2023 m. lapkričio 7 d.

PRANEŠIMAS ŽINIASKLAIDAI

**Aktyvėjant finansiniams sukčiams, ekspertas atkreipia dėmesį į pagrindinius jų manipuliacijų metodus**

**Bankams ir teisėsaugai pavyksta sulaikyti vis didesnę dalį finansinių sukčių ir jų mėgintas išvilioti lėšas sugrąžinti gyventojams, tačiau nusikaltėlių aktyvumas nepaliauja augti. Trečiąjį šių metų ketvirtį kibernetiniai nusikaltėliai išviliojo 5,1 mln. eurų – tai 21 proc. daugiau nei praėjusį ketvirtį, rodo Pinigų plovimo prevencijos kompetencijų centro duomenys. Šaltuoju sezonu dar labiau aktyvėjant kibernetinėms atakoms, „Citadele“ banko ekspertas atskleidžia pagrindinius finansinių sukčių bruožus ir manipuliacijų metodus, kuriuos verta išmokti atpažinti.**

„Atėjus šaltajam sezonui ir prasidėjus mokslo metams sukčiai vėl darosi aktyvesni. Natūralu – daugiau laiko būname namuose, naršome internete, mokiniai ir studentai praleidžia daugiau laiko prie ekranų mokslo ir laisvalaikio tikslais. Nusikaltėliams atsiveria daugiau galimybių visus pasiekti, tad vertėtų įsiminti esminius sukčių bruožus, kuriuos atpažinę galėsite apsaugoti savo finansus“, – sako „Citadele“ banko Baltijos šalių lėšų valdymo ir prekybos finansavimo tarnybos vadovas Romas Čereška.

**Bando įtikinti, kad įvyko kažkas blogo**

Siekdami atkreipti dėmesį, kibernetiniai nusikaltėliai dažnai bando priversti žmogų sunerimti. Pavyzdžiui, sukčiai gali siųsti netikrus el. laiškus ar žinutes, kuriais įspėja apie užblokuotus mokėjimus ar banko sąskaitas, nepristatytą pašto siuntą, neteisingai nurodytą pristatymo adresą, nesumokėtus mokesčius ar net teismo šaukimus.

Pirmiausia pamąstykite kritiškai – pavyzdžiui, ar tikrai užsisakinėjote prekes internetu ir laukėte jų pristatymo? Jei esate gąsdinami užblokuota banko sąskaita, nespauskite ant pranešime nurodytos nuorodos. Įsitikinti, kokia situacija yra iš tiesų, galite tiesiogiai prisijungę prie el. bankininkystės ar paskambinę į banką. Taip pat atidžiai perskaitykite pranešimo tekstą – dažnai bandymą sukčiauti galima atpažinti pagal tekste esančias gramatines klaidas.

**Sukčius išduoda skubinimas**

Žmogaus protas linkęs susipainioti situacijose, kai reikia greito sprendimo. Todėl bandydami išvilioti pinigus, sukčiai skambina ar siunčia SMS pranešimus, raginančius nedelsiant atlikti tam tikrą veiksmą. Apimti emocijų žmonės neretai nesupratę, kodėl iš jų prašoma tam tikrų duomenų, pateikia savo asmeninę informaciją.

Tokiu būdu nusikaltėliai pasisavina duomenis, kad prisijungtų prie asmens banko sąskaitos ar tapatybės patvirtinimo įrenginių ir naudojasi jais kito žmogaus vardu, tvirtindami pirkinių įsigijimą, imdami greituosius vartojimo kreditus.

Todėl, jei pastebite, kad esate raginamas kuo skubiau pervesti pinigų sumą ar įvesti banko duomenis be jokio papildomo paaiškinimo, tikėtina, kad papuolėte į finansinių sukčių rankas. Tokiu atveju ignoruokite ir ištrinkite gautus pranešimus. Apie juos galite pranešti savo bankui.

**Dalina pernelyg gerus pažadus**

Dar viena sukčių taktika – pradžiuginti ir sukelti žmogui viltį. Tikriausiai nemaža dalis žmonių yra gavę žinutę su sveikinimu, kad laimėjo naujausią telefoną ar automobilį. Norint atsiimti prizą, žmogus raginimas paspausti ant nuorodos arba suvesti savo banko duomenis. Nemažai patikinčių ar besiviliančių, kad tai tiesa, pasiduoda apgavikų nurodymams.

Taip pat niekada nereikėtų priimti pasiūlymų užsidirbti internetu, kur žadamas neįtikėtino dydžio pelnas, pavyzdžiui, tiesiog pervedant iš savo sąskaitos neaiškios kilmės pinigus kitur ir už tai gaunant dalį sumos. Dėl to gali kilti ne tik finansinių bėdų, bet ir gali grėsti baudžiamoji atsakomybė už pinigų plovimą – tokie veiksmai yra neteisėti ir baudžiami.

**Bando apsimesti kitais**

Sukčiai dažnai bando apsimesti tam tikra įmone ar institucija, atsiųsdami el. laiškus, tačiau bandoma prieiti prie žmogaus, sukeliant kuo mažiau įtarimo. Pavyzdžiui, rūbų mainų programėlėse, daiktų ar naudotų automobilių skelbimų portaluose, sukčiai neretai apsimeta norintys įsigyti prekę. Iš pirmo žvilgsnio gali nepasirodyti nieko įtartino – žmogus teiraujamasi apie prekę, paprašoma el. pašto, kuriuo galėtų atsiųsti savo adresą.

Tačiau juo pasidalinus, sukčiai į el. paštą atsiunčia ne savo adresą, o netikrą, tarsi nuo programėlės ar portalo gautą laišką, kuriame pranešama, kad prekė nupirkta, o jums reikia paspausti nuorodą ir patvirtinti savo el. bankininkystę.

Reikėtų pagalvoti, ar įprastas pirkimo – pardavimo procesas programėlėje tikrai toks? Jei nesate tikras, reikėtų atidžiai patikrinti el. pašto adresą ir siuntėją. Sukčiai sukuria tokį el. pašto adresą, kuris atrodo kaip tikras, tačiau jame trūksta raidės arba panaudoti kiti simboliai. Interneto paieškos sistemoje įvedus el. pašto adresą galima patikrinti, ar jis sutampa su siuntėju.

**Papildoma informacija:**

Aurelija Grikinaitė-Čepėnienė

Korporatyvinės komunikacijos vadovė Lietuvoje

„Citadele“ bankas

aurelija.grikinaite-cepeniene@citadele.lt

[www.citadele.lt](http://www.citadele.lt)