

Artėjant Juodojo penktadienio išpardavimams, socialiniuose tinkluose padaugėja elektroninių parduotuvių, skelbiančių, neva užsidaro ir išparduoda visas prekes. Deja, nemaža dalis tokių pardavėjų tėra sukčiai, pasinaudojantys pirkėjų noru sutaupyti. Kaip atpažinti tokią apgaulę ir nuo jos apsisaugoti, pataria „Luminor“ banko sukčiavimo prevencijos skyriaus vadovas Mindaugas Kutkaitis.

Netikrų el. parduotuvių įprastai ima daugėti prieš Juodąjį penktadienį bei Kalėdas, pasak „Avast“ kompanijos tyrimų. Vien per 2024 m. paskutinį ketvirtį pasauliniu mastu aptikta daugiau kaip 80 tūkst. tokių pardavėjų, iš kurių dauguma dingo ar pakeitė pavadinimus vos po kelių savaičių. Šių metų pirmąjį ketvirtį tokių atvejų skaičius pasaulyje išaugo net 790 proc., lyginant su ankstesniais metais.

„Gen Threat Report“ duomenimis, net 23 proc. visų socialinių tinklų sukčiavimo atvejų sudaro netikros el. parduotuvės. Daugiausia jų aptinkama „Facebook“ ir „Instagram“ platformose, kur vartotojai viliojami itin patraukliomis kainomis ir profesionaliai atrodančiais reklaminiais įrašais.

Veikia pagal panašią schemą

Pasak M. Kutkaičio, netikros e. parduotuvės veikia panašiu būdu. Iš pradžių socialiniuose tinkluose pasirodo reklama, siūlanti brangias prekes už itin mažą kainą. Skelbimas veda į tikroviškai atrodančią svetainę, o joje pateikiami vogti produktų atvaizdai, netikri klientų atsiliepimai ir tariami „patikimumo“ ženklai.

„Pirkėjui įvedus kortelės duomenis ir atlikus apmokėjimą, prekės dažniausiai nesulaukiama. Kai kuriais atvejais atsiunčiamos nekokybiškos kopijos, o netrukus ir pati parduotuvė dingsta iš interneto platybių. Sukčiai tuo metu jau būna pasisavinę pirkėjo mokėjimo duomenis, kuriuos gali panaudoti neteisėtiems pirkimams arba parduoti tamsiajame internete (angl. *Dark web*)“, – pasakoja „Luminor“ ekspertas.

Anot jo, šios schemos atrodo profesionaliai ir patikimai, puslapiai sukurti taip, kad nesukeltų įtarimų. Tačiau net smulkūs požymiai, tokie kaip keistai suformuluotas svetainės adresas ar neįprastai didelės nuolaidos, turėtų paskatinti pirkėjus elgtis atsargiau.

Klesti dėl noro sutaupyti

Ekspertas pažymi, kad šiuos sukčiavimus dažnai skatina pirkėjų noras sutaupyti. Žmonės vis dažniau ieško „gerų pasiūlymų“, o sukčiai tuo pasinaudoja, siūlydami tariamai pigesnes prekes.

„Be to, dalis naujų el. parduotuvių veikia pagal vadinamąjį *dropshippingo* modelį, kai prekės siunčiamos tiesiai iš tiekėjo, o pats pardavėjas sandėlio neturi. Nors šis modelis teisėtas, jis dažnai pasitelkiamas ir apgaulės tikslais. Pavyzdžiui, netikros parduotuvės nurodo svetimus įmonių duomenis arba visai jų neskelbia“, – sako M. Kutkaitis.

Turi kelis esminius požymius

Netikros el. parduotuvės dažnai pasižymi keliais bendrais bruožais. Pavyzdžiui, atkreipkite dėmesį į tokius požymius kaip klaidos ar neįprasti domenai svetainės adrese (.shop, .top ar kt.), taip pat kontaktinės informacijos trūkumas ar visiškas jos nebuvimas.

„Be abejo, įtarimą turėtų kelti ir itin dideli, neadekvatūs nuolaidų procentai, vienodi ar dirbtini klientų atsiliepieimai bei riboti atsiskaitymo būdai. Patikimos įmonės naudoja integruotus mokėjimo sprendimus, tokius kaip „MakeCommerce“ ar kitus oficialius partnerius, kurie tikrina prekybininkų patikimumą“, – pabrėžia ekspertas.

Kaip apsisaugoti?

Norėdami išvengti tokių sukčių, prieš atliekant pirkimą pasidomėkite, ar pardavėjo įmonė yra registruota ir ar turi tikrus kontaktus. Taip pat paieškokite atsiliepieimų apie pardavėją nepriklausomuose šaltiniuose ir venkite skelbimų, žadančių neįprastai dideles nuolaidas.

„Perkant prekę saugiausia mokėti per patikimus mokėjimo partnerius, kurie leidžia susigrąžinti pinigus ginčo atveju. Reikėtų vengti tiesioginių pavedimų, kriptovaliutų ar dovanų kortelių, kadangi tokius būdus sukčiai mėgsta labiausiai“, – pataria M. Kutkaitis.

Jeigu vis dėlto tapote tokio sukčiavimo auka, nedelsdami susisieki su savo banku, sustabdykite mokėjimą ir praneškite apie incidentą policijai. Kuo greičiau pranešite apie nusikaltimą, tuo didesnė tikimybė atgauti prarastas lėšas ar užkirsti kelią tolesniems sukčiams veikti jūsų vardu.

