KRÜPTOPETTUSED JA KELMUSED

OLE VALVEL JA KAITSE ENNAST

Krüptovarade ja nende eriomaduste – üleilmne juurdepääsetavus, kiirus, anonüümsus ja sageli ka tehingu tagasipööramise võimaluse puudumine – kiire levik muudab sind küberkurjategijate peamiseks sihtmärgiks. Petturid ja kelmid kasutavad sinu raha kätte saamiseks keerukaid taktikaid, nagu Ponzi skeemid, fiktiivsed investeerimisvõimalused, tasuta pakkumised sotsiaalmeedias ja eksitavad sõnumid. Samuti kasutavad nad sinu rahakotini jõudmiseks erinevaid investeerima kutsuvaid petuskeeme või tuttavana näivaid aadresse. Sageli võtavad nad ühendust sotsiaalmeedia, sõnumirakenduste, e-kirjade ja ootamatute telefonikõnede kaudu, mis näivad tõepärased. Nii võivad sind ähvardada rahaline kahju, identiteedivargus ja emotsionaalne pinge.

Ole ettevaatlik ja pea silmas neid näpunäiteid:

Ole valvas võimalike krüptopettuste ja kelmuste suhtes:
saa rohkem teavet eri liiki pettuste ja kelmuste kohta (vt lk 5, 6, 7 ja 8).

Pane tähele ohumärke:
õpi kahtlast käitumist, sõnumeid või pakkumisi ära tundma (vt lk 2).

Kaitse ennast ja oma vara:
hoia oma isikuandmeid turvaliselt (vt lk 3).

Tea, mida teha, kui satud pettuse või kelmuse ohvriks
(vt lk 4).

Ohumärgid

Lubadus, mis tundub liiga hea, et olla tõsi.

Soovimatu pakkumine.

Garanteeritud kiire ja kõrge tootlus.

Surve tegutseda kiiresti (nt piiratud ajaga pakkumised, mis survestavad kohe reageerima).

Maksetaotlus jälgitamatuid meetodeid kasutades (nt krüptoraha, kinkekaardid, raha ülekanded või ettemakstud deebetkaardid).

Kutse lingil klõpsamiseks, QR-koodi skannimiseks või rakenduse allalaadimiseks.

Taotlus privaatvõtmete ja taastefraaside saatmiseks või jagamiseks (sõnade loend krüptorahakotile juurdepääsuks ja selle taastamiseks).

Kahtlane või vale URL.

Väikeste moonutustega logo – veebisait, mis kopeerib tegeliku ettevõtte veebisaidi välimust või näeb välja professionaalne, kuid millel puuduvad kontrollitud kontaktandmed, ettevõtte registreerimisteave, varasemad andmed või kontrollitav aktiivsus.

Tundmatu vahetusplatvorm.

Kahtlane manus, eriti .exe, .scr, .zip või makrotoega Office'i fail (.docm, .xlsm).

Sammud enda kaitsmiseks:

1 Peatu ja mõtle, enne kui tegutsed:

Ära kiirusta investeerimisega, teabe jagamisega ega linkidel klõpsamisega – petturid tekitavad teadlikult tunde, et asjaga on kiire. Kahtluste korral, isegi kui need on väikesed, ära reageeri ega investeeri ning kontrolli allikat hoolikalt.

2 Kontrolli allikat hoolikalt:

- Veendu alati, kust sõnumid, kõned, e-kirjad ja lingid tulevad, isegi kui need näivad olevat ametlikud, pärit sõbralt, pereliikmelt või ka avaliku elu tegelaselt. Otsi õigekirjavigu, kahtlaseid URL-e või puuduvaid turvaindikaatoreid, nt kontrolli, kas veebisaidi link sisaldab HTTPS juures s-tähte, et veenduda veebisaidi turvalisuses, ning kas ettevõtte nimes on liigseid või puuduvaid tähti.
- Ära ava soovimatutes sõnumites olevaid linke, lae rakendusi alla vaid usaldusväärsete pakkujate juurest ning ära skanni tundmatuid QR-koode.
- Isegi kui pakkumine tundub ametlik, kontrolli see alati ettevõtte veebisaidilt või sotsiaalmeedia kontolt üle (et sel oleks nt ametlikud kontrolltähised).
- Kasuta kontrollitud kontaktandmeid, et jõuda otse ettevõtte või üksikisikuni, ja ära kunagi tugine võimaliku petturi esitatud andmetele (nt otsi ettevõtte nime ise, kasuta ametlikke äriregistreid). Kelmid võivad väita, et neil on olemas tegevusluba või jäljendada loaga ettevõtte veebisaiti. Saad veenduda, kas krüptoteenuse osutajal on ELis tegevusluba, kontrollides ESMA registrit (↖). Võid vaadata ka oma riigi finantsjärelevalveasutuse veebisaiti (https://www.fi.ee), et näha, kas ettevõttele on väljastatud hoiatusi või lisatud musta nimekirja, või külastada IOSCO I-SCANi nimekirja (iosco.org/i-scan/).

3 Ära kunagi jaga paroole, privaatvõtmeid ega taastefraase:

Igaüks, kellel on neile juurdepääs, võib sinu varadele ligi pääseda. Seaduslikud ettevõtted ei küsi kunagi sinu paroole ega turvakoode e-posti, teksti või telefoni teel.

4 Hoia seadmed ja privaatvõtmed turvalisena:

Kasuta iga krüptokonto jaoks tugevaid ja kordumatuid paroole, hoia oma parooli salajas ja väldi samade paroolide kasutamist erinevatel platvormidel. Luba võimaluse korral mitmeastmeline autentimine. Vt mõned näpunäited salasõnade kohta (↖). Hoia oma tarkvara ja viirusetõrje ajakohased ning aktiveeritud.

5 Ole ootamatute investeerimispakkumistega ettevaatlik:

Ole ettevaatlik investeeringute suhtes, mis lubavad suurt tulu. Kui see kõlab liiga hästi, et tõsi olla, see ilmselt nii see ongi.

6 Mõtle enne, kui jagad sotsiaalmeedias teavet:

Vestlusrühmad, foorumid, sotsiaalmeedia postitused ja fotod võivad olla petturitele väärtuslikud teabeallikad. Liiga palju enda või oma investeeringute kohta avaldamine võid muuta sind kergeks sihtmärgiks.

Mida teha, kui oled langenud pettuse või kelmuse ohvriks

Peata tehingud kohe,

Et blokeerida kõik edasised ülekanded kahtlastele kontodele ja vältida täiendavaid kahjusid. Lõpeta petturitega kõik kontaktid – eira nende kõnesid ja e-kirju ning blokeeri saatja.

Muuda oma paroolid kõigis seadmetes ja rakendustes/veebisaitidel.

Petturid ostavad internetis lekkinud paroole ja proovivad neid mitmel kontol. Ainult ühe salasõna muutmisest ei piisa; veendu, et muudad ära kõik, et petturid ei saaks neid uuesti kasutada.

Katkesta ja tühista juurdepääs:

Tühista oma digitaalses lepingus kahtlased load, mis toimivad automaatselt plokiahelas (nutilepingud), et takistada petturitel sinu tokeneid ilma sinu nõusolekuta kasutamast. Paljud rahakotid ja plokiahela analüüsijad pakuvad vahendeid, mis võimaldavad näha, millistel nutilepingutel on praegu sinu tokenite kasutamiseks juurdepääs. Selleks võid:

- kasutada usaldusväärset loakontrolli, mis veendub, kas kasutaja või plokiahela aadress on toimingu tegemiseks loa saanud;
- vaadata läbi tüübikinnituste loetelu ja
- kasutada nuppu „Tühista“ otse platvormil.

Vii oma raha mujale:

Kui sinu rahakott on ohus, liiguta oma olemasolevad varad kohe uude turvalisse rahakotti.

Võta ühendust oma krüptoteenuse pakkujaga:

Teavita oma krüptoteenuse pakkujat võimalikult kiiresti, kasutades ametlikke kontaktkanaleid, et uurida võimalike variantide kohta. Isegi kui enamikul juhtudel ei ole plokiahela tehingu tagasipööramine võimalik, võib teenuseosutaja siiski petturi konto külmutada (kui see on nende platvormil) ja kanda rahakoti aadressi musta nimekirja.

Teavita ja hoiata:

Teata juhtumist politseile või oma riiklikule finantsjärelevalveasutusele (https://www.fi.ee) ja teavita oma võrgustikku (nt sõpru ja pereliikmeid), et suurendada teadlikkust. See on parim viis ennast ja teisi kaitsta.

Hoidu täiendava pettuse eest:

Pettur võib teie kui varasema pettuse ohvriga ühendust võtta, väites, et ta on avaliku sektori asutus (nt politsei, maksu- või järelevalveasutus) ning pakkuda teie kaotatud raha tasu eest tagasi. See on sageli järjekordne katse sind petta. Pea meeles: see, et sind on üks kord petetud, ei takista sul uuesti ohvriks langemast.

Vt krüptovaradega seotud riskide kohta lisateabe saamiseks Euroopa järelevalveasutuste ühishoiatust (↖) ja teabelehte „Krüptovara selgitus: Mida tähendab krüptovaraturgude määrus sinu kui tarbija jaoks“ (↖).

Euroopa Pangandusjärelevalve, Euroopa Kindlustus- ja Tööandjapensionide Järelevalve, Euroopa Väärtpaberiturujärelevalve, 2025

Luxembourg: Euroopa Liidu Väljaannete Talitus, 2025

Taasesitamine on lubatud tingimusel, et viidatakse allikale.
Illustrations: © Nadezhda Buravleva / madedee / Orapun- StockAdobe.com.

PDF ISBN 978-92-9407-267-2 doi:10.2853/1220718 DZ-01-25-155-ET-N

KRÜPTOPETTUSTE TÜÜBID

Pump-and-dump skeem või *rug pull*

Näed sotsiaalmeedias või veebisaidil reklaami, mis kuvab piiratud aja jooksul krüptosse investeerimise võimalust ja soovitab investeerida uude krüptotokenisse või-projekti. Pärast huvi väljendamist võetakse sinuga ühendust ja suunatakse krüptovahetusplatvormile või sõnumikanalisse (nt Telegram, Viber või WhatsApp). Näiliselt usaldusväärne kontakt lubab kiiret kasumit või suurt tulu, kui investeerid kiiresti. Sind julgustatakse investeerima väikest summat ja seejärel survestatakse investeerima rohkem.

Mis võib juhtuda:

Avastad, et investeeritud token on väärtusetu ja kontakt, kellega olete ühenduses olnud, ei vasta enam. Kui proovid oma raha välja võtta, ei ole veebisaiti enam olemas ja ettevõte on kättesaamatu. Petturid paisutasid või hindasid kunstlikult väikese väärtusega krüptot üle, et selle väärtust suurendada (pump), seejärel müüsid oma varad maha (dump), põhjustades väärtuse kokkukukkumise ja jättes investorid kahjumisse. Teise võimalusena võivad nad projekti lõpetada ja kogutud rahaga kaduda (rug pull).

Identiteedipettus

Pärast seda, kui oled postitanud sotsiaalmeedia platvormile või veebisaidile küsimuse krüptorahakoti probleemi kohta, saad ootamatu otsesõnumi (DM) või e-kirja kelleltki, kes teeskleb usaldusväärset kontakti (nt krüptobörs, rahakotiteenuse pakkuja, IT-tugi või isegi sõber). Isik küsib sinu taastefraasi (st sõnade jada, mis on su digitaalsele rahakotile juurdepääsu keskne varukoopia), paroole või privaatvõtmeid (automaatselt genereeritud krüptograafiline kood, mis tõendab digitaalsete varade omandiõigust).

Mis võib juhtuda:

Kui jagad oma taastefraasi, paroole või privaatvõtmeid, kasutab pettur neid sinu krüpto või muude vahendite varastamiseks. Pea meeles, et privaatvõtmete kaotamine toob kaasa juurdepääsu sinu krüptovarale ja omandiõiguse püsiva ning pöördumatu kadumise. Erinevalt pangatehingutest on krüptoülekannete puhul pärast raha kadumist selle tagasi saamine peaaegu võimatu.

Andmepüük

Sulle saadetakse e-posti, telefoni, hüpikakna või sotsiaalmeedia kaudu ootamatu sõnum, mis on väidetavalt tuntud krüptovarateenuse osutajalt. Sõnum kutsub sind kuhugi sisse logima või uut rakendust alla laadima. Samuti võid saada e-kirja, mis näib olevat pärit sinu krüptorahakoti rakendusest, kutsudes üles turvaprobleemi lahendama, mitteametliku allika pakutaval lingil klõpsama või rakendust värskendama.

Mis võib juhtuda:

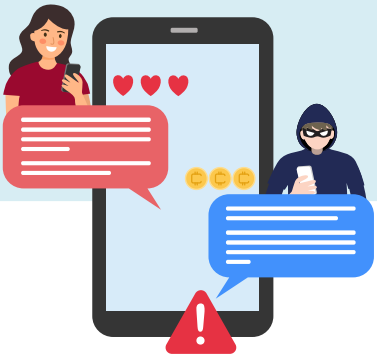
Klõpsates lingil, laadides alla rakenduse või skaneerides QR-koodi, installid pahavara, mis võimaldab petturil teabele juurde pääseda ja seda sinu krüptovara või raha varastamiseks kasutada.

Kingituspettus

Sa kohtad sotsiaalmeedias teadaannet, et ettevõtted annavad pärast väikest krüptoinvesteeringut vastu krüptovara. Need hõlmavad videot või postitust, mis sisaldab fotosid kuulsusest või kaubamärgist, mis on tavaliselt võltsitud või ilma loata saadud ning lubavad sinu krüpto kahekordistada, kui esmalt raha saadad. Logo, kujundus, iseloomustused ja kasutatud keel näevad välja professionaalsed ja ametlikud, nagu ka veebisait, kuhu sind suunatakse.

Mis võib juhtuda:

Pärast krüpto saatmist ei saa sa midagi vastu ja oled saadetud raha kaotanud. Kingitus oli pettus ja postitus või otseülekanne, mis kujutas kuulsusi või ettevõtteid, oli mõeldud sinu eksitamiseks.



Armukelmus

Sinuga on sotsiaalmeedias, tutvumisrakendustes või telefoni/teksti teel ühendust võtnud keegi, keda sa pole päriselus kohanud. See isik võib vestelda sinuga sagedasti, isiklikel ja romantilistel teemadel, luues võltsitud profiilide abil usaldust. Järk-järgult juhib ta vestluse rahaliste võimaluste poole, väites tohutut kasumit krüptoinvesteeringutest ja julgustades sind suure tulu ja madala riski lubadustega investeerima. Ta juhendab sind konto loomisel ja väikese esialgse sissemakse tegemisel, et skeem tunduks seaduslik.

Petturid loovad võltsitud veebiprofiile ja kasutavad sinu poole pöördumiseks varastatud või tehisintellekti loodud pilte.

Mis võib juhtuda:

Pettur kogub nii palju raha kui võimalik, seejärel katkestab suhtluse ja kaob. Võltsitud investeerimisveebisait või -rakendus eemaldatakse võrguühenduseta, jättes sulle juurdepääsu väidetavatele investeeringutele. Mõnel juhul võivad petturid kasutada pettuse käigus saadud teavet sinu sõprade ja perekonna sihikule võtmiseks ning identiteedivarguse toime panemiseks, millel võivad olla sulle rahalised või õiguslikud tagajärjed (nt pettur võib sinu nimel kinnitada varastatud rahakotte ja sind võidakse pidada vastutavaks sinu nime all toime pandud võlgade või kuritegude eest, kuni ei ole tõendatud vastupidist).

Ponzi skeem

Sind kutsutakse osalema projektis, mis lubab krüptovarainvesteeringutelt püsivalt suurt tulu, mida sageli toetavad iseloomustused või võltsitud edulood. Skeemi võib esitleda mitmetasandilise turundusvõimalusena, kus teenid kasu mitte ainult oma investeeringust, vaid ka teiste värbamisest. Varajased investorid näivad saavat väljamakseid, mis julgustab rohkem inimesi skeemiga ühinema ja seda edendama.

Tegelikkuses reaalset äritegevust ega kasumit ei teki. Selle asemel tuleb raha üksnes uuemate investorite panusest, mida kasutatakse tulu maksmiseks kava korraldajatele ja esimestele osalejatele.

Mis võib juhtuda:

Kui uued investeeringud vähemaks jäävad, variseb skeem kokku ja sina, nagu enamik osalejaid, kaotad oma raha. Korraldajad kaovad, jätmata võimalust raha tagasi saada. Mitmetasandiline struktuur aitab pettusel kiiresti levida, kuna ohvrid saavad enda teadmata skeemi edendajateks.

Sarnane aadress, mis mürgitab sinu rahakoti

Pärast krüptotehingu tegemist märkad oma rahakoti ajaloos uut aadressi. See aadress sarnaneb aadressiga, millega oled varem suhelnud. Petturid saavad sinu tehingute ajaloos kuvada võltsitud rahakoti aadresse, saates sinu rahakotti sarnaselt aadressilt väikese koguse krüptot. Lõpuks salvestad sa oma rahakoti viimasesse tegevusse või pakud automaatselt petturi loodud valeaadressi. Petturid loovad sarnaseid aadresse sihilikult, muutes nende tuvastamise vältimiseks ainult mõnda märki, sageli aadressi keskel.

Mis võib juhtuda:

Kui proovid saata krüptot ja kopeerida vale aadressi oma rahakoti ajaloost, saadad raha tahtmatult petturi rahakotti. Kuna krüptotehingud on sageli tagasipööramatud, kaob sinu raha enamikul juhtudel jäädavalt. See pettus tugineb visuaalsele eksitamisele ja kasutaja tehtud veale, tuginedes rahakoti aadresside kopeerimise ja kleepimise harjumusele ilma hoolika kontrollita.