

Finansiniai sukčiai iš gyventojų ir verslo pernai išviliojo 10,2 mln. eurų

Finansiniai sukčiai iš Lietuvos gyventojų ir įmonių pernai išviliojo 10,2 milijono eurų - dukart daugiau nei 2020-aisiais, kai nuostoliai sudarė 4,8 milijono eurų, rodo Lietuvos bankų asociacijos (LBA) duomenys. Pustrečio karto išaugo sukčiavimo atvejų skaičius: labiausiai padaugėjo „fišingo“ (angl. phishing) ir telefoninio sukčiavimo. Specialistų vertinimu, nuostoliai būtų dar didesni, nesant finansų įstaigų bei institucijų taktinio bendradarbiavimo.

Praėjusiais metais LBA priklausantys finansų bei kredito rinkos dalyviai fiksavo 3511 sukčiavimo incidentų elektroninėje erdvėje, palyginti su 1336 incidentais 2020 metais. Net šešis kartus išaugo „fišingo“ (apgaulės būdo, kai sukčiai pateikia nuorodas į suklastotas internetines svetaines) incidentų skaičius - pernai fiksuota 914 „fišingo“ atvejų, dėl kurių gyventojai patyrė apie 0,8 mln. eurų nuostolių. Daugiau nei du kartus pagausėjo ir telefoninio sukčiavimo atvejų, dėl kurių patirta žala pernai sudarė apie 1,3 mln. eurų. Daugiausiai nuostolių pernai patirta dėl incidentų, kai sukčiai perima susirašinėjamą elektroniniu paštu - iš viso taip išviliota apie 2,7 mln. eurų.

„Tendencija aiški - sukčiai neketina trauktis iš Lietuvos elektroninės erdvės bei nuolat didina resursus, nukreiptus į atakų organizavimą. Tiek bankų fiksuotas sukčiavimo incidentų skaičius, tiek gyventojų ir verslo patirti nuostoliai pernai augo kartais ir tai rodo tik viena - turime būti dar kritiškesni informacijai, gaunamai nuotolinėmis ryšio priemonėmis - tai įgūdis, be kurio naudotis skaitmeninės erdvės pranašumais ateityje bus tiesiog neįmanoma“, - akcentavo LBA prezidentė dr. Eivilė Čipkutė.

Veikia taktinis bendradarbiavimas

Specialistai atkreipia dėmesį, kad finansinio sukčiavimo apimtys šiek tiek nuslūgo paskutinįjį 2021 metų ketvirtį - fiksuota apie 10 proc. mažiau sukčiavimo incidentų (1133 atvejų) ir apie 20 proc. mažesni finansiniai nuostoliai nei 2021 m. trečiąjį ketvirtį. Iš viso paskutinįjį 2021 m. ketvirtį finansiniai nusikaltėliai iš įmonių ir gyventojų išviliojo 2,3 mln. eurų, palyginti su 2,9 mln. eurų trečiąjį metų ketvirtį.

Sumažinti sukčių atakų mastą ir daromą žalą siekiama ne vien informacijos sklaida. Pernai gegužę veiklą pradėjęs Pinigų plovimo prevencijos kompetencijų centras, kurį kartu įsteigė Finansų ministerija, Lietuvos bankas ir 8 šalyje veikiančios komerciniai bankai, įsteigė taktinio bendradarbiavimo grupę. Joje dalyvaujantys finansų bei kredito įstaigų ir teisėsaugos specialistai keičiasi informacija dėl aktualios situacijos finansinių sukčiavimų ir jų prevencijos srityje.

Vasarą buvo padaugėję „fišingo“ atakų, nukreiptų į šalies piliečius, kai finansiniai sukčiai

Finansiniai sukčiai iš gyventojų ir verslo pernai išviliojo 10,2 mln.
eurų

apsimesdavo bankų darbuotojais ir, bendraudami su jų klientais rusų kalba, neteisėtai įsibraudavo į asmenines bankų sąskaitas bei pasisavindavo santaupas. Skaičiuojama, jog vien tik šios atakos metu finansiniams sukčiams iš gyventojų pavyko išvilioti apie 400 000 eurų. Fiksuojant augantį atvejų skaičių, taktinio bendradarbiavimo grupė koordinavo nuolatinį partnerių keitimąsi informacija ir prevencinių priemonių diegimą, o Lietuvos policijos įsitraukimo ir bendradarbiavimo dėka pavyko užkardyti tolesnes nusikalstamas veikas bei finansinius praradimus.

„Žinoma, šis pasiekimas – ne ilgalaikis rezultatas. Sukčiai greitai mokosi, tobulina savo nusikalstamų veikų schemas, atakos darosi vis sudėtingesnės, todėl skiriamas dėmesys pinigų plovimo rizikos atsparumo gerinimui privalo išlikti aktualus visuomet. Turime ir toliau ieškoti būdų ir bendrų bendradarbiavimo taškų tarp viešojo ir privataus sektorių atstovų tam, jog galėtume efektyviau kovoti su vis įmantresnėmis sukčiavimo schemomis, tik tokiu būdu galėsime dar labiau sumažinti išviliojamų pinigų sumas. Esame įsitikinę, kad naujosios Centro kuruojamos iniciatyvos ženkliai prisidės prie sukčiavimo prevencijos sistemos gerinimo“, – pabrėžia Eimantas Vytuvlis, Pinigų plovimo prevencijos kompetencijų centro vadovas.

Sukčių taikinyje - ir verslas

Paskutinįjį 2021 m. ketvirtį laikotarpiu daugiausiai fiksuota „fišingo“ ir kitokių (įvairių sukčiavimo būdų, kurių negalima priskirti vienai kategorijai) incidentų. Taip pat fiksuotas santykinai didelis incidentų, kai sukčiai apsimeta įmonių vadovais, skaičius – pasak specialistų, gyventojams tampant atidesniais ir vis dažniau atpažįstant populiariausius atakų būdus, nusikaltėliai daugiau dėmesio nukreipia į verslą ir naujus sukčiavimo metodus, apie kuriuos gyventojai dar nebūtų girdėję.

„Akivaizdu, kad sukčiai eksperimentuoja ir taiko vis platesnį spektrą sukčiavimo metodų – pastaruoju metu bankų klientai praneša apie suklastotas kurjerių tarnybų internetines svetaines, melagingas trumpąsias žinutes, kuriose pateikiamos nuorodos apie neva gautą siuntą ir pan. Galima sakyti, kad nusikaltėliai ieško individualaus priėjimo prie konkretaus asmens ir tai neramina, nes atpažinti suklastotą informaciją darosi vis sudėtingiau“, – teigė E. Čipkutė.

Daugiausiai nuostolių paskutinį 2021 metų ketvirtį patirta dėl investicinio sukčiavimo (0,82 mln. eurų) ir kitokių sukčiavimo metodų (0,56 mln. eurų).

Per 2021 m. paskutinį ketvirtį bankai klientams grąžino apie 13 proc. visų patirtų nuostolių – tokią dalį incidentų pavyko sustabdyti. Taip pat buvo sustabdytos įtartinos piniginės

Finansiniai sukčiai iš gyventojų ir verslo pernai išviliojo 10,2 mln. eurų

operacijos, kurių vertė siekė apie 1,1 mln. eurų – beveik 60 proc. daugiau nei trečiąjį metų ketvirtį. Sustabdyti ar sugrąžinti mokėjimo operacijas pavyksta tik išimtiniais atvejais, kai klientai apie sukčiavimo incidentą praneša nedelsiant.

Dažniausiai naudojami sukčiavimo metodai:

1. Suklastotas el. laiškas arba SMS žinutė - „fišingas“ (angl. phishing)

Sukčiai siunčia suklastotus elektroninius laiškus ar SMS žinutes, kurios atrodo panašios į jūsų banko ar kitų naudojamų paslaugų tiekėjų siunčiamą informaciją. Šiuo metodu siekiama iš jūsų išgauti internetinio banko prisijungimo duomenis, patvirtinti sukčių atliekamus pavedimus ir pan. Atidžiai vertinkite visą informaciją gautą nuotolinėmis ryšio priemonėmis: peržiūrėkite informacijos siuntėjo duomenis, bendrą el. laiško struktūrą. Lietuvoje veikiančios finansų ir kredito įstaigos niekada neprašys jūsų atskleisti prisijungimo prie banko sąskaitos duomenų ar atlikti mokėjimo pavedimą – jei sulaukėte tokio prašymo, jį ignoruokite.

2. Skambučiai, apsimetant banko ar kitos įstaigos darbuotoju

Sukčiai, prisistatantys jūsų banko arba valstybės institucijos atstovais, mėgina užmegzti kontaktą, kad priverstų jus pasidalinti savo asmenine, finansine arba prisijungimo informacija. Bendra rekomendacija – niekada nepasiduoti emocijoms ir neskubėti, neatsakyti į klausimus, jei nesate tikri su kuo kalbate.

3. Investicinis sukčiavimas

Įkyrūs skambučiai, laišakai, réksmingi skelbimai internete – viskas tam, kad priverstų patikėti, kad jums teikiamas labai patrauklus investavimo pasiūlymas arba proga įsigyti fantastišką prekę. Jeigu tai skamba per daug gerai, kad būtų tiesa – ko gero, tai ir yra apgaulė.

4. Susirašinėjimo elektroniniu paštu perėmimas

Sukčiai įsilaužia į elektroninį susirašinėjimą tarp dviejų šalių, pavyzdžiui, prekės pirkėjo ir jos pardavėjo, ir sulaukę patogaus momento informuoja mokėtoją apie pasikeitusią banko sąskaitą. Tam, kad nepakliūtumėte į tokias pinkles, rekomenduojama sulaukus panašaus el. laiško pirmiausiai tiesiogiai susiekti su prekės ar paslaugų tiekėju ir įsitikinti, kad informaciją gavote tikrai iš jo.

5. Sukčiavimas, apsimetant įmonės vadovu

Finansiniai sukčiai iš gyventojų ir verslo pernai išviliojo 10,2 mln.
eurų

Finansų specialistai dažnai būna vieni mėgstamiausių sukčių taikinių. Jeigu tvarkote didelės bendrovės finansus, galite sulaukti netikėto skambučio iš tariamo įmonės generalinio direktoriaus, kuris prašo nedelsiant apmokėti sąskaitą faktūrą arba pervesti pinigų, nes esą sprendžia įmonės problemas. Nepaisykite skambinančiojo pažadų atsidėkoti, skubėjimo arba grasinimų ir neskubėkite – tai gali būti sukčių manipuliacija. Visada laikykitės įmonėje įprastos mokėjimų tvarkos. Būtinai pasitarkite su kompetentingu kolega ir vadovais.

6. Romantinė apgavystė

Dažniausiai šis būdas sutinkamas internetinėse pasimatymų svetainėse, tačiau sukčiai dažnai pasinaudoja ir socialiniais tinklais arba elektroniniu paštu, kad užmegztų kontaktą. Įtarimų jie gali sukelti neiškart: pradžioje – romantiškas bendravimas, vėliau – prašymai pasidalyti savo intymiomis nuotraukomis ar vaizdo įrašais, tada – šantažas, prašant pervesti pinigų. Tad dalintis informacija, kuri gali tapti kompromituojančia, virtualioje aplinkoje visai nereikėtų.

