FRODI U SCAMS FINANZJARJI ONLINE F'DINJA TA' INTELLIGENZA ARTIFIĊJALI

OQGĦOD ATTENT U IPPROTEĠI LILEK INNIFSEK

Il-frodi u l-iscams finanzjarji online mhumiex ġodda, iżda l-Intelliġenza Artifiċjali (AI) għamlithom aktar sofistikati u diffiċli biex jiġu identifikati. Il-kriminali issa jużaw messaġġi u websajts foloz, profili foloz ta' ċelebritajiet, u saħansitra vuċijiet jew vidjows iġġenerati mill-AI li jidhru bħall-bankier tiegħek, il-ħbieb tiegħek jew il-familja tiegħek biex iqarrqu bik.

Ħafna drabi jikkuntattjawk 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 stress emozzjonali. Oqgħod attent u segwi dawn il-pariri ewlenin biex tibqa' sikur:

Kun konxju tal-frodi u scams finanzjarji online eżistenti li jużaw AI
eż., l-impersonazzjoni, il-phishing, *l-iscams tal-investiment u tal-assigurazzjoni, u saħansitra l-frodi u l-iscams romantiċi. Ikklikkja* hawn *biex titgħallem aktar dwar tipi differenti ta' frodi u scams* ara paġni 5-7.

U hawnhekk *għall-frodi* u l-iscams speċifiċi għall-kripto ( ).

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

Ipproteġi lilek innifsek:
Żomm l-informazzjoni personali tiegħek *sikura* (ara paġna 3*);* u

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

Sinjali ta’ twissija

Wegħda li tidher tajba wisq biex tkun vera.

Telefonata mhux mistennija minn numru mhux magħruf.

Talba urġenti għal flus jew informazzjoni personali, inkluż jekk tidher li ġejja minn xi ħadd li taf, bħal membru tal-familja, ħabib, jew saħansitra figura pubblika.

Talba biex jittieħed kontroll tad-device tiegħek, tniżżel app, tiskennja kodiċi QR jew tikklikkja fuq link.

Talba għal informazzjoni personali jew dettalji bankarji (eż. passwords, numri tal-karti tal-kreditu, kredenzjali bankarji, jew kodiċijiet tas-sigurtà).

Talba għal ħlas permezz ta’ metodi li ma jistgħux jiġu traċċati (eż. kriptos, gift cards, wire transfers, jew kards ta’ debitu mħallsa minn qabel).

Indirizz jew link tal-email suspettuż jew mhux korrett (eż. żbalji fl-ortografija fil-URL jew indirizzi tal-web mhux tas-soltu).

Attachments minn sors mhux magħruf, speċjalment .exe, .scr, .zip, jew fajl tal-Office makro-attivat (.docm, .xlsm).

Grammatika fqira jew l-ifformattjar ħażin f’dokument li jidher uffiċjali, għalkemm l-AI tista’ tippermetti lill-frodaturi jaħbu dawn id-difetti b’mod aktar effettiv.

Sit web li jidher professjonali iżda mingħajr dettalji ta’ kuntatt jew reġistrazzjoni verifikati.

Intonazzjoni li tinstema mhux naturali, m’għandhiex pawżi u tidher fluwenti ż-żejjed jew robotika. Oqgħod attent għall-klonazzjoni tal-vuċi, għalkemm id-diskors iġġenerat mill-AI jista’ jinstema’ wkoll naturali ħafna.

Vidjows fejn il-vuċi tista’ tinstema’ robotika jew wisq uniformi, il-movimenti tax-xufftejn u l-espressjonijiet tal-wiċċ jistgħu jkunu allinjati ħażin mad-diskors, jew fejn l-isfond, id-dawl u d-dellijiet jistgħu jkunu inkonsistenti. Dawn spiss ikunu vidjos iġġenerati mill-AI (deepfakes).

Passi biex tipproteġi lilek innifsek

1 **Qatt taqsam informazzjoni personali jew bankarja:**

Il-kumpaniji leġittimi qatt ma jitolbuk l-PINs, il-passwords, id-dettalji bankarji, jew il-kodiċijiet ta' sigurtà tiegħek permezz ta' email, SMS, midja soċjali, jew bit-telefown.

2 **Aħseb darbtejn qabel ma taġixxi:**

Tgħaġġilx biex tibgħat il-flus, taqsam l-informazzjoni, jew tikklikkja fuq links - l-iscammers deliberatament joħolqu sens ta' urġenza (eż. kwistjonijiet tal-IT mal-bank tiegħek, sejħiet ta' emerġenza li jinvolvu lill-ħbieb u lill-membri tal-familja tiegħek, lingwaġġ ta' theddid, eċċ.). F'każ ta' xi dubji, anki żgħar, taġixxix; temm il-kuntatt u ivverifika s-sors jew l-identità bir-reqqa.

3 **Iċċekkja s-sors/l-identità bir-reqqa:**

- Dejjem ivverifika minn fejn jiġu l-messaġġi, it-telefonati, l-emails, u l-links - anke jekk jidhru uffiċjali, jidhru li ġejjin minn ħabib jew mill-familja tiegħek, jew saħansitra minn figura pubblika. Pereżempju, ċempel jew ibgħat messaġġ lill-familja u l-ħbieb tiegħek billi tuża numru magħruf permezz ta' mod ta' komunikazzjoni ta' fiduċja; 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 ikun sigur, u ċċekkja għal xi ittri 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.

- Aqbel mal-familja tiegħek dwar 'kelma sigura'- fraži sigrieta li tista' tuża biex tikkonferma l-identità jekk xi ħadd b'vuċi familjari jsejjaħlek talba urġenti għall-flus u jiddikjara li huwa membru tal-familja (eż. ġenituri, oħt/oħt, tifel/tifla).

- 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, u metodi ta' kuntatt ikkonfermati). Scammers jistgħu jiddikjaraw li huma awtorizzati jew jimitaw is-sit web ta' kumpanija awtorizzata. Ivverifika jekk inħarġitx xi twissija mill-awtorità finanzjarja nazzjonali tiegħek (https://www.mfsa.mt/) jew ġietx inkluża fil-lista IOSCO I-SCAN (iosco.org/i-scan/). Għall-fornituri tal-kripto, iċċekkja jekk humiex awtorizzati fl-UE (eż., iċċekkja r-reġistru tal-ESMA ( ).

4 **Oqgħod attent għal-qerq potenzjali tal-AI:**

Bil-progress tat-teknoloġija l-iscams tal-AI qed isiru aktar konvinċenti minn qatt qabel. Jekk xi ħaġa tħossha mhux tas-soltu jew tinduna b'sinjal ta' twissija, ieqaf u erġa' evalwa s-sitwazzjoni.

5 **Qatt tinstalla softwer ta' aċċess b'mod remote jew tixxerja l-iskrin tiegħek:**

Il-banek u l-istituzzjonijiet finanzjarji qatt mhuma se jitolbu dan mingħandek.

6 **Żomm l-apparat u l-kontijiet siguri:**

Uża passwords b'saħħithom u uniċi, żommhom sigrieti, u evita li terġa' tuża l-istess kredenzjali fuq pjattaformi differenti. Ippermetti 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 mixgħula dejjem.

7 **Oqgħod attent minn opportunitajiet ta' investiment mhux mistennija u ta' żmien limitat:**

Jekk jidher tajjeb wisq biex ikun veru, probabbilment huwa.

8 **Aħseb qabel ma taqsam informazzjoni fuq il-midja soċjali:**

Il-gruppi taċ-chat, il-fora, il-posts tal-midja soċjali u r-ritratti jistgħu jkunu sorsi siewja ta' infomazzjoni 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.

Ikkuntattja l-bank jew il-kumpanija finanzjarja tiegħek:

Informa lill-bank jew lill-kumpanija finanzjarja tiegħek immedjatament permezz ta’ modi ta’ kuntatt uffiċjali, biex tesplora għażliet għall-iffriżar jew għat-treġġigħ lura tat-tranżazzjonijiet.

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

Il-frodaturi jixtru passwords mikxufa 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.

Irraporta u għarraf:

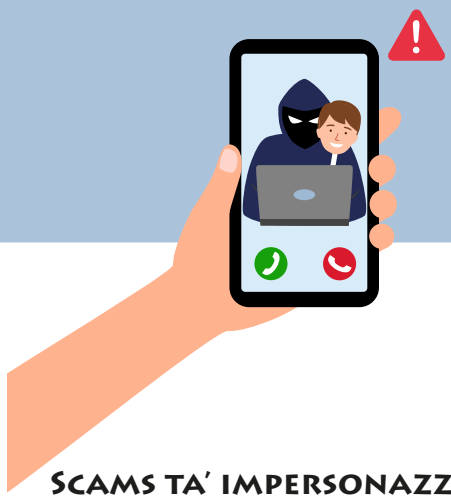
Irrapporta l-każ lill-pulizija jew lill-awtorità finanzjarja nazzjonali tiegħek (https://www.mfsa.mt/) u għarraf ukoll lill-ħbieb u lill-familja tiegħek, biex tqajjem kuxjenza. Dawn l-azzjonijiet jistgħu jgħinuk tipproteġi lilek innifsek u lil ħaddieħor.

Oqgħod attent għall-frodi “Recovery Room”:

Il-frodatur jista’ jikkuntattjak wara li jkun jaf li inti vittma ta’ scam preċedenti, fejn 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 tkun scammed darba ma jżommokx milli tiġi scammed mill-ġdid.

PDF ISBN 978-92-9407-215-3 doi:10.2853/6062796 DZ-01-25-103-MT-N

Tipi ta’ Frodi Online imħaddma mill-AI



Scams ta’ impersonazzjoni u l-użu ta’ deep fake

Inti tirċievi telefonata mhux mistennija minn xi ħadd li jiddikjara li huwa l-bank tiegħek, awtorità pubblika (eż. il-pulizija, l-awtorità tat-taxxa jew finanzjarja eċċ.), distributur tal-assigurazzjoni, kumpanija tal-IT, jew saħansitra membru tal-familja. Min iċempel jista’ jħeġġek tittrasferixxi fondi biex iżżommhom sikuri, billi jikkwota attività suspettuża fuq il-kont tiegħek jew il-polza tal-assigurazzjoni tiegħek. Huma jistgħu wkoll jitolbuk tiżvela d-dettalji bankarji tiegħek (eż. in-numru tal-karta tal-ħlas, il-kredenzjali bankarji tal-internet, jew il-passwords), tikklikkja fuq link, jew tinstalla softwer, u jgħidu li jistgħu jsolvu l-kwistjoni malajr. Min iċempel jista’ juża numru falsifikat, li spiss jaqbel man-numru tat-telefon tal-bank tiegħek biex jidher leġittimu (spoofing).

L-iscammers jistgħu jużaw l-AI biex joħolqu vidjows, immaġnijiet, jew awdjo foloz li jimitaw il-vuċi ta’ xi ħadd (eż. il-bankier tiegħek jew membru tal-familja), il-wiċċ (eż. ċelebrità), jew il-movimenti. **Dan huwa magħruf bħala “Deepfake”.**

X’jista’ jiġri:

Billi jsemmi d-dettalji personali u joħloq sens ta’ urġenza, l-iscammer iqarraq bik sabiex tieħu azzjonijiet li kieku ma tiħux - bħal tibgħat flus fil-kont tagħhom, tikklikkja fuq link malizzjuż, jew tinstalla malware fuq l-apparat tiegħek. Dan jista’ jagħti lill-iscammer aċċess dirett għall-kredenzjali bankarji tiegħek. B’din l-informazzjoni, jistgħu jibdlu l-passwords tiegħek, jidħlu fil-kont bankarju tiegħek, u jisirqulek il-flus. Ftakar: jekk min iċempel jaf dettalji personali dwarek ma jfissirx li hu/hi ta’ fiduċja.

Il-phishing u s-Social Engineering

Tirċievi email jew messaġġ li jidher li ġej mill-bank tiegħek jew minn kumpanija finanzjarja, li jwissik dwar “attività suspettuża” fil-kont tiegħek. Il-logo, id-disinn, u l-lingwa jidhru professjonali, u l-messaġġ jista’ jidher fl-istess bħal konverżazzjonijiet oħra mill-bank tiegħek. Il-messaġġ iħeġġek tikklikkja fuq link biex tivverifika l-kont tiegħek jew tirrisettja l-password tiegħek. Il-link twassal għal websajt falza li tidher identika għall-internet banking tiegħek. Mingħajr ma tirrealizzaha, iddaħħal id-dettalji tiegħek f’websajt imfassla biex tisraq l-informazzjoni personali tiegħek.

L-iscammers jużaw l-AI biex ifasslu messaġġi ta’ phishing konvinċenti billi janalizzaw id-data tal-media soċjali biex jidentifikaw il-vittmi tagħhom u jadattaw il-kontenut għal kull mira.

X’jista’ jiġri:

L-iscammer jaċċessa l-kont bankarju tiegħek u jisraq flusek jew joħloq profil falz bid-dettalji personali tiegħek biex iwettaq frodi.

Scam tal-investiment jew tal-assigurazzjoni

Tara reklam fuq il-midja soċjali jew sit web li jippromwovi “opportunità ta’ investiment limitata b’riskji baxxi” jew “jew offerta speċjali fuq assigurazzjoni”. Spiss jużaw ritratti ta’ ċelebritajiet jew rakkomandazzjonijiet li jidhru professjonali imma huma foloz. Wara li tesprimi interess billi tikklikkja fuq link jew timla formola, tiġi kkuntattjat u ridirezzjonat lejn pjattaforma jew kanal ta’ messaġġi fejn tirċievi pariri u dokumenti professjonali. Tiġi imħeġġeġ tinvesti ammont żgħir, segwit minn somom akbar, jew tħallas il-primjum f’dak li jidher li huwa kont sigur.

Il-frodaturi jużaw għodod tal-AI biex jagħmlu dawn il-proposti foloz jew emails foloz konvinċenti ħafna u diffiċli biex jiġu identifikati. Huma jużaw ukoll bots tal-media soċjali li jaħdmu bl-AI biex joħolqu kontijiet foloz li jinteraġixxu miegħek, ixerrdu miżinformazzjoni, u jissimulaw imġiba reali biex jiksbu fiduċja u jinfluwenzaw id-deċiżjonijiet tiegħek.

X’jista’ jiġri:

Meta tipprova titlob flusek lura, il-kuntatt jisparixxi. Inti tiskopri li l-kumpanija ma teżistix jew li r-riskju li assigurajt mhuwiex kopert. Imbagħad tirrealizza li bgħatt flus direttament lil scammer bħala parti minn scam frodulenti. Sfortunatament, ma tistax tieħu flusek lura, u d-dettalji personali u finanzjarji tiegħek jistgħu jintużaw biex titwettaq aktar frodi (eż. l-iffirmar ta’ kuntratti f’ismek li jistgħu jwassluk biex titlef saħansitra aktar flus).

Il-frodi u l-iscams romantiċi

Int tiġi ikkuntattjat fuq il-midja soċjali, applikazzjonijiet tad-dating, jew bit-telefon / messaġġ minn xi ħadd li ma ltqajtx magħha 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 flus jew opportunitajiet finanzjarji, bħal investimenti kripto b’wegħdiet ta’ redditi għoljin u riskju baxx. Il-persuna titolbok tittrasferixxi l-flus f’kont jew tiggwidak billi tistabbilixxi kont u tagħmel depożitu inizjali żgħir biex l-iscam tidher leġittima qabel ma tinkoraġġik tinvesti aktar.

Il-frodaturi jużaw l-AI biex jiġġeneraw profili foloz, jidentifikaw il-vittmi tagħhom fuq il-media soċjali/ apps tad-dating billi jużaw data li tkun għamilt disponibbli. Xi drabi saħansitra jużaw chatbots biex jiġġeneraw messaġġi.

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. Minbarra t-telf finanzjarju, l-informazzjoni personali li qsamt tista’ tintuża biex timmira l-ħbieb u l-familja tiegħek jew għal serq tal-identità li jista’ jkollu konsegwenzi finanzjarji jew legali għalik (eż. il-frodatur jista’ jixtri, jieħu self f’ismek, jew tista’ tinżamm responsabbli għal djun jew reati mwettqa taħt ismek sakemm jiġi ppruvat mod ieħor).

Scams fuq xiri onlajn

Tiltaqa ma' offerta attraenti online. Il-bejjiegħ jitolbok tħallas barra mill-pjattaforma, u jibgħatlek link biex tħallas. Il-link jidderieġik lejn paġna falza li tidher bħal tal-bank tiegħek, fejn tiġi mitlub iddaħħal id-dettalji bankarji tiegħek.

L-AI jintuża biex jinħolqu siti web foloz, konfermi tal-ordnijiet, u "invoices" konvinċenti ħafna. L-AI tgħinhom jimitaw it-ton, il-brand, u l-istil ta' kumpaniji reali. F'xi każijiet, jużaw chatbots AI biex iwieġbu mistoqsijiet u jagħmlu l-ftehim jidher aktar kredibbli.

X'jista' jiġri:

Il-pagament permezz ta' link ta' parti terza jevita l-protezzjonijiet tas-suq. L-iscammer jikseb l-informazzjoni tal-login tiegħek fil-kont bankarju tiegħek u jisraq flusek.