**Pranešimas žiniasklaidai**

2024 m. birželio 12 d.

**Gudriausi sukčių metodai stebina: įkliūva net atsargiausi**

**Finansinių nusikaltėlių atakų aktyvumui nemažėjant, jų metodai tampa vis išradingesni ir sunkiai atpažįstami net patiems kritiškiausiems. Pasak „Citadele“ banko Baltijos šalių lėšų valdymo ir prekybos finansavimo tarnybos vadovo Romo Čereškos, vasarą gyventojai dar labiau atsipalaiduoja, todėl sukčiams, besinaudojantiems tam tikrais metodais, gyventojai neretai tampa lengvu grobiu. Banko ekspertas atskleidė šiuo metu populiariausias gudrybes, kuriomis sukčiai sėkmingai išvilioja pinigus.**

**Patikimumą pelno patys pervesdami pinigų**

Kone sunkiausiai atpažįstamos tokios sukčių atakos, kuriomis sukčiai pirmiausia vartotojui įrodo, kad pasiūlymai nėra melagingi, ir taip pelno žmonių pasitikėjimą.

„Šiuo metu aktyviai plinta investicinis sukčiavimas – nusikaltėliai pasiūlo vartotojui investuoti ir uždirbti didelę grąžą, kuri pradžioje skamba neįtikėtinai. Norėdami įgyti žmogaus pasitikėjimą, sukčiai iš pradžių paragina pervesti nedidelę sumą pinigų ir patiems įsitikinti pelno augimu. Jį pamatę žmonės perveda didesnę sumą, o sukčiai vėliau dingsta“, – komentuoja Romas Čereška.

Uždirbti sukčiai siūlo ne tik investuojant, bet ir naudojantis papildomo darbo galimybėmis. Paskutiniu metu plinta žinutės su pasiūlymu per dieną užsidirbti nuo 5 iki 250 eurų „Youtube“ platformoje, spaudžiant „patiktukus“ ant tam tikrų vaizdo įrašų. Tai padarius, sukčiai iš tikrųjų perveda 5 eurus, vėliau 10 eurų, sukurdami patikimą įvaizdį. Tačiau norint uždirbti didesnes pinigų sumas, pasiūloma įsigyti 500 eurų kainuojančius kursus. Susigundę lengvu uždarbiu, vartotojai perveda pinigus, gauna kursų medžiagą, tačiau jokio žadėto uždarbio.

„Atpažinti pinkles, kai iš pradžių pačiam vartotojui yra pervedami pinigai, sudėtinga. Tačiau reikia išlikti budriems ir nepamiršti, kad bet kokiems darbo santykiams ar investavimo sandoriams reikalinga sutartis. Jei jos nėra, pasiūlymas iškart turėtų kelti įtarimų“, – sako banko atstovas.

Pasak pašnekovo, galimybė susigrąžinti sukčiams pervestus pinigus išlieka, tačiau proceso sėkmė priklauso nuo to, kokiu būdu iš sąskaitos buvo išsiųsti pinigai. „Atliekant mokėjimą kortele, susigrąžinti lėšas lengviau, nes pinigai iškart nepasiekia gavėjo, jie yra rezervuojami. Sudėtingiau atliekant pavedimą, ypač, jei lėšos jau pateko į sukčių rankas“, – teigia R. Čereška.

**Pasinaudoja net komunalinių paslaugų remonto darbais**

Tai, kad sukčiai siunčia melagingus laiškus ar SMS žinutes, apsimesdami valstybinėmis, paslaugų įmonėmis, ir ragina sumokėti pradelstas įmokas už elektrą, vandenį ar kitus mokesčius, daugumai nebėra naujiena. Tačiau nusikaltėliai šį metodą įsigudrino paversti dar labiau įtikinamu.

Pasižiūrėję oficialių valstybinių įstaigų svetaines, kuriose galima pasitikrinti, kada tam tikriems rajonams ar daugiabučiams dėl šilumos tinklų remonto bus atjungtas karštas vanduo, sukčiai nusitaiko į konkrečių namų gyventojus. Rajono ar daugiabučių „Facebook“ grupėse susiradę jose prisijungusius vartotojus, jiems išsiuntinėja pranešimus su nuorodomis į apmokėjimą ir informacija, kad dėl pradelsto mokėjimo, gyventojui atjungiamas karštas vanduo.

Nežinodami apie remonto darbus ir dėl to atjungtą karštą vandenį, kai kurie gyventojai gavę tokį pranešimą tampa lengviau įtikinami, kad iš tiesų pradelsė apmokėti sąskaitą. Tačiau „Citadele“ banko ekspertas patikina, kad nei bankai, nei valstybinės įstaigos niekada nesiunčia pranešimų su nuorodomis. Todėl gavus tokį pranešimą, tai turėtų būti pirmas faktorius, leidžiantis identifikuoti melagingą informaciją.

„Sukčiai visada bando sukelti skubos jausmą, kad reikia atlikti veiksmą greitai. Tačiau kilus įtarimui, jokiu būdu nespauskite ant nuorodos, prisijunkite prie banko ar kitos įstaigos svetainės tiesiogiai ir įsitikinkite, ar iš tikrųjų gavote tokį pranešimą“, – pataria R. Čereška.

Net ir nedarant to, ko prašo nusikaltėliai, pasak pašnekovo, reikėtų pranešti įstaigai, kuria apsimetinėjama, ir policijai, siekiant užkirsti kelią tolimesniems atvejams. „Galbūt nuo to paties sukčiaus nukentėjo ne vienas žmogus, o pranešdami prisidėsite prie jo sugavimo. Pilietiška pranešti ne tik kai pakliūvame patys, bet ir kai matome, kad galima pakliūti kitiems“, – pataria banko atstovas.

**Apsimeta klientų aptarnavimo specialistais**

Pasak R. Čereškos, vartotojams besiregistruojantiems prie naujų svetainių ar programėlių, svarbu turėti omenyje tai, kad kibernetiniai nusikaltėliai nepraleidžia progos nusitaikyti į naujai prisijungusius vartotojus.

Pavyzdžiui, susikūrus pardavėjo paskyrą rūbų mainų programėlėje ir patalpinus skelbimą, sukčiai, apsimesdami oficialiais programėlės klientų aptarnavimo specialistais, gali atsiųsti pranešimą, raginantį patvirtinti tapatybę. Tai padaryti prašoma, paspaudžiant ant nuorodos, su tikslu, kad įdėtas skelbimas būtų iškeltas aukščiau. Tačiau ir vėl reikėtų prisiminti, kad laiškus su nuorodomis siuntinėja dažniausiai sukčiai.

„Kai kurie vartotojai supranta, kad yra apgaudinėjami tik paspaudę ant nuorodos ir tolimesnių veiksmų nebeatlieka, tačiau tai nereiškia, kad nieko neatsitiks. Sukčiai gali instaliuoti kenkėjiškas programėles, todėl tokius atvejus reikia pranešti oficialiam klientų aptarnavimo skyriui“, – teigia R. Čereška.

Taip pat, anot eksperto, verta pasirūpinti papildomą saugumą suteikiančiomis priemonėmis – nustatyti banko 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.