TIEŠSAISTES FINANŠU KRĀPŠANA MĀKSLĪGĀ INTELEKTA PASAULĒ

ESI MODRS UN SARGĀ SEVI

Tiešsaistes finanšu krāpšana nav nekas jauns, bet mākslīgais intelekts (MI) ir padarījis to gudrāku un grūtāk atklājamu. Noziedznieki izmanto viltus ziņas un tīmekļa vietnes, viltus slavenību profilus un pat ar MI ģenerētas balsis vai videoklipus, kuros, lai maldinātu, tevi šķietami uzrunā tavas bankas pārstāvis, draugi vai ģimenes locekļi.

Krāpnieki bieži uzrunā tevi, izmantojot sociālos medijus, ziņapmaiņas lietotnes, e-pastu un negaidītus tālruņa zvanus, un šķiet, ka viņu teiktais ir pilnīgi reāls.

Tu vari saskarties ar tādiem riskiem kā finansiāli zaudējumi, identitātes zādzība un emocionālas ciešanas. Esi piesardzīgs un, lai pasargātu sevi, ņem vērā šos padomus:

Uzmanies no tiešsaistes finanšu krāpšanas, kurā izmanto MI. Piemēram, no uzdošanās par citu personu, pikšķerēšanas, ieguldījumu un apdrošināšanas krāpšanas un pat no romantiskās krāpšanas. Uzzini vairāk par dažādiem krāpšanas veidiem 5., 6. un 7. lpp.

Uzzini par krāpšanu ar kriptoaktīviem: .

Atpazīsti brīdinājuma signālus – iemācies atpazīt aizdomīgu rīcību, ziņojumus vai piedāvājumus (sk. 2. lpp.).

Aizsargā sevi – aizsargā savus personas datus (sk. 3. lpp.).

Zini, ko darīt, ja esi kļuvis par krāpšanas upuri (sk. 4. lpp.).

Brīdinājuma signāli

Solījumi, kas šķiet pārāk labi, lai būtu patiesi.

Negaidīts zvans no nezināma numura.

Steidzams naudas vai personīgās informācijas pieprasījums, tostarp no personas, kas izliekas par ģimenes locekli, draugu vai pat par sabiedrībā labi zināmu personu.

Pieprasījums pārņemt kontroli pār tavu ierīci, lejupielādēt lietotni, skenēt kvadrātkodu (QR kodu) vai noklikšķināt uz saites.

Personas datu vai bankas datu pieprasījums (piemēram, paroles, kredītkaršu numuri, internetbankas pieteikšanās dati vai drošības kodi).

Pieprasījums veikt maksājumu, izmantojot neizsekojamus paņēmienus (piemēram, kriptoaktīvi, dāvanu kartes, pārvedumi vai priekšapmaksas debetkartes).

Aizdomīga vai nepareiza e-pasta adrese vai saite (piemēram, pareizrakstības kļūdas tīmekļa vietņu saitēs (URL) vai neparastas tīmekļa vietņu adreses).

Pielikums no nezināma avota, īpaši tādas datnes kā .exe, .scr, .zip vai *Office* datnes ar automatizētām (makro) komandām (.docm, .xlsm).

Gramatikas kļūdas vai neatbilstošs formatējums šķietami oficiālā dokumentā, lai gan MI ļauj krāpniekiem labāk slēpt šos trūkumus.

Tīmekļa vietne, kas izskatās profesionāla, bet tajā nav pārbaudītas kontaktinformācijas vai uzņēmuma reģistrācijas datu.

Intonācija, kas izklausās nedabiska, runa ir bez pauzēm, pārāk raita vai mehāniska. Atceries par “balss klonēšanu”, jo ar MI ģenerēta runa var izklausīties arī ļoti dabiska.

Videomateriāli, kuros balss var skanēt pārāk raiti vai mehāniski vai lūpu kustības un sejas izteiksmes var neatbilst runai, vai arī fons, apgaismojums un ēnas var būt neatbilstošas. Šādi video bieži vien ir ģenerēti ar MI (dziļviltojumi).

Darbības sevis pasargāšanai

1 **Nekad nedalies ar saviem personas datiem vai bankas informāciju –**

Likumīgi uzņēmumi nekad nelūgs tavus PIN kodus, paroles, internetbankas pieteikšanās datus vai drošības kodus e-pastā, īsziņā, sociālajos medijos vai zvanot.

2 **Pirms rīkojies, padomā –**

Nesteidzies sūtīt naudu, dalīties ar informāciju vai klikšķināt uz saites, jo krāpnieki apzināti rada steidzamības sajūtu (piemēram, IT problēmas ar tavu banku, zvani par negadījumiem, kuros iesaistīti tavi draugi un ģimenes locekļi, iebiedēšana utt.). Ja tev ir kaut mazākās šaubas, nedari to, ko tev lūdz. Pārtrauc zvanu un rūpīgi pārbaudi sūtīšanas vietu un sūtītāja identitāti.

3 **Rūpīgi pārbaudi sūtīšanas vietu un sūtītāja identitāti:**

- vienmēr pārbaudi, no kurienes tiek sūtītas ziņas, e-pasta vēstules un saites vai tiek veikti tālruņa zvani, pat ja šķiet, ka ziņa vai zvans ir no kādas iestādes, drauga, ģimenes locekļa vai sabiedrībā zināmas personas. Piemēram, zvani vai nosūti īsziņas saviem ģimenes locekļiem un draugiem, izmantojot zināmu numuru un uzticamu kanālu, raugies, vai nav pareizrakstības kļūdu, aizdomīgu tīmekļa vietnes saišu (URL) un vai netrūkst norāžu par drošu darījumu (piemēram, pārbaudi, vai tīmekļa vietnes saites daļā "HTTPS" ir iekļauts burts "s", lai pārliecinātos, ka tīmekļa vietne ir droša. Tāpat pārbaudi, vai uzņēmuma nosaukumā nav lieku burtu vai netrūkst kāda burta);

- neatver saites nevēlamos ziņojumos, instalē tikai oficiālas lietotnes no uzticamiem lietotņu veikaliem un neskenē nezināmus kvadrātkodus (QR kodus);

- vienojies ar saviem ģimenes locekļiem par "drošo vārdu", proti, slepenu frāzi, ko var izmantot, lai pārliecinātos par identitāti, ja kāda persona šķietami zināmā balsī tev zvana, lūdzot veikt steidzamu naudas pārvedumu, un apgalvo, ka ir tavs ģimenes loceklis (piemēram, vecāks, māsa/brālis, bērns);

- izmanto pārbaudītu kontaktinformāciju, lai tieši sazinātos ar uzņēmumu vai citu personu. Nekad nepaļaujies uz kontaktinformāciju, ko sniedzis iespējamais krāpnieks (piemēram, pats atrodi uzņēmuma nosaukumu, izmanto pārbaudītus uzņēmumu katalogus un iepriekš apstiprinātas saziņas metodes). Krāpnieki var apgalvot, ka šie uzņēmumi ir viņus pilnvarojuši, vai var atdarināt darbības atļauju saņēmuša uzņēmuma tīmekļa vietni. Pārbaudi, vai tavas valsts finanšu iestāde nav sniegusi brīdinājumus vai norādījusi tos Starptautiskās Vērtspapīru komisiju organizācijas I-SCAN sarakstā (iosco.org/i-scan/). Attiecībā uz kriptoaktīvu pakalpojumu sniedzējiem pārbaudi, vai tie ir saņēmuši darbības atļauju ES (piemēram, skati Eiropas Vērtspapīru un tirgu iestādes reģistru ( )).

4 **Pievērs uzmanību iespējamiem MI trikiem –**

MI tehnoloģijai attīstoties, krāpšana ir kļuvusi daudz pārliecinošāka, pat neskatoties uz vislabākajiem padomiem par drošību. Ja kaut kas šķiet neparasts vai ietver kādu no iepriekš minētajiem brīdinājuma signāliem, nedari prasīto un izvērtē notiekošo vēlreiz.

5 **Nekad neinstalē attālinātās piekļuves programmatūru un nekopīgo ekrānu –**

Bankas un finanšu iestādes nekad tev to nepieprasīs.

6 **Aizsargā ierīces un kontus –**

Izmanto drošas un unikālas paroles, glabā tās slepenībā un izvairies no to pašu pieteikšanās datu atkārtotas izmantošanas dažādās platformās. Ja iespējams, izmanto daudzfaktoru autentifikāciju. Dažus padomus par parolēm skati šeit: . Atjaunini un aktivizē savu programmatūru un pretvīrusu aizsardzību.

7 **Ievēro piesardzību, ja tev tiek piedāvātas negaidītas un laika ziņā ierobežotas ieguldījumu iespējas, –**

Ja kaut kas izklausās pārāk labi, lai būtu patiesība, visticamāk, tā nav patiesība.

8 **Padomā, pirms kopīgo informāciju sociālajos medijos, –**

Tērzēšanas grupas, forumi, ieraksti sociālajos medijos un fotogrāfijas var būt vērtīgi informācijas avoti krāpniekiem. Atklājot pārāk daudz informācijas par sevi vai saviem ieguldījumiem, vari kļūt par vieglu mērķi.

Ko darīt, ja esi kļuvis par krāpšanas upuri

Nekavējoties pārtrauc darījumus,

Lai bloķētu jebkādus turpmākus pārskaitījumus uz aizdomīgiem kontiem un izvairītos no papildu zaudējumiem. Pārtrauc jebkādu saziņu ar krāpniekiem – ignorē viņu zvanus un e-pasta vēstules un bloķē sūtītāju.

Sazinies ar savu banku vai finanšu iestādi –

Nekavējoties informē savu banku vai finanšu iestādi, izmantojot oficiālus saziņas kanālus, lai uzzinātu par iespējām iesaldēt vai atcelt darījumus.

Nomaini paroles visās savās ierīcēs un lietotnēs/tīmekļa vietnēs –

Krāpnieki tiešsaistē iegādājas nopludinātas paroles un mēģina tās lietot vairākos kontos. Ar vienas paroles maiņu vien nepietiek. Pārliecinies, ka tiek nomainītas visas paroles, lai krāpnieki nevarētu tās izmantot atkārtoti.

Ziņo un brīdini –

Ziņo par incidentu policijai un informē savus draugus un ģimenes locekļus, lai arī viņi par to zinātu. Tas var palīdzēt tev aizsargāt sevi un citus.

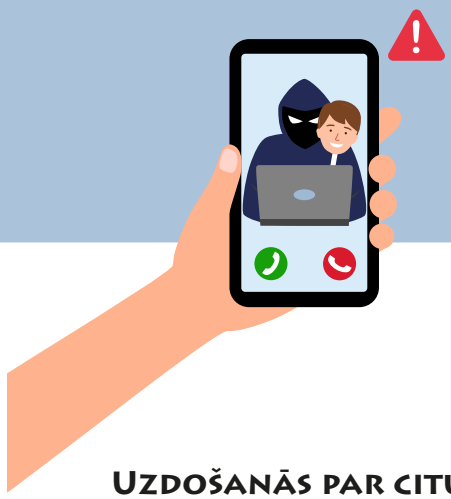
Uzmanies no krāpšanas, ja vienreiz jau esi kļuvis par krāpšanas upuri, –

Krāpnieks var sazināties ar tevi, zinot, ka jau iepriekš tiki apkrāpts. Viņš var apgalvot, ka ir no valsts iestādes (piemēram, no policijas, nodokļu vai finanšu iestādes utt.), un piedāvāt par maksu atgūt zaudēto naudu. Tas bieži ir vēl viens mēģinājums tevi apkrāpt. Atceries, ka vienreiz apkrāpta persona var tikt apkrāpta atkārtoti.

Eiropas Banku iestāde, Eiropas Apdrošināšanas un aroda pensiju iestāde, Eiropas Vērtspapīru un tirgu iestāde, 2025
Luksemburga: Eiropas Savienības Publikāciju birojs, 2025

PDF ISBN 978-92-9407-271-9 doi:10.2853/7379787 DZ-01-25-159-LV-N

TIEŠSAISTES FINANŠU KRĀPŠANA AR MI



Uzdošanās par citu personu un dziļviltojumu izmantošana

Tu saņem negaidītu zvanu no personas, kas apgalvo, ka ir tavas bankas, valsts iestādes (piemēram, policijas, nodokļu vai finanšu iestādes utt.) pārstāvis, apdrošināšanas aģents, IT uzņēmuma pārstāvis vai pat ģimenes loceklis. Zvanītājs var mudināt tevi pārskaitīt līdzekļus, lai tos aizsargātu, apgalvojot, ka tavā kontā vai ar tavu apdrošināšanas polisi tiek veiktas aizdomīgas darbības. Šī persona var arī lūgt tev atklāt savus bankas datus (piemēram, maksājumu kartes numuru, internetbankas pieteikšanās datus vai paroles), noklikšķināt uz saites vai instalēt programmatūru, apgalvojot, ka tā var ātri atrisināt šķietamo problēmu. Zvanītājs var izmantot viltotu numuru, kas bieži vien atbilst tavas bankas tālruņa numuram, lai zvans šķistu īsts (izlikšanās jeb *spoofing*).

Krāpnieki var izmantot MI, lai izveidotu neīstus video, attēlus vai audio ierakstus, kas atdarina noteiktas personas (piemēram, tavas bankas pārstāvja vai ģimenes locekļa) balsi, seju (piemēram, slavenības) vai kustības. **Šādus viltojumus sauc par dziļviltojumiem.**

Kas varētu notikt?

Minot personas datus un radot steidzamības sajūtu, krāpnieks liek tev rīkoties tā, kā nebiji plānojis, piemēram, sūtīt naudu uz krāpnieka kontu, noklikšķināt uz ļaunprātīgas saites vai instalēt ļaunatūru savā ierīcē. Tas var dot krāpniekam tiešu piekļuvi taviem bankas pieteikšanās datiem. Izmantojot šo informāciju, krāpnieks var mainīt tavu paroli, piekļūt tavam bankas kontam un nozagt tavu naudu. Atceries! Tas, ka zvanītājs zina tavus personas datus, nenozīmē, ka viņš ir uzticams.

Pikšķerēšana un sociālā inženierija

Tu saņem e-pasta vēstuli vai ziņojumu, ko šķietami sūtījusi tava banka vai finanšu iestāde, brīdinot tevi par aizdomīgām darbībām tavā kontā. Logotips, izkārtojums un valoda izskatās profesionāli, un ziņojums var būt iekļauts tajā pašā saziņas pavedienā, kurā notiek cita tava saziņa ar savu banku. Ziņojumā tevi mudina noklikšķināt uz saites, lai skatītu savu kontu vai atiestatītu paroli. Noklikšķinot uz saites, tu nonāc neīstā tīmekļa vietnē, kas izskatās identiski tavai internetbankai. Neapzinoties to, tu ievadi savus datus tīmekļa vietnē, kas paredzēta tavu personas datu zādzībai.

Krāpnieki izmanto MI, lai sagatavotu pārliecinošus pikšķerēšanas ziņojumus, analizējot sociālo mediju datus savu upuru identificēšanai un pielāgojot saturu katram mērķim.

Kas varētu notikt?

Krāpnieki piekļūst tavam bankas kontam un nozog tavu naudu vai izveido viltus profilu ar taviem personas datiem, lai veiktu krāpšanu.

Ieguldījumu un apdrošināšanas krāpšana

Tu sociālajos medijos vai tīmekļa vietnē redzi reklāmu, kurā tiek reklamēta "ieguldījumu iespēja ar zemu risku, kas pieejama tikai ierobežotu laiku" vai labi zināma uzņēmuma apdrošināšanas polises iegādes "atlaide, kas pieejama ierobežotu laiku". Reklāmā ir redzama slavenība un ieteikumi, kas bieži vien ir neīsti. Kad paud savu interesi, noklikšķinot uz saites vai aizpildot veidlapu, ar tevi sazinās un novirza uz platformu vai ziņapmaiņas kanālu, kur tu saņem šķietami profesionālus padomus un dokumentus. Tevi aicina ieguldīt nelielu summu, kam seko lielākas summas, vai iemaksāt apdrošināšanas prēmiju šķietami drošā kontā.

Krāpnieki izmanto MI rīkus, lai padarītu šos neīstos piedāvājumus vai e-pasta vēstules ļoti pārliecinošas un grūti atklājamas. Viņi arī izmanto sociālo mediju MI botus, lai izveidotu neīstus kontus, kas mijiedarbojas ar tevi, izplata maldinošu informāciju un simulē reālu uzvedību, lai gūtu uzticību un ietekmētu tavus lēmumus.

Kas varētu notikt?

Pēc tam, kad esi mēģinājis izņemt savu naudu vai iesniegt prasību, kontaktpersona pārtrauc atbildēt. Tu atklāj, ka uzņēmums nepastāv vai ka apdrošināšanas risks nav segts. Tad tu saproti, ka vai nu esi nosūtījis naudu tieši krāpniekam, vai tā ir daļa no krāpnieciskas shēmas. Diemžēl naudu atgūt nevari, un tavus personas un finanšu datus var izmantot, lai īstenotu citas krāpšanas (piemēram, parakstot līgumus tavā vārdā, kā rezultātā var zaudēt vēl vairāk naudas).

Romantiskā krāpšana

Kāda persona, kuru neesi saticis reālajā dzīvē, sazinās ar tevi sociālajos medijos, iepazīšanās lietotnēs vai pa tālruni/ar īsziņu. Šī persona bieži ar tevi sarunājas par personiskām un romantiskām tēmām un panāk uzticēšanos, izmantojot viltus profilus. Laika gaitā sarunu biedrs min naudu vai finanšu iespējas, piemēram, ieguldījumus kriptoaktīvos, solot lielu atdevi un zemu risku. Šī persona lūdz tev pārskaitīt naudu uz kādu kontu vai palīdz izveidot kontu un iemaksāt nelielu sākotnējo depozītu, lai shēma šķistu likumīga, pirms mudina tevi ieguldīt vairāk.

Krāpnieki izmanto MI, lai izveidotu viltus profilus un apzinātu upurus sociālajos medijos/iepazīšanās lietotnēs, izmantojot upuru atklātos datus, vai izvēlas sarunbotus, lai sagatavotu ziņojumus.

Kas varētu notikt?

Krāpnieks izkrāpj pēc iespējas vairāk naudas, pēc tam pārtrauc saziņu un pazūd. Krāpnieciskā ieguldījumu vietne vai lietotne vairs nav pieejama tiešsaistē, un tu vairs nevari piekļūt it kā veiktajiem ieguldījumiem. Papildus finansiāliem zaudējumiem tavi kopīgotie personas dati var tikt izmantoti, lai vērstos pret taviem draugiem un ģimenes locekļiem vai veiktu identitātes zādzību, kas tev var radīt finansiālas vai juridiskas sekas (piemēram, krāpnieks var veikt pirkumus, ņemt aizdevumus tavā vārdā vai tev var nākties uzņemties atbildību par parādiem vai tavā vārdā izdarītiem noziegumiem, kamēr nav pierādīts pretējais).

Ar pirkumiem saistīta krāpšana

Tu ieraugi labu piedāvājumu tiešsaistes tirdzniecības vietā. Uzņēmums, kas piedāvā šo iespēju, prasa veikt maksājumu ārpus oficiālās platformas, apgalvojot, ka tas izmanto "drošu maksājumu sistēmu", un nosūta tev saiti pirkuma pabeigšanai. Noklikšķinot uz saites, tu nonāc krāpnieciskā bankas autentifikācijas lapā, kura izveidota tā, lai izskatītos kā bankas oficiālā tīmekļa vietne, un kurā izmanto tās logotipu un tīmekļa vietnei raksturīgo izskatu, lai tu varētu ievadīt savus internetbankas datus maksājuma veikšanai.

Krāpnieki izmanto MI, lai izveidotu ļoti pārliecinošas neīstas banku tīmekļa vietnes, pasūtījumu apstiprinājumus un rēķinus. MI palīdz atdarināt īstu uzņēmumu saziņas veidu, zīmolu un stilu. Dažos gadījumos krāpnieki izmanto MI sarunbotus, lai atbildētu uz jautājumiem un padarītu darījumu ticamāku.

Kas varētu notikt?

Maksājums, izmantojot trešās personas saiti, apiet tirdzniecības vietas nodrošinātos aizsardzības pasākumus. Krāpnieks iegūst tavus bankas konta pieteikšanās datus un nozog tavu naudu.