HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

HRVATSKA NARODNA BANKA
EUROSUSTAV

KRIPTOPRIJEVARE I OBMANE

BUDITE OPREZNI I ZAŠTITITE SE

Brz rast kriptoimovine i njezine specifične karakteristike – globalna dostupnost, brzina, anonimnost i često nepovratnost transakcija – čine vas potencijalnom metom za kiberkriminalce. Prevaranti koriste napredne metode kako bi vas prevarili, kao što su „Ponzijeve sheme", lažne mogućnosti ulaganja, besplatne ponude na društvenim mrežama i prijevarne poruke. Koriste i investicijske prijevare u romantičnim odnosima ili lažne adrese koje izgledaju vjerodostojno kako bi kompromitirali vaš novčanik. Prevaranti vas nerijetko mogu kontaktirati putem društvenih mreža, aplikacija za razmjenu poruka, e-pošte i neočekivanih telefonskih poziva koji se čine vjerodostojnima. U takvim slučajevima možete se suočiti s rizicima kao što su financijski gubitak, krađa identiteta i uznemirenost.

Budite oprezni i slijedite ove ključne savjete kako biste ostali sigurni:

Budite na oprezu u pogledu mogućih prijevara i obmana povezanih s kriptovalutama:
kako biste saznali više o različitim vrstama prijevara (pogledajte str. 5., 6., 7. i 8.).

Uočite znakove upozorenja:
naučite prepoznati sumnjivo ponašanje, poruke ili ponude (pogledajte str. 2.).

Zaštitite sebe i svoju imovinu:
zaštitite svoje osobne podatke (pogledajte str. 3.).

Naučite što poduzeti ako postanete žrtva prijevare ili obmane
(pogledajte str. 4.).

Znakovi upozorenja

Obećanje koje se čini predobro da bi bilo istinito

Ponuda koju niste tražili

Zajamčeni brz i visok prinos

Hitno djelovanje (npr. nudi vam se ograničeno vrijeme uz pritisak da odmah djelujete)

Zahtjev za plaćanje kanalima kojima je transakciju teško ili nemoguće pratiti (npr. kriptovalutama, darovnim karticama, elektroničkim prijenosom sredstava ili karticama s unaprijed uplaćenim sredstvima)

Poziv da kliknete na poveznicu, skenirate QR kod ili preuzmete aplikaciju

Zahtjev za slanje ili dijeljenje privatnih ključeva i *seed* fraza (niz riječi za pristup i oporavak vašeg kriptonovčanika)

Sumnjiv ili netočan URL

Blago iskrivljeni logotip, internetska stranica koja imitira izgled stvarne internetske stranice poduzeća ili izgleda profesionalno, ali nema provjerene podatke za kontakt, podatke o registraciji poduzeća, povijest poslovanja ili provjerljivu prisutnost

Nepoznata platforma za razmjenu

Sumnjivi privitak, posebno .exe, .scr, .zip ili datoteka sustava Office s makronaredbama (.docm, .xlsm).

Kako se zaštititi:

1 Zastanite i razmislite prije nego što nešto poduzmete:

Nemojte žuriti s ulaganjem, dijeljenjem informacija ili klikom na poveznice – prevaranti namjerno stvaraju osjećaj hitnosti. U slučaju bilo kakvih sumnji, čak i manjih, nemojte ništa poduzimati ni ulagati te pažljivo ispitajte izvor.

2 Pažljivo provjerite izvor:

- Uvijek provjerite odakle dolaze poruke, pozivi, e-pošta i poveznice, čak i ako izgledaju službeno, odnosno čini se da dolaze od prijatelja, člana obitelji ili čak javne osobe. Obratite pažnju na pravopisne pogreške, čudne URL-ove ili izostanak sigurnosnih pokazatelja, npr. provjerite sadržava li poveznica na internetsku stranicu „s" u „HTTPS" kako biste se uvjerili u sigurnost te internetske stranice i provjerite jesu li u naziv poduzeća dodana neka slova ili možda neka nedostaju.
- Ne otvarajte poveznice iz neželjenih poruka, instalirajte samo službene aplikacije putem pouzdanih trgovina aplikacija i ne skenirajte nepoznate QR kodove.
- Čak i ako ponuda izgleda službeno, uvijek je dodatno provjerite na internetskim stranicama poduzeća ili provjerite je li račun na društvenim mrežama verificiran (npr. sa službenom kvačicom).
- Koristite provjerene podatke za kontakt kako biste izravno stupili u kontakt s poduzećem ili pojedincem i nikada se ne oslanjajte na podatke za kontakt koje je dostavio potencijalni prevarant (npr. samostalno pretražite naziv poduzeća, upotrebljavajte provjerene poslovne imenike). Prevaranti mogu tvrditi da su ovlašteni pružatelji usluga ili oponašati internetske stranice ovlaštenog poduzeća. Provjerom registra ESMA-e (↖) možete provjeriti ima li pružatelj usluga povezanih s kriptoimovinom odobrenje za rad u EU-u. Možete pogledati i internetske stranice svojeg nacionalnog financijskog regulatora (https://www.hanfa.hr i https://www.hnb.hr) kako biste vidjeli jesu li izdana upozorenja odnosno crne liste ili provjerite IOSCO-ov popis I-SCAN (iosco.org/i-scan/).

3 Nikada ne dijelite lozinke, privatne ključeve ili *seed* fraze:

Svatko tko ima pristup njima može preuzeti kontrolu nad vašim sredstvima. Legitimna poduzeća nikada neće tražiti vaše lozinke ili sigurnosne kodove putem e-pošte, tekstualne poruke ili telefona.

4 Pobrinite se za sigurnost svojih uređaja i privatnih ključeva:

Upotrebljavajte snažne i jedinstvene lozinke za svaki od svojih kriptoračuna, čuvajte svoju lozinku u tajnosti i izbjegavajte ponovno korištenje istih vjerodajnica na različitim platformama. Omogućite višefaktorsku autentifikaciju ako je to moguće. Pročitajte nekoliko savjeta u vezi s lozinkama ovdje (↖). Održavajte svoj softver i antivirusnu zaštitu ažuriranima i aktiviranima.

5 Budite oprezni u pogledu neočekivanih ponuda za ulaganje:

Budite oprezni s ulaganjima koja obećavaju visoke prinose. Ako nešto zvuči predobro da bi bilo istinito, vjerojatno nije istinito.

6 Razmislite prije nego što podijelite informacije na društvenim mrežama:

Chat grupe, forumi, objave i fotografije na društvenim mrežama mogu biti vrijedni izvori znanja za prevarante. Otkrivanje previše toga o sebi ili svojim ulaganjima može vas učiniti lakom metom.

Što učiniti kada postanete žrtva prijevare ili obmane:

Odmah zaustavite transakcije

Kako biste blokirali sve daljnje prijenose na sumnjive račune i izbjegli dodatne gubitke. Prekinite svaki kontakt s prevarantima – ignorirajte njihove pozive i e-poštu i blokirajte pošiljatelja.

Promijenite lozinke na svim uređajima i aplikacijama / internetskim stranicama.

Prevaranti kupuju kompromitirane lozinke na internetu i isprobavaju ih na više računa. Promjena samo jedne lozinke nije dovoljna; svakako ih promijenite sve kako ih prevaranti ne bi mogli ponovno upotrijebiti.

Onemogućite povezivanje i opozovite pristup:

Opozovite sumnjive dozvole u svojem digitalnom ugovoru koje se automatski pokreću na *blockchainu* (pametni ugovor) kako biste spriječili prevarante da troše vaše tokene bez vašeg pristanka. Mnogi novčanici i *blockchain* pretraživači nude alate koji vam omogućuju da provjerite koji pametni ugovori trenutačno imaju pristup za trošenje vaših tokena. Da biste to učinili, možete:

- upotrebljavati pouzdani „kontrolor dopuštenja”, kojim se provjerava je li korisnik ili adresa *blockchaina* ovlaštena za izvršenje operacije
- revidirati popis odobrenja i
- upotrijebiti gumb „Opozovi” izravno s platforme.

Premjestite svoja sredstva:

Ako je vaš novčanik ugrožen, odmah prenesite preostalu imovinu u novi sigurni novčanik.

Kontaktirajte svojeg pružatelja kriptousluga:

Obavijestite svojeg pružatelja kriptousluga što je prije moguće putem službenih kanala za kontakt kako biste istražili moguće opcije. Čak i ako, u većini slučajeva, poništenje transakcije u *blockchainu* neće biti moguće, pružatelj usluga i dalje može zamrznuti račun prevaranta (ako se nalazi na njegovoj platformi) i staviti adresu novčanika na crnu listu.

Prijavite i upozorite:

Prijavite incident policiji ili svojem nacionalnom financijskom regulatoru (https://www.hanfa.hr i https://www.hnb.hr) i obavijestite svoju okolinu (npr. prijatelje i obitelj) radi podizanja svijesti. To je najbolji način da zaštitite sebe i druge.

Čuvajte se ponovne prijevare kojom se nudi „oporavak”:

Prevarant vas može kontaktirati kao žrtvu prethodne prijevare, tvrdeći da je predstavnik javnog tijela (npr. policije, porezne uprave ili financijskog regulatora itd.) i nuditi vam povrat izgubljenog novca uz naknadu. To je često još jedan pokušaj prijevare. Zapamtite: ako ste jednom bili prevareni, to ne znači da ne možete biti prevareni ponovo.

Pogledajte zajedničko upozorenje europskih nadzornih tijela kako biste saznali više o rizicima povezanima s kriptoimovinom (↖) i informativni članak „Pojašnjenje o kriptoimovini: Što Uredba MiCA znači za vas kao potrošača?” (↖).

Europsko nadzorno tijelo za bankarstvo, Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje, Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala, 2025.

Luxembourg: Ured za publikacije Europske unije, 2025.

Umnožavanje je dopušteno uz uvjet navođenja izvora.
Illustrations: © Nadezhda Buravleva / madedee / Orapun- StockAdobe.com.

PDF ISBN 978-92-9407-209-2 doi:10.2853/8581704 DZ-01-25-097-HR-N

VRSTE KRIPTOOBMANA

SHEMA *PUMP-AND-DUMP* ILI *RUG PULL*

Vidjeli ste oglas na društvenim mrežama ili internetskoj stranici kojim se promiče „mogućnost ulaganja u kriptovalute koja traje ograničeno vrijeme" i preporučuje ulaganje u novi kriptotoken ili projekt. Nakon što ste pokazali interes, kontaktiraju vas i preusmjeravaju na platformu za razmjenu kriptovaluta ili kanal za razmjenu poruka (npr. Telegram, Viber ili WhatsApp). Naizgled vjerodostojan kontakt obećava brzu dobit ili visoke prinose ako odmah uložite. Potiču vas da uložite mali iznos, a zatim potiču da uložite više.

Što bi se moglo dogoditi:

Otkrivate da je token u koji ste uložili bezvrijedan, a osoba s kojom ste bili u kontaktu prestala je odgovarati. Kada pokušate podići svoj novac, internetska stranica više ne postoji, a poduzeće je nedostupno. Prevaranti su umjetno napuhali ili precijenili kriptovalutu niske vrijednosti kako bi povećali njezinu vrijednost („pump"), a zatim prodali svoju imovinu („dump"), što je dovelo do pada vrijednosti i ostavilo ulagatelje s gubicima. Druga je mogućnost da ugase projekt i nestanu sa sredstvima („rug pull").

PRIJEVARA S LAŽNIM PREDSTAVLJANJEM

Nakon što na platformi društvenih medija ili internetskoj stranici objavite pitanje o problemu s kriptonovčanikom, primate neočekivanu izravnu poruku ili e-poštu od nekoga tko se pretvara da je pouzdan kontakt (npr. kriptomjenjačnica, pružatelj usluga novčanika, IT podrška ili čak prijatelj). Osoba traži vašu *seed* frazu (tj. niz riječi koje služe kao središnja sigurnosna kopija za pristup vašem digitalnom novčaniku), lozinke ili privatne ključeve (automatski generirani kriptografski kod koji dokazuje vlasništvo nad digitalnom imovinom).

Što bi se moglo dogoditi:

Nakon što podijelite svoju seed frazu, lozinke ili privatne ključeve, prevarant ih koristi za krađu vaše kriptoimovine ili drugih sredstava. Imajte na umu da gubitak privatnih ključeva dovodi do trajnog i nepovratnog gubitka pristupa i vlasništva nad kriptoimovinom. Za razliku od bankovnih transakcija, u slučaju kriptoprijenosa, nakon što vaša sredstva nestanu, oporavak je gotovo nemoguć.

Phishing

Putem e-pošte, telefona, skočnog prozora ili društvenih medija dobivate neočekivanu poruku, koja tvrdi da je riječ o poznatom pružatelju kriptoimovine. Poruka vas poziva da se prijavite ili preuzmete novu aplikaciju. Također možete primiti e-poštu koja djeluje kao da je iz aplikacije kriptonovčanika, kojom vas se poziva da riješite sigurnosni problem klikom na poveznicu koju pruža neslužbeni izvor ili ažuriranjem aplikacije.

Što bi se moglo dogoditi:

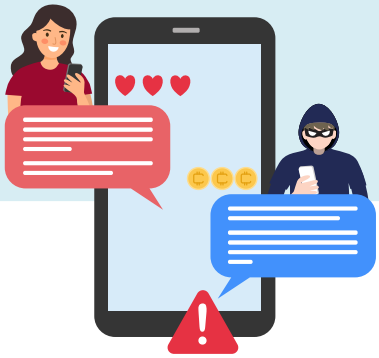
Klikom na poveznicu, preuzimanjem aplikacije ili skeniranjem QR koda instalirate zlonamjerni softver, koji prevarantu omogućuje pristup informacijama i njihovu upotrebu za krađu vaše kriptoimovine ili sredstava.

Lažno darivanje

Naišli ste na objavu na društvenim mrežama u kojoj se tvrdi da poduzeća poklanjaju kriptoimovinu nakon malog kriptoulaganja. Uključuje videozapis ili objavu s fotografijama slavne osobe ili robne marke, obično lažne ili dobivene bez odobrenja, kojima se obećava da će „udvostručiti kriptoimovinu" ako prvo pošaljete novac. Logotip, izgled, svjedočanstva i jezik koji se koristi izgledaju profesionalno i službeno, kao i internetska stranica na koju ste preusmjereni.

Što bi se moglo dogoditi:

Nakon slanja kriptovalute, ne primate ništa zauzvrat i izgubili ste poslani novac. Darivanje je bilo lažno, a objava ili video u kojem su lažno predstavljene slavne osobe ili poduzeća osmišljen je kako bi vas prevario.



Investicijska prijevara u romantičnom odnosu

Na društvenim mrežama, aplikacijama za upoznavanje ili putem telefona/poruke kontaktirao vas je netko koga u stvarnom životu nikad niste upoznali. Ta se osoba upušta u česte, osobne i romantične razgovore, gradeći povjerenje pomoću lažnih profila. Postupno usmjerava razgovor prema financijskim mogućnostima, tvrdeći da možete ostvariti veliku dobit od kriptoulaganja i potičući vas da ulažete s obećanjima visokog prinosa i niskog rizika. Vodi vas kroz proces otvaranja računa i uplatu malog početnog iznosa kako bi se shema činila legitimnom.

Prevaranti stvaraju lažne internetske profile i koriste ukradene slike ili slike generirane umjetnom inteligencijom kako bi vam pristupili.

Što bi se moglo dogoditi:

Prevarant izvlači što je više moguće novca, a zatim prekida svu komunikaciju i nestaje. Prijevarna internetska stranica ili aplikacija za ulaganje uklonjena je s interneta, zbog čega nemate pristup navodnim ulaganjima. U nekim slučajevima prevaranti mogu upotrijebiti informacije dobivene tijekom prijevare kako bi ciljali vaše prijatelje i obitelj te počinili krađu identiteta, koja može imati financijske ili pravne posljedice za vas (npr. prevaranti mogu koristiti ukradene novčanike u vaše ime, a vi možete biti odgovorni za dugove ili kaznena djela počinjena pod vašim imenom dok se ne dokaže suprotno).

Ponzijeva shema

Pozvani ste da sudjelujete u projektu koji obećava dosljedno visoke povrate od ulaganja u kriptoimovinu, često poduprte svjedočanstvima ili lažnim pričama o uspjehu. Shema može biti predstavljena kao prilika višerazinskog marketinga, gdje nagrade ne ostvarujete samo vlastitim ulaganjem, već i uključivanjem drugih. Čini se da prvi ulagači primaju isplate, potičući više ljudi da se pridruže i promoviraju shemu.

U stvarnosti, ne postoji istinski posao i ne generira se dobit. Umjesto toga, novac dolazi isključivo od doprinosa novijih ulagača koji se koriste za plaćanje povrata organizatorima i prvim sudionicima sheme.

Što bi se moglo dogoditi:

Nakon što se nova ulaganja uspore, shema se ruši, a vi, kao i većina sudionika, gubite svoj novac. Organizatori nestaju, bez mogućnosti povrata sredstava. Višerazinska struktura pomaže da se prijevara brzo proširi jer žrtve nesvjesno postaju promotori.

Lažna adresa koja kompromitira vaš novčanik

Nakon što ste izvršili kriptotransakciju, primijetili ste novu adresu koja se pojavljuje u povijesti novčanika. Ova adresa nalikuje onoj s kojom ste prethodno komunicirali. Prevaranti mogu prikazati lažne adrese u vašoj povijesti transakcija slanjem male količine kriptovaluta s adrese koje nalikuju pravoj u vaš novčanik. Na taj način lažna adresa koju je stvorio prevarant završava u nedavnoj aktivnosti vašeg novčanika ili automatskim prijedlozima. Prevaranti namjerno stvaraju adrese koje nalikuju pravima mijenjajući samo nekoliko znakova, često u sredini adrese, kako bi izbjegli da ih se otkrije.

Što bi se moglo dogoditi:

Kada pokušate poslati kriptovalutu i kopirati pogrešnu adresu iz povijesti novčanika, nesvjesno šaljete sredstva u novčanik prevaranta. Budući da su kriptotransakcije često nepovratne, vaša se sredstva u većini slučajeva trajno gube. Ova prijevara oslanja se na vizualnu obmanu i korisničku pogrešku, iskorištavajući naviku kopiranja i lijepljenja adresa iz novčanika bez pomnog pregleda.