

Pastaruoju metu suaktyvėjo sukčiai, išsityjantys populiariausių svetainių raktažodžius ir paieškos rezultatuose iškeliantys netikras, bet vizualiai autentiškai atrodančias svetaines. Jose suvedus prisijungimo duomenis, galime netekti visų sąskaitoje esančių pinigų. Kaip atpažinti tokias apgaules bei nuo jų apsisaugoti, pasakoja „Luminor“ banko Sukčiavimo rizikos valdymo skyriaus vadovas Linas Sadeckas.

Įprastai prisijungiant prie interneto banko ar kitų svarbių paslaugų, pirmasis žingsnis yra paieškos laukelyje įvesti žodį „X bankas“, „Sodra“, „X elektros tiekėjas“ ar „X draudimo bendrovė“ ir spausti pirmą pasitaikiusią nuorodą. Deja, tai tapo dar viena patogia priemone sukčiams, kurie paieškos sistemose nusiperka reklaminius raktinius žodžius ir iškelia suklustotas svetaines aukščiausiose rezultatų pozicijose. Panaudoję suklustotą prisijungimo laukelį, gyventojai patys atiduoda prisijungimo duomenis, o netrukus – ir visą savo sąskaitos turinį.

„Pastebime, kad ši sukčiavimo schema pastarąjį ketvirtį buvo pati populiariausia. Viena iš pagrindinių priežasčių – žmonių įpročiai jungtis prie svarbių paslaugų ne tiesiogiai, o per paieškos sistemas. Sukčiams pakanka sukurti netikrą puslapį ir nusipirkti reklamas su populiariais raktažodžiais – taip jų klastotės atsiduria paieškos viršuje ir atrodo kaip tikros nuorodos“, – sako L. Sadeckas.

Nusikaltėliai investuoja į profesionaliai atrodančius puslapius – anot eksperto, juose atkuriami tikri logotipai, spalvos, net išpėjamieji tekstai, būdingi realiam bankui ar įmonei. Keletas skirtumų – adreso juostoje puslapio viršuje esantis nežinomas ar klaidingas interneto adresas, ne pilnai veikiantis svetainės funkcionalumas ar neveikiantys visi autentikavimo būdai.

„Net ir patyrę interneto vartotojai kartais neatpažįsta suklustotų puslapių, nes jie atrodo praktiškai identiški tikriesiems. Tačiau vos suvedus į juos savo prisijungimo duomenis, šie patenka į sukčių rankas, o pastarieji iškart inicijuoja pinigų pervedimus“, – teigia L. Sadeckas.

Eksperto teigimu, šis pavojus aktualus ne tik bankų klientams. Tokiu pačiu principu sukuriamos netikros Sodros, Registrų centro, komunalinių paslaugų ar kitų institucijų svetainės. Jose gyventojų prašoma ne tik prisijungimo duomenų, bet ir asmens kodo, banko sąskaitų ar kitos jautrios informacijos.

Vien lyginant šių metų pirmąjį ketvirtį su antruoju, atveju, kuomet klientai nukentėjo nuo sukčių „Google“ paieškos lange radę suklustotą įstaigų tinklapį, išaugo daugiau nei

dvigubai, t. y. apie 230 proc. Vidutinė išviliojama suma siekė beveik 1 500 EUR.

„Sukčiai rinkosi visas paslaugų įmones, kurios įgalina prisijungimą prie banko – draudimo, komunalinių paslaugų, valstybės įmonių ar valdžios vartų, mokesčių inspekcijos, socialinės apsaugos ar kt. Jei buvo galimybė prisijungti prie tam tikros svetainės per banką ar sumokėti už paslaugas jungiantis per banką, tų įmonių puslapiai buvo klastojami“, – sako „Luminor“ banko ekspertas.

Nacionalinio kibernetinio saugumo centro duomenimis, š. m. liepos mėnesį vidutinis DNS užkardos suveikimo skaičius per dieną siekė apie 37 tūkst. bandymų. Tai reiškia, kad tiek kartų užblokuotas svetainės kasdien bando pasiekti vartotojai.

Kaip apsisaugoti

Pirmiausia, atidžiai naudokitės paieškos sistemų rezultatais jungdamiesi prie svarbių finansinių ar kitų asmeninių paslaugų svetainių. Tiek interneto bankų, tiek valstybinių įstaigų adresus patikimiausia įvesti tiesiogiai adresu juostoje arba išsisaugoti kaip nuorodas naršyklėje.

„Prisijungdami prie svarbių paskyrų neskubėkite, naudokitės tik oficialiais internetinių svetainių adresais, nespauskite nuorodų tiesiai iš paieškos ar pirmos nuorodos, atitikusios paieškos žodį, tikrinkite svetainės adresą naršyklės adresu juostoje“, – pabrėžia L. Sadeckas.

Jei įtariate, kad pateikėte savo duomenis netikroje svetainėje, kuo greičiau susisieki su savo banku, kuris gali laikinai sustabdyti prieigą prie interneto banko, sąskaitos, pagelbėti teikiant prašymus lėšų gavėjo bankui atšaukti mokėjimus. Taip pat nedelsdami pakeiskite visus su incidentu susijusius slaptažodžius – ne tik interneto banko, bet ir el. pašto ar kitų paskyrų, jei jungiantis buvo prašoma juos įvesti.

