KRYPTOPETOKSET JA -HUIJAUKSET

PYSY VALPPAANA JA SUOJELE ITSEÄSI

Kryptovarojen vauhdikas kasvu ja erityispiirteet – maailmanlaajuinen saatavuus, nopeus, nimettömyys ja usein tapahtumien peruuttamattomuus – tekevät sinusta erinomaisen kohteen kyberrikollisille. Petokset ja huijarit käyttävät kehittyneitä taktiikoita huijatakseen sinua, kuten Ponzi-järjestelmiä, teennäisiä sijoitusmahdollisuuksia, ilmaisia tarjouksia sosiaalisessa mediassa ja valheellisia viestejä. He käyttävät myös rakkaushuijauksia tai vääriä, mutta oikean osoitteen kanssa samannäköisiä osoitteita saastuttaakseen lompakkosi. He tavoittavat sinut usein sosiaalisen median, viestintäsovellusten, sähköpostien ja odottamattomien puheluiden avulla. Yhteydenotot vaikuttavat todellisilta. Voit altistua riskeille, kuten taloudellisille menetyksille ja identiteettivarkauksille ja voit joutua kohtaamaan stressiä ja ahdistusta.

Ole varovainen ja noudata näitä keskeisiä vinkkejä pysyäksesi turvassa:

Pysy valppaana mahdollisten kryptopetosten ja -huijausten varalta:
opi lisää erityyppisistä petoksista ja huijauksista (katso sivut 5, 6, 7 ja 8)

Huomaa varoitusmerkit:
opi tunnistamaan epäilyttävä käyttäytyminen, viestit ja tarjoukset (katso sivu 2)

Suojaa itsesi ja omaisuutesi:
turvaa henkilökohtaiset tietosi (katso sivu 3)

Tiedä, mitä tehdä, jos joudut petoksen tai huijauksen uhriksi
(katso sivu 4)

Varoitusmerkit

Lupaus, joka tuntuu liian hyvältä ollakseen totta.

Pyytämättä saatu tarjous.

Taattu nopea ja korkea tuotto.

Tarve nopeaan toimintaan (esim. rajoitetun ajan voimassa olevat tarjoukset, jotka painostavat toimimaan välittömästi).

Pyyntö käyttää vaikeasti jäljitettäviä maksutapoja (esim. kryptot, lahjakortit, sähköiset varainsiirrot tai prepaid-maksukortit).

Kutsu klikata linkkiä, skannata QR-koodi tai ladata sovellus.

Pyyntö lähettää tai jakaa yksityisiä avaimia ja palautuslausekkeita (eng. *seed phrase*) (sanaluettelo, joka on tarkoitettu kryptolompakon käyttämiseen ja palauttamiseen).

Epäilyttävä tai virheellinen verkko-osoite (URL-osoite).

Logo, jossa on pieniä vääristymiä, verkkosivusto, joka kopioi todellisen yrityksen verkkosivuston ulkoasun tai näyttää ammattimaiselta, mutta josta puuttuvat todennetut yhteystiedot, yrityksen rekisteröintitiedot, tausta, ansiot tai todennettava olemassaolo.

Tuntematon vaihtoalusta.

Epäilyttävä liite, erityisesti .exe-, .scr-, .zip- tai makroja tukevat Office-tiedostot (.docm, .xlsm).

Tee näin suojautuaksesi:

1 **Pysähdy ja mieti ennen kuin toimit:**

Älä kiirehdi sijoittamaan, jakamaan tietojasi tai napsauttamaan linkkejä – huijarit luovat tarkoituksella kiireellisyyden tunteen. Jos sinulla on vähäisiäkään epäilyksiä, älä toimi tai sijoita.

2 **Tarkista lähde huolellisesti:**

- Tarkista aina, mistä viestit, puhelut, sähköpostit ja linkit tulevat, vaikka ne näyttäisivät virallisilta, näyttävät tulevan ystävältäsi tai perheeltäsi tai jopa julkisuuden henkilöltä. Tarkkaile kirjoitusvirheitä, outoja verkko-osoitteita tai puuttuvia turvatekijöitä. Tarkista esimerkiksi, että verkkosivuston linkissä on ”s” kohdassa ”HTTPS”, jotta voit varmistaa, että verkkosivusto on turvallinen. Tarkista, onko yrityksen nimeen lisätty tai puuttuuko siitä kirjaimia.
- Älä avaa linkkejä ei-toivotuista tai pyytämättä saapuneista viesteistä. Asenna vain virallisia sovelluksia luotettavien sovelluskauppojen kautta. Älä skannaa tuntemattomia QR-koodeja.
- Vaikka tarjous näyttäisi viralliselta ja aidolta, tarkista se aina vertaamalla sitä yrityksen verkkosivustoon tai tarkista, että sosiaalisen median tili on vahvistettu (esim. virallisten tarkastusmerkkien avulla).
- Käytä vahvistettuja yhteystietoja tavoittaakseni yrityksen tai henkilön suoraan, äläkä koskaan luota epäillyn huijarin antamiin yhteystietoihin (esim. etsi yrityksen nimi itsenäisesti, käytä vahvistettuja yrityshakemistoja). Huijarit voivat väittää olevansa valtuutettuja tai luvanvaraisia palveluntarjoajia tai jäljitellä toimiluvallisen yrityksen verkkosivustoa. Voit tarkistaa ESMAn rekisteristä, onko kryptopalveluntarjoajalla toimilupa EU:ssa (↖). Voit myös tarkistaa kansallisen finanssiviranomaisen verkkosivustolta (↖) mahdolliset varoitukset ja mustat listat, tai IOSCOn I-SCAN-luettelon (iosco.org/i-scan/).

3 **Älä koskaan jaa salasanoja, yksityisiä avaimia tai palautuslausekkeita (eng. *seed phrase*):**

Kuka tahansa, jolla on pääsy niihin, voi ottaa varasi hallintaansa. Laillisesti toimivat yritykset eivät koskaan pyydä salasanojasi tai turvakoodejasi sähköpostitse, tekstiviestillä tai puhelimitse.

4 **Pidä laitteet ja yksityiset avaimet turvassa:**

Käytä vahvoja ja ainutkertaisia salasanoja jokaiselle kryptotilillesi, pidä salasanasi salassa ja vältä samojen tunnusten uudelleenkäyttöä eri alustoilla. Ota monivaiheinen todennus käyttöön aina, kun mahdollista. Katso joitakin salasanavinkkejä täältä (↖). Pidä ohjelmistosi ja virustorjuntasi ajan tasalla ja aktivoituina.

5 **Varo odottamattomia sijoitustarjouksia:**

Varo sijoituksia, joista luvataan valtavia tuottoja. Jos jokin kuulostaa liian hyvältä ollakseen totta, se todennäköisesti on juuri sitä.

6 **Mieti ennen kuin jaat tietoa sosiaalisessa mediassa:**

Chat-ryhmät, foorumit, sosiaalisen median päivitykset ja valokuvat voivat olla arvokkaita tietolähteitä huijareille. Liiallinen itseesi tai sijoituksiisi liittyvien tietojen paljastaminen voi tehdä sinusta helpon kohteen.

Mitä tehdä, kun olet joutunut petoksen tai huijauksen uhriksi

Lopeta maksut välittömästi:

Estääksesi lisäsiirrot epäilyttäville tileille ja välttääksesi lisätappiot. Lopeta kaikki yhteydenpito huijareihin – jätä huomiotta heidän puhelunsa ja sähköpostinsa ja estä lähettäjä.

Vaihda salasanasi kaikilla laitteillasi ja sovelluksissasi/verkkosivustoillasi:

Huijarit ostavat vuodettuja tai vuotaneita salasanoja verkossa ja kokeilevat niitä useilla tileillä. Pelkästään yhden salasanan vaihtaminen ei riitä. Varmista, että vaihdat ne kaikki, jotta huijarit eivät voi käyttää niitä uudelleen.

Katkaise yhteys ja kumoa käyttöoikeudet:

Peruuta epäilyttävät käyttöoikeudet automaattisesti lohkoketjussa toimivissa digitaalisissa sopimuksissasi (älysopimus), jotta huijarit eivät käytä tokeneitasi ilman suostumustasi. Monet lompakot ja lohkoketjuhakukoneet (eng. *blockchain explorer*) tarjoavat työkaluja, joiden avulla voit nähdä, millä älysopimuksilla on tällä hetkellä pääsy tokeneihisi. Tätä varten voit:

- käyttää luotettavaa käyttöoikeuksien tarkistustyökalua (eng. *permission checker*), joka tarkistaa, onko käyttäjällä tai lohkoketjun osoitteella oikeudet suorittaa toiminto.
- tarkistaa suostumusluettelon ja
- käyttää ”kumoa”-painiketta suoraan alustalla.

Siirrä varasi:

Jos lompakkosi vaarantuu, siirrä jäljellä olevat varasi välittömästi uuteen turvalliseen lompakkoon.

Ota yhteyttä kryptopalveluntarjoajaasi:

Ilmoita kryptopalveluntarjoajallesi mahdollisimman pian virallisia yhteyskanavia käyttäen, jotta voit selvittää mahdollisia toimintavaihtoehtoja. Vaikka lohkoketjutapahtuman peruuttaminen ei useimmissa tapauksissa ole mahdollista, palveluntarjoaja voi silti pystyä jäädyttämään huijarin tilin (jos se on heidän alustallaan) ja asettaa lompakko-osoitteen mustalle listalle.

Raportoi ja varoita:

Ilmoita tapauksesta poliisille ja tarvittaessa kansalliselle finanssivalvontaviranomaiselle *(*www.finanssivalvonta.fi*)* ja kerro asiasta verkostollesi (esim. ystävillesi ja perheellesi) tietoisuuden lisäämiseksi. Nämä toimet ovat paras tapa suojella itseäsi ja muita.

Varo jatkohuijauksia:

Jos olet joutunut aiemmin petoksen uhriksi, huijari voi ottaa sinuun yhteyttä ja väittää olevansa viranomainen (esim. poliisi, vero- tai finanssivalvontaviranomainen jne.) ja tarjoutua auttamaan sinua hankkimaan menettämäsi rahat takaisin maksua vastaan. Tämä on usein toinen yritys huijata sinua. Muista: se, että sinua on huijattu kerran, ei estä sinua tulemasta huijatuksi uudelleen.

Ks. Euroopan valvontaviranomaisten yhteisvaroitus, jossa kerrotaan tarkemmin kryptovaroihin liittyvistä riskeistä (), ja tietokooste ”Kryptovarat selitettyinä: mitä MiCA tarkoittaa kuluttajalle” ().

Euroopan pankkiviranomainen, Euroopan vakuutus- ja lisäeläkeviranomainen, Euroopan arvopaperimarkkinaviranomainen, 2025

Luxemburg: Euroopan unionin julkaisutoimisto, 2025

Jäljentäminen on sallittua, kunhan lähde mainitaan.
Illustrations: © Nadezhda Buravleva / madedee / Orapun- StockAdobe.com.

PDF ISBN 978-92-9407-236-8 doi:10.2853/2566510 DZ-01-25-124-FI-N

Kryptohuijaustyypit

”Pump-and-dump” tai ”rug pull”

Näet sosiaalisessa mediassa tai verkkosivustolla mainoksen, jossa mainostetaan ”sijoitusmahdollisuutta vain rajoitetun ajan” kryptoihin ja suositellaan sijoittamista uuteen kryptotokeniin tai -hankkeeseen. Kiinnostuksenilmaisun jälkeen sinuun otetaan yhteyttä ja sinut ohjataan kryptovaihtoalustalle tai viestikanavalle (esim. Telegram tai WhatsApp). Näennäisesti uskottava kontakti lupaa nopeita voittoja tai korkeita tuottoja, jos sijoitat äkkiä. Sinua kannustetaan sijoittamaan pieni määrä ja sen jälkeen painostetaan sijoittamaan enemmän.

Mitä voi tapahtua:

Huomaat, että sijoituskohteena oleva token on arvoton ja kontakti, johon olet ollut yhteydessä, lakkaa vastaamasta. Kun yrität nostaa rahasi, verkkosivustoa ei enää ole, ja yritys ei ole tavoitettavissa. Huijarit keinotekoisesti kasvattivat tai liioittelivat vähäarvoista kryptoa lisätäkseen sen arvoa (”pumppaus”) ja myivät sitten varansa (”dumppaus”), mikä aiheutti krypton arvon romahtamisen ja jätti sijoittajille tappioita. Vaihtoehtoisesti huijarit voivat lopettaa hankkeen ja kadota varojen mukana (”rug pull” eli maton jalkojen alta vetäminen).

Esiintyminen toisena henkilönä tai yrityksen edustajana

Kun olet lähettänyt kysymyksen sosiaalisen median alustalle tai verkkosivustolle kryptolompakko-ongelmasta, saat odottamattoman yksityisviestin (eng. *direct message, DM*) tai sähköpostiviestin joltakulta, joka teeskentelee olevansa luotettava yhteyshenkilö (esim. kryptopörssi, lompakon tarjoaja, IT-tuki tai jopa ystävä). Henkilö pyytää palautuslausekettasi (eli sanaluetteloa, joka toimii keskeisenä varmuuskopiona digitaalisen lompakon käyttämiselle), salasanoja tai yksityisiä avaimia (automaattisesti luodut salauskoodit, jotka todistavat digitaalisten varojen omistajuuden).

Mitä voi tapahtua:

Kun jaat palautuslausekkeesi, salasanasi tai yksityiset avaimesi, huijari käyttää niitä varastaakseen kryptosi tai muita varoja. Muista, että yksityisten avainten menettäminen johtaa pääsyn ja omistajuuden pysyvään ja peruuttamattomaan menettämiseen kryptovaroihisi. Kun varat ovat kryptosiirtojen tapauksessa kadonneet, niiden takaisin saaminen on lähes mahdotonta, toisin kuin pankkitapahtumissa.

Tietojenkalastelu

Saat odottamattoman viestin sähköpostitse, puhelimitse, ponnahdusikkunassa tai sosiaalisessa mediassa, jonka väitetään olevan tunnetulta kryptopalveluntarjoajalta. Viestissä sinua pyydetään kirjautumaan sisään tai lataamaan uusi sovellus. Saatat myös saada sähköpostiviestin, joka näyttää olevan kryptolompakkosovelluksestasi ja jossa sinua kehotetaan ratkaisemaan turvallisuusongelma napsauttamalla epävirallisen lähteen tarjoamaa linkkiä tai päivittämällä sovellus.

Mitä voi tapahtua:

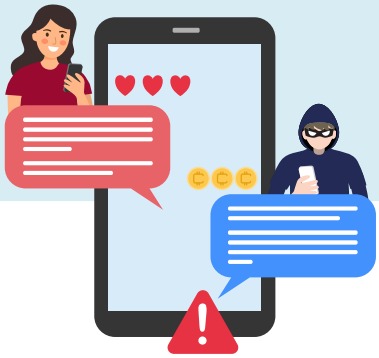
Napsauttamalla linkkiä, lataamalla sovelluksen tai skannaamalla QR-koodin asennat haittaohjelman, jonka avulla huijari pääsee käsiksi tietoihisi ja voi käyttää niitä kryptovarojesi tai varojesi varastamiseen.

Näennäisen ilmaiset lahjat

Olet törmännyt ilmoitukseen sosiaalisessa mediassa, jossa väitetään, että yritykset antavat ilmaiseksi kryptovaroja pienen kryptosijoituksen jälkeen. Tällaisia ilmoituksia voi olla videona tai julkaisuna, jossa on kuvia julkkiksesta tai tuotemerkistä- yleensä väärennettynä tai ilman lupaa käyttöön otettuna – ja niissä voidaan luvata tuplata kryptojesi arvo, jos lähetät itse ensin rahaa. Käytetyt logo, ulkoasu, suosittelut ja kieli näyttävät ammattimaisilta ja virallisilta, samoin kuin verkkosivusto, jolle sinut ohjataan.

Mitä voi tapahtua:

Kun olet lähettänyt kryptosi, et saa mitään vastineeksi, ja olet menettänyt lähetetyt rahat. Ilmaislahjoja ei ollut oikeasti jaossa, ja julkaisu tai suoratoisto, jossa oli mukana julkkiksia tai yrityksiä, oli suunniteltu huijaamaan sinua.



Rakkaushuijaus

Sinuun on ottanut yhteyttä sosiaalisessa mediassa, deittisovelluksissa tai puhelimitse/tekstiviestitse joku, jota et ole tavannut tosielämässä. Tämä henkilö voi ryhtyä kanssasi tiiviisiin, henkilökohtaisiin ja romanttisiin keskusteluihin, ja rakentaa luottamusta tekaistujen profiilien avulla. Vähitellen he ohjaavat keskustelua kohti taloudellisia mahdollisuuksia, väittämällä saatavilla olevan valtavia voittoja kryptosijoituksista ja kannustavat sinua sijoittamaan lupauksilla korkeasta tuotosta ja alhaisesta riskistä. He opastavat sinua tilin perustamisessa ja pienen alkutalletuksen tekemisessä, jotta toiminta näyttäisi uskottavalta ja asialliselta.

Huijarit luovat väärillä tiedoilla verkkoprofiileja ja käyttävät varastettuja tai tekoälyn tuottamia kuvia lähestyäkseen sinua.

Mitä voi tapahtua:

Huijari kerää mahdollisimman paljon rahaa, sitten katkaisee kaiken yhteydenpidon ja katoaa. Vilpillinen sijoitussivusto tai -sovellus viedään offline-tilaan, jolloin sinulla ei ole pääsyä oletettuihin sijoituksiin. Joissakin tapauksissa huijarit voivat käyttää huijauksen aikana saatuja tietoja tähdätäkseen ystäviisi ja perheeseesi ja tehdäkseen identiteettivarkauksia, millä voi olla taloudellisia tai oikeudellisia seurauksia sinulle (esim. huijari voi laittaa varastetut lompakot nimiisi ja sinut voidaan asettaa vastuuseen nimissäsi tehdyistä veloista tai rikoksista, kunnes toisin todistetaan).

Ponzi-järjestelmä (esim. pyramidihuijaus ja ketjukirje)

Sinut kutsutaan osallistumaan usein suositteluin tai tekaistuin menestystarinoin tuettuun projektiin, josta luvataan jatkuvaa korkeaa tuottoa kryptovarasijoituksista. Järjestelmä voidaan esittää monitasoisena markkinointimahdollisuutena, jossa ansaitset palkkioita paitsi omasta sijoituksestasi myös rekrytoimalla muita. Varhaiset sijoittajat näyttävät saavan maksuja, mikä kannustaa yhä useampia ihmisiä liittymään järjestelmään ja edistämään sitä.

Todellisuudessa ei ole aitoa liiketoimintaa tai synny oikeaa voittoa. Sen sijaan rahat tulevat yksinomaan uudempien sijoittajien maksamista osuuksista, joita käytetään tuottojen maksamiseen järjestelmän järjestäjille ja ensimmäisille osallistujille.

Mitä voi tapahtua:

Kun uudet sijoitukset hidastuvat, järjestelmä romahtaa, ja sinä, kuten useimmat osallistujat, menetät rahasi. Järjestäjät katoavat, joten varoja ei voi saada takaisin. Monitasoinen rakenne auttaa huijausta leviämään nopeasti, kun uhreista tulee tietämättään edistäjiä.

SAMANNÄKÖINEN OSOITE, JOKA SAASTUTTAA LOMPAKKOSI

Tehtyäsi kryptosiirron, huomaat uuden osoitteen ilmestyneen lompakkohistoriaasi. Tämä osoite näyttää samanlaiselta kuin jokin sellainen, jonka kanssa olet aiemmin ollut vuorovaikutuksessa. Huijarit voivat saada vääriä lompakko-osoitteita näkymään tapahtumahistoriassasi lähettämällä pienen määrän kryptoa oikean osoitteen kanssa samannäköisestä osoitteesta lompakkoosi. Päädyt tallentamaan huijarin luoman petollisen ja väärän osoitteen lompakon viimeaikaisiin toimintoihin tai automaattisiin ehdotuksiin. Huijarit luovat tarkoituksellisesti samannäköisiä osoitteita muuttamalla vain muutamia merkkejä, usein osoitteen keskellä, havaitsemisen välttämiseksi.

Mitä voi tapahtua:

Kun yrität lähettää kryptoja ja kopioit väärän osoitteen lompakkohistoriastasi, lähetät tietämättäsi varoja huijarin lompakkoon. Koska kryptosiirrot ovat usein peruuttamattomia, varat on useimmissa tapauksissa menetetty pysyvästi. Huijaus perustuu näön harhauttamiseen ja käyttäjän virheeseen, hyödyntäen tottumusta kopioida ja liittää lompakko-osoitteita ilman tarkkaa tarkistusta.