**Pranešimas žiniasklaidai**

2024 m. rugpjūčio 12 d.

**Pastebėjote, jog sukčiai turi jūsų telefono numerį ar el. paštą? Štai, ką turėtumėte padaryti nedelsiant**

**Internete plintančios apgaulės, kuriomis siekiama išvilioti pinigus ar gauti prieigą prie jautrių vartotojų duomenų, kasdien pasiekia vis daugiau žmonių. Dauguma vartotojų jau sėkmingai atpažįsta sukčių mėginimus pasipelnyti, tačiau kartais sukčiams pakanka išgauti tik tokius duomenis, kaip el. paštas ar telefono numeris, kad jie pasiektų savo tikslą. Ekspertas atskleidžia, kaip asmeninė informacija patenka į sukčių rankas bei pataria, kokių priemonių imtis, kad jūsų duomenys netaptų įrankiu internetinėms apgaulėms įgyvendinti.**

**El. paštas – kelias jautrios informacijos link**

Elektroninio pašto adresas naudojamas ne tik bendravimui el. laiškais, tačiau dažnai yra susiejamas ir su kitomis paskyromis bei paslaugomis. Todėl pastaraisiais metais vis dažniau susiduriama su masinio duomenų nutekinimo atvejais. Sukčiai įsilaužę į el. parduotuves ar paslaugų platformas, kuriose esate užsiregistravę, gauna prieigą prie tokių vartotojų asmeninių duomenų, kaip vardas, gyvenamosios vietos adresas, el. pašto adresas ar telefono numeris.

Pasak „Citadele“ banko Baltijos šalių lėšų valdymo ir prekybos finansavimo tarnybos vadovo Romo Čereškos, internetiniams sukčiams sužinojus jūsų el. pašto adresą, gali kilti pavojus jūsų ir jūsų draugų, šeimos narių, ar kitų kontaktų asmeninei informacijai. Tai, kaip lengvai sukčiai, turėdami jūsų el. pašto adresą, gali pasiekti ir kitus jautrius duomenis, priklauso nuo kelių veiksnių.

„Prieinamumą prie kitos jūsų asmeninės informacijos iš esmės nulemia tai, kiek laiko turite savo el. pašto adresą, kaip dažnai juo dalijatės ir prie kiek skirtingų svetainių prisijungiant naudojate tą patį adresą. Kuo ilgiau ir plačiau yra naudojamas el. pašto adresas, tuo lengviau sukčiams išgauti kitą jautrią informaciją – programišiai gali sužinoti, kur atliekate bankininkystės operacijas, kokias turite socialinės medijos, el. prekybos paskyras. O įvykus duomenų nutekėjimui – ir gauti prieigą prie jose patalpintos asmeninės informacijos“, – teigia R. Čereška.

Be to, jei sukčiai žino jūsų elektroninio pašto adresą, jie gali užsiimti internetinėje erdvėje kone labiausiai paplitusia sukčiavimo forma – siųsti apgaulingus el. laiškus. Jei nebūsite budrūs, galite suteikti įsilaužėliams papildomos informacijos, kuri padės jiems padaryti dar daugiau žalos.

**Telefono numeris jau sukčių rankose – ar reikėtų sunerimti?**

Daugelis nesijaudina dėl galimo sukčiavimo, kai savo mobiliojo telefono numerį pateikia apsiperkant internetu ar pridedant jį prie įvairių internetinių paskyrų. Gali net atrodyti visiškai natūralu ir reikalinga nurodyti savo telefono numerį „Facebook“, „LinkedIn“ paskyrose ar internetinėse prekyvietėse esančiuose skelbimuose.

Apgavikai, R. Čereškos teigimu, gavę jūsų telefono numerį gali kėsintis pavogti asmeninę informaciją ir nulaužti įvairių paskyrų slaptažodžius bei į jūsų telefoną ir kitus mobiliuosius įrenginius bandyti įdiegti kenkėjiškas ar šnipinėjimo programas. Tiesa, tam padaryti vien telefono numerio neužtenka.

„Jūsų telefono numeriui pakliuvus sukčiams į rankas, jis gali tapti priemone vykdyti neteisėtus veiksmus. Gali pasipilti skambučiai ir žinutės su įvairiausiais triukais ir melagystėmis, siekiant pasipelnyti jūsų asmeninių lėšų sąskaita. Tačiau jei tokiose situacijose neprarasite kritinio mąstymo ir neatliksite papildomų veiksmų – jūsų duomenims papildoma rizika nekils“, – dalijasi ekspertas.

**Apgavystės tampa įmantresnės, tačiau apsisaugoti – nesudėtinga**

Būdų, kaip sukčiai siekia išvilioti pinigus, yra pačių įvairiausių – jie gali apsimesti valstybinėmis įstaigomis, skelbti apie laimėjimą loterijoje ar informuoti apie artimuosius, neva pakliuvusius į nelaimingą atsitikimą.

R. Čereška pastebi, jog apgaulingi el. laiškai ar pranešimai pastaruoju metu gali atrodyti itin tikroviškai ir sudaryti įspūdį, jog yra siunčiami iš patikimų tarptautinių bendrovių. 2024 m. ypač dažnai fiksuojami sukčiavimo atvejai apsimetant tokių korporacijų, kaip „Facebook“, „Netflix“, „Microsoft“ ar „Apple“ atstovais.

„Būkite atidūs – visad patikrinkite, iš kokio adreso siunčiami laiškai bei ieškokite kitų apgaulingų laiškų identifikavimo ženklų – gramatinių klaidų, netaisyklingos kalbos, ar prašymų skubiai atidaryti nuorodas ir pateikti asmeninius duomenis. Atminkite, kad internetiniai sukčiai dažnai siunčia didelę emociją sukeliančias ir greitos reakcijos reikalaujančias žinutes“, – pataria jis.

Taip pat, anot eksperto, pastebėjus, jog sukčių rankose jau atsidūrė pirminė jūsų kontaktinė informacija, verta pasirūpinti papildomą saugumą suteikiančiomis priemonėmis. R. Čereška rekomenduoja nustatyti dviejų faktorių autentifikavimą, apriboti savo kortelių atsiskaitymo geografiją, nustatyti kortelių limitus, kurie papuolus į sukčių akiratį padėtų išvengti nuostolių, net jei sukčiai sugebėtų įtikinti savo melagystėmis.

„Būtinai naudokite ir stiprius, unikalius slaptažodžius. Jei keliose svetainėse naudojate tą patį slaptažodį, įsilaužėliams prireiks daug mažiau pastangų, kad galėtų pasiekti jūsų paskyras“, – teigia R. Čereška.