Sukčiai kiekvieną dieną ieško naujų apgaulės būdų ir aukų, kurios neįžvelgtų klastos. Ir jeigu prieš 10-15 metų pasipelnyti buvo bandoma telefoninių skambučių pagalba, dabar pastebima, jog apgaulės vis dažniau keliasi į internetinę erdvę.

Anot Kauno apskrities vyriausiojo policijos komisariato (toliau – Kauno APVK) Komunikacijos skyriaus vedėjos Odetos Vaitkevičienės, Kauno apskrities vyriausiame policijos komisariate per pirmąjį 2022-ųjų ketvirtį pradėti 5 ikiteisminiai tyrimai dėl kibernetinio sukčiavimo. Pašnekovės teigiamu, pinigų išviliojimo schemos nuolat keičiasi, taip pat modifikuojamos jau išbandytos, todėl negalima įvardinti vieno ar kelių dažniausiai pasitaikančių kibernetinių apgaulių būdų.

„Esminis apgaulės elektroninėje erdvėje pagrindas remiasi socialine inžinerija, kuomet asmuo apgaule įtikinamas greitai atlikti tam tikrus, iš pirmo žvilgsnio nekaltus, veiksmus. Kai atsiduriama sukčiavimo pinklėse, sekantys aukos veiksmai sudaro prielaidas žalai atsirasti – t. y. prisijungimo duomenų atskleidimas, mokėjimo instrumentų duomenų pateikimas, finansinės operacijos patvirtinimas elektroninėmis identifikavimo priemonėmis“, – teigia O. Vaitkevičienė.

Pasiteiravus pašnekovės, ar aferistai yra labiau linkę kurtis fiktyviais el. svetaines ar visgi bando apgauti soc. tinkluose, galime teigti, kad, siekiant didesnės žalos nukentėjusiam padarymo, sukčiai atitinkamai investuoja į nusikaltimo priemones. Norint išvilioti didesnę sumą pinigų kuriamos sudėtingos svetainės ir jas palaikantys šaltiniai, naudojamos skambučius atliekančios VOIP (internetinė telefonija, kai balso ryšys perduodamas naudojant interneto protokolą) paslaugos. Tiesa, greitai, smulkiai apgaulei dažniau naudojamos netikros socialinės paskyros.

Sukčiavimo būdų gausa

Kaip teigia O. Vaitkevičienė, kibernetiniai sukčiavimai pasižymi įvairove, tad niekuomet negali žinoti, ko tikėtis. „Pastaruoju metu dažnai registruoti įvykiai, kuomet gaunami SMS pranešimai apie blokuotas sąskaitas su imituojančiomis banką nuorodomis, skatinančiomis prisijungti prie el. bankininkystės ir suvesti mokėjimo kortelės ar banko sąskaitos prisijungimo duomenis. Taip pat nemažėja sukčiavimų, kuomet kompromituojamas įmonių vadovų elektroninis susirašinėjimas, įmonės direktoriaus vardu siunčiant laiškus finansininkui ir prašant skubiai pervesti pinigus į užsienio sąskaitas pagal išgalvotą sutartį ar klastotą sąskaitą faktūrą. Pastaraisiais metais taip pat labai paplito investiciniai sukčiavimai, kuomet nukentėję asmenys, sekdami tariamai investicinių svetainių kūrėjų nurodymus, perka kriptovaliutas ir jas perveda į nežinomų asmenų sąskaitas, mato fiktyviose svetainėse kylančius skaičius, o ketindami atsiimti pinigus jų negauna.“

Vienas iš pašnekovės minimų sukčiavimo būdų – imituojami prekių pirkimai pagal skelbimų portaluose nurodytus pardavėjų duomenis siunčiant pranešimu informaciją, kad už prekę sumokėta vežėjui, o pardavėjui reikia registruotis siuntos tarnyboje nurodant mokėjimo kortelės duomenis su CCV kodu. Su tokia sukčiavimo schema susidūrė ir siuntų gabenimo platforma „Siųsk pigiau“ – pinigų išviliojimui sukurta svetainė priminė minėtąją platformą.

„Radus skelbimą, sukčiai susisiekia su pardavėju ir pradeda klausinėti apie parduodamą prekę. Kai jau sutariama dėl pirkimo, pardavėjui atsiunčiama nuoroda su nukreipimu į fiktyvų puslapį, kuris vizualizacijomis bei stiliumi primena „Siųsk pigiau“ svetainę. Tariamas pirkėjas parašo, jog laukia savo užsakymo patvirtinimo. Pateikiama sekimo informacija neva skelbia, kad tolimesniam užsakymo vykdymui reikalinga priimti siunčiamus pinigus. Tam įgyvendinti svetainėje būna mygtukas „Gaukite lėšas“, o jį paspaudus prašoma pateikti kortelės duomenis. Po jų pateikimo ir atsiskleidžia klasta: pinigų, deja, negaunama – jie nuskaitomi nuo pardavėjo sąskaitos“, – apie schemą pasakoja „Siųsk pigiau“ vadovas Mindaugas Šilkūnas.

Apie sukčiavimo atvejus, kai pinigų išviliojimui pasitelkiama „Siųsk pigiau“ svetainės kopija, pašnekovas teigia sužinojęs iš nukentėjusiųjų, šiems kreipusis dėl pinigų nuskaitymo. „Visais atvejais stengiamės kuo operatyviau atsakyti į užklausas ir paaiškinę visą schemą, patariame nedelsiant kreiptis į teisėsaugą.“

Netikras svetaines išduoda smulkūs niuansai

Apsidžiaugus potencialiu pardavimu ir gavus nuorodą, kurioje prašoma pateikti kortelės duomenis, kad neva gautumėte pinigus už prekę, nereikėtų pamesti racionalumo. Anot Kauno AVPK pareigūnų, internetinėje erdvėje visuomet derėtų būti šiek tiek įtariu. Visų pirma, rekomenduojama neatidaryti nepatikimų nuorodų, o jeigu visgi ši yra atidaroma – dairytis apgaulę galinčių atskleisti ženklų.

„Pagrindiniai melagingos svetainės požymiai – domeno (kitaip – svetainės vardo) įgijimo, interneto svetainės startavimo data. Šios dažniausiai būna registruotos kelios dienos ar savaitės prieš veiklą. Taip pat įtartinas SSL sertifikato nenaudojimas – visos saugios svetainės naršyklėje būna pažymėtos spynos prie adreso ikona. Galiausiai, išdaviku gali būti ir klaidinantis svetainės adresas pvz. seb-bankas.com vietoje seb.lt,“ – pasakoja O. Vaitkevičienė.

Jei kalbama apie elektroninės prekybos svetaines, įtarimus, anot pareigūnų, turėtų kelti viešos informacijos internete apie svetainę ar nurodytą įmonę nebuvimas, mažos kainos, didelės nuolaidos ir raginimas įsigyti paskutines prekes.

Dalijasi patarimais, ką daryti nukentėjus

Kilus įtarimui, jog tapote kibernetinių sukčių auka, O. Vaitkevičienė pirmiausia rekomenduoja kreiptis į savo banką, atšaukiant mokėjimus. „Jei tai padaroma greitai, ženkliai padidėja tikimybė lėšas įšaldyti. Jei buvo panaudoti kortelės duomenys, reikia nedelsiant kortelę blokuoti arba išjungti atsiskaitymus internetu, jei tokią galimybę numato bankas.“

Pašnekovė prideda, jog visais atvejais reikia informuoti policijos pareigūnus skubios pagalbos telefonu 112 ar pasinaudojant policijos elektroninių paslaugų sistema www.epolicija.lt bei stengtis išsaugoti kaip galima daugiau įrodymų: susirašinėjimus, svetainės atvaizdus (ar nuotraukas), naudotus kontaktus ir t.t.