KRIPTO GOLJUFIJE & PREVARE

BODITE POZORNI IN SE ZAŠČITITE

Zaradi hitre rasti kriptosredstev in njihove posebne značilnosti – hitrosti, anonimnosti in pogosto nemogočega preklica transakcij – ste uporabniki glavna tarča kibernetskih kriminalcev. Goljufi in prevaranti vas prevarajo s prefinjenimi taktikami, kot so „Ponzijeve sheme“, lažne naložbene priložnosti, brezplačne ponudbe na družbenih medijih in lažna sporočila. Pošiljajo vam sporočila iz lažnih naslovov in tudi ljubezenske prevare. Pogosto do vas pristopijo prek družbenih omrežij, aplikacij za sporočanje, e-pošte in nepričakovanih telefonskih klicev, ki delujejo resnično. Vse te ponudbe lahko delujejo resnično. Bodite previdni, saj se lahko soočite s tveganji, kot so finančna izguba, kraja identitete in čustvena stiska.

Ravnajte skrajno previdno in sledite naslednjim ključnim nasvetom, da ostanete varni:

Bodite pozorni na morebitne goljufije in prevare s kriptovalutami:
izvedite več o različnih vrstah goljufij in prevar (strani 5, 6, 7 in 8).

Seznanite se s posameznimi opozorilnimi znaki:
naučite se prepoznati sumljivo vedenje, sporočila ali ponudbe (stran 2).

Zaščitite sebe in svoje premoženje:
zavarujte svoje osebne podatke (stran 3).

Naučite se, kako ravnati, če postanete žrtev goljufije ali prevare
(stran 4).

Opozorilni znaki

Obljuba, ki je videti preveč dobra, da bi bila resnična.

Neželena ponudba.

Zagotovljen hiter in visok zaslužek.

Nujnost ukrepanja (npr. časovno omejena ponudba, ki vas sili k takojšnjemu ukrepanju).

Zahteva za plačilo preko nesledljivih metod (npr. s kriptovalutami, darilnimi karticami, elektronskimi prenosi ali predplačniškimi debetnimi karticami).

Vabilo, da kliknete na povezavo, skenirate kodo QR ali prenesete aplikacijo.

Zahteva za pošiljanje ali skupno rabo zasebnih ključev in gesel (seznam besed za dostop do vaše kripto denarnice in njeno obnovitev).

Sumljiv ali napačen URL.

Logotip z manjšimi popačenji ali spletno mesto, ki kopira videz pravega spletnega mesta ali resničnega podjetja, vendar nima preverljivih kontaktnih podatkov ali podatkov o registraciji podjetja.

Neznana platforma za izmenjavo.

Sumljiva priloga, zlasti datoteke s končnico .exe, .scr, .zip ali Officeova datoteka z omogočenimi makri (.docm, .xlsm).

Koraki do vaše zaščite :

1 **Preden ukrepate, razmislite:**

Ne hitite z vlaganjem, izmenjavo informacij ali klikanjem na povezave – prevaranti namerno ustvarjajo občutek nujnosti. V primeru kakršnih koli dvomov, tudi manjših, ne ukrepajte in ne vlagajte.

2 **Preverite vir:**

- Vedno preverite, od kod prihajajo sporočila, klici, e-poštna sporočila in povezave, tudi če so videti uradni, ali prihajajo od prijatelja ali vaše družine ali celo javne osebnosti. Poiščite pravopisne napake, čudne URL-je ali manjkajoče varnostne kazalnike, npr. preverite, ali povezava spletnega mesta vključuje „s“ v „HTTPS“, da se prepričate, ali je spletno mesto varno, in preverite, ali so v imenu podjetja dodane ali manjkajoče črke.
- Ne odpirajte povezav iz neželenih sporočil, namestite samo uradne aplikacije in ne skenirajte neznanih QR kod.
- Tudi če je ponudba videti uradna, jo vedno navzkrižno preverite na spletišču podjetja, preverite, ali je račun družbenega medija preverjen.
- Uporabite preverjene kontaktne podatke za neposreden stik s podjetjem ali posameznikom in se nikoli ne zanašajte na kontaktne podatke, ki jih zagotovi domnevni goljuf . Ali ima kripto ponudnik dovoljenje v EU, lahko preverite v registru ESMA (). Na spletni strani nacionalnega pristojnega organa () lahko preverite tudi, ali so bila izdana opozorila ali črni seznami ali seznam IOSCO I-SCAN (iosco.org/i-scan/).

3 **Nikoli ne delite gesel ali zasebnih ključev:**

Vsakdo, ki ima dostop do njih, lahko prevzame nadzor nad vašim premoženjem. Zakonita podjetja ne bodo nikoli zahtevala vaših gesel ali varnostnih kod po e-pošti, sporočilih ali telefonu.

4 **Zaščitite naprave in zasebne ključe:**

Uporabite močna in edinstvena gesla za vsakega od vaših kripto računov, ohranite svoje geslo tajno in se izogibajte ponovni uporabi istih gesel na različnih platformah. Omogočite večfaktorsko avtentikacijo, kjer je to mogoče. Nekaj nasvetov za gesla je na voljo tukaj (). Naj bo vaša programska oprema in protivirusna zaščita posodobljena in aktivirana.

5 **Bodite previdni pri nepričakovanih naložbenih ponudbah:**

Bodite previdni pri naložbah, ki obljubljajo visoke donose. Če se sliši preveč dobro, da bi bilo res, verjetno je.

6 **Razmislite, preden delite informacije na družbenih omrežjih:**

Skupine za klepet, forumi, objave na družbenih omrežjih in fotografije so lahko dragocen vir podatkov za goljufe. Če razkrijete preveč o sebi ali svojih naložbah, lahko postanete lahka tarča.

Kaj storiti, ko postanete žrtev goljufije ali prevare

Takoj ustavite transakcije,

Da blokirate nadaljnje prenose na sumljive račune in se izognete dodatnim izgubam. Preprečite vse stike s prevaranti – prezrite njihove klice in elektronsko pošto ter blokirajte pošiljatelja.

Spremenite gesla v vseh svojih napravah in aplikacijah/spletnih mestih:

Goljufi na spletu kupujejo razkrita gesla in jih preizkušajo na več računih. Spreminjanje samo enega gesla ni dovolj. Poskrbite za spremembo vseh gesel, da jih goljufi ne bodo mogli ponovno uporabiti.

Prekinite povezavo in prekličite dostop:

Prekličite sumljiva dovoljenja v vašem digitalnem sporazumu, ki se samodejno zaženejo pri veriženju blokov (pametnih pogodbah), da bi preprečili prevarantom, da bi porabili vaše žetone brez vašega soglasja. Številne denarnice in raziskovalci blokov ponujajo orodja, ki vam omogočajo, da trenutno vidite, katere pametne pogodbe imajo o dostop, da porabijo vaše žetone. Če želite to narediti, lahko:

- uporabite zaupanja vreden „preveritelj dovoljenj“, ki preveri, ali je naslov uporabnika ali blokovne verige pooblaščen za izvedbo operacije,
- pregledate sezname odobritev in
- uporabite gumb „prekliči“ neposredno na platformi.

Premaknite svoja sredstva:

Če je vaša denarnica ogrožena, takoj prenesite preostalo premoženje v novo varno denarnico.

Obrnite se na svojega kripto ponudnika:

Čim prej obvestite svojega kripto ponudnika prek uradnih kontaktnih kanalov, da raziščete morebitne možnosti. Četudi razveljavitev transakcije verižnih blokov v večini primerov ne bo mogoča, lahko ponudnik še vedno zamrzne račun prevaranta (če je na njegovi platformi) in naslov denarnice uvrsti na črno listo.

Prijavite in opozorite:

Prijavite incident policiji ali svojemu nacionalnemu pristojnemu organu (www.atvp.si) in obvestite svojo mrežo (npr. prijatelje in družino), da jih opozorite. To je najboljši način za zaščito sebe in drugih.

Pazite se prevar s povračilom sredstev (»recovery rooms«):

Prevarant lahko stopi v stik z vami kot žrtvijo prejšnje prevare in trdi, da je pooblaščeni organ (npr. policija, davčni ali finančni organ itd.), ter vam ponudi povračilo izgubljenega denarja, če mu zato plačate. To je pogosto ponoven poskus prevare. Zapomnite si: če ste bili enkrat prevarani, še ne pomeni, da vas ne bodo ponovno poskusili prevarati.

Glej opozorilo skupnih evropskih nadzornih organov za več informacij o tveganjih, povezanih s kriptosredstvi (↖) ter informativno zloženko „Razlaga kriptosredstev: Kaj MiCA pomeni za vas kot potrošnika“ (↖).

Evropski bančni organ, Evropski organ za zavarovanja in poklicne pokojnine, Evropski organ za vrednostne papirje in trge, 2025

Luxembourg: Urad za publikacije Evropske unije, 2025

PDF ISBN 978-92-9407-235-1 doi:10.2853/7872422 DZ-01-25-113-SL-N

VRSTE KRIPTO PREVAR

Shema „dvigni in prodaj (pump and dump)" ali sistem „nenadne ukinitve (rug pull)"

Pojavi se oglas na družbenih omrežjih ali spletnem mestu, ki promovira „priložnost za naložbo v omejenem času" v kripto in priporoča vlaganje v nov kripto žeton ali projekt. Ko izrazite zanimanje, vas kontaktirajo in preusmerijo na platformo za kripto izmenjavo ali aplikacijo za sporočanje (npr. WhatsApp, Telegram, Viber). Navidezno verodostojen stik obljublja hiter dobiček ali visoke donose, če se za naložbo hitro odločite. Spodbujajo vas, da vložite majhen znesek in nato pritisnejo na vas, da vložite več.

Kaj se lahko zgodi:

Odkrili boste, da je vloženi žeton brez vrednosti in se oseba, s katero ste bili v stiku, preneha odzivati. Ko poskušate dvigniti svoj denar, spletna stran ne obstaja več in podjetje je nedosegljivo. Goljufi so umetno napihnili ali precenili kriptovalute z nizko vrednostjo, da bi povečali njihovo vrednost („pump"), nato pa razprodali svoja sredstva („dump"), kar je povzročilo padec vrednosti in izgube vlagateljem. Druga možnost je, da projekt zaprejo in izginejo s sredstvi („nenadna ukinitev oz. rug pull").

Prevare z lažnimi predstavljanjem

Ko na platformi družbenega omrežja ali spletnem mestu objavite vprašanje o težavah s kripto denarnico, prejmete nepričakovano neposredno sporočilo ali e-pošto od nekoga, ki se pretvarja, da je zaupanja vredna oseba (npr. menjalnica kriptovalut, ponudnik denarnice, podpora IT ali celo prijatelj). Oseba zahteva vaše vstopno geslo (tj. zaporedje besed, ki služi kot osrednja varnostna kopija za dostop do vaše digitalne denarnice), druga gesla ali zasebne ključe (samodejno ustvarjena kriptografska koda, ki dokazuje lastništvo digitalnih sredstev).

Kaj se lahko zgodi:

Ko delite svoje geslo ali zasebne ključe, jih prevarant uporablja za krajo kriptovalut ali drugih sredstev. Ne pozabite, da izguba zasebnih ključev povzroči trajno in nepovratno izgubo dostopa do vaših kriptosredstev in lastništva nad njimi.

Ribarjenje za podatki ali zvabljanje (phishing)

Prek e-pošte, telefona, pojavnega okna ali družbenih omrežij prejmete nepričakovano sporočilo, ki naj bi bilo od znanega ponudnika kriptosredstev. V sporočilu vas vabijo k prijavi ali prenosu nove aplikacije. Morda boste prejeli tudi e-pošto, ki je videti, kot da je iz vaše aplikacije, kjer imate kripto denarnico, in vas poziva, da odpravite varnostno težavo s klikom na povezavo, ki jo je zagotovil neuradni vir, ali s posodobitvijo aplikacije.

Kaj se lahko zgodi:

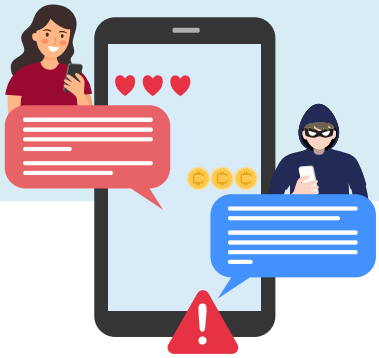
S klikom na povezavo, prenosom aplikacije ali skeniranjem QR kode namestite zlonamerno programsko opremo, ki prevarantu omogoča dostop do informacij in njihovo uporabo za krajo vaših kriptosredstev ali drugih sredstev.

Goljufija z nagradnimi igrami

Na družbenih omrežjih naletite na obvestilo, ki prikazuje podjetja, ki podarjajo kriptosredstva po manjši naložbi v kripto naložbe. Vključujejo videoposnetek ali objavo s fotografijami slavne osebe ali blagovne znamke, ki je običajno ponarejena ali pridobljena brez dovoljenja in obljublja, da bo „podvojila vašo kripto naložbo“, če najprej pošljete denar. Logotip, postavitev, pričevanja in uporabljeni jezik izgledajo strokovno in uradno, kot tudi spletna stran, na katero ste preusmerjeni.

Kaj se lahko zgodi:

Po pošiljanju kripto sredstev ne prejmete ničesar v zameno, poslani denar pa ste izgubili. Nagradna igra je bila lažna, objava ali prenos v živo, ki je predstavljal znane osebe ali podjetja, pa je bila zasnovana tako, da vas zavede.



Romantična investicijska prevara

Na družbenih omrežjih, aplikacijah za zmenke ali po telefonu / SMS vas kontaktira nekdo, ki ga niste nikoli srečali. Ta oseba se lahko pogosto pogovarja z vami ter v pogostih, osebnih in romantičnih pogovorih, gradi zaupanje z uporabo lažnih profilov. Postopoma usmerjajo pogovor o finančnih priložnostih, govorijo o ogromnih dobičkih iz kripto naložb in vas spodbujajo, da vlagate z obljubami o visokih donosih in nizkem tveganju. Vodijo vas skozi postopek odprtja računa in majhnega začetnega depozita, da se shema zdi zakonita.

Goljufi ustvarjajo lažne spletne profile in uporabljajo ukradene fotografije, da se vam približajo.

Kaj se lahko zgodi:

Ko goljufi izvlečejo čim več denarja, nenadoma prekinejo vso komunikacijo in izginejo. Goljufiva spletna stran ali aplikacija za naložbe je onemogočena in vam ne pusti dostopa do domnevnih naložb. V nekaterih primerih lahko prevaranti uporabijo podatke, pridobljene med prevaro, za krajo identitete ali napade na vaše prijatelje ali družino.

Ponzijeva shema

Vabljeni ste k sodelovanju v projektu, ki obljublja redne visoke donose iz naložb v kriptosredstva, pogosto podprte s pričanji ali lažnimi zgodbami o uspehu. Shema se lahko predstavi kot priložnost za mrežni marketing, kjer zaslužite nagrade ne le iz lastne naložbe, temveč tudi s pridobivanjem drugih v shemo. Zdi se, da zgodnji vlagatelji prejemajo izplačila, kar spodbuja več ljudi, da se pridružijo shemi in jo promovirajo.

V resnici ne gre za ustvarjanje resničnega posla ali dobička. Namesto tega denar izvira izključno iz naložb novejših vlagateljev, ki se uporablja za plačilo donosov organizatorjem in prvim udeležencem sheme.

Kaj se lahko zgodi:

Ko se nove naložbe upočasnijo, se shema zruši in tako kot večina udeležencev izgubite denar. Organizatorji izginejo, tako da ni mogoče izterjati sredstev. Več nivojska struktura sheme pomaga pri hitrem širjenju prevare, saj žrtve nevede postanejo promotorji.

Lažni naslovi v kripto denarnici

Ko opravite kripto transakcijo, opazite nov naslov, ki se pojavi v zgodovini vaše denarnice. Ta naslov je podoben tistemu, s katerim ste prej komunicirali. Prevaranti lahko ponarejene naslove denarnice prikažejo v zgodovini transakcij tako, da v vašo denarnico pošljejo majhno količino kriptovalut iz naslova, podobnega videza. Na koncu shranite v svojo denarnico nedavno dejavnost ali uporabite samodejno predlagani lažni naslov, ki ga je ustvaril prevarant. Prevaranti namerno ustvarjajo podobne naslove tako, da spremenijo le nekaj znakov, pogosto na sredini naslova, da se izognejo odkritju.

Kaj se lahko zgodi:

Ko poskušate poslati kriptovalute in kopirati napačen naslov iz zgodovine denarnice, nevede pošiljate sredstva v denarnico prevaranta. Ker so kripto transakcije pogosto nepovratne, so vaša sredstva v večini primerov trajno izgubljena. Ta prevara temelji na vizualni prevari in uporabniški napaki, ki izkorišča navado kopiranja in lepljenja naslovov denarnice brez natančnega pregleda.