INTERNETINĖS FINANSINĖS APGAULĖS IR SUKČIAVIMAS DIRBTINIO INTELEKTO PASAULYJE

BŪKITE BUDRŪS IR APSAUGOKITE SAVE

Internetinės finansinės apgaulės ir sukčiavimo atvejai nėra naujiena, tačiau dirbtinis intelektas (DI) juos padarė sumanesnius ir sunkiau atpažįstamus. Nusikaltėliai naudoja netikras žinutes ir svetaines, suklastotas garsenybių paskyras, o kartais ir DI sugeneruotus balsus ar vaizdo įrašus, kurie atrodo kaip jūsų banko darbuotojas, draugas ar šeimos narys, siekdami jus apgauti.

Jie dažnai susisiekia per socialinius tinklus, el. paštą, netikėtus skambučius ir susirašinėjimo programėles, ir visa tai gali skambėti labai įtikinamai.

Jums gali kilti rizika patirti finansinių nuostolių, galite tapti tapatybės vagystės ar emocinės žalos auka. Būkite atsargūs ir vadovaukitės toliau pateiktais patarimais.

Būkite atidūs dėl DI skatinamų internetinių finansinių apgaulių ir sukčiavimo,
pvz., apsimetėlių (impersonavimo), fišingo, investavimo ir draudimo apgaulių, taip pat romantinio sukčiavimo. Kad sužinotumėte daugiau apie skirtingas apgaulių rūšis žr. 5- 7 psl.

O čia – apie su kriptoturtu susijusias apgaules ir sukčiavimą ( ).

Atpažinkite įspėjamuosius ženklus:
išmokite atpažinti įtartiną elgesį, žinutes ar pasiūlymus (žr. 2 psl.);

Apsaugokite save:
saugokite savo asmeninę informaciją (žr. 3 psl.) ir

Žinokite, ką daryti, jei nukentėjote nuo sukčiavimo
(žr. 4 psl.)

Įspėjamieji požymiai

Pažadas, kuris skamba per gerai, kad būtų tiesa.

Netikėtas skambutis iš nežinomo numerio.

Skubus prašymas pervesti pinigus ar pateikti asmeninę informaciją, net jei kreipiasi šeimos narys, draugas ar viešas asmuo.

Prašymas perimti jūsų įrenginio valdymą, atsisiųsti programėlę, nuskenuoti QR kodą ar spustelėti nuorodą.

Prašymas pateikti asmeninę informaciją arba banko duomenis (pvz., slaptažodžius, mokėjimo kortelių numerius, internetinės bankininkystės duomenis arba saugos kodus).

Prašymas atsiskaityti nesekamais būdais, pavyzdžiui, kriptoturtu, dovanų kortelėmis, banko pervedimais ar išankstinio apmokėjimo kortelėmis.

Įtartinas arba neteisingas el. pašto adresas arba nuoroda (pvz., rašybos klaidos URL arba neįprasti interneto adresai).

Priedas iš nežinomo šaltinio, ypač.exe, .scr, .zip arba makrokomandos įgalintas „Office“ failas (.docm, .xlsm).

Prasta gramatika ar formatavimas oficialiai atrodančiame dokumente, nors dirbtinis intelektas gali padėti sukčiams šiuos trūkumus geriau užmaskuoti.

Svetainė, kuri atrodo profesionaliai, tačiau trūksta patikrintų kontaktinių duomenų ar įmonės registracijos informacijos.

Intonacija, kuri skamba nenatūraliai, trūksta pauzių ir atrodo pernelyg sklandi ar robotiška. Atkreipkite dėmesį į vadinamąjį balso klonavimą, nors dirbtinio intelekto sukurta kalba taip pat gali skambėti labai natūraliai.

Vaizdo įrašai, kuriuose balsas gali skambėti robotiškai arba pernelyg sklandžiai, lūpų judesiai ir veido išraiškos gali būti nesuderintos su kalba arba fonas, apšvietimas ir šešėliai gali būti nenuoseklūs. Tai dažnai yra dirbtinio intelekto sukurti vaizdo įrašai (angl. „deepfake“).

Veiksmai, kaip apsisaugoti

1 **Niekada nesidalinkite asmenine ar banko informacija:**

Teisėtos įmonės niekada neprašys jūsų PIN kodų, slaptažodžių, internetinės bankininkystės duomenų ar saugos kodų el. paštu, žinute, socialiniuose tinkluose ar telefonu.

2 **Pristabdykite ir pagalvokite prieš imdamiesi veiksmų:**

Neskubėkite siųsti pinigų, dalintis informacija ar spausti nuorodų – sukčiai sąmoningai sukuria skubos jausmą (pvz., praneša apie IT problemas jūsų banke, skambina dėl skubios šeimos nario situacijos ar naudoja grasinančią kalbą. Iškilus bet kokioms abejonėms, net ir nedidelėms, nesiimkite veiksmų; nutraukite skambutį ir atidžiai patikrinti šaltinį ar tapatybę.

3 **Atidžiai patikrinkite šaltinį/tapatybę:**

- Visada patikrinkite, iš kur gaunami pranešimai, skambučiai, el. laiškai ir nuorodos- net jei jie atrodo oficialūs ar gauti draugo, šeimos nario ar viešo asmens vardu. Pavyzdžiui, skambinkite arba rašykite savo šeimai ir draugams naudodami žinomą numerį per patikimą kanalą; ieškokite rašybos klaidų, keistų URL adresų arba trūkstamų saugumo rodiklių (pvz., patikrinkite, ar svetainės nuorodoje HTTPS yra „s“, kad įsitikintumėte, jog svetainė yra saugi, ir patikrinkite, ar įmonės pavadinime nėra pridėtų ar trūkstamų raidžių).

- Neatidarykite nuorodų iš neužsakytų pranešimų, įdiekite tik oficialias programėles iš patikimų programėlių parduotuvių ir neskenuokite nežinomų QR kodų.

- Susitarkite su savo šeima dėl “slapto žodžio”- slaptos frazės, kurią galite naudoti tapatybei patvirtinti, jei kas nors, turintis pažįstamą balsą, skambina jums skubiu prašymu dėl pinigų ir teigia, kad yra šeimos narys (pvz., tėvai, sesuo/brolis, vaikas).

- Naudokite patikrintus kontaktinius duomenis, kad tiesiogiai pasiektumėte įmonę ar asmenį, ir niekada nesiremkite įtariamo sukčiautojo pateikta kontaktine informacija (pvz., savarankiškai ieškokite įmonės pavadinimo, naudokite patikrintus verslo katalogus, anksčiau patvirtintus kontaktinius metodus). Sukčiai gali teigti, kad yra įgalioti, arba imituoti įgaliotos bendrovės svetainę. Patikrinkite, ar jūsų nacionalinė finansų priežiūros institucija yra pateikusi įspėjimų arba bendrovės yra įtrauktos į IOSCO I-SCAN sąrašą (iosco.org/i-scan/). Kriptoturto paslaugų teikėjų atveju patikrinkite, ar jie turi ES veiklos leidimą (pvz., patikrinkite ESMA registrą ( )).

4 **Atkreipkite dėmesį į galimus dirbtinio intelekto triukus:**

Tobulėjant DI technologijoms, apgaulės tampa įtikinamesnės net laikantis geriausių saugumo patarimų. Jei kas nors atrodo nejprasta ar pastebite kurį nors iš aukščiau nurodytų įspėjamųjų ženklų, sustokite ir dar kartą įvertinkite situaciją.

5 **Niekada neįdiekite nuotolinės prieigos programinės įrangos ir nesidalinkite savo ekranu:**

Bankai ir finansų įstaigos niekada to neprašys.

6 **Saugokite įrenginius ir paskyras:**

Naudokite stiprius ir unikalius slaptažodžius, laikykite juos paslaptyje ir venkite pakartotinai naudoti tuos pačius duomenis skirtingose platformose. Jei įmanoma, įjunkite kelių žingsnių autentifikavimą. Slaptažodžių patarimų rasite čia ( ). Nuolat atnaujinkite programinę įrangą ir antivirusinę apsaugą bei laikykite jas įjungtas.

7 **Būkite atsargūs su netikėtomis ir riboto laiko investavimo galimybėmis:**

Jei tai skamba per daug gerai, kad būtų tiesa, tai tikriausiai taip ir yra.

8 **Pagalvokite prieš dalindamiesi informacija socialiniuose tinkluose:**

Pokalbių grupės, forumai, įrašai ir nuotraukos sukčiams gali būti vertingas informacijos šaltinis. Pernelyg atvirai skelbiama informacija apie save ar investicijas padaro jus lengvu taikiniu.

Ką daryti, jei tapote apgaulės ar sukčiavimo auka

Nedelsdami sustabdykite operacijas,

Kad užkirstumėte kelią tolesniems pervedimams į įtartinas paskyras ir papildomiems nuostoliams. Nutraukite visą ryšį su sukčiais, ignoruokite jų skambučius ir el. laiškus, užblokuokite siuntėją.

Kreipkitės į savo banką arba finansų įmonę:

Nedelsdami informuokite savo banką ar finansų įmonę oficialiais kontaktiniais kanalais, kad būtų įvertintos galimybės užšaldyti ar atšaukti operacijas.

Pakeiskite savo slaptažodžius visuose savo įrenginiuose ir programose/svetainėse.

Sukčiai perka nutekintus slaptažodžius internete ir bando juos naudoti daugelyje paskyrų. Pakeisti tik vieną slaptažodį nepakanka; pasirūpinkite, kad jie visi būtų pakeisti, kad sukčiai negalėtų jų pakartotinai panaudoti.

Ataskaita ir įspėjimas:

Praneškite apie incidentą policijai arba savo nacionalinei finansų priežiūros institucijai (https://www.lb.lt/) ir informuokite savo aplinką, pavyzdžiui, draugus ir šeimos narius, kad didintumėte informuotumą. Šie veiksmai padeda apsaugoti jus ir kitus.

Saugokitės „pakartotinio išviliojimo“ apgaulių.

Sukčius gali su jumis susisiekti žinodamas, kad jau esate ankstesnės apgaulės auka, apsimesti viešąja institucija, pavyzdžiui, policija ar mokesčių ar finansų institucija, ir siūlyti „už mokestį“ atgauti prarastus pinigus. Tai dažnai dar vienas bandymas jus apgauti. Prisiminkite, kad kartą apgautas asmuo gali būti apgautas ir vėl**.**

Europos bankininkystės institucija, Europos draudimo ir profesinių pensijų institucija, Europos vertybinių popierių ir rinkų institucija, 2025

Liuksemburgas: Europos Sąjungos leidinių biuras, 2025

PDF ISBN 978-92-9407-273-3 doi:10.2853/2434668 DZ-01-25-161-LT-N

DI SKATINAMŲ INTERNETINIŲ FINANSINIŲ APGAULIŲ IR SUKČIAVIMO RŪŠYS

Apsimetėlių apgaulė ir „deepfake“ naudojimas.

Gaunate netikėtą skambutį iš asmens, kuris teigia esąs jūsų bankas, viešoji institucija (pavyzdžiui, policija ar mokesčių ar finansų institucija), draudimo platinimo įmonė, IT bendrovė ar net šeimos narys. Skambintojas gali raginti pervesti lėšas „saugiai“, nurodydamas tariamą įtartiną veiklą jūsų sąskaitoje ar draudimo polise. Jis taip pat gali prašyti pateikti banko duomenis, pavyzdžiui, mokėjimo kortelės numerį, internetinės bankininkystės duomenis ar slaptažodžius, paprašyti spustelėti nuorodą ar įsidiegti programėlę, esą ji greitai išspręs problemą. Gali būti naudojamas suklastotas numeris, atitinkantis jūsų banko telefono numerį, kad skambutis atrodytų teisėtas (numerio klastojimas).

Sukčiai gali naudoti DI, kad sukurtų netikrus vaizdo įrašus, nuotraukas ar garsą, imituojančius kieno nors balsą (pavyzdžiui, jūsų banko darbuotojo ar šeimos nario), veidą (pavyzdžiui, garsenybės) ar judesius. Tai vadinama „deepfake“.

Kas gali atsitikti:

Pasinaudodamas asmenine informacija ir sukūręs skubos jausmą, sukčius priverčia jus atlikti veiksmus, kurių neketinote, pavyzdžiui, pervesti pinigus į jo sąskaitą, spustelėti kenkėjišką nuorodą ar įdiegti kenkėjišką programą. Taip sukčius gali gauti prieigą prie jūsų banko prisijungimų. Turėdamas šią informaciją, jis gali pakeisti slaptažodį, prisijungti prie banko ir pavogti jūsų pinigus. Atminkite, kad tai, jog skambintojas žino asmeninių detalių apie jus, savaime nereiškia, jog juo galima pasitikėti.

Fišingas ir socialinė inžinerija

Gaunate el. laišką ar žinutę, kuri, regis, yra iš jūsų banko ar finansų įmonės ir perspėja apie „įtartiną veiklą“ sąskaitoje. Logotipas, maketas ir kalba atrodo profesionalūs, žinutė gali pasirodyti toje pačioje temoje kaip ir ankstesni pokalbiai su banku. Raginama spustelėti nuorodą, kad patvirtintumėte paskyrą ar atstatytumėte slaptažodį. Nuoroda veda į netikrą svetainę, kuri atrodo identiška jūsų internetinei bankininkystei. Nepastebėdamas to, asmuo suveda duomenis svetainėje, sukurtoje asmens informacijai pavogti.

Sukčiai pasitelkia DI, kad kurtų įtikinamas fišingo žinutes, analizuoja socialinių tinklų duomenis aukoms identifikuoti ir pritaiko turinį kiekvienam taikiniui.

Kas gali nutikti:

Sukčius prisijungia prie jūsų banko ir pavagia pinigus arba su jūsų asmens duomenimis sukuria netikrą paskyrą ir vykdo sukčiavimą.

Sukčiavimas investicijų ar draudimo srityje

Socialiniuose tinkluose ar svetainėje matote reklamą, kuri skelbia „riboto laiko investavimo galimybę su maža rizika“ arba „riboto laiko nuolaidą“ draudimui iš žinomos įmonės. Skelbime naudojama garsenybės nuotrauka ir rekomendacijos, kurios dažnai būna suklastotos. Pareiškus susidomėjimą spustelint nuorodą ar užpildant formą, su jumis susisiekiama ir nukreipiama į platformą ar žinučių kanalą, kur pateikiami profesionaliai atrodantys patarimai ir dokumentai. Raginama investuoti nedidelę sumą, po to didesnes sumas, arba sumokėti draudimo įmoką į „saugią“ sąskaitą.

Sukčiai naudoja DI įrankius, kad padarytų netikrus pasiūlymus ar el. laiškus labai įtikinamus ir sunkiai atpažįstamus. Taip pat naudojami DI valdomi socialinių tinklų botai, kurie kuria netikras paskyras, bendrauja, skleidžia dezinformaciją ir imituoja tikrą elgesį, kad pelnytų pasitikėjimą ir darytų įtaką sprendimams.

Kas gali atsitikti:

Bandant atsiimti pinigus ar pateikti pretenziją, kontaktas nustoja atsakinėti. Paaiškėja, kad įmonė neegzistuoja arba kad draudimo rizika neapdrausta. Vėliau suprantate, kad pinigus pervedėte tiesiai sukčiui kaip dalį apgaulės schemos. Deja, pinigų dažnai atgauti nepavyksta, o jūsų asmens ir finansiniai duomenys gali būti panaudoti tolesniam sukčiavimui, pavyzdžiui, sudarant sutartis jūsų vardu.

Romantiškas sukčiavimas

Su jumis socialiniuose tinkluose, pažinčių programėlėse arba telefonu ar žinutėmis susisiekia asmuo, kurio nesate sutikę realiame gyvenime. Jis dažnai, asmeniškai ir romantiškai bendrauja, naudodamas netikras anketas. Laikui bėgant pokalbis pasukamas pinigų tema arba siūlomos finansinės „galimybės“, pavyzdžiui, kriptoturto investicijos su „didele grąža ir maža rizika“. Asmuo prašo pervesti pinigus į sąskaitą arba pamokina, kaip susikurti paskyrą ir atlikti nedidelį pradinį įnašą, kad schema atrodytų teisėta, o vėliau ragina investuoti daugiau.

Sukčiai naudoja DI, kad generuotų netikrus profilius, identifikuotų aukas socialiniuose tinkluose ar pažinčių programėlėse pagal jūsų paskelbtus duomenis, arba naudoja pokalbių robotus žinutėms kurti.

Kas gali nutikti:

Sukčius išvilioja kiek įmanoma daugiau lėšų, tada nutraukia visą bendravimą ir dingsta. Netikra investavimo svetainė ar programėlė išjungiama, o jūs nebegalite pasiekti tariamų investicijų. Be finansinių nuostolių, jūsų pateikta asmeninė informacija gali būti panaudota taikantis į jūsų draugus ir šeimą arba tapatybės vagystei, kas gali turėti finansinių ar teisinių pasekmių, pavyzdžiui, pirkimai ar paskolos jūsų vardu.

Pirkimo apgaulė

Interneto prekyvietėje randate patrauklų pasiūlymą įsigyti prekę. Pasiūlymą teikianti įmonė prašo apmokėti ne per oficialią platformą, tvirtina, kad naudoja „saugų mokėjimo metodą“, ir atsiunčia nuorodą pirkiniui užbaigti. Nuoroda nukreipia į netikrą banko autentifikavimo puslapį, kuris imituoja oficialią banko svetainę ir naudoja jos logotipą bei dizainą, todėl suvedate internetinės bankininkystės duomenis, kad atliktumėte mokėjimą.

Sukčiai naudoja DI, kad sukurtų labai įtikinamas netikras bankų svetaines, užsakymų patvirtinimus ir sąskaitas. DI padeda imituoti tikrų įmonių toną, ženklodarą ir stilių. Kai kuriais atvejais naudojami DI pokalbių robotai klausimams atsakyti, kad sandoris atrodytų patikimesnis.

Kas gali atsitikti:

Mokėjimas per trečiosios šalies nuorodą apeina prekyvietės apsaugas. Sukčius gauna jūsų prisijungimo prie banko duomenis ir pavagia pinigus.