KRĀPŠANA AR KRIPTOAKTĪVIEM

ESI MODRS UN SARGĀ SEVI

Kriptoaktīvu popularitātes straujais pieaugums un to īpašības, proti, globālā pieejamība, izmantošanas ātrums, anonimitāte un bieži vien darījumu neatgriezeniskums, padara tevi par kibernoziedznieku galveno mērķi. Krāpnieki, lai tevi apkrāptu, izmanto sarežģītas metodes, piemēram, Ponci shēmas, neīstas ieguldījumu iespējas, bezmaksas piedāvājumus sociālajos medijos un nepatiesas ziņas. Viņi izmanto arī romantisko krāpšanu vai īstajām adresēm līdzīgas adreses, lai saindētu (*poison*) tavu maku. Krāpnieki bieži uzrunā tevi, izmantojot sociālos medijus, ziņapmaiņas lietotnes, e-pastu un negaidītus tālruņa zvanus, un šķiet, ka viņu teiktais ir pilnīgi reāls. Tu vari saskarties ar tādiem riskiem kā finansiāli zaudējumi, identitātes zādzība un emocionālas ciešanas.

Esi piesardzīgs un, lai pasargātu sevi, ņem vērā šos ieteikumus:

Uzmanies no iespējamas krāpšanas ar kriptoaktīviem – uzzini vairāk par dažādiem krāpšanas veidiem (5., 6., 7. un 8. lpp.).

Atpazīsti brīdinājuma signālus – iemācies atpazīt aizdomīgu rīcību, ziņojumus vai piedāvājumus (sk. 2. lpp.).

Aizsargā sevi un savus aktīvus un personas datus (sk. 3. lpp.).

Zini, ko darīt, ja esi kļuvis par krāpšanas upuri (sk. 4. lpp.).

Brīdinājuma signāli

Solījumi, kas šķiet pārāk labi, lai būtu patiesi.

Uzmācīgi piedāvājumi.

Garantēta ātra un liela atdeve.

Aicinājums rīkoties steidzami (piemēram, laikā ierobežots piedāvājums, kas liek tev rīkoties nekavējoties).

Pieprasījums veikt maksājumu, izmantojot neizsekojamus paņēmienus (piemēram, kriptoaktīvi, dāvanu kartes, pārvedumi vai priekšapmaksas debetkartes).

Aicinājums noklikšķināt uz saites, skenēt kvadrātkodu (QR kodu) vai lejupielādēt lietotni.

Pieprasījums nosūtīt vai koplietot privātās atslēgas un atslēgas (*seed*) frāzes (vārdu virkne, kas ļauj piekļūt kriptovalūtu makam vai atgūt to).

Aizdomīga vai nepareiza tīmekļa saite (URL).

Logotips ar nelielām izmaiņām, tīmekļa vietne, kura nokopēta no reāla uzņēmuma tīmekļa vietnes vai izskatās profesionāli izstrādāta, bet kurā trūkst pārbaudītas kontaktinformācijas vai uzņēmuma reģistrācijas informācijas, kā arī nav informācijas par līdzšinējo pieredzi vai kura neļauj pārliecināties par uzņēmuma pastāvēšanu.

Nezināma apmaiņas platforma.

Aizdomīgs pielikums, jo īpaši .exe, .scr, .zip vai *Office* datnes ar automatizētām (makro) komandām (.docm, .xlsm).

Darbības sevis pasargāšanai

1 **Pirms rīkojies, padomā –**

Nesteidzies ieguldīt, dalīties ar informāciju vai klikšķināt uz saites, jo krāpnieki apzināti rada steidzamības sajūtu. Ja tev ir kaut mazākās šaubas, nedari to, ko tev lūdz, neieguldi un rūpīgi pārbaudi informācijas avotu.

2 **Rūpīgi pārbaudi avotu:**

- vienmēr pārbaudi, no kurienes tiek sūtīti ziņojumi, e-pasta vēstules un saites vai tiek veikti tālruņa zvani, pat ja tie šķiet oficiāli vai zvana kāds draugs vai ģimenes loceklis, vai sabiedrībā zināma persona. Raugies, vai nav pareizrakstības kļūdu, aizdomīgu tīmekļa vietnes saišu (URL) un vai netrūkst norāžu par drošu darījumu, piemēram, pārbaudi, vai tīmekļa vietnes saites daļā "HTTPS" ir iekļauts burts "s", lai pārliecinātos, ka tīmekļa vietne ir droša. Tāpat pārbaudi, vai uzņēmuma nosaukumā nav kāda lieka vai trūkstoša burta;
- neatver saites nevēlamos ziņojumos, instalē tikai oficiālas lietotnes no uzticamiem lietotņu veikaliem un neskenē nezināmus kvadrātkodus (QR kodus);
- pat ja piedāvājums izskatās oficiāls, vienmēr pārbaudi to uzņēmuma tīmekļa vietnē. Tāpat pārbaudi, vai sociālo mediju konts ir verificēts (piemēram, tam ir oficiāla atzīme);
- izmanto pārbaudītu kontaktinformāciju, lai tieši sazinātos ar uzņēmumu vai kādu personu, un nekad nepaļaujies uz kontaktinformāciju, ko sniedzis iespējamais krāpnieks (piemēram, pats atrodi uzņēmuma nosaukumu, izmanto pārbaudītus uzņēmumu katalogus). Krāpnieks var apgalvot, ka ir pilnvarots, vai atdarināt darbības atļauju saņēmuša uzņēmuma tīmekļa vietni. Vari pārbaudīt, vai kriptoaktīvu pakalpojumu sniedzējs ir saņēmis darbības atļauju ES, skatot Eiropas Vērtspapīru un tirgu iestādes reģistru (↖). Vari arī pārbaudīt, vai uzņēmums atrodams Latvijas Bankas tirgus dalībnieku datubāzē (↖) un ir saņēmis darbības atļauju, vai par to ir publiskoti brīdinājumi, vai tas ir iekļauts Starptautiskās Vērtspapīru komisiju organizācijas I-SCAN sarakstā (iosco.org/i-scan/).

3 **Nekad neatklāj paroles, privātās atslēgas vai atslēgas frāzes –**

Visas personas, kam ir piekļuve šai informācijai, var pārņemt kontroli pār taviem aktīviem. Likumīgi uzņēmumi nekad neprasīs tavas paroles vai drošības kodus e-pastā, īsziņā vai pa tālruni.

4 **Aizsargā ierīces un privātās atslēgas –**

Izmanto drošas un unikālas paroles visiem saviem kriptoaktīvu kontiem, neatklāj savas paroles un izvairies no to pašu pieteikšanās datu atkārtotas izmantošanas dažādās platformās. Ja iespējams, izmanto daudzfaktoru autentifikāciju. Dažus padomus par parolēm skati šeit: ↖. Atjaunini un aktivizē savu programmatūru un pretvīrusu aizsardzību.

5 **Ievēro piesardzību, izvērtējot negaidītus ieguldījumu piedāvājumus, –**

Uzmanies no ieguldījumiem, kas sola milzīgu atdevi. Ja kaut kas izklausās pārāk labi, lai būtu patiesība, visticamāk, tā nav patiesība.

6 **Padomā, pirms kopīgo informāciju sociālajos medijos, –**

Tērzēšanas grupas, forumi, ieraksti sociālajos medijos un fotogrāfijas var būt vērtīgi informācijas avoti krāpniekiem. Atklājot pārāk daudz informācijas par sevi vai saviem ieguldījumiem, vari kļūt par vieglu mērķi.

Ko darīt, ja esi kļuvis par krāpšanas upuri

Nekavējoties pārtrauc darījumus,

Lai bloķētu jebkādus turpmākus pārskaitījumus uz aizdomīgiem kontiem un izvairītos no papildu zaudējumiem. Pārtrauc jebkādu saziņu ar krāpniekiem – ignorē viņu zvanus un e-pasta vēstules un bloķē sūtītāju.

Nomaini paroles visās savās ierīcēs un lietotnēs/tīmekļa vietnēs –

Krāpnieki tiešsaistē iegādājas nopludinātas paroles un mēģina tās lietot vairākos kontos. Ar vienas paroles maiņu vien nepietiek – pārliecinies, ka tiek nomainītas visas paroles, lai krāpnieki nevarētu tās izmantot atkārtoti.

Atvieno un atsauc piekļuvi –

Atcel savā digitālajā līgumā aizdomīgas atļaujas, kas automātiski darbojas blokķēdē (viedais līgums), lai neļautu krāpniekiem tērēt tavus žetonus bez tavas piekrišanas. Daudzi maki un blokķēžu pārlūki piedāvā rīkus, kas ļauj redzēt, kuri viedie līgumi pašlaik nodrošina piekļuvi, lai varētu tērēt tavus žetonus. Šajā nolūkā vari:

- izmantot uzticamu "atļauju pārbaudītāju" – rīku, kas pārbauda, vai lietotājam vai blokķēdes adresei ir tiesības veikt attiecīgo darbību;
- pārskatīt atļauju sarakstu;
- izmantot atsaukšanas pogu tieši platformā.

Pārvieto savus līdzekļus –

Ja ar tavu maku ir notikušas manipulācijas, nekavējoties pārsūti atlikušos aktīvus uz jaunu, drošu maku.

Sazinies ar savu kriptoaktīvu pakalpojumu sniedzēju –

Pēc iespējas ātrāk informē savu kriptoaktīvu pakalpojumu sniedzēju, izmantojot oficiālos saziņas kanālus, lai uzzinātu par pieejamajām iespējām. Lai gan vairumā gadījumu blokķēdes darījuma atcelšana nebūs iespējama, pakalpojumu sniedzējs var iesaldēt krāpnieka kontu (ja tas ir pakalpojumu sniedzēja platformā) un iekļaut maka adresi melnajā sarakstā.

Ziņo un brīdini –

Ziņo par incidentu policijai vai savas valsts finanšu uzraudzības iestādei (↖) un informē savus draugus un ģimenes locekļus, lai arī viņi par to zinātu. Šis ir labākais veids, kā aizsargāt sevi un citus.

Uzmanies no krāpšanas, ja vienreiz jau esi kļuvis par krāpšanas upuri.

Krāpnieks var sazināties ar tevi, zinot, ka jau iepriekš tiki apkrāpts. Viņš var apgalvot, ka ir no valsts iestādes (piemēram, no policijas, nodokļu vai finanšu iestādes utt.), un piedāvāt par maksu atgūt zaudēto naudu. Tas bieži ir vēl viens mēģinājums tevi apkrāpt. Atceries, ka vienreiz apkrāpta persona var tikt apkrāpta atkārtoti.

Sk. kopīgo Eiropas uzraudzības iestāžu brīdinājumu, lai uzzinātu vairāk par riskiem, kas saistīti ar kriptoaktīviem (↖), un faktu lapu "Kriptoaktīvi. Ko MiCA regula nozīmē jums kā patērētājam" (↖).

Eiropas Banku iestāde, Eiropas Apdrošināšanas un aroda pensiju iestāde, Eiropas Vērtspapīru un tirgu iestāde, 2025
Atļauts reproducēt, norādot avotu.
Illustrations: © Nadezhda Buravleva / madedee / Orapun- StockAdobe.com.
Luksemburga: Eiropas Savienības Publikāciju birojs, 2025
PDF ISBN 978-92-9407-224-5 doi:10.2853/0718135 DZ-01-25-112-LV-N

KRĀPŠANAS AR KRIPTOAKTĪVIEM VEIDI

CENAS NEPATIESAS PAAUGSTINĀŠANAS (*PUMP-AND-DUMP*) SHĒMA UN JAUNU KRĀPNIECISKU KRIPTOAKTĪVU (*RUG PULL*) SHĒMA

Tu sociālajos medijos vai tīmekļa vietnē redzi reklāmu, kura popularizē "iespēju ieguldīt kriptoaktīvos, kas pieejama ierobežotu laiku" un kurā tiek ieteikts ieguldīt jaunā kriptožetonā vai projektā. Ja paud interesi, ar tevi kāds sazinās un novirza uz kriptovalūtu biržas platformu vai ziņapmaiņas kanālu (piemēram, *Telegram*, *Viber* vai *WhatsApp*). Šķietami uzticama kontaktpersona sola ātru vai lielu peļņu, ja ieguldījumu veiksi nekavējoties. Tevi mudina investēt nelielu summu, bet pēc tam spiež ieguldīt vairāk.

Kas varētu notikt?

Tu atklāj, ka iegādātais žetons ir bezvērtīgs, un kontaktpersona, ar kuru pirms tam sazinājies, vairs neatbild. Kad mēģini izņemt savu naudu, izrādās, ka tīmekļa vietne vairs nepastāv un ka uzņēmums nav atrodams. Krāpnieki mākslīgi palielina vai pārāk augstu novērtē zemas vērtības kriptoaktīvu, lai palielinātu tā vērtību (pump), bet pēc tam pārdod savus aktīvus (dump), izraisot strauju vērtības kritumu un radot zaudējumus ieguldītājiem. Citā gadījumā krāpnieki var izbeigt projektu un pazust ar visiem līdzekļiem (rug pull).

UZDOŠANĀS PAR CITU PERSONU

Kad tu sociālo mediju platformā vai tīmekļa vietnē uzdod jautājumu par kādu kriptovalūtu maka problēmu, tu negaidīti saņem tiešu ziņu vai e-pasta vēstuli no kādas personas, kas izliekas par uzticamu kontaktpersonu (piemēram, no kriptovalūtu biržas, maka pakalpojumu sniedzēja, IT atbalsta sniedzēja vai pat drauga). Šī persona lūdz tev norādīt savu atslēgas frāzi (t. i., vārdu virkni, ko izmanto kā galveno rezerves paroli, lai piekļūtu digitālajam makam), paroles vai privātās atslēgas (automātiski ģenerēts kriptogrāfisks kods, kas pierāda īpašumtiesības uz digitālajiem aktīviem).

Kas varētu notikt?

Ja tu dalies ar savu atslēgas frāzi, parolēm vai privātajām atslēgām, krāpnieks šo informāciju izmanto, lai nozagtu tavus kriptoaktīvus vai citus līdzekļus. Atceries, ka privāto atslēgu nozaudēšana nozīmē galīgu un neatgriezenisku piekļuves un īpašumtiesību uz taviem kriptoaktīviem zaudēšanu. Atšķirībā no bankas darījumiem kriptoaktīvu pārvedumu gadījumā ir gandrīz neiespējami atgūt pārskaitītos līdzekļus.

Pikšķerēšana

Tu pa e-pastu, tālruni, uznirstošajā logā vai sociālajā medijā saņem negaidītu ziņojumu, kura sūtītājs apgalvo, ka pārstāv plaši zināmu kriptoaktīvu pakalpojumu sniedzēju. Ziņojumā tevi aicina pieteikties kādā lietotnē vai lejupielādēt jaunu lietotni. Tu vari saņemt arī šķietami no tava kriptovalūtu maka lietotnes sūtītu e-pasta vēstuli, kurā tiec mudināts risināt kādu drošības problēmu, noklikšķinot uz saites, ko nosūtījis neoficiāls sūtītājs, vai atjauninot lietotni.

Kas varētu notikt?

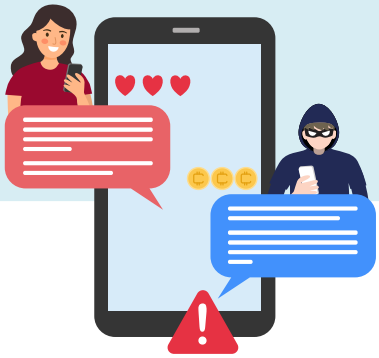
Noklikšķinot uz saites, lejupielādējot lietotni vai skenējot kvadrātkodu (QR kodu), tu instalē ļaunatūru, kas krāpniekiem ļauj piekļūt informācijai un izmantot to, lai nozagtu tavus kriptoaktīvus vai līdzekļus.

Krāpšana, solot dāvanu (*giveaway*)

Tu sociālajos medijos izlasi paziņojumu, kurā apgalvots, ka uzņēmumi, saņemot nelielu ieguldījumu kriptovalūtā, dāvina kriptoaktīvus. Tajos ir video vai vēstījumi ar kādas slavenības vai zīmola fotogrāfijām, kas parasti ir viltotas vai iegūtas bez atļaujas, un šajos video vai vēstījumos tiek solīts "dubultot kriptovalūtu summu", ja vispirms iemaksāsi naudu. Logotips, izkārtojums, atsauksmes un izmantotā valoda izskatās profesionāli un oficiāli, tāpat kā tīmekļa vietne, uz kuru tiec novirzīts.

Kas varētu notikt?

Pēc kriptovalūtas nosūtīšanas tu neko nesaņem un parasti zaudē nosūtīto naudu. Solījums par dāvanu nebija īsts, un ziņa vai tiešraide, kurā kāda persona uzdevās par slavenību vai uzņēmuma pārstāvi, bija paredzēta, lai tevi maldinātu.



Romantiskā krāpšana, lai saņemtu ieguldījumus

Kāda persona, kuru neesi saticis reālajā dzīvē, sazinās ar tevi sociālajos medijos, iepazīšanās lietotnēs vai pa tālruni/ar īsziņu. Šī persona bieži sarunājas ar tevi par personiskām un romantiskām tēmām un panāk uzticēšanos, izmantojot viltus profilus. Tā pakāpeniski uzvedina uz sarunām par finanšu iespējām, apgalvojot, ka no ieguldījumiem kriptoaktīvos var gūt milzīgu peļņu, un mudina ieguldīt, solot lielu atdevi un mazu risku. Šī persona palīdz izveidot kontu un iemaksāt nelielu sākotnējo depozītu, lai shēma šķistu likumīga.

Krāpnieki izveido neīstus tiešsaistes profilus un izmanto nozagtus vai ar MI radītus attēlus, lai uzrunātu tevi.

Kas varētu notikt?

Krāpnieks izkrāpj pēc iespējas vairāk naudas, pēc tam pārtrauc saziņu un pazūd. Krāpnieciskā ieguldījumu vietne vai lietotne vairs nav pieejama tiešsaistē, un tu vairs nevari piekļūt it kā veiktajiem ieguldījumiem. Dažos gadījumos papildus finansiāliem zaudējumiem tavi kopīgotie personas dati var tikt izmantoti, lai vērstos pret taviem draugiem un ģimenes locekļiem vai veiktu identitātes zādzību, kas tev var radīt finansiālas vai juridiskas sekas (piemēram, krāpnieks var tavā vārdā verificēt nozagtus makus vai tev var nākties uzņemties atbildību par parādiem vai tavā vārdā izdarītiem noziegumiem, kamēr nav pierādīts pretējais).

Ponci shēma

Tevi aicina piedalīties projektā, kurā tiek solīta liela pastāvīga atdeve no ieguldījumiem kriptoaktīvos. Bieži tiek norādītas arī pozitīvas atsauksmes vai viltus veiksmes stāsti. Šī shēma var tikt prezentēta kā daudzlīmeņu mārketinga iespēja, kurā atlīdzība tiek pelnīta ne tikai no taviem ieguldījumiem, bet arī par citu personu iesaisti. Pirmie ieguldītāji izmaksas šķietami saņem, mudinot vēl vairāk cilvēku pievienoties shēmai un popularizēt to.

Patiesībā īsta uzņēmējdarbība nenotiek, un nav arī peļņas. Tā vietā nauda tiek iegūta tikai no jaunāko ieguldītāju iemaksām, kuras tiek izmantotas, lai maksātu shēmas organizatoriem un pirmajiem dalībniekiem.

Kas varētu notikt?

Kad jaunu ieguldījumu plūsma apsīkst, shēma sabrūk, un tu, tāpat kā lielākā daļa dalībnieku, naudu zaudē. Organizatori pazūd, liedzot iespēju atgūt līdzekļus. Šāda daudzlīmeņu struktūra palīdz krāpšanai izplatīties ātri, jo upuri, to neapzinoties, kļūst par krāpšanas sekmētājiem.

Īstai adresei līdzīgas adreses, kas saindē tavu maku

Pēc darījuma ar kriptovalūtu savā makā pamani jaunu adresi. Šī adrese izskatās līdzīga tai, kuru iepriekš izmantoji. Krāpnieki var panākt, ka šādas viltus maku adreses parādās tavā darījumu vēsturē, nosūtot nelielu kriptovalūtas summu no īstajai adresei līdzīgas adreses uz tavu maku. Tādējādi maka neseno darījumu vai automātiski piedāvāto adrešu sarakstā nonāk viltus adrese, ko izveidojis krāpnieks. Šādas adreses tiek veidotas apzināti, mainot vien dažas rakstzīmes – bieži adreses vidū –, lai izvairītos no to atpazīšanas.

Kas varētu notikt?

Kad mēģināsi nosūtīt kriptovalūtu un nokopēsi nepareizu adresi no sava maka vēstures, to neapzinoties, nosūtīsi līdzekļus uz krāpnieka maku. Tā kā kriptovalūtu darījumi bieži vien ir neatgriezeniski, vairumā gadījumu savus līdzekļus vairs nevarēsi atgūt. Šī krāpšana balstās uz vizuālu maldināšanu un lietotāja neuzmanību, izmantojot ieradumu kopēt un ielīmēt maka adreses, tās rūpīgi nepārbaudot.