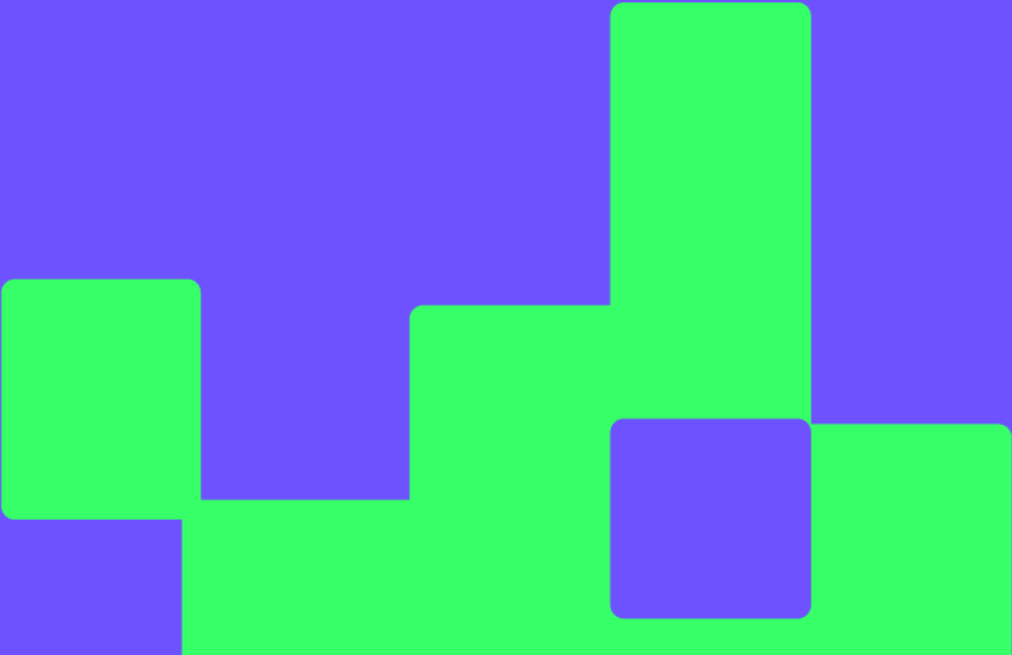


3 NAČINI NA KATERE GOLJUFI POSKUŠAJO UKRASTI VAŠO NALOŽBO TER KAKO TO ENOSTAVNO PREPREČITI

*S tem vodnikom se boste enostavno
zaščitili pred najbolj pogostimi poskusi
kraje vaših sredstev.*



Problem

Pri vlaganju v kriptovalute lahko postanete žrtve goljufij, ki vam lahko povzročijo:

- velike izgube
- ogrožen finančni položaj
- stres, sram, jezo in celo depresijo

Rešitev

Naučim se prepoznati tipične kripto goljufije in zaščititi svoj kapital.

Kazalo

Kazalo.....	3
1. Uvod.....	4
2. Prepoznajte varnostne grožnje in se zaščitite.....	6
A. Goljufije preko spletnih oglasov.....	6
Kako se odvije poskus goljufije?.....	6
Kako se zaščititi?.....	7
B. Goljufije preko hladnih telefonskih klicev.....	8
Kako se odvije poskus goljufije?.....	8
Kako se zaščititi?.....	9
C. Phishing napadi.....	10
Tipi phishing napadov.....	10
Kako se zaščititi?.....	11
D. Vdori v uporabniške račune.....	12
Kako se odvije?.....	12
Kako se zaščititi?.....	13
3. Varnostni seznam pred kripto transakcijo.....	14
3. Zaključek.....	17

1. Uvod

Vlagatelji v kriptovalute se srečujejo z različnimi varnostnimi grožnjami in prevarami. Razne goljufije še posebej ciljajo na začetnike in osebe z osnovnim računalniškim znanjem.

Namen tega učbenika je opremiti tako začetnike kot tudi izkušene vlagatelje z znanjem in orodji za zaščito pred varnostnimi grožnjami.

Raziskali bomo, kako prepoznati in se zaščititi pred goljufijami preko spletnih oglasov, hladnih telefonskih klicev ter drugimi prevarantskimi taktikami. Prav tako se bomo naučili zaščititi svoj uporabniški račun pred vdori, šibkimi gesli in drugimi varnostnimi pomanjkljivostmi. Prejeli pa boste tudi celovit seznam varnostnih ukrepov, ki vam bodo pomagali zavarovati vaše naložbe pred morebitnimi tveganji med opravljanjem kripto transakcij.

Z uporabo tega vodiča boste postali bolj opremljeni za varno in samozavestno vlaganje v svet kriptovalut. Vaša varnost je naše poslanstvo, zato vas vabimo, da izkoristite vse koristne nasvete ter strategije, ki vam jih ta vodnik ponuja.



Starejši ljudje so privlačna tarča za goljufe. Goljufi jih skušajo premamiti z zgodbami o hitrem zaslužku in pridobiti njihovo zaupanje.

2. Prepoznajte varnostne grožnje in se zaščitite

V tem poglavju si bomo pogledali najbolj razširjene tipe goljufij, katerih so žrtve kripto vlagatelji. Goljufi ponavadi računajo na naivnost in željo po hitrem zaslužku potencialnih žrtev. Te šibkosti izkoriščajo z glavnim namenom, da bi žrtvam ukradli denar.

A. Goljufije preko spletnih oglasov

Goljufije preko spletnih oglasov predstavljajo pogost način, kako prevaranti zvabijo nedolžne vlagatelje v pasti lažnih obljub o hitrih dobičkih v svetu kriptovalut. V tem poglavju bomo raziskali, kako se tovrstne goljufije odvijajo in kako se lahko zaščitite pred njimi.

Kako se odvije poskus goljufije?

1. **Lažni oglasi:** Prevaranti ustvarijo lažne spletne oglase, ki obljubljajo izjemno donosne naložbene priložnosti v kriptosvetu. Ti oglasi se pogosto pojavljajo na spletnih straneh, povezanih s kriptovalutami, financami ali spletnim trgovanjem.
2. **Ponujajo nerealne obljube:** Goljufi v oglasih obljubljajo hitre in velike donose pri vlaganju v kriptovalute. Uporabljajo prepričljive besedne zveze, kot so "zagotovljeni dobički" ali "hitra obogatitev", da pritegnejo pozornost nedolžnih vlagateljev.
3. **Preusmeritev na lažne spletne strani:** Ko uporabnik klikne na oglas, ga preusmerijo na lažno spletno stran, ki izgleda zelo podobno pristni platformi za trgovanje s kriptovalutami. Ta stran je običajno oblikovana tako, da vzbudi zaupanje in prepriča uporabnike, da ustvarijo račun in vložijo denar.
4. **Pretvarjanje:** Na lažnih spletnih straneh se prevaranti pogosto pretvarjajo, da so uradni predstavniki znanih borznih platform ali

investicijskih podjetij. Ponujajo "ekskluzivne" priložnosti za trgovanje in vlaganje, ki jih je težko zavrniti.

5. **Zbiranje osebnih podatkov:** Ko uporabnik ustvari račun na lažni spletni strani, ga prevaranti pogosto prosijo, da vpiše svoje osebne podatke, kot so ime, naslov, telefonska številka in celo bančni podatki. Te podatke nato uporabijo za nadaljnje goljufije ali pa jih prodajo na črnem trgu.

Kako se zaščititi?

1. **Preverite verodostojnost oglasa:** Bodite pozorni na nenavadne ali preveč dobrosrčne oglase, ki obljublajo hitre in velike donose. Preverite verodostojnost platforme ali podjetja, ki oglašuje, in se izogibajte dvomljivim ponudbam.
 - A. **Preverite spletno stran:** Preden ustvarite račun ali vložite denar na spletni strani za trgovanje s kriptovalutami, preverite njen URL in certifikate varnosti. Preverite tudi ocene uporabnikov in mnenja na spletnih forumih ali družabnih omrežjih.
 - B. **Ne delite osebnih podatkov:** Nikoli ne razkrivajte svojih osebnih podatkov, kot so gesla, bančni podatki ali osebne identifikacijske številke, na spletnih straneh, ki se zdijo sumljive ali nepooblaščne.
 - C. **Ostanite informirani:** Redno se izobražujte o prevarantskih praksah in varnostnih tveganjih v svetu kriptovalut. Bodite pozorni na novice o goljufijah in se naučite prepoznavati rdeče zastave, ki kažejo na morebitno prevaro.

B. Goljufije preko hladnih telefonskih klicev

Ali ste se že kdaj znašli v situaciji, ko ste prejeli nenavaden klic ali elektronsko sporočilo, ki ponuja izjemno donosno naložbeno priložnost v kriptosvetu? V

tem poglavju bomo raziskali, kako prepoznati in se zaščititi pred tovrstnimi goljufijami.



Pri goljufijah preko spletnih oglasov ali telefonskih klicev prevaranti nudijo lažno svetovanje o naložbah v kriptovalute.

Kako se odvije poskus goljufije?

1. **Lažna identiteta:** Goljufi se pogosto predstavijo kot investicijski svetovalci ali uslužbenci priljubljenih kripto platform, kot je na primer Kriptomat.
2. **Odprtje računa na menjalnici:** Cilj prevarantov je, da vas prepričajo v to, da odprete račun na Kriptomatu in vanj vložite denar, s katerim nato kupite kriptovalute, kot je npr. Bitcoin.
3. **Prevzem nadzora nad računalnikom:** Ob tem vam prevarantje ponudijo "pomoč" pri postopku in vas poskušajo prepričati, da prevzamejo nadzor nad vašim računalnikom preko orodij za oddaljeni dostop, kot so TeamViewer, AnyDesk ipd.
4. **Pretveza oplemenitenja sredstev:** Vaša naložba v Bitcoin se nato prenese na zunanjo Bitcoin denarnico, ki je v lasti goljufov, pod pretvezo, da bodo vaša sredstva oplemenitena. Pogosto se omenjajo donosi 10x ali 100x; torej vložite 1000 evrov, in zaslužili boste 10000 evrov v zelo kratkem času.
5. **Namišljen dobiček:** Prevarantje uporabljajo lažne posnetke zaslona, ki prikazujejo namišljen dobiček, da vas prepričajo v dodatna vlaganja. Ko želite dvigniti sredstva ali izplačati dobiček, prevaranti prekinejo stike, in vi ostanete brez svojega denarja.

Kako se zaščititi?

1. **Bodite pazljivi, ko vas kliče neznana številka:** Če prejmete klic z neznane številke, bodite pozorni. Prevaranti se običajno ne predstavijo ustrezno ali pa govorijo slabo slovensko. Če je ponudba preveč dobra, da bi bila resnična, je verjetno prevara.
2. **Nikoli ne delite oddaljenega dostopa do svojega računalnika z neznanci:** Če vas nekdo prosi za oddaljen dostop do vašega računalnika, naj bo to rdeča zastava. Prevaranti lahko s takšnim dostopom dostopajo do vaših osebnih podatkov in kripto sredstev.
3. **Nikoli po telefonu ne delite svojega gesla in osebnih podatkov:** Legitimna podjetja ali platforme nikoli ne bodo zahtevala vašega gesla ali občutljivih osebnih podatkov preko telefona.
4. **Ne pošiljajte denarja brez preverjanja:** Preden nakažete denar, natančno preverite identiteto osebe ali platforme, ki jo prejimate. Preverite, ali ima platforma ustrezne licence in dobre ocene uporabnikov.
5. **Preverite identiteto:** Če vam nekdo ponuja donosno naložbo, vedno preverite njihovo identiteto. Če ste v dvomih, se obrnite na uradne podporne kanale platforme, s katero nameravate trgovati.
6. **Ne verjemite obljubam o donosih:** Preveč dobre ponudbe so pogosto prevara. Če vam nekdo zagotavlja donos, ki se zdi predober, da bi bil resničen, je verjetno prevara.



Če vas neznanec prosi za oddaljen dostop do vašega računalnika, nemudoma prekinite klic in blokirajte kakršen koli kontakt s to osebo.

C. Phishing napadi preko email in SMS sporočil

Tako imenovani *phishing** (izgovorjava "fišing") napadi so ena najpogostejših spletnih prevar, s katerimi se srečujejo vlagatelji v kriptovalute. Pri teh prevarah goljufi poskušajo pridobiti občutljive podatke, kot so gesla, podatki bančne kartice in zasebni ključi kripto denarnic, tako da se pretvarjajo, da so zaupanja vredne osebe ali podjetja.

*Izraz "*phishing*" izhaja iz besede "fishing" oziroma "ribarjenje", kot v smislu "ribarjenje po informacijah". Pri napadih s phishingom goljufi vržejo vabo v obliki lažnih elektronskih sporočil, SMS-sporočil ali spletnih strani, s katerimi skušajo zvabiti nedolžne posameznike, da jim posredujejo občutljive informacije, kot so gesla, številke kreditnih kartic ali druge osebne podatke. Analoga ribarjenju je torej primerna, saj goljufi uporabljajo zvižaco, da "ulovijo" svoje žrtve in pridobijo njihove osebne podatke.



Pri phishing napadih prevaranti skušajo pridobiti občutljive podatke, (gesla, podatki bančne kartice, zasebne ključe kripto denarnic) s pretvarjanjem, da so zaupanja vredne osebe ali podjetja.

Tipi phishing napadov

1. **Elektronska in SMS-sporočila:** Goljufi pošiljajo ponarejena elektronska sporočila ali SMS-e, v katerih se pretvarjajo, da so predstavniki priljubljenih menjalnic ali denarnic, včasih pa tudi bančnih računov. S tem poskušajo prepričati vlagatelje, da razkrijejo svoje prijavnne podatke.
2. **Družbena omrežja:** Prevaranti ustvarijo lažne profile vplivnežev ali podjetij na družbenih omrežjih, kot so Twitter, Telegram itd. Pogosto uporabljajo imena znanih oseb, da bi naredili svoje ponarejene profile bolj prepričljive oziroma jim dali kredibilnost. S tem poskušajo zvabiti uporabnike na lažne spletne strani, kjer jih potem prepričujejo, da razkrijejo občutljive informacije.

3. **Google oglasi:** Prevaranti ustvarijo oglase za prevarantske spletne strani, ki se pojavijo na vrhu rezultatov iskanja kot kupljeni oglasi. Spletni naslovi teh lažnih strani je pogosto le rahlo drugačen od dejanskega naslova priljubljene platforme. Mnogi uporabniki ne opazijo razlike in s poskusom prijave na račun goljufo razkrijejo občutljive podatke (gesla, zaupne podatke kreditne kartice itd.).

Kako se zaščititi?

1. **Ne klikajte sumljivih povezav:** Če prejmete sumljivo elektronsko sporočilo ali SMS, se izogibajte klikanju na povezave v njem.
2. **Ne razkrivajte občutljivih informacij:** Nikoli ne vnašajte svojih gesel, podatkov bančne kartice ali zasebnih ključev denarnic na sumljive spletne strani.
3. **Bodite pozorni na sponzorirane povezave v Googlu:** Pred klikom na sponzorirane povezave v Googlu natančno preverite URL naslove in se prepričajte, da ste na pravi spletni strani.
4. **Preverite spletni naslov:** Preden vnesete svoje podatke, trikrat preverite, da ste na pravilnem naslovu. Na primer, lahko se znajdete na naslovu *kriiptomat.io* in ne opazite, da je stran lažna (vsebuje namreč dve črki "i" namesto ene).
5. **Izogibajte se javnim brezžičnim omrežjem:** Za kripto transakcije se izogibajte uporabi javnih brezžičnih omrežij, saj so pogosto slabo zavarovana in lahko omogočajo prevarantom dostop do vaših občutljivih informacij.

D. Vdori v uporabniške račune

V tem poglavju se bomo posvetili enemu najbolj prefinjenih načinov spletnih goljufij – vdoru v uporabniške račune. To so napadi, ki se najpogosteje zgodijo zaradi slabih varnostnih praks ali pa zaradi prevelike zaupljivosti uporabnika.



Najbolj pogosto gre za vdore v slabo zavarovane račune ali če uporabnik sam razkrije prijavnne podatke, ker zaupa goljufu.

Kako se odvije?

1. **Uporaba šibkih gesel:** Goljufi pogosto izkoriščajo račune, ki uporabljajo šibka gesla, ki so enostavna za uganiti ali prelisičiti. Takšna gesla so pogosto kombinacije enostavnih besed, rojstnih datumov ali drugih osebnih podatkov, ki jih je mogoče preprosto uganiti.
2. **Prenos podatkov:** V nekaterih primerih uporabnik sam posreduje svoje prijavnne podatke, bodisi prek prevarantskih spletnih strani ali prek goljufivih klicev, ki smo jih opisali v prejšnjih poglavjih.
3. **Izkoriščanje ranljivosti:** Napadalci izkoristijo morebitne ranljivosti v varnostni programski opremi žrtvine naprave, s čimer pridobijo dostop do sredstev in osebnih informacij uporabnikov.



Pri Kriptomatu uporabljamo številne varnostne mehanizme, s katerimi preprečujemo vse vrste napadov.

Kako se zaščititi?

1. **Uporaba močnih gesel:** Za vsak račun, povezan s kriptovalutami, ustvarite edinstveno in močno geslo, ki vsebuje kombinacijo črk, števil in posebnih znakov. Izogibajte se uporabi enostavnih gesel, ki jih je lahko uganiti.
2. **Dvostopenjsko preverjanje:** Omogočite dvostopenjsko preverjanje (2FA) na vseh računih, povezanih s kripto naložbami, kar dodatno oteži vdor v vaše račune. 2FA zahteva, da poleg gesla vnesete tudi drugo obliko preverjanja, kot je koda, poslana na vaš telefon ali uporaba avtentikatorja aplikacije.
3. **Ne delite gesel:** Nikoli ne delite gesel s tretjimi osebami in se izogibajte posredovanju gesel prek telefonskih klicev ali elektronske pošte. Ne glede na to, kako prepričljivo se zdi prošnja, vedno ohranjajte zasebnost svojih prijavnih podatkov.
4. **Varovanje zasebnosti:** Ne delite podrobnosti svojih kripto naložb na družbenih omrežjih ali drugih javnih platformah, saj lahko to poveča tveganje za ciljane napade. S tem se izognete privabljanju pozornosti goljufom, ki bi lahko izkoristili vaše podatke za napade ali krajo.

3. Varnostni seznam pred kripto transakcijo

V tem poglavju se bomo osredotočili na varnostni seznam, ki vam bo pomagal zagotoviti varno izvedbo vsake kripto transakcije. S pregledom in izvajanjem priporočil v tem seznamu boste lahko zmanjšali tveganja za izgubo sredstev in zagotovili varno in zanesljivo izkušnjo pri upravljanju s kriptovalutami.

A. Pred transakcijo

1. Preverite vir

- ☐ **Ali je vir naložb zaupanja vreden in preverjen?** Preverjanje zanesljivosti in ugleda vira naložbe je ključno za preprečevanje goljufij.
- ☐ **Ali je platforma, ki jo uporabljam, zaupanja vredna in varna?** Preverite, ali je platforma licencirana in regulirana.
- ☐ **Sem preveril/a spletne naslove in e-poštne naslove?** Pogosto se goljufi pretvarjajo, da so legitimna podjetja ali storitve, zato bodite pozorni na morebitne spremembe v spletnih naslovih ali e-poštnih domenah.

2. Zavarujte svojo napravo

- ☐ **Ali uporabljam varno napravo z ažurirano protivirusno programsko opremo in požarnim zidom?** Redno posodabljanje programske opreme in uporaba zaščitnih programov pomaga preprečiti vdore ali napade zlonamerne programske opreme.
- ☐ **Ali sem na varnem in zasebnem Wi-Fi omrežju?** Izogibajte se uporabi javnih Wi-Fi omrežij, saj so pogosto tarča napadov.

3. Uporabljajte močna, edinstvena gesla in 2FA

- ☐ **Ali so vsi računi (menjalnice, denarnice, e-pošta) zaščiteni z močnimi, edinstvenimi gesli?** Uporaba kompleksnih in raznolikih gesel za vsak račun povečuje varnost vaših naložb.
- ☐ Ali je dvostopenjska verifikacija (2FA) omogočena na mojem računu? 2FA dodatno zaščiti vaše račune z zahtevanjem dodatne avtentikacije ob prijavi ali izvedbi transakcij.

B. Med transakcijo

- ☐ **Ali sem skrbno pregledal/a podrobnosti transakcije?** Pred potrditvijo transakcije natančno preglejte vse podrobnosti, vključno z naslovi prejemnikov in zneski transakcije. Preverite, ali se podatki ujemajo z vašimi pričakovanji in namenom transakcije.
- ☐ **Ali so provizije pregledne in razumne?** Preverite, ali so stroški transakcije jasno izraženi in ali so v skladu s tržnimi standardi. Ne pozabite upoštevati morebitnih dodatnih stroškov, ki jih lahko zaračunajo borze ali druge storitve.

3. Zaključek

Goljufi se zavedajo, da je veliko ljudi, ki se s kriptovalutami srečujejo prvič in so zato lahka tarča za prevare.

Upamo, da vam je ta vodič nudil jasen vpogled v najpogostejše varnostne grožnje, povezane z vlaganjem v kriptovalute, in vas je opremil s potrebnim znanjem ter orodji, da se jim lahko uspešno izognete.

Ključno je, da ostanete vedno pozorni, informirani in da se zavedate svojih odločitev ter tveganj. S pravilnim razumevanjem in uporabo varnostnih ukrepov boste lahko veliko vlagali veliko bolj samozavestno.

Hvala, ker ste izbrali naš vodič. Želimo vam obilo sreče pri vaših kripto naložbah!



Želite kupovati in prodajati kriptovalute na preprosti in varni platformi v slovenskem jeziku? Odprite Kriptomat račun in zgradite svoj kripto portfelj že danes!

ZAČNI INVESTIRATI