**Pranešimas žiniasklaidai**

2025 m. lapkričio 14 d.

**Pigūs pasiūlymai gali kainuoti brangiai: kaip atpažinti netikras e. parduotuves?**

**Lapkritį išpardavimais gyventojus vilioja ne tik dideles nuolaidas siūlantys prekybininkai, bet ir internetiniai sukčiai. Tarptautiniai tyrimai rodo, kad šiuo laikotarpiu netikrų e. parduotuvių ir sukčiavimo atvejų gerokai padaugėja. Artėjant didžiausiam nuolaidų savaitgaliui, „Citadele“ banko plėtros vadovas Romas Čereška pataria, kaip atpažinti apgaulingas e. parduotuves ir nepakliūti į sukčių spąstus.**

**Sukčiai remiasi Juodojo penktadienio psichologija**

Dirbtinio intelekto sprendimus kibernetinio saugumo srityje kuriančios įmonės „Darktrace“ duomenimis, per praėjusių metų Juodojo penktadienio savaitę pasaulyje kalėdinės tematikos sukčiavimo atakų padaugėjo daugiau nei tris kartus, o Juodojo penktadienio netikrų pasiūlymų – beveik 7 kartus.

Pastaraisiais metais sukčiai ne tik aktyvėja, bet ir tobulina savo taktikas. Remiantis kibernetinio saugumo bendrovės „Avast“ duomenimis, per 2024 m. Juodojo penktadienio ir šventinį laikotarpį internete buvo aptikta daugiau nei 80 tūkst. fiktyvių e. parduotuvių visame pasaulyje. Dalis jų imitavo žinomus prekių ženklus, o dalis buvo sukurta specialiai Juodojo penktadienio savaitės išpardavimams.

R. Čereškos teigimu, pagrindinis netikrose e. parduotuvėse veikiančių sukčių tikslas – ne parduoti, o surinkti mokėjimo ar asmeninius duomenis, tad vartotojų budrumas šiuo laikotarpiu itin svarbus.

„Kibernetiniai nusikaltėliai veikia pagal emocijų principą – jie žino, kad Juodojo penktadienio metu žmonės priima sprendimus greičiau, vedini noro nepraleisti geros progos. Tai vadinamoji FOMO (angl. *fear of missing out*) psichologija. Matydami, kad pasiūlymas galioja tik kelias valandas, pirkėjai dažnai pasiduoda spontaniškam pirkimui, nepatikrinę svetainės patikimumo“, – teigia R. Čereška.

Pasak eksperto, jau kurį laiką sukčiai nebeapsiriboja tik netikrais el. laiškais ar trumposiomis SMS žinutėmis. Jie vis dažniau investuoja į profesionaliai atrodančias svetaines, kurių dizainas ir kalba sukurti taip, kad sukeltų pasitikėjimą.

**Netikrą e. parduotuvę išduoda kelios detalės**

Anot pašnekovo, net ir profesionaliai atrodančią apgaulę galima atpažinti, kai pirkėjas žino, į kokias detales reikia atkreipti dėmesį. Vienas iš pagrindinių signalų – neįprastas svetainės adresas. Sukčiai dažnai kuria domenus, labai panašius į žinomų prekės ženklų pavadinimus, tik prideda papildomų raidžių, brūkšnelių ar papildomų žodžių, pavyzdžiui „sale“ (liet. išpardavimas). Kitas požymis – gramatinės klaidos ir netaisyklinga kalba.

„Daugelis fiktyvių svetainių yra verčiamos automatiškai. Jeigu matote netaisyklingą kalbą, netiksliai išverstus terminus ar prastai suformatuotus tekstus – tai signalas, kad tokią parduotuvę reikėtų patikrinti nuodugniau“, – sako R. Čereška.

Pasak eksperto, taip pat svarbu įvertinti, ar svetainėje yra aiškūs kontaktai, įmonės rekvizitai, grąžinimo politika, o mokėjimo metu – ar matote saugų ryšį („https“) ir užrakto simbolį naršyklėje.

Prieš atliekant mokėjimą R. Čereška pataria atlikti tris paprastus veiksmus:

* interneto paieškos sistemoje suvesti svetainės pavadinimą su žodžiais „scam“ arba „review“ ir patikrinti rezultatus;
* patikrinti domeno registracijos statusą nemokamais specialiais įrankiais, pvz.,  *whois.lt*, *domreg.lt* ar kt.
* pasidomėti, ar svetainė turi atsiliepimų „Google“, „Rekvizitai“, „Trustpilot“ ar socialiniuose tinkluose.

„Papildomas aspektas, galintis atskleisti, ar e. parduotuvė yra saugi – jos veikimo laikas. Kibernetinių nusikaltėlių sukurtos netikros e. parduotuvės veikia trumpą laiką – savaitę ar dvi. Todėl jeigu svetainė sukurta visai neseniai, o nuolaidos atrodo neįtikėtinos – tai turėtų būti papildomas raudonas signalas“, – pabrėžia „Citadele“ atstovas.

**Apsisaugoti padeda atsakingas elgesys**

Pinigų plovimo prevencijos kompetencijų centro duomenimis, 2025 m. pirmąjį pusmetį registruota 7,7 tūkst. bandymų išvilioti gyventojų pinigų, o nukentėjusieji sukčiams pervedė jau 11,5 mln. eurų.

Pasak „Citadele“ atstovo, svarbiausia apsaugos nuo tokių nuostolių priemonė – sveikas skepticizmas ir atsakingas elgesys su mokėjimo duomenimis. Pirkdami internetu pirkėjai turėtų naudoti tik patikimus, saugius atsiskaitymo būdus, vengti tiesioginių pavedimų nežinomiems gavėjams ir niekada nevesti kortelės duomenų per nuorodas, gautas trumposiomis SMS žinutėmis ar el. laiškais.

Jei visgi pirkėjas spustelėjo „pirkti“ nepatikimoje e. parduotuvėje ir tapo neaišku, kam pervedė pinigus, R. Čereška primena, kokių veiksmų reikėtų imtis:

* Nedelsiant susisiekti su savo banku ir pranešti apie galimą sukčiavimo atvejį.
* Blokuoti kortelę arba sustabdyti pavedimą, jei tai įmanoma.
* Patikrinti, ar svetainėje yra kontaktai ar rekvizitai, ir, jei įmanoma, fiksuoti įtarimą – užfiksuoti ekrano nuotrauką ar išsisaugoti susirašinėjimo el. laiškais kopijas.
* Stebėti banko sąskaitą dėl neįprastų operacijų ir prireikus kreiptis į policiją arba vartotojų apsaugos institucijas.

„Jei kyla nors menkiausia abejonė – geriau susilaikyti nuo apsipirkimo. Vertėtų daugiau pasidomėti apie e. parduotuvę, patikrinti atsiliepimus. Nuolaidos, kurios atrodo per geros, kad būtų tiesa, dažniausiai ir yra apsukrus sukčių masalas pasisavinti vartotojų pinigus“, – priduria pašnekovas.