

Nors lietuviai finansiniams sukčiams dažniausiai pasiekiami telefonu, apgaulės sparčiai keliai ir į socialines medijas – sukūrę netikras paskyras sukčiai apsimeta prekių ženklais, darbdaviais, pirkėjais, mylimaisiais. Kodėl apgaule patikime, kokios populiariausios jos rūšys ir kaip apsisaugoti nuo sukčių internete, komentuoja „Luminor“ banko Sukčiavimo rizikos valdymo skyriaus vadovas Linas Sadeckas.

Pagrindinis finansinių apgavysčių tikslas – gauti asmens pinigus. Socialinių tinklų atveju tai prilygsta vartotojo paskyros duomenų gavimui. Įgyvendinę šią užduotį sukčiai lengvai pasieks ir visą kitą reikalingą informaciją – nuo kontaktų, adresų iki banko sąskaitos duomenų.

„Gauti vartotojo asmeninius duomenis ir išvilioti jo pinigus socialiniuose tinkluose yra įvairiausių būdų. Pavyzdžiui, „Facebook“ tinkle ypač dažnai susiduriame su netikrais konkursais ir darbo pasiūlymais, reikalaujančiais veikti kaip tarpininkams ir pervesti iš kitų asmenų gautas sumas, rečiau – draugų atsiųstais apgaulingais vaizdo įrašais, kuriuos atidarius gavėjo informacija iš karto nuteka trečiosioms šalims“, – pasakoja L. Sadeckas.

Jis pratešia, kad „Facebook“ pasitaiko ir žaidybinės formos klausimynų, skirtų išsiaiškinti daugiau bendro pobūdžio informacijos apie vartotoją, jo pomėgius, interesus, ir vėliau jais manipuluoti susirašinėjant. Taip pat dažnai gyventojai susiduria su apsišaukėliais produktų pardavėjais ir pirkėjais. Tai yra, žmonėmis, parduodančiais netikrus produktus socialinėse medijose neadekvačiai žemomis kainomis, bei asmenimis, kurie nusipirkę prekę internetu tvirtina niekada jos negavę.

„Instagram“ – siūlymai bendradarbiauti

„Instagram“ platformoje, be jau minėtų apgavysčių, klesti nuomonės formuotojais bei prekių ženklais apsimetantys bendradarbiavimą siūlantys asmenys.

„Dažniausiai su vartotoju sukčiai susisiečia naudodami asmeninių žinučių funkciją ir prisistato susidomėjusia įmone, pagiria paskyrą ir pasiūlo bendradarbiavimą. Atidžiau panagrinėjus tokius pasiūlymus galima pastebėti, kad žmogus skatinamas susisiekti su įmone pats, siunčiant pranešimą į kitą paskyrą. Būtina prisiminti, kad bet kokia bendradarbiavimą siūlanti organizacija niekada nesikreips į vartotoją per trečiuosius asmenis, tai greičiausiai padarys elektroniniu paštu ar kitomis jūsų nurodytomis susisiektimo priemonėmis“, – atkreipia dėmesį L. Sadeckas.

Daugėja investavimo ekspertų

Vartotojų pranešimai ir interesai socialinėse medijose dažnai vienaip ar kitaip yra viešai prieinama informacija, kuria gali pasinaudoti ir sukčiai. Kylančios Lietuvos gyventojų susidomėjimu investavimu, natūraliai auga ir investavimo sukčių verslas socialiniuose tinkluose. Su šia sukčiavimo rūšimi yra susidūręs net ketvirtadalis Lietuvos gyventojų, rodo 2023 m. rugpjūčio ir rugsėjo mėnesiais „Luminor“ banko užsakymu atliktas tyrimas.

„Internetine žinute susisiekę su atsitiktiniu žmogumi investiciniai brokeriai rodo dėmesį, pasistengia sužavėti neva dideliu pelnu, kuria ryšį, artumo ir bendrystės jausmą. Susirašinėjimas socialiniame tinkle tęsiamas kurį laiką, kol galiausiai sukčiai pasidalina neva išskirtine galimybe investuoti. Investuojantiems į kriptovaliutas sukčiai prisistato šio investavimo būdo ekspertais ir savo aukoms žada padėti greitai ir sėkmingai praturtėti. Pasitaiko ir priešingų taktikų, kuomet ryšys nėra kuriamas, o vartotojas yra skubinamas atlikti veiksmus kuo greičiau tam, kad nespėtų niekam pranešti“, – pasakoja L. Sadeckas.

Asmeniui susidomėjus, prasideda dar gilesnis susirašinėjimas, apgavikai papasakoja apie tolesnį procesą, konsultuoja, galiausiai paprašo atlikti mokėjimą, vėliau siūlo investuoti dar daugiau ir galiausiai pradingsta.

„Jeigu kas nors atrodo pernelyg gerai, kad būtų tiesa, greičiausiai taip ir yra – venkite įsivelti į tokias istorijas. Jei reikalaujama gautą informaciją slėpti nuo kitų, į atsiųstą pasiūlymą reaguoti greitai, tikėtina, kad jus kalbina sukčiai, siekiantys, kad taip pat greitai iš banko sąskaitos dingtų ir jūsų pinigai“, – sako L. Sadeckas.

„Luminor“ banko ekspertas pataria, kad norėdami išvengti investicinių apgaulių, prieš perduodami pinigus ar investuodami, visada pasikonsultuotumėte su pažįstamais žmonėmis arba savo banko finansininku. Jei įtariate, kad pakliuvote į sukčių pinkles, nedelsdami kreipkitės į savo mokėjimo paslaugų tiekėją bei informuokite Lietuvos policiją.

Viena populiariausių formų - romantinės apgavystės

Dar viena itin dažnai socialiniuose tinkluose pasitaikanti apgaulės forma - romantinis sukčiavimas. Su šiomis pinklėmis yra susidūręs kas dešimtas Lietuvos gyventojas, rodo „Luminor“ banko užsakymu atliktas tyrimas.

Romantinių apgavysčių mastas išaugo pasaulį užklupus pandemijai, kai visas bendravimas persikėlė į nuotolinę erdvę. Santykių sukčiai užmezga su pažeidžiamu ir vienišu romantinių pažinčių socialinių tinklų, „Instagram“ ar „Facebook“ naudotoju. Netrukus ima kalbėtis apie ateitį, šeimą, domėtis žmogaus svajonėmis.

„Žmogui vis labiau atsiveriant, ryšys stiprėja, išauga pasitikėjimas, netrukus nusikaltėliai tuo pasinaudoja – ima prašyti nedidelių paslaugų, o galiausiai ir pinigų. Sukčiai labai dažnai pasitelkia prieštarinę informaciją, pavyzdžiui, teigia užimantys aukštas pareigas, bet paprašo pervesti pinigų sergantiems giminaičiams – taip sukliamas gailestis ir auka pakliūva į spąstus“, – pasakoja L. Sadeckas.

Vienas iš užsienio sukčių Lietuvoje naudotų scenarijų – apsimesti JAV karininku, baigiančiu tarnauti specialiojoje misijoje Azijoje ar Afrikoje ir neva tuoj turinčiu grįžti iš tarnybos. Bendravimas greitai tapdavo romantinis ir apsimetėlis imdavo prašyti pagalbos tvarkant muito mokesčius už daiktų, svarbių dokumentų ar dovanų siuntimą. Lietuvoje taip pat žinoma ir atvejų, kai pinigus iš merginų viliojo vaikinai, apsimitę žinomu šalies krepšininku.

Svarbiausia - nuolat atnaujinti žinias

Nuo internetinių apgavysčių apsisaugoti galima, tereikia elgtis atsargiai, domėtis sukčių taikomomis technikomis, nuolat atnaujinti savo žinias ir neatsilikti nuo įvykių, teigia L. Sadeckas.

„Svarbu kritiškai žvelgti į kiekvieną asmeninę žinutę atsiuntusį nepažįstamąjį ir pastebėti, kai santykiai vystosi įtartinais per greitai, imama spausti atlikti tam tikrus veiksmus, skubinama. Niekada nepervedinėkite pinigų žmogui, kurio nesate sutikę gyvai. Jei tai įmonė, įsitikinkite jos tikrumu – pasidomėkite internete galimais apgaulės atvejais paieškos lauke įvedę įmonės pavadinimą ir pridėję žodį „scam“ (liet. – „apgaulė“), – pastebi L. Sadeckas.

Jis prideda, kad asmens duomenys yra interneto ir socialinių tinklų valiuta, kurią labai dažnai trokšta pasisavinti sukčiai. Svarbu atminti, kad socialiniai tinklai neprivalo iki smulkmenų žinoti, kas jūs esate. Kuriant naują paskyrą pakanka užpildyti būtiniausius, privalomais pažymėtus laukelius. Asmeninio gyvenimo detales geriau palikti paslapyje – kraštutiniais atvejais jos gali tapti šantažavimo pagrindu. Svarbiausia išlaikyti budrumą ir akylumą informacijai, kuria dalinamės, pataria „Luminor“ ekspertas.

