KRYPTO SVINDEL

VÆR OPMÆRKSOM OG BESKYT DIG SELV

Den hurtige vækst i kryptoaktiver og deres særlige karakteristika — global tilgængelighed, hastighed, anonymitet og ofte uigenkaldelige transaktioner — gør dig til et primært mål for cyberkriminelle. Svindlere bruger sofistikerede taktikker til at narre dig, f.eks. pyramidespil, falske investeringsmuligheder, gratis tilbud på sociale medier og falske beskeder. De anvender også kærligheds- og investerings svindel eller look-alike adresser til at øge risikoen for at du foretager fejlagtige overførsler. De kontakter dig ofte via sociale medier, beskedapps, e-mails og uventede telefonopkald, der lyder ægte. Du kan stå over for risici som økonomisk tab, identitetstyveri og følelsesmæssig nød.

Vær forsigtig og følg disse vigtige tips til at forblive sikker:

Vær opmærksom på mulig kryptosvindel:
For at lære mere om forskellige typer af svindel (se side 5 til 8);

Genkend advarselstegn:
lær at genkende mistænkelig adfærd, meddelelser eller tilbud (se side 2);

Beskyt dig selv og dine aktiver:
sikre dine personoplysninger (se side 3);

Vid hvad du skal gøre, hvis du bliver offer for svig eller svindel
(se side 4).

Advarselstegn

Et løfte, der virker for godt til at være sandt.

Uopfordret tilbud.

Et garanteret hurtigt og højt afkast.

Hastværk (f.eks. tidsbegrænsede tilbud, der presser dig til at handle med det samme).

En anmodning om betaling via metoder, der ikke kan spores (f.eks. krypto, gavekort, bankoverførsler eller forudbetalte debetkort).

En invitation til at klikke på et link, scanne en QR-kode eller downloade en app.

En anmodning om at sende eller dele private nøgler og "seed phrases" (liste over ord der giver adgang til din krypto tegnebog).

Mistænkelig eller forkert URL

Logo med små ændringer, et websted, der kopierer udseendet af en rigtig virksomheds websted eller ser professionel ud, men mangler verificerede kontaktoplysninger, CVR oplysninger, track record eller verificerbar eksistens.

Ukendt vekslingsplatform.

En mistænkelig vedhæftet fil, især .exe, .scr, .zip eller makroaktiveret Office-fil (.docm, .xlsm).

Skridt til at beskytte dig selv:

1 **Pause og tænk dig om, før du handler:**

Du skal ikke skynde dig at investere, dele oplysninger eller klikke på links – svindlere skaber bevidst en følelse af, at det haster. I tilfælde af tvivl, selv i mindre tilfælde, skal du ikke handle eller investere, men kontrollere kilden omhyggeligt.

2 **Kontrollér kilden omhyggeligt:**

- Kontrollér altid hvor meddelelser, opkald, e-mails og links kommer fra, selvom de ser officielle ud, ser ud til at komme fra en ven eller din familie eller endda en offentlig figur. Kig efter stavefejl, mærkelige webadresser eller manglende sikkerhedsindikatorer, f.eks. kontrollér, at linket til webstedet indeholder et "s" i "HTTPS" for at sikre, at webstedet er sikkert, og kontrollér, om der er tilføjet eller mangler bogstaver i virksomhedens navn.
- Åbn ikke links fra uopfordrede beskeder, installér kun officielle applikationer gennem pålidelige appbutikker, og scan ikke ukendte QR-koder.
- Selvom et tilbud ser officielt ud skal du altid krydstjekke det med virksomhedens websted eller kontrollere, at kontoen på de sociale medier er verificeret (f.eks. med officielle kontrolmærker).
- Brug verificerede kontaktoplysninger til at kontakte virksomheden eller den enkelte direkte og stol aldrig på de kontaktoplysninger, som den mistænkte svindler har angivet (f.eks. søg efter virksomhedens navn uafhængigt, brug verificerede virksomhedsfortegnelser). Svindlere kan hævde at være godkendt eller efterligne webstedet for en autoriseret virksomhed. Du kan kontrollere, om kryptoudbyderen er godkendt i EU, ved at tjekke ESMA's register (). Du kan også konsultere din nationale tilsynsmyndigheds websted (https://www.finanstilsynet.dk) for at se, om der er udstedt advarsler eller sortlister, eller IOSCO's I-SCAN-liste (iosco.org/i-scan/).

3 **Del aldrig adgangskoder, private nøgler eller "seed phrases":**

Enhver med adgang til dem kan tage kontrol over dine aktiver. Legitime virksomheder vil aldrig bede om dine adgangskoder eller sikkerhedskoder via e-mail, sms eller telefon.

4 **Hold enheder og private nøgler sikre:**

Brug stærke og unikke adgangskoder til hver af dine kryptokonti, hold din adgangskode hemmelig, og undgå at genbruge de samme legitimationsoplysninger på forskellige platforme. Aktivér multifaktorgodkendelse, hvor det er muligt. Se nogle tips til adgangskoder her (). Hold din software- og antivirusbeskyttelse opdateret og aktiveret.

5 **Vær forsigtig med uventede investeringstilbud:**

Vær på vagt over for investeringer, der lover store afkast. Hvis det lyder for godt til at være sandt, så er det formentlig ikke sandt.

6 **Tænk før du deler oplysninger på sociale medier:**

Chatgrupper, fora, opslag på sociale medier og fotos kan være værdifulde kilder til viden for svindlere. At afsløre for meget om dig selv eller dine investeringer kan gøre dig til et nemt mål.

Hvad skal du gøre, når du er blevet offer for svindel

Straks stoppe transaktioner

For at blokere yderligere overførsler til mistænkelige konti og undgå yderligere tab. Stoppe al kontakt med svindlerne – ignorer deres opkald og e-mails og blokér afsenderen.

Skift dine adgangskoder på alle dine enheder og apps/hjemmesider.

Svindlere køber lækkede adgangskoder online og prøver dem på flere konti. Det er ikke nok kun at ændre ét password. Sørg for at ændre dem alle, så svindlere ikke kan genbruge dem.

Afbrydelse og tilbagekaldelse af adgang:

Tilbagekald mistænkelige tilladelser i din digitale aftale, der kører automatisk på blockchain (smart kontrakt) for at stoppe svindlere fra at bruge dine tokens uden dit samtykke. Mange tegnebøger og blockchain søgemaskiner tilbyder værktøjer, der giver dig mulighed for at se, hvilke smarte kontrakter i øjeblikket har adgang til at bruge dine tokens. For at gøre dette kan du:

- anvende en pålidelig "tilladelseskontrol", som kontrollerer, om en bruger- eller blockchainadresse er autoriseret til at udføre en handling.
- gennemgå listen over godkendelser og
- bruge knappen "Tilbagekald" direkte fra platformen.

Flyt dine penge:

Hvis din tegnebog er kompromitteret, skal du straks overføre dine resterende aktiver til en ny sikker tegnebog.

Kontakt din kryptoudbyder:

Informere din kryptoudbyder så hurtigt som muligt ved hjælp af officielle kontaktkanaler for at undersøge potentielle løsninger. Selv om det i de fleste tilfælde ikke vil være muligt at vende blockchaintransaktionen, kan udbyderen stadig fastfryse svindlerens konto (hvis den er på deres platform) og sortliste tegnebogsadressen.

Indberetning og varsling:

Indberet hændelsen til politiet eller din nationale tilsynsmyndighed og informer dit netværk (f.eks. venner og familie) for at øge bevidstheden. Disse handlinger er den bedste måde at beskytte dig selv og andre.

Pas på svindel i forbindelse med indrivelse:

Svindleren kan kontakte dig som offer for et tidligere svindelnummer og hævde at være en offentlig myndighed (f.eks. politi, skatte- eller tilsynsmyndighed osv.) og tilbyde at inddrive dine tabte penge mod et gebyr. Dette er ofte et andet forsøg på at snyde dig. Husk: at blive snydt én gang forhindrer dig ikke i at blive snydt igen.

Se advarslen fra de fælles europæiske tilsynsmyndigheder for at få mere at vide om de risici, der er forbundet med kryptoaktiver (↖) og faktabladet "Kryptoaktiver forklaret: hvad MiCA betyder for dig som forbruger (↖).

Den Europæiske Banktilsynsmyndighed, Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger, Den Europæiske Værdipapir- og Markedstilsynsmyndighed, 2025

Luxembourg: Den Europæiske Unions Publikationskontor, 2025

PDF ISBN 978-92-9407-227-6 doi:10.2853/8564714 DZ-01-25-116-DA-N

TYPER AF KRYPTO SVINDEL

»Pump-and-dump« eller »rug pull«

Du ser en annonce på sociale medier eller et websted, der promoverer en "tidsbegrænset investeringsmulighed" indenfor krypto, og som anbefaler at investere i en ny kryptotoken eller et nyt kryptoprojekt. Efter du har udtrykt interesse, bliver du kontaktet og omdirigeret til en kryptoplatform eller beskedtjeneste (f.eks. Telegram, Viber eller WhatsApp). En tilsyneladende troværdig kontakt lover hurtig fortjeneste eller højt afkast, hvis du investerer hurtigt. Du opfordres til at investere et lille beløb og derefter presset til at investere mere.

Hvad kan der ske:

Du opdager, at den investerede token er værdiløs, og den kontaktperson, du har været i kontakt med, holder op med at svare. Når du forsøger at hæve dine penge, eksisterer hjemmesiden ikke længere, og virksomheden er utilgængelig. Svindlerne har kunstigt oppustet eller overevalueret en kryptovaluta med lav værdi for at øge dens værdi ("pumpe"), og solgte derefter deres aktiver ("dump"), hvilket fik værdien til at gå ned og efterlod investorerne med tabet. Alternativt kan de lukke projektet og forsvinde med midlerne ("rug pull").

Identitetssvindel

Når du har sendt et spørgsmål på en social medieplatform eller et websted om et problem med en kryptotegnebog, modtager du en uventet direkte besked (DM) eller en e-mail fra en person, der foregiver at være en betroet kontakt (f.eks. en kryptoveksler, tegnebogsudbyder, IT-support eller endda en ven). Personen beder om din "seed phrase" (dvs. sekvens af ord, der tjener som den centrale backup for at få adgang til din digitale tegnebog), adgangskoder eller private nøgler (en automatisk genereret kryptografisk kode, der beviser ejerskab af digitale aktiver).

Hvad kan der ske:

Når du deler din "seed phrase", adgangskoder eller private nøgler, bruger svindleren dem til at stjæle din krypto eller andre midler. Husk, at tab af private nøgler resulterer i permanent og uigenkaldeligt tab af adgang og ejerskab til dine kryptoaktiver. I modsætning til banktransaktioner er genopretning næsten umuligt så snart dine midler er væk i tilfælde af kryptooverførsler.

Phishing

Du modtager en uventet besked via e-mail, telefon, pop-up eller sociale medier, der hævder at være fra en velkendt kryptoaktiv udbyder. Meddelelsen opfordrer dig til at logge ind eller downloade en ny app. Du kan også modtage en e-mail, der ser ud til at være fra din kryptotegnebog-app, som opfordrer dig til at løse et sikkerhedsproblem ved at klikke på et link, der leveres af en uofficiel kilde, eller ved at opdatere appen.

Hvad kan der ske:

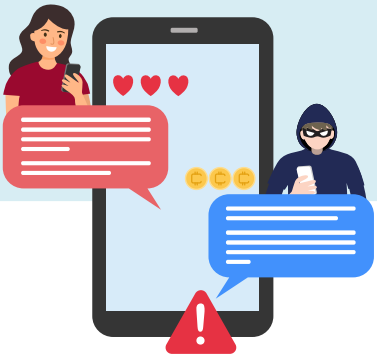
Ved at klikke på linket, downloade appen eller scanne en QR-kode installerer du en malware, der gør det muligt for svindleren at få adgang til og bruge oplysningerne til at stjæle dine kryptoaktiver eller dine midler.

Giveaway-svindel

Du støder på en meddelelse på sociale medier, der hævder, at virksomheder giver væk kryptoaktiver efter en lille kryptoinvestering. De omfatter en video eller et indlæg med billeder af en berømt person eller et velkendt mærke — normalt falske eller opnået uden tilladelse — der lover at "dobbelte din krypto", hvis du sender penge først. Logoet, layoutet, udtalelserne og det anvendte sprog ser professionelt og officielt ud, og det samme gør det websted, du omdirigeres til.

Hvad kan der ske:

Efter at have sendt din krypto, modtager du intet til gengæld, og du har mistet de sendte penge. Giveawayen var falsk, og indlægget eller livestreamen, der efterlignede berømtheder eller virksomheder, var designet til at bedrage dig.



Kærligheds- og investeringssvindel

Du er blevet kontaktet på sociale medier, dating apps eller telefon / sms af en person, du ikke har mødt i den virkelige verden. Denne person indgår i hyppige, personlige og romantiske samtaler, opbygger tillid ved hjælp af falske profiler. Gradvist styrer de samtalen mod økonomiske muligheder, hævder enorme overskud fra kryptoinvesteringer og opfordrer dig til at investere med løfter om højt afkast og lav risiko. De guider dig gennem oprettelse af en konto og foretage en lille indledende indbetaling for at få svindlen til at virke legitim.

Svindlere opretter falske onlineprofiler og bruger stjålne eller kunstig intelligens-genererede billeder til at henvende sig til dig.

Hvad kan der ske:

Svindleren trækker så mange penge ud som muligt, afskærer derefter al kommunikation og forsvinder. Den falske investeringshjemmeside eller -app er taget offline, så du ikke har adgang til de formodede investeringer. I nogle tilfælde kan svindlere bruge de oplysninger, der er opnået under svindelen, til målrettet svindel mod dine venner og familie og begå identitetstyveri, hvilket kan have økonomiske eller juridiske konsekvenser for dig (f.eks. kan svindleren kontrollere stjålne tegnebøger i dit navn, og du kan blive holdt ansvarlig for gæld eller forbrydelser begået under dit navn, indtil det modsatte er bevist).

Pyramidespil

Du inviteres til at deltage i et projekt, der lover konsekvent høje afkast fra investeringer i kryptoaktiver, ofte understøttet af vidnesbyrd eller falske succeshistorier. Spillet kan præsenteres som en multi-level markedsførings mulighed, hvor du tjener belønninger ikke kun fra din egen investering, men også ved at rekruttere andre. Tidlige investorer synes at modtage udbetalinger, hvilket tilskynder flere mennesker til at tilslutte sig og fremme ordningen.

I virkeligheden er der ingen reel forretning eller overskud, der genereres. Pengene kommer i stedet udelukkende fra bidrag fra nyere investorer, som anvendes til at betale afkast til ordningens arrangører og første deltagere.

Hvad kan der ske:

Når nye investeringer bremse, kollapser spillet, og du, ligesom de fleste deltagere, mister dine penge. Initiativtagerne forsvinder og giver ingen mulighed for at inddrive midler. Den multilevel struktur hjælper svindlen med at spredes hurtigt, som ofre ubevidst promoverer.

En look-alike adresse

Når du har foretaget en kryptotransaktion, bemærker du en ny adresse, der vises i din tegnebogshistorik. Denne adresse ligner en, du tidligere har interageret med. Svindlere kan få falske tegnebogsadresser til at blive vist i din transaktionshistorik ved at sende en lille mængde krypto fra en look-alike-adresse til din tegnebog. Du ender med at gemme adressen i din tegnebogs seneste aktivitet eller den falske adresse bliver automatisk forslået til dig. Svindlere skaber bevidst look-alike-adresser ved kun at ændre nogle få tegn, ofte midt i adressen, for at undgå at blive opdaget.

Hvad kan der ske:

Når du forsøger at sende krypto og kopiere den forkerte adresse fra din tegnebogshistorik, sender du ubevidst penge til svindlerens tegnebog. Fordi kryptotransaktioner ofte er irreversible, går dine midler tabt og i de fleste tilfælde permanent. Denne svindel er afhængig af visuel bedrag og brugerfejl, der udnytter vanen med at kopiere og indsætte tegnebogsadresser uden tæt inspektion.