KRIPTOTURTO APGAULĖS IR SUKČIAVIMAS

BŪKITE BUDRŪS IR APSAUGOKITE SAVE

Dėl spartaus kriptoturto populiarėjimo ir jo specifinių savybių – visuotinio prieinamumo, spartos, anonimiškumo ir , dažnu atveju, sandorių negrįžtamumo – esate pagrindinis kibernetinių nusikaltėlių taikinys. Apgavikai ir sukčiai, siekdami jus apgauti, sukčiai taiko įvairias rafinuotas taktikas, pavyzdžiui, „Ponzio schemas“, netikras investavimo galimybes, „nemokamas dovanas“ socialiniuose tinkluose ir melagingas žinutes. Jie taip pat naudoja romantinio investavimo apgavystes ir „adreso užnuodijimą“ (angl. *address poisoning*), kai piniginės istorijoje atsiranda į Jūsų tikruosius gavėjų adresus panašių įrašų. Dažniausiai jie susisiekia per socialinius tinklus, el. paštą, netikėtus telefono skambučius ir susirašinėjimo programėles – visa tai gali skambėti labai įtikinamai. Rizikuojate patirti finansinių nuostolių, tapti tapatybės vagystės ar emocinės žalos aukomis.

Būkite atsargūs ir vadovaukitės toliau pateiktais patarimais.

Būkite budrūs dėl galimų kriptoturto apgaulių ir sukčiavimo:
Kad sužinotumėte daugiau apie skirtingas apgaulių rūšis (žr. 5, 6, 7 ir 8 psl.).

Atpažinkite įspėjamuosius ženklus:
išmokite atpažinti įtartiną elgesį, žinutes ar pasiūlymus (žr. 2 psl.).

Apsaugokite save ir savo turtą:
apsaugokite savo asmeninę informaciją (žr. 3 psl.).

Žinokite, ką daryti, jei nukentėjote nuo sukčiavimo ar apgaulės
(žr. 4 psl.).

Įspėjamieji ženklai

Pažadas, kuris skamba per gerai, kad būtų tiesa.

Neprašytas (neteikėte paklausimo) pasiūlymas.

Garantuota, greita ir didelė grąža.

Skubinimas imtis veiksmų (pvz., „tik ribotą laiką“ galiojančios akcijos, verčiančios skubėti).

Prašymas atsiskaityti nesekamais būdais (pvz., kriptoturtu, dovanų kortelėmis, banko pervedimais ar išankstinio apmokėjimo kortelėmis).

Kvietimas spustelėti nuorodą, nuskaityti QR kodą arba atsisiųsti programėlę.

Prašymas siųsti arba dalintis privačiais raktais ir slaptafrazėmis (angl. *seed phrase* – žodžių seka, skirta prieigai prie kriptoturto piniginės ir jos atkūrimui).

Įtartinas arba neteisingas URL

Logotipo iškraipymai; svetainė, kopijuojanti tikrosios bendrovės svetainę arba atrodanti profesionaliai, bet neturinti patikimų kontaktinių duomenų, registracijos duomenų, veiklos istorijos ar patikrinamos reputacijos.

Nežinoma keityklos platforma.

Įtartini priedai, ypač .exe, .scr, .zip arba makrokomandomis įgalinti „Office“ failai (*.docm*, *.xlsm*).

Žingsniai, kaip apsisaugoti:

1 **Pristabdykite ir pagalvokite prieš imdamiesi veiksmų:**

Neskubėkite investuoti, dalintis informacija ar spustelėti nuorodų – sukčiai sąmoningai sukuria skubos jausmą. Kilus bet kokioms abejonėms, net ir nedidelėms, neveikite ar neinvestuokite ir atidžiai patikrinkite šaltinį.

2 **Atidžiai patikrinkite šaltinį:**

- Visada patikrinkite, iš kur gaunami pranešimai, skambučiai, el. laiškai ir nuorodos, net jei jie atrodo oficialūs, pateikiami jūsų draugų ar šeimos narių ar net viešojo asmens. Ieškokite rašybos klaidų, keistų URL adresų arba trūkstamų saugumo rodiklių, pvz., patikrinkite, ar svetainės nuorodoje „HTTPS“ yra „s“, kad įsitikintumėte, jog svetainė yra saugi, ir patikrinkite, ar įmonės pavadinime nėra papildomų ar trūkstamų raidžių.
- Neatidarykite nuorodų iš neužsakytų pranešimų, įdiekite tik oficialias programėles iš patikimų programėlių parduotuvių ir nenuskaitykite nežinomų QR kodų.
- Net jei pasiūlymas atrodo oficialus, visada patikrinkite jį bendrovės interneto svetainėje arba įsitikinkite, kad socialinio tinklo paskyra yra patvirtinta (pvz., turi oficialų žymėjimą).
- Naudokite patikrintus kontaktinius duomenis, kad tiesiogiai pasiektumėte įmonę ar asmenį, ir niekada nesiremkite įtariamo sukčiautojo pateikta kontaktine informacija (pvz., savarankiškai ieškokite įmonės pavadinimo, naudokite patikrintus verslo katalogus). Sukčiai gali teigti, kad yra įgalioti, arba imituoti įgaliotos bendrovės svetainę. Ar kriptoturto paslaugų teikėjas ES yra licencijuotas, galite patikrinti ESMA registre (↖). Taip pat galite pasitikrinti savo nacionalinės priežiūros institucijos svetainėje (↖), ar apie įmonę nėra įspėjimų arba, jog ji neįtraukta į juoduosius sąrašus, peržiūrėkite IOSCO I-SCAN sąrašą (iosco.org/i-scan/https://www.iosco.org/i-scan/).

3 **Niekada nesidalinkite slaptažodžiais, privačiais raktais ar slaptafrazėmis:**

Turėdami šią informaciją, kiti gali perimti Jūsų turtą. Tinkamos įmonės niekada neprašys jūsų slaptažodžių ar saugos kodų el. paštu, žinute ar telefonu.

4 **Laikykite įrenginius ir privačius raktus saugiai:**

Naudokite stiprius ir unikalius slaptažodžius kiekvienai savo kriptografinei paskyrai, saugokite savo slaptažodį paslaptyje ir venkite pakartotinai naudoti tuos pačius kredencialus skirtingose platformose. Jei įmanoma, įjunkite kelių žingsnių autentifikavimą. Žr. kai kuriuos slaptažodžių patarimus čia (↖) *[jei taikoma, pakeiskite nacionalinėmis nuorodomis]*. Nuolat atnaujinkite ir aktyvuokite savo programinę įrangą ir antivirusinę apsaugą.

5 **Būkite atsargūs su netikėtais investiciniais pasiūlymais:**

Būkite atsargūs su investicijomis, kurios žada didelę grąžą. Jei tai skamba per daug gerai, kad būtų tiesa, tai tikriausiai taip ir yra.

6 **Pagalvokite prieš dalindamiesi informacija socialiniuose tinkluose:**

Pokalbių grupės, forumai, socialinės žiniasklaidos įrašai ir nuotraukos sukčiams gali būti vertingas informacijos šaltinis. Per didelis atvirumas apie save ar investicijas padaro jus lengvu taikiniu.

Ką daryti, jei tapote apgaulės ar sukčiavimo auka

Nedelsdami sustabdykite operacijas,

Kad užkirstumėte kelią tolesniems pervedimams į įtartinas paskyras ir papildomiems nuostoliams. Nutraukite bet kokį kontaktą su sukčiais – ignoruokite jų skambučius ir e. laiškus ir užblokuokite siuntėją.

Pakeiskite savo slaptažodžius visuose savo įrenginiuose ir programose/svetainėse.

Sukčiai perka nutekintus slaptažodžius internete ir bando juos naudoti daugelyje paskyrų. Pakeisti tik vieną slaptažodį nepakanka; pasirūpinkite, kad jie visi būtų pakeisti, kad sukčiai negalėtų jų pakartotinai panaudoti.

Atjunkite ir atšaukite suteiktas prieigas.

Atšaukite įtartinus leidimus jūsų skaitmeninėse sutartyse, kurios automatiškai vykdomos blokų grandinėje (išmaniosios sutartys), kad sukčiai negalėtų be jūsų sutikimo išleisti žetonų. Daugelis piniginių ir blokų grandinių naršyklių leidžia matyti, kurios išmaniosios sutartys turi teisę leisti jūsų žetonus. Galite:

- naudoti patikimą „leidimų tikrintuvą“ (angl. *permission checker*) – jis parodo, ar naudotojas ar adresas turi teisę atlikti veiksmą;
- peržiūrėti suteiktų leidimų sąrašą;
- naudotis **„revoke“** (atšaukti) funkcija tiesiogiai platformoje.

Perkelkite savo lėšas:

Jei jūsų piniginė yra pažeista, nedelsdami perkelkite likusį turtą į naują, saugią piniginę.

Susisiekite su savo kriptoturto paslaugų teikėju:

Kuo greičiau praneškite oficialiais kanalais – net jei dažniausiai blokų grandinės operacijų atšaukti neįmanoma, paslaugų teikėjas gali užšaldyti sukčiaus paskyrą (jei ji jų platformoje) ir įtraukti piniginės adresą į juodąjį sąrašą.

Praneškite ir perspėkite.

Praneškite policijai ar savo nacionalinei finansų priežiūros institucijai (https://www.lb.lt/) ir informuokite savo aplinką (draugus, šeimą) – taip didinsite informuotumą. Šie veiksmai geriausiai padeda apsaugoti jus ir kitus.

Saugokitės „pakartotinio išviliojimo“ apgaulių (angl. *recovery room*).

Sukčiai gali vėl su jumis susisiekti kaip ankstesnės apgaulės auka, apsimesti viešąja institucija (pvz., policija, mokesčių ar finansų institucija) ir siūlyti „už mokestį“ atgauti prarastus pinigus. Dažniausiai tai – dar viena apgaulė. Atminkite: jei buvote apgauti kartą, tai nereiškia, kad nebūsite apgauti vėl.

Daugiau informacijos: bendra Europos priežiūros institucijų (ESA) įspėjamoji žinutė apie su kriptoturtu susijusią riziką ( )ir informacinį pranešimą„Kriptoturtas: Ką MiCA reiškia vartotojui“ .

Europos bankininkystės institucija, Europos draudimo ir profesinių pensijų institucija, Europos vertybinių popierių ir rinkų institucija, 2025
Liuksemburgas: Europos Sąjungos leidinių biuras, 2025

PDF ISBN 978-92-9407-260-3 doi:10.2853/3429697 DZ-01-25-148-LT-N

KRIPTOTURTO SUKČIAVIMO RŪŠYS.

„Pump-and-dump" schema arba „rug pull"

Matote reklamą (reklamą) socialinėje žiniasklaidoje arba interneto svetainėje, kurioje reklamuojama „riboto laiko investavimo galimybė" į kriptoturtą ir rekomenduojama investuoti į naują kriptoturto žetoną arba projektą. Išreiškus susidomėjimą su jumis susisiekiama ir nukreipiama į kriptoturto keityklą ar šifruotų žinučių kanalą (pvz., „Telegram", „Viber" ar „WhatsApp"). Iš pažiūros patikimas kontaktinis asmuo žada greitą pelną ar didelę grąžą, jei investuosite nedelsiant. Skatinama investuoti nedidelę sumą, o vėliau skatinama investuoti daugiau.

Kas gali nutikti:

Paaiškėja, kad žetonas bevertis, o kontaktas nebeatsako. Bandant išsiimti pinigus, svetainė nebeveikia, įmonės neįmanoma pasiekti. Sukčiai dirbtinai išpūtė menkavertį kriptoturtą, kad pakeltų kainą („pump"), o tada savo turtą pardavė („dump"), sukeldami kainos griūtį ir palikdami investuotojus su nuostoliais. Arba jie tiesiog uždarė projektą ir dingo su lėšomis („rug pull").

Apsimetėlių apgaulė.

Po to, kai socialinės žiniasklaidos platformoje ar svetainėje paskelbėte klausimą apie kriptoturto piniginės problemą, gaunate netikėtą privačią žinutę arba el. laišką nuo asmens, apsimetančio patikimu kontaktu (pvz., keitykla, piniginės teikėju, IT pagalba ar net draugu). Jūsų prašoma slaptafrazės, slaptažodžių ar privačių raktų.

Kas gali atsitikti:

Pasidalijus slaptafrazėmis, slaptažodžiais ar privačiais raktais, sukčius pasisavina Jūsų kriptoturtą ar kitas lėšas. Praradus privačius raktus, prieiga ir nuosavybė į kriptoturtą paprastai prarandama negrįžtamai. Skirtingai nei banko operacijos, kriptoturto pervedimai dažniausiai negrąžinami.

Fišingas.

Netikėtai gaunate el. laišką, skambutį, iššokantį langą ar žinutę socialiniuose tinkluose, esą nuo žinomo kriptoturto paslaugų teikėjo. Jūsų prašoma prisijungti arba atsisiųsti naują programėlę; taip pat galite gauti laišką, kuris atrodo nuo jūsų piniginės programėlės, raginantį „išspręsti saugumo problemą“ spustelint neoficialią nuorodą ar atnaujinti programėlę.

Kas gali atsitikti:

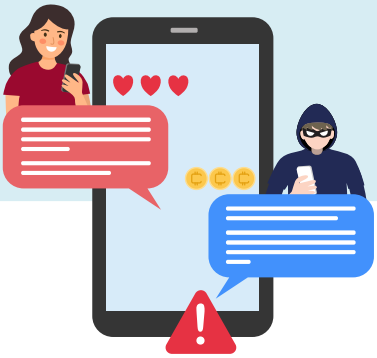
Spustelėję nuorodą, atsisiuntę programėlę ar nuskenavę QR kodą, įdiegiate kenkėjišką programą, kuri leidžia sukčiui pasisavinti informaciją ir pavogti jūsų kriptoturtą ar lėšas.

„Giveaway“ (dovanojimo) apgaulė.

Socialiniuose tinkluose matote skelbimą, kad „įmonės dalija kriptoturtą“ mainais už nedidelę jūsų kriptoturto įmoką. Pridedamas vaizdo įrašas ar įrašas su žinomu asmeniu ar prekės ženklu – paprastai netikras arba naudojamas be leidimo – žadantis „padvigubinti Jūsų kriptoturtą“, jei pirmiausia padarysite pavedimą. Logotipas, dizainas, atsiliepimai ir kalba atrodo profesionalūs, taip pat ir nukreipiama svetainė.

Kas gali atsitikti:

Pervedę kriptoturtą nieko negaunate, o siųsti pinigai prarandami. „Dovana“ buvo netikra, o įrašas ar transliacija – apgaulingai imitavo žinomus asmenis ar įmones.



Romantinis investicinis sukčiavimas

Socialiniuose tinkluose, pažinčių programėlėse ar telefonu/žinutėmis su jumis susisiekia asmuo, kurio nesate sutikę realiame gyvenime. Jis palaiko dažnus, asmeniškus ir romantiškus pokalbius, naudodamas netikras anketas, palaipsniui pokalbį nukreipia į „finansines galimybes“, žada didelę grąžą iš kriptoturto investicijų ir ragina jus investuoti su „didele grąža ir maža rizika“. Jus paskatina susikurti paskyrą ir atlikti nedidelį pradinį įnašą, kad viskas atrodytų teisėta.

Dažnai naudojamos vogtos ar dirbtinio intelekto sugeneruotos nuotraukos.

Kas gali atsitikti:

Sukčiai išvilioja kuo daugiau lėšų, tuomet nutraukia ryšį ir dingsta. Netikra investavimo svetainė ar programėlė išjungiama, Jūs netenkate prieigos prie tariamų investicijų. Kartais sukčiai panaudoja surinktą informaciją taikydamiesi į jūsų artimuosius ar vykdydami tapatybės vagystę, kas gali turėti finansinių ar teisinių pasekmių (pvz., sukčius gali patvirtinti pavogtas pinigines jūsų vardu, o jūs galite būti laikinai laikomi atsakingais už skolas ar nusikaltimus iki kol tai paneigiama).

Ponzio schema.

Jums pasiūloma dalyvauti projekte, žadančiame pastovią didelę grąžą iš kriptoturto investicijų; pateikiami liudijimai ar netikros sėkmės istorijos. Schema gali būti pristatoma kaip daugiapakopė rinkodara – uždirbate ne tik nuo savo investicijos, bet ir už naujų dalyvių pritraukimą.

Pirmieji investuotojai regis gauna išmokas, todėl prisijungia vis daugiau žmonių.

Kas gali atsitikti:

Iš tikrųjų pelnas negaunamas – išmokos mokamos iš naujų dalyvių įnašų, kurie keliauja schemos organizatoriams ir ankstyviesiems dalyviams. Sulėtėjus naujoms įmokoms schema subyra, o dauguma dalyvių praranda pinigus; organizatoriai dingsta ir lėšų atgauti nepavyksta. Daugiapakopė struktūra padeda apgaulei plisti, nes aukos nesąmoningai tampa jos platintojais.

Į TIKRĄ ADRESĄ PANAŠUS ADRESAS, „UŽNUODIJANTIS“ JŪSŲ PINIGINĘ (ANGL. *ADDRESS POISONING*).

Atlikę kriptoturto operaciją, piniginės istorijoje pastebite naują adresą, panašų į tą, su kuriuo anksčiau bendravote. Sukčiai gali jūsų istorijoje sukurti netikrų adresų įspūdį – jie iš panašaus adreso atsiunčia labai mažą kriptoturto sumą, todėl tas adresas išsaugomas Jūsų „paskutinėse operacijose“ ar automatinėse siūlymų sąrašuose. Paprastai pakeičiamos kelios vidurinės simbolių sekos, kad apgaulė būtų sunkiau pastebima.

Kas gali atsitikti:

Vėliau kopijuodami neteisingą adresą iš istorijos netyčia pervedate lėšas sukčiaus piniginei. Kadangi kriptoturto operacijos dažnai negrįžtamos, lėšos dažniausiai prarandamos visam laikui. Apgaulė remiasi vizualiniu klaidinimu ir įpročiu „kopijuoti–įklijuoti“ neįsižiūrint.