KRYPTOBEDRÄGERIER & SCAMS

VAR VAKSAM OCH SKYDDA DIG

Den snabba tillväxten av kryptotillgångar och deras särdrag – global räckvidd, snabbhet, anonymitet och ofta oåterkalleliga transaktioner – gör dig till en måltavla för cyberbrottslingar. Bedragare använder sofistikerade metoder för att lura dig, t.ex. pyramidspel, falska investeringsmöjligheter, kostnadsfria erbjudanden på sociala medier och falska budskap. De använder också romansbedrägerier eller snarlika (“look alike”) adresser för att skada din plånbok. De når dig ofta via sociala medier, chattappar, e-post och oväntade telefonsamtal com låter verkliga. Du kan utsättas för risker som ekonomisk förlust, identitetsstöld och psykiskt lidande.

Var försiktig och följ dessa tips för att vara säker:

Var uppmärksam på eventuella kryptobedrägerier och scams:
lära dig mer om olika typer av bedrägerier (se sidorna 5, 6, 7 och 8)

Upptäck varningssignaler:
lär dig att känna igen misstänkta beteenden, meddelanden eller erbjudanden (se sidan 2)

Skydda dig själv och dina tillgångar:
skydda dina personuppgifter (se sidan 3)

Ha koll på vad du ska göra om du faller offer för bedrägerier
(se sidan 4)

Varningssignaler

Ett löfte som verkar för bra för att vara sant.

Ett oönskat erbjudande.

Garanterad snabb och hög avkastning.

Brådskande åtgärder (t.ex. tidsbegränsade erbjudanden som pressar dig att agera omedelbart).

En begäran om betalning via ospårbara metoder (t.ex. kryptotillgångar, presentkort, elektroniska överföringar av medel eller förbetalda betalkort).

En inbjudan att klicka på en länk, skanna en QR-kod eller ladda ner en app.

En begäran om att skicka eller dela privata nycklar och så kallade “seed phrases” (lista över ord för att komma åt och återställa din kryptoplånbok).

Misstänkt eller felaktig URL-adress.

Logotyp med små snedvridningar, en webbplats som kopierar utseendet på ett riktigt företags webbplats eller ser professionell ut men saknar verifierade kontaktuppgifter, information om företaget är registrerat, meriter eller verifierbart säte.

Okänd kryptobörs.

En misstänkt bifogad fil, särskilt .exe, .scr, .zip eller makroaktiverad Office-fil (.docm, .xlsm).

Åtgärder för att skydda dig:

1 Pausa och tänk efter innan du agerar:

Skynda dig inte att investera, dela information eller klicka på länkar – bedragare skapar medvetet en känsla av brådska. Vid eventuella tvivel, även mindre, agera inte eller investera och kontrollera källan noggrant.

2 Kontrollera källan noga:

- Kontrollera alltid var meddelanden, samtal, e-postmeddelanden och länkar kommer ifrån, även om de ser officiella ut, verkar komma från en vän eller din familj, eller till och med en offentlig person. Leta efter stavfel, konstiga webbadresser eller säkerhetsindikatorer som saknas, t.ex. kontrollera att webbplatslänken innehåller ett ”s” i ”HTTPS” för att se till att webbplatsen är säker, och kontrollera om några bokstäver i företagsnamnet har lagts till eller saknas.
- Öppna inte länkar från oönskade meddelanden, installera bara officiella applikationer via betrodda appbutiker och skanna inte okända QR-koder.
- Även om ett erbjudande ser officiellt ut, dubbelkontrollera det alltid mot företagets webbplats eller kontrollera att det sociala mediekontot är verifierat (t.ex. med officiella verifieringsmärken).
- Använd verifierade kontaktuppgifter för att nå företaget eller individen direkt och lita aldrig på de kontaktuppgifter som tillhandahålls av den misstänkta bedragaren (t.ex. sök efter företagets namn självständigt, använd verifierade företagskataloger). Bedragare kan hävda att de är auktoriserade eller efterlikna ett auktoriserat företags webbplats. Du kan kontrollera om kryptoleverantören är auktoriserad i EU genom att kontrollera Esmas register (shorturl.at/zZwVI). Du kan också besöka din nationella finansiella tillsynsmyndighets webbplats (↖) för att se om det har utfärdats några varningar eller svarta listor eller Ioscos I-SCAN-lista (iosco.org/i-scan/).

3 Dela aldrig lösenord, privata nycklar eller så kallade “seed phrases”:

Alla som har tillgång till dem kan ta kontroll över dina tillgångar. Legitima företag kommer aldrig att be om dina lösenord eller säkerhetskoder via e-post, sms eller telefon.

4 Håll enheter och privata nycklar säkra:

Använd starka och unika lösenord för vart och ett av dina kryptokonton, håll ditt lösenord hemligt och undvik att återanvända samma autentiseringsuppgifter på olika plattformar. Aktivera multifaktorautentisering där det är möjligt. Se några tips om lösenord här (↖) Håll din programvara och ditt antivirusskydd uppdaterat och aktiverat.

5 Var försiktig med oväntade investeringserbjudanden:

Var försiktig med investeringar som lovar stor avkastning. Om det låter för bra för att vara sant, är det förmodligen det.

6 Tänk efter innan du delar information på sociala medier:

Chattgrupper, forum, inlägg på sociala medier och foton kan vara värdefulla kunskapskällor för bedragare. Att avslöja för mycket om dig själv eller dina investeringar kan göra dig till ett enkelt mål.

Vad du ska göra om du har blivit offer för bedrägeri eller scams

Stoppa omedelbart transaktioner:

För att blockera ytterligare överföringar till misstänkta konton och undvika ytterligare förluster. Stoppa all kontakt med bedragarna – ignorera deras samtal och e-postmeddelanden och blockera avsändaren.

Ändra dina lösenord på alla dina enheter och appar/webbplatser:

Bedragare köper läckta lösenord online och försöker använda dem på flera konton. Det räcker inte med att bara byta ett lösenord. Se till att ändra alla, så att bedragare inte kan återanvända dem.

Koppla bort och återkalla åtkomsten:

Återkalla misstänkta behörigheter i ditt digitala avtal som körs automatiskt på blockkedjan (smart kontrakt) för att stoppa bedragare från att spendera dina tokens utan ditt samtycke. Många plånböcker och så kallade “blockchain explorers” erbjuder verktyg som låter dig se vilka smarta kontrakt som för närvarande har tillgång till att spendera dina tokens. För att göra det kan du:

- Använda en betrodd så kallad ”‘permission checker” som kontrollerar om en användares eller blockkedjeadress har tillstånd att utföra en operation.
- Se över förteckningen över godkännanden, och
- Använd knappen ”återkalla” direkt från plattformen.

Flytta dina pengar:

Om din plånbok äventyras, överför omedelbart dina återstående tillgångar till en ny säker plånbok.

Kontakta din kryptoleverantör:

Informera din kryptoleverantör så snart som möjligt med hjälp av officiella kontaktkanaler, för att utforska möjliga alternativ. Även om det i de flesta fall inte är möjligt att återkalla blockkedjetransaktionen kan leverantören fortfarande frysa bedragarens konto (om det finns på deras plattform) och svartlista plånboksadressen.

Rapport och varning:

Anmäl incidenten till polisen eller din nationella finansiella tillsynsmyndighet (https://www.finanssivalvonta.fi/sv) och informera ditt nätverk (t.ex. vänner och familj) för att öka medvetenheten. Dessa åtgärder är det bästa sättet att skydda dig själv och andra.

Se upp för återhämtningsbedrägerier:

Bedragaren kan kontakta dig som blivit offer för en tidigare bluff, som påstår sig vara en offentlig myndighet (t.ex. polis, skatte- eller finansiell myndighet etc.) och erbjuder sig att återkräva dina förlorade pengar mot en avgift. Detta är ofta ett nytt försök att lura dig. Kom ihåg: att bli lurad en gång hindrar dig inte från att bli lurad igen.

Se de gemensamma europeiska tillsynsmyndigheternas varning för att få veta mer om riskerna med kryptotillgångar (↖) och faktabladet ”Förklaring av kryptotillgångar: Vad betyder Mica för dig som konsument?” (↖).

Europeiska bankmyndigheten, Europeiska försäkrings- och tjänstepensionsmyndigheten, Europeiska värdepappers- och marknadsmyndigheten, 2025

Luxemburg: Europeiska unionens publikationsbyrå, 2025

PDF ISBN 978-92-9407-218-4 doi:10.2853/6486543 DZ-01-25-106-SV-N

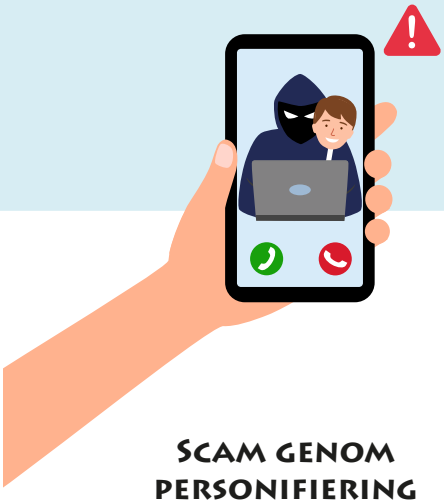
Typer av KRYPTO-SCAMS

"Pump-and-dump" eller "rug pull"

Du ser en annons på sociala medier eller en webbplats som marknadsför en "tidsbegränsad investeringsmöjlighet" i krypto och rekommenderar att du investerar i en ny kryptotillgång eller ett nytt kryptoprojekt. Efter att ha uttryckt intresse kontaktas du och omdirigeras till en kryptobörs eller meddelandekanal (t.ex. en till synes trovärdig kontakt lovar snabb vinst eller hög avkastning om du investerar snabbt). Du uppmuntras att investera ett litet belopp och pressas sedan att investera mer.

Detta kan hända:

Du upptäcker att den investerade kryptotillgången är värdelös och den du har varit i kontakt med slutar svara. När du försöker ta ut dina pengar finns webbplatsen inte längre och företaget går inte att nå. Bedragare blåste artificiellt upp eller överskattade en kryptotillgång av lågt värde för att öka dess värde ("pump") och sålde sedan sina tillgångar ("dump"), vilket ledde till att värdet kraschade och lämnade investerare med förluster. Alternativt kan de stänga projektet och försvinna med pengarna ("rug pull").



Scam genom personifiering

När du har lagt upp en fråga på en social medieplattform eller en webbplats om ett kryptoplånboksproblem får du ett oväntat direktmeddelande (DM) eller ett e-postmeddelande från någon som låtsas vara en betrodd kontakt (t.ex. en kryptobörs, plånboksleverantör, IT-support eller till och med en vän). Personen frågar efter din så kallade "seed phrase" (dvs. ordföljd som fungerar som den centrala säkerhetskopian för åtkomst till din digitala plånbok), lösenord eller privata nycklar (en automatiskt genererad kryptografisk kod som bevisar ägande av digitala tillgångar).

Detta kan hända:

När du delar din så kallade "seed phrase", lösenord eller privata nycklar använder bedragaren dem för att stjäla din krypto eller andra medel. Tänk på att förlust av privata nycklar resulterar i permanent och oåterkallelig förlust av åtkomst och ägande till dina kryptotillgångar. När dina medel är borta när det gäller kryptoöverföringar är återhämtning, till skillnad från vid banktransaktioner, nästan omöjligt.

Nätfiske ("Phishing")

Du får ett oväntat meddelande via e-post, telefon, popup-fönster eller sociala medier som påstår sig vara från en välkänd kryptoleverantör. Meddelandet inbjuder dig att logga in eller ladda ner en ny app. Du kan också få ett e-postmeddelande som verkar vara från din kryptoplånboksapp som uppmanar dig att lösa ett säkerhetsproblem genom att klicka på en länk som tillhandahålls av en inofficiell källa eller genom att uppdatera appen.

Detta kan hända:

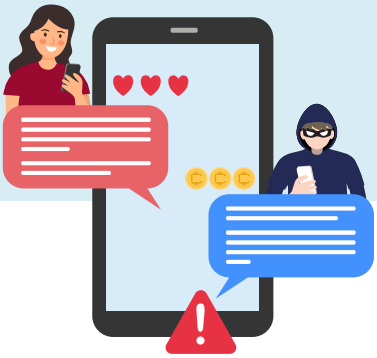
Genom att klicka på länken, ladda ner appen eller skanna en QR-kod installerar du en skadlig kod som gör det möjligt för bedragaren att komma åt och använda informationen för att stjäla dina kryptotillgångar eller dina medel.

"Giveaway"-scam

Du stöter på ett tillkännagivande på sociala medier som hävdar att företag ger bort kryptotillgångar efter en liten kryptoinvestering. De innehåller en video eller ett inlägg med foton av en kändis eller ett varumärke – vanligtvis falska eller erhållna utan tillstånd – som lovar att "dubbla din krypto" om du skickar pengar först. Logotypen, layouten, vittnesmålen och språket som används ser professionellt och officiellt ut, liksom webbplatsen du omdirigeras till.

Detta kan hända:

Efter att ha skickat din krypto får du ingenting i gengäld och du har förlorat de skickade pengarna. Giveawayen var falsk, och inlägget eller livestreamen som utgav sig för att vara kändisar eller företag var utformade för att lura dig.



Romansbedrägeri

Du har blivit kontaktad på sociala medier, datingappar, eller telefon / sms av någon du inte har träffat i verkliga livet. Den här personen kan delta i frekventa, personliga och romantiska samtal och bygga förtroende med hjälp av falska profiler. Gradvis styr de samtalet mot ekonomiska möjligheter, hävdar enorma vinster från kryptoinvesteringar och uppmuntrar dig att investera med löften om hög avkastning och låg risk. De guidar dig genom att skapa ett konto och göra en liten första insättning för att systemet ska verka vara legitimt.

Bedragare skapar falska onlineprofiler och använder stulna eller AI-genererade bilder för att närma sig dig.

Detta kan hända:

Bedragaren lurar till sig så mycket pengar som möjligt, stänger sedan av all kommunikation och försvinner. Den bedrägliga investeringswebbplatsen eller appen tas offline, vilket ger dig ingen tillgång till de förmodade investeringarna. I vissa fall kan bedragare använda den information som erhållits under bedrägeriet för att rikta in sig på dina vänner och familj och begå identitetsstöld som kan få ekonomiska eller rättsliga konsekvenser för dig (t.ex. kan bedragaren verifiera stulna plånböcker i ditt namn och du kan hållas ansvarig för skulder eller brott som begåtts i ditt namn tills motsatsen bevisats).

Pyramidspel ("Ponzi schemes")

Du är inbjuden att delta i ett projekt som lovar konsekvent hög avkastning från investeringar i kryptotillgångar, ofta med stöd av vittnesmål eller falska framgångshistorier. Programmet kan presenteras som en marknadsföringsmöjlighet på flera nivåer, där du får belöningar inte bara från din egen investering utan också genom att rekrytera andra. Tidiga investerare verkar få utbetalningar, uppmuntra fler människor att gå med och främja systemet.

I själva verket finns det ingen verklig verksamhet eller vinst som genereras. Pengarna kommer i stället enbart från bidrag från nyare investerare som används för att betala avkastning till systemets organisatörer och första deltagare.

Detta kan hända:

När nya investeringar saktar ner kollapsar systemet och du, som de flesta deltagare, förlorar dina pengar. Organisatörerna försvinner, vilket inte lämnar något sätt för dig att kunna återkräva dina pengar. Flernivåstrukturen hjälper bluffen att sprida sig snabbt, eftersom offren omedvetet blir förespråkare.

En snarlik adress som skadar din plånbok

När du har gjort en kryptotransaktion märker du att en ny adress visas i din plånbokshistorik. Den här adressen liknar en som du tidigare har interagerat med. Bedragare kan få falska plånboksadresser att visas i din transaktionshistorik genom att skicka en liten mängd krypto från en plånboksadress som liknar din plånbok (“look alike”-adress) till din plånbok. Du börjar lagra i din plånboks senaste aktivitet eller den falska adressen som skapats av bedragaren som föreslås automatiskt. Bedragare skapar medvetet snarlika plånboksadresser genom att bara ändra några tecken, ofta i mitten av adressen, för att undvika upptäckt.

Detta kan hända:

När du försöker skicka krypto och kopiera fel adress från din plånbokshistorik skickar du omedvetet pengar till bedragarens plånbok. Eftersom kryptotransaktioner ofta är oåterkalleliga förloras dina pengar i de flesta fall permanent. Denna bluff bygger på ett visuellt bedrägeri och användarfel, utnyttjar vanan att kopiera och klistra in plånboksadresser utan noggrann inspektion.