FRODI U SCAMS RELATATI MAL-KRIPTO

KUN ATTENT U PPROTEĠI LILEK INNIFSEK

It-tkabbir rapidu tal-kriptoassi u l-karatteristiċi speċifiċi tagħhom – l-aċċessibbiltà globali, il-veloċità, l-anonimità, u l-irriversibbiltà tat-tranżazzjonijiet – jagħmluhom mira ewlenija għaċ-ċiber-kriminali. Il-frodaturi u l-iscammers jużaw tattiċi sofistikati biex iqarrqu bik, bħal "skemi Ponzi", opportunitajiet ta' investiment foloz, offerti b'xejn fuq il-media soċjali u messaġġi foloz. Huma jużaw ukoll scams romantiċi jew indirizzi li jixbħu lil dawk familjari biex johdulek flusek. Ħafna drabi jilħquk permezz tal-midja soċjali, apps ta messaġġi, emails u telefonati mhux mistennija li jinstemgħu reali. Tista' tiffaċċja riskji bħal telf finanzjarju, serq tal-identità, u diffikultà emozzjonali.

Oqgħod attent u segwi dawn il-pariri ewlenin biex tibqa' sikur:

Kun attent minn frodi kripto u scams oħra:
Tgħallem aktar dwar tipi differenti ta' frodi u scams (ara paġni 5-8);

Sinjali ta' twissija:
Tgħallem irrikonoxxi mġieba, messaġġi jew offerti suspettużi (ara paġna 2);

Ipproteġi lilek innifsek u l-assi tiegħek:
Ipprotegi l-informazzjoni personali tiegħek (ara paġna 3);

Kun af x'għandek tagħmel jekk tisfa' vittma ta' frodi jew scams
(ara paġni 4).

Sinjali ta’ twissija

Offerta li tidher tajba wisq biex tkun vera.

Offerta mhux mitluba.

Garanzija ta’ ritorn għoli u mgħaġġel.

Urġenza għall-azzjoni (eż. offerti ta’ żmien limitat li jagħmlulek pressjoni biex taġixxi immedjatament).

Talba għal pagament permezz ta’ metodi mhux traċċabbli (eż. kriptoassi, gift cards, trasferimenti telefoniċi, jew kards ta’ debitu mħallsa minn qabel).

Stedina biex tikklikkja fuq link, tiskennja kodiċi QR jew tniżżel app.

Talba biex tibgħat jew taqsam “private keys” jew “seed phrases” (lista ta’ kliem biex taċċessa u tirkupra l-kartiera kripto tiegħek).

URL suspettuż jew mhux korrett.

Logo b’distorsjonijiet żgħar, sit web li jikkopja d-dehra ta’ sit web ta’ kumpanija reali jew li jidher professjonali iżda li ma għandux dettalji ta’ kuntatt ivverifikati, informazzjoni dwar ir-reġistrazzjoni tal-kumpanija, rekord ta’ prestazzjoni, jew preżenza verifikabbli.

Pjattaforma ta’ skambju mhux magħrufa.

Attachments suspettużi, speċjalment .exe, .scr, .zip, jew fajl tal- Office makro-attivat (.docm, .xlsm).

Passi biex tipproteġi lilek innifsek:

1 Stenna u aħseb qabel ma taġixxi:

Tgħaġġilx biex tinvesti, taqsam l-informazzjoni, jew tikklikkja fuq il-links- l-iscammers deliberatament joħolqu sens ta' urġenza. F'każ ta' kwalunkwe dubju, anki minuri, taġixxix u tinvestix qabel ma tverifika is-sors.

2 Iċċekkja s-sors b'attenzjoni:

- Dejjem ivverifika minn fejn jiġu l-messaġġi, it-telefonati, l-emails, u l-links, anke jekk jidhru uffiċjali, jidhru li ġejjin minghand ħabib jew mill-familja tiegħek, jew saħansitra minn figura pubblika. Fittex żbalji ortografiċi, URLs strambi, jew indikaturi tas-sigurtà neqsin eż. ivverifika li l-link tas-sit web jinkludi "s" f'"HTTPS" biex tiżgura li s-sit web ikun sigur, u ċċekkja għal kwalunkwe ittra miżjuda jew nieqsa fl-isem tal-kumpanija.
- Tiftaħx links minn messaġġi mhux mitluba, installa biss applikazzjonijiet uffiċjali permezz ta' app stores fdati, u tiskannjax kodiċijiet QR mhux magħrufa.
- Anki jekk offerta tidher uffiċjali, dejjem agħmel kontroverifika tagħha mas-sit web tal-kumpanija jew iċċekkja li l-kont tal-media soċjali jiġi vverifikat (eż. b'marki ta' kontroll uffiċjali).
- Uża d-dettalji ta' kuntatt ivverifikati biex tasal għand il-kumpanija jew l-individwu direttament u qatt ma sserraħ fuq l-informazzjoni ta' kuntatt ipprovduta mill-frodatur suspettat (eż. fittex l-isem tal-kumpanija b'mod indipendenti, uża direttorji tan-negozju vverifikati). Scammers jistgħu jiddikjaraw li huma awtorizzati jew jimitaw is-sit web ta' kumpanija awtorizzata. Tista' tivverifika jekk il-fornitur tal-kriptoassi huwiex awtorizzat fl-UE billi tiċċekkja r-reġistru tal-ESMA (). Tista' tikkonsulta wkoll is-sit web tal-awtorità finanzjarja nazzjonali tiegħek (https://www.mfsa.mt/) biex tara jekk inħarġux xi twissijiet jew il-lista tal IOSCO I-SCAN (iosco.org/i-scan/).

3 Qatt taqsam passwords, "private keys" jew "seed phrases":

Kull min għandu aċċess għalihom jista'jieħu kontroll tal-assi tiegħek. Kumpaniji leġittimi qatt ma jitolbu l-passwords jew il-kodiċijiet tas-sigurtà tiegħek bl-email, b'messaġġi jew bit-telefown.

4 Żomm l-apparat u "private keys" siguri:

Uża passwords b'saħħithom u uniċi għal kull wieħed mill-kontijiet kripto tiegħek, żomm il-passwords tiegħek sigrieta, u evita li terġa' tuża l-istess kredenzjali fuq pjattaformi differenti. Attiva l-awtentikazzjoni b'diversi fatturi fejn possibbli. Ara xi suġġerimenti dwar il-passwords hawnhekk (). Żomm is-softwer u l-protezzjoni kontra l-virus tiegħek aġġornati u attivati.

5 Oqgħod attent meta tirċievi offerti ta' investiment mhux mistennija:

Oqgħod attent mill-investimenti li jippromettu redditi enormi. Jekk jidher tajjeb wisq biex ikun veru, probabbilment hekk hu.

6 Aħseb qabel ma taqsam l-informazzjoni fuq il-midja soċjali:

Il-gruppi taċ-chat, il-fora, il-posts tal-midja soċjali u r-ritratti jistgħu jkunu sorsi siewja ta' għarfien għall-frodaturi. Li tikxef wisq dwarek innifsek jew dwar l-investimenti tiegħek jista' jagħmlek mira faċli.

X’għandek tagħmel meta tkun vittma ta’ frodi jew scam

Waqqaf minnufih it-tranżazzjonijiet

Waqqaf kwalunkwe trasferiment ta’ flus lejn kontijiet suspettużi biex tevita telf addizzjonali. Waqqaf kull kuntatt mal-iscammers – injora t-telefonati u l-emails tagħhom u mblokka lil min jibgħathom.

Ibdel il-passwords tiegħek fuq l-apparati u l-apps/is-siti web kollha tiegħek.

Il-frodaturi jixtru passwords żvelati online u jippruvawhom fuq diversi kontijiet. It-tibdil ta’ password waħda biss mhuwiex biżżejjed; kun żgur li tbiddilhom kollha, għalhekk il-frodaturi ma jkunux jistgħu jerġgħu jużawhom.

Skonnettja u rrevoka l-aċċess:

Irrevoka permessi suspettużi fil-ftehim diġitali tiegħek li jaħdmu awtomatikament fuq il-blockchain (smart contracts) biex twaqqaf lill-iscammers milli jonfqu t-tokens tiegħek mingħajr il-kunsens tiegħek. Ħafna kartieri u esploraturi tal-blockchain joffru għodod li jippermettulek tara liema smart contracts għandhom aċċess biex jonfqu t-tokens tiegħek. Biex tagħmel dan tista’:

- tuża “kontrollur tal-permess” fdat, li jivverifika jekk utent jew indirizz tal-blockchain huwiex awtorizzat jeżegwixxi operazzjoni;
- tirrevedi l-lista ta’ approvazzjonijiet; u
- tuża l-buttuna “revoke” direttament mill-pjattaforma.

Ċaqlaq il-fondi tiegħek:

Jekk il-kartiera tiegħek tiġi kompromessa, ittrasferixxi immedjatament l-assi li jifdallek għal kartiera sigura ġdida.

Ikkuntattja lill-fornitur tal-kripto tiegħek:

Informa lill-fornitur tal-kriptoassi tiegħek malajr kemm jista’ jkun bl-użu ta’ modi ta’ kuntatt uffiċjali biex tesplora għażliet potenzjali. Anke jekk, fil-biċċa l-kbira tal-każijiet, it-treġġigħ lura tat-tranżazzjoni blockchain ma jkunx possibbli, il-fornitur xorta jista’ jiffriża l-kont tal-iscammer (jekk ikun fuq il-pjattaforma tiegħu) u jelenka l-indirizz tal-kartiera.

Rapport u twissija:

Irrapporta l-inċident lill-pulizija jew lill-awtorità superviżorja finanzjarja nazzjonali tiegħek (https://www.mfsa.mt/), u informa lin-network tiegħek (eż. ħbieb u familja) biex tqajjem kuxjenza. Dawn l-azzjonijiet huma l-aħjar mod biex tipproteġi lilek innifsek u lill-oħrajn.

Oqgħod attent għal frodi “Recovery Room”:

Il-frodatur jista’ jikkuntattjak bħala vittma ta’ scam preċedenti, billi jiddikjara li huwa awtorità pubblika (eż. il-pulizija, l-awtorità tat-taxxa jew finanzjarja eċċ.), u joffri li jirkupra l-flus mitlufa tiegħek bi ħlas. Ħafna drabi dan ikun tentattiv ieħor biex iqarrqu bik. Ftakar: li tiġi scammed darba ma jżommokx milli tiġi scammed mill-ġdid.

Ara t-twissija tal-Awtoritajiet Superviżorji Ewropej Konġunti biex issir taf aktar dwar ir-riskji relatati mal-kriptoassi (↖) u l-iskeda informattiva “Kripto-Assi spjegat: Xi tfisser il-MiCA għalik bħala konsumatur” (↖).

Il-Lussemburgu: L-Uffiċċju tal-Pubblikazzjonijiet tal-Unjoni Ewropea, 2025 PDF ISBN 978-92-9407-261-0 doi:10.2853/2985869 DZ-01-25-149-MT-N

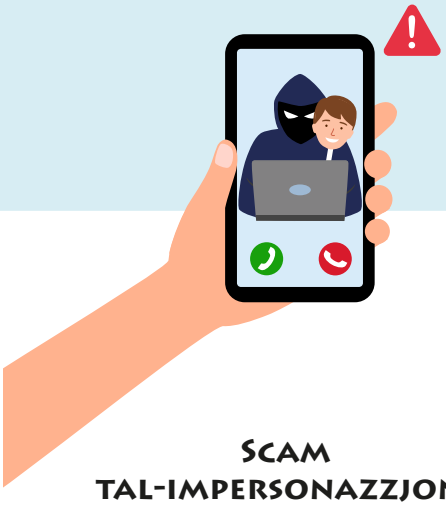
It-tipi ta' SCAMS ta' KRIPTO

Skema ta' "Pump-and-dump" jew "Rug pull"

Tara reklam fuq il-midja soċjali jew sit web li jippromwovi "opportunità ta' investiment f'ħin limitat" fil-kripto, li jirrakkomanda investiment f'token jew proġett kripto ġdid. Wara li tesprimi interess, tiġi kkuntattjat u ridirett lejn pjattaforma tal-iskambju tal-kripto jew kanal tal-messaġġi (eż. Telegram, Viber, jew WhatsApp). Kuntatt li jidher kredibbli jwiegħed profitti mgħaġġla jew redditi għoljin jekk tinvesti fil-pront. Tiġi imħeġġeġ tinvesti ammont żgħir u mbagħad tiġi pressat biex tinvesti aktar.

X'jista' jiġri:

Tiskopri li t-token investit huwa inutli u l-kuntatt tiegħek jieqaf iwieġeb. Meta tipprova tirtira l-flus tiegħek, tiskopri li l-websajt m'għadhiex teżisti, u l-kumpanija ma tistax tintlaħaq. Scammers ikunu artifiċjalment neffħu jew esaġerataw il valur ta' kripto baxx biex iżidu l-valur tiegħu ("pump"), imbagħad ibiegħu l-assi tagħhom ("dump"), u b'hekk ikkawżaw il-valuri biex jikkraxxjaw u jħallu lill-investituri b'telf. Inkella, jistgħu jagħlqu l-proġett u jisparixxu bil-fondi ("rug pull").



Scam tal-impersonazzjoni

Wara li tpoġġi mistoqsija fuq pjattaforma tal-midja soċjali jew websajt dwar kwistjoni tal-"crypto wallet", tirċievi messaġġ diretta mhux mistenni (DM) jew email minn xi ħadd li jiddikjara li jkun kuntatt fdat (eż., kripto-skambju, wallet provider, IT support, jew saħansitra ħabib). Il-persuna titlob is-"seed phrase" tiegħek (jiġifieri sekwenza ta' kliem li sservi bħala l-backup ċentrali għall-aċċess tal-kartiera diġitali tiegħek), passwords, jew "private keys" (kodiċi kriptografiku ġġenerat awtomatikament li juri s-sjieda tal-assi diġitali).

X'jista' jiġri:

Ladarba taqsam is-"seed phrase", il-passwords, jew "private keys" tiegħek, l-iscammer jużahom biex jisraq il-kripto tiegħek jew fondi oħra. Żomm f'moħħok li t-telf ta' "private keys" jirriżulta fit-telf permanenti u irriversibbli ta' aċċess u sjieda għall-kriptoassi tiegħek. B'differenza ghat tranżazzjonijiet bankarji, fil-każ ta' trasferimenti kripto, ladarba l-fondi tiegħek huma mitlufa, huwa kważi impossibbli li jiġu rkuprati.

Il-phishing

Tirċievi messaġġ mhux mistenni permezz ta' email, telefon, pop-up, jew midja soċjali, li jiddikjara li huwa mingħand fornitur tal-kriptoassi magħruf sew. Il-messaġġ jistiednek tilloggja jew tniżżel app ġdida. Tista' wkoll tirċievi email li tidher li hija mill-app tal-wallet tal-kripto tiegħek, u tħeġġek biex issolvi kwistjoni ta' sigurtà billi tikklikkja fuq link ipprovdut minn sors mhux uffiċjali, jew billi taġġorna l-app.

X'jista' jiġri:

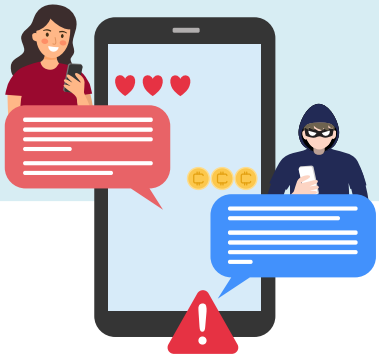
Billi tikklikkja fuq il-link, tniżżel l-app, jew tiskennja kodiċi QR, tinstalla malware li jippermetti lill-iscammer jaċċessa u juża l-informazzjoni biex jisraq il-kriptoassi jew il-fondi tiegħek.

Scam ta' Giveaway

Inti tiltaqa' ma' avviż fuq il-media soċjali li jiddikjara li kumpaniji qed jagħtu kriptoassi wara investiment żgħir fil-kriptoassi. Dawn jinkludu filmat jew post li fih ritratti ta' ċelebrità jew ta' ditti – normalment foloz jew miksuba mingħajr awtorizzazzjoni – li jippromettu li "tirdoppja l-kripto tiegħek" jekk tibgħat il-flus l-ewwel. Il-logo, it-tqassim, it-testimonjanzi, u l-lingwa użata jidhru professjonali u uffiċjali, l-istess bħas-sit web li int ridirett lejh.

X'jista' jiġri:

Wara li tibgħat il-kripto tiegħek, ma tirċievi xejn lura, u titlef il-flus mibgħuta. L-għotja kienet falza, u l-post jew livestream li jimpersona ċelebritajiet jew kumpaniji kien iddisinjat biex iqarraq bik.



Scam ta' Investiment Romantiċi:

Int tiġi ikkuntattjat fuq il-midja soċjali, applikazzjonijiet tad-dating, jew it-telefon / SMS minn xi ħadd li qatt ma ltqajt miegħu fil-ħajja reali. Din il-persuna tinvolvi ruħha f'konverżazzjonijiet frekwenti, personali u romantiċi, filwaqt li tibni l-fiduċja bl-użu ta' profili foloz. Maż-żmien, il-konverżazzjoni timxi lejn opportunitajiet finanzjarji, jiddikjaraw profitti kbar minn investimenti kripto u jħeġġuk tinvesti b'wegħdiet ta' redditi għoljin u riskju baxx. Huma jiggwidawk billi jistabbilixxu kont u jagħmlu depożitu inizjali żgħir biex jagħmlu l-iskema tidher leġittima.

Scammers joħolqu profili online foloz u jużaw stampi misruqa jew iġġenerati mill-Intelliġenza Artifiċjali biex javviċinawk.

X'jista' jiġri:

L-iscammer jiġbed kemm jista 'jkun flus, imbagħad jaqta' l-komunikazzjoni kollha u jisparixxi. Is-sit web jew l-app ta' investiment frodulenti titneħħa offline, u b'hekk ma tkunx tista' taċċessa l-investimenti preżunti. F'xi każijiet, l-iscammers jistgħu jużaw l-informazzjoni miksuba matul l-iscam biex jimmiraw il-ħbieb u l-familja tiegħek u jwettqu serq tal-identità li jista' jkollu konsegwenzi finanzjarji jew legali għalik (eż. il-frodatur jista' jivverifika wallets misruqa f'ismek u tista' tinżamm responsabbli għal djun jew reati mwettqa taħt ismek sakemm ma jiġix ippruvat mod ieħor).

Skema Ponzi

Tiġi mistieden tieħu sehem fi proġett li jwiegħed redditi għoljin konsistenti minn investimenti fil-kriptoassi, spiss appoġġati minn testimonjanzi jew stejjer ta' suċċess foloz. L-iskema tista' tiġi ppreżentata bħala opportunità ta' kummerċjalizzazzjoni f'diversi livelli, fejn taqla' premjijiet mhux biss mill-investiment tiegħek stess, iżda wkoll billi tirrekluta oħrajn. L-investituri tal-bidu jirċievu xi pagamenti, u b'hekk iħeġġu aktar nies biex jissieħbu u jippromwovu l-iskema.

Fir-realtà, ma hemm l-ebda negozju jew profitt ġenwin li qed jiġi ġġenerat. Minflok, il-flus jiġu biss mill-kontribuzzjoni ta' investituri aktar ġodda li tintuża biex jitħallsu r-redditi lill-organizzaturi tal-iskema u lill-ewwel parteċipanti.

X'jista' jiġri:

Ladarba l-investimenti l-ġodda jonqsu, l-iskema tikkollassa, u int, bħall-biċċa l-kbira tal-parteċipanti, titlef il-flus tiegħek. L-organizzaturi jisparixxu, u ma jħallu l-ebda mod kif jiġu rkuprati l-fondi. L-istruttura f'diversi livelli tgħin biex l-iscam jinfirex malajr, hekk kif il-vittmi, mingħajr ma jafu li hija scam, jsiru promoturi.

Indirizz li jixbah tieghek li qed "jivvelena" l-kartiera tiegħek

Wara li tagħmel tranżazzjoni kripto, tinnota indirizz ġdid li jidher fl-istorja tal-kartiera tiegħek. Dan l-indirizz jidher simili għal dak li qabel kont tinteraġixxi miegħu. Scammers jistgħu jagħmlu l-indirizzi tal-kartieri foloz jidhru fl-istorja tat-tranżazzjoni tiegħek billi jibagħtu ammont żgħir ta' kripto minn indirizz li jixbah lil dak tal-kartiera tiegħek. Int tispiċċa taħżen fl-attività reċenti tal-kartiera tiegħek jew permezz ta' suġġerimenti awtomatiċi fl-indirizz falz maħluq mill-iscammer. Scammers deliberatament joħolqu indirizzi look-alike billi jibdlu biss ftit karattri, ħafna drabi fin-nofs tal-indirizz, biex jevitaw id-detezzjoni.

X'jista' jiġri:

Meta tipprova tibgħat kripto u tikkopja l-indirizz ħażin mill-istorja tal-kartiera tiegħek, mingħajr ma tkun taf tkun qed tibgħat fondi lill-kartiera tal-iscammer. Minħabba li t-tranżazzjonijiet kripto huma spiss irriversibbli, il-fondi tiegħek jintilfu fil-biċċa l-kbira tal-każijiet b'mod permanenti. Dan l-iscam jiddependi fuq qerq viżwali u żball tal-utent, li jisfrutta d-drawwa ta' "copy and paste" tal-indirizzi tal-kartieri mingħajr spezzjoni mill-qrib.