkheid is dat zij het project stoppen en met de activa verdwijnen ("rug pull").

Identiteitsfraude

Nadat u een vraag hebt geplaatst op een sociaal mediaplatform of een website over een crypto-walletprobleem, ontvangt u een onverwacht direct bericht (DM) of een e-mail van iemand die zich voordoet als een vertrouwd contact (bijvoorbeeld een crypto-exchange, walletprovider, IT-ondersteuning of zelfs een vriend). De persoon vraagt om uw herstelzin (de volgorde van woorden die dient als de centrale back-up voor toegang tot een digitale portemonnee), wachtwoorden of private key (een automatisch gegenereerde cryptografische code die het eigendom van digitale activa bewijst).

Wat kan er gebeuren:

Zodra u uw herstelzin, wachtwoorden of privésleutels deelt, gebruikt de oplichter deze om uw crypto of andere tegoeden te stelen. Houd er rekening mee dat het verlies van privésleutels resulteert in het permanente en onomkeerbare verlies van toegang tot en eigendom van uw cryptoactiva. In tegenstelling tot banktransacties is herstel in het geval van crypto bijna onmogelijk zodra het geld is verdwenen.

Phishing

U ontvangt een onverwacht bericht via e-mail, telefoon, pop-up of sociale media dat beweert van een bekende aanbieder van cryptoactiva te zijn. Het bericht nodigt uit om in te loggen of een nieuwe app te downloaden. U kunt ook een e-mail ontvangen die afkomstig lijkt te zijn van een crypto-wallet-app, waarin wordt aangespoord om een beveiligingsprobleem op te lossen door te klikken op een link van een niet-officiële bron of door de app bij te werken.

Wat kan er gebeuren:

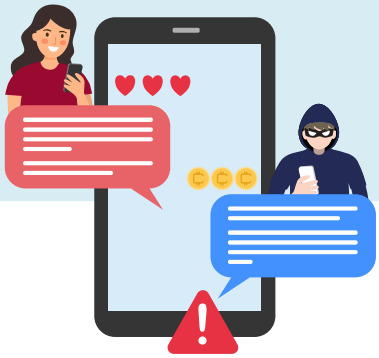
Door op de link te klikken, de app te downloaden of een QR-code te scannen, installeert u malware waarmee de oplichter toegang heeft tot informatie die gebruikt kan worden om cryptoactiva of geld te stelen.

Nep-winactie

U komt een aankondiging tegen op sociale media waarin wordt beweerd dat bedrijven crypto-activa weggeven na een kleine crypto-investering. De aankondiging bevat een video of een bericht met foto's van een beroemdheid of een merk – meestal nep of zonder toestemming verkregen – waarin wordt beloofd dat "je crypto wordt verdubbeld" als u ze eerst geld stuurt.. Het logo, de lay-out, de klantbeoordelingen en de gebruikte taal zien er professioneel en officieel uit, net als de website waarnaar wordt doorverwezen.

Wat kan er gebeuren:

Nadat u uw crypto hebt verzonden, ontvangt u niets terug en bent u het verzonden geld kwijt. De actie was nep en de post of livestream die zich voordeed als van een beroemdheid of bedrijf was ontworpen om u te misleiden.



Datingfraude

Je bent gecontacteerd op sociale media, dating-apps of telefoon/sms door iemand die u in het echte leven niet hebt ontmoet. Deze persoon begint frequente, persoonlijke en romantische gesprekken, om met behulp van valse profielen vertrouwen op te bouwen. Geleidelijk sturen ze het gesprek naar financiële kansen, claimen ze enorme winsten uit crypto-investeringen behaald te hebben en moedigen ze u aan om te investeren met beloften van hoog rendement en laag risico. Ze begeleiden u bij het opzetten van een account en het maken van een kleine initiële storting om de oplichting legitiem te laten lijken.

Oplichters maken valse online profielen en gebruiken gestolen of AI-gegenereerde foto's.

Wat kan er gebeuren:

De oplichter haalt zoveel mogelijk geld binnen, verbreekt vervolgens alle communicatie en verdwijnt. De frauduleuze beleggingswebsite of -app wordt offline gehaald, waardoor u geen toegang hebt tot de veronderstelde beleggingen. In sommige gevallen kunnen oplichters de tijdens de oplichting verkregen informatie gebruiken om zich op uw vrienden en familie te richten en identiteitsdiefstal te plegen die voor u financiële of juridische gevolgen kan hebben (de oplichter kan bijvoorbeeld gestolen wallets op uw naam verifiëren en u kunt verantwoordelijk worden gehouden voor schulden of misdaden die onder uw naam zijn gepleegd totdat het tegendeel is bewezen).

Ponzifraude

U wordt uitgenodigd om deel te nemen aan een project dat een consistent hoog rendement belooft van beleggingen in cryptoactiva, vaak ondersteund door getuigenissen of nepsuccesverhalen. De constructie kan worden gepresenteerd als multi-level marketing, waarbij u niet alleen beloond wordt vanuit uw eigen investering, maar ook door anderen te werven. Vroege investeerders lijken uitbetalingen te ontvangen, waardoor meer mensen worden aangemoedigd om zich aan te sluiten en de constructie te promoten.

In werkelijkheid is er geen echte bedrijfsvoering of gegenereerde winst. In plaats daarvan is het geld uitsluitend afkomstig van de bijdrage van nieuwere investeerders en dat geld wordt gebruikt om rendement te betalen aan de organisatoren en eerdere deelnemers.

Wat kan er gebeuren:

Zodra nieuwe investeringen afnemen, stort de constructie in en verliest u, zoals de meeste deelnemers, uw geld. De organisatoren verdwijnen, waardoor er geen manier is om geld terug te vorderen. De multilevelstructuur helpt de fraude zich snel te verspreiden, omdat slachtoffers onbewust promotors worden.

"Address poisoning"

Nadat u een crypto-transactie hebt uitgevoerd, ziet u een nieuw adres verschijnen in uw wallet-geschiedenis. Dit adres lijkt op een adres waarmee u eerder hebt gecommuniceerd. Oplichters kunnen nep-wallet-adressen in uw transactiegeschiedenis laten verschijnen door een kleine hoeveelheid crypto van een look-alike-adres naar uw wallet te sturen. Hierdoor slaat u uiteindelijk het valse adres dat door de oplichter is gemaakt op in de recente activiteit van uw wallet of automatische suggesties. Oplichters creëren doelbewust look-alike adressen door slechts een paar tekens te veranderen, vaak in het midden van het adres, om detectie te voorkomen.

Wat kan er gebeuren:

Wanneer u probeert crypto te verzenden en het verkeerde adres uit uw wallet-geschiedenis kopieert, stuurt u onbewust geld naar de wallet van de oplichter. Omdat crypto-transacties vaak onomkeerbaar zijn, gaat uw geld in de meeste gevallen permanent verloren. Deze oplichting is gebaseerd op visuele misleiding en gebruikersfouten, waarbij gebruik wordt gemaakt van de gewoonte om wallet-adressen te kopiëren en te plakken zonder ze zorgvuldig te controleren.