SANS SECURITY AWARENESS
PERLAS

OUCH! | 2017 m. lapkričio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Netikros internetinės parduotuvės
- Jūsų kompiuteris arba mobilusis įrenginys
- Jūsų kredito kortelė

Kaip saugiai apsipirkti internetu?

Apžvalga

Artėjant šventiniam laikotarpiui, milijonai žmonių visame pasaulyje ieškos, kur galima nusipirkti puikių dovanų. Dauguma mūsų, ieškodami gerų pasiūlymų, vengdami ilgų eilių ir nekantrios žmonių minios, rinksis apsipirkimą internetu. Deja, tai taip pat yra toks metų laikas, kai dauguma kibernetinių nusikaltėlių kuria netikras internetines parduotuves, kuriomis siekia apgauti kitus ir pavogti jų pinigus ar informaciją. Žemiau paaiškinsime, kokia rizika kyla apsiperkant internetu ir kaip galite gauti gerus bei saugius pasiūlymus.

Kviestinė redaktorė

Lenny Zeltser kuria saugumo produktus įmonėje „Minerva Labs“ ir dėsto apie kovą su kenkimo programomis SANS institute. Lenny aktyviai dalyvauja „Twitter“ paskyroje **@lennyzeltser** ir rašo tinklaraštį apie saugumą svetainėje **zeltser.com**.

Netikros internetinės parduotuvės

Nors dauguma interneto svetainių veikia teisėtai, tačiau internete taip pat galima rasti netikrų svetainių, kuriamų kibernetinių nusikaltėlių. Tokias netikras svetaines nusikaltėliai kuria atkartodami oficialių svetainių išvaizdą arba naudodami gerai žinomų parduotuvių bei prekių ženklų pavadinimus. Tokios suklastotos svetainės yra naudojamos siekiant atkreipti geriausių pasiūlymų ieškančių žmonių dėmesį. Į tokias svetaines galite patekti internete ieškodami pačių pigiausių kainų. Prieš pasirinkdami svetainę, kurioje pirksite, atkreipkite dėmesį į kitas svetaines, kuriose siūlomos drastiškai mažesnės kainos nei bet kur kitur, arba svetaines, kuriose siūlomi produktai yra parduodami visoje šalyje. Tikroji priežastis, dėl kurios šie produktai yra tokie pigūs arba prieinami, yra todėl, kad tai yra neteisėta arba padirbta, o kai kuriais atvejais to produkto išvis negausite. Apsisaugokite imdamiesi tolimesnių veiksmų:

- Apsipirkinėkite svetainėse, kurios jums yra gerai žinomos, patikimos ir kuriose jau esate ką nors pirkę.
- Įsitikinkite, ar svetainėje yra nurodytas oficialus įmonės pašto adresas ir telefono numeris, kuriuo galite susisiekti su pardavimų skyriumi arba gauti atsakymus į jums kilusius klausimus. Jei svetainė atrodo įtartinai, paskambinkite ir pašnekėkite su jos atstovu. Jei negalite su niekuo pasikalbėti, tai turėtų būti laikoma vienu iš požymių, kad svetainė yra netikra.
- Ieškokite akivaizdžių įspėjamųjų ženklų, tokių kaip pasiūlymai, kurie yra per geri, kad tai būtų tiesa, arba tekste matoma prasta gramatika ir klaidinga rašyba.

Kaip saugiai apsipirkti internetu?

- Būkite itin įtarūs, jei svetainė atrodo kaip tiksli, anksčiau naudotos, žinomos svetainės kopija, tačiau jos adresas arba pavadinimas truputį skiriasi. Pavyzdžiui, galbūt anksčiau esate pirkę svetainėje „Amazon“, kurios oficialus adresas yra https://www.amazon.com. Tačiau įtarimas turėtų kilti apsilankius tariamoje „Amazon“ svetainėje, kurios adresas yra http://store-amazoncom.com.
- Įveskite parduotuvės pavadinimą arba adresą į paieškos sistemą ir paskaitykite, kaip apie ją praeityje atsiliepė kiti žmonės. Ieškokite tokių terminų kaip „apgavystė“, „suklastota“, „daugiau niekada“ arba „netikra“. Atsiliepimų trūkumas taip pat gali būti ženklu, rodančiu, kad svetainė yra nauja arba galėtų būti nepatikima.
- Prieš pirkdami kokias nors prekes, įsitikinkite, kad jūsų ryšys su svetaine yra šifruojamas. Daugumoje naršyklių šifruojamą ryšį vaizduoja užrakintos žalios spynelės ženkliukas ir/arba prieš svetainės adresą esantis trumpinys „HTTPS“.

Apsisaugokite internetu apsipirkinėdami tik gerą reputaciją turinčiose, patikimose svetainėse.

Prisiminkite, kad vien todėl, kad svetainė atrodo profesionaliai, nereiškia, kad ji yra teisėta. Jei nesate užtikrinti svetaine – nesinaudokite ja. Vietoj to, susiraskite gerai žinomą svetainę, kuria galite pasitikėti arba kuria saugiai naudojotės praeityje. Galbūt joje nerasite geriausio pasiūlymo, tačiau tikėtina, jog įsigysite legalų produktą, o jūsų asmeniniai ir finansiniai duomenys nebus pavogti.

Jūsų kompiuteris arba mobilusis įrenginys

Be apsipirkinėjimo teisėtose svetainėse, turėtumėte įsitikinti, kad jūsų kompiuteris arba kitas įrenginys yra saugus. Kibernetiniai nusikaltėliai bandys jūsų įrenginius užkrėsti virusais ir taip gauti prieigą prie jūsų banko sąskaitų, kredito kortelės informacijos ir slaptažodžių. Norėdami apsaugoti savo įrenginius, imkitės tolimesnių veiksmų:

- Jei namuose yra vaikų, apsvarstykite galimybę turėti du įrenginius – vieną vaikams, kitą suaugusiems. Vaikai smalsiai ir aktyviai domisi technologijomis, todėl yra didesnė tikimybė, jog jie jūsų įrenginį užkrės virusais. Naudodami atskirą kompiuterį arba planšetę internetinėms operacijoms, pavyzdžiui, internetinei bankininkystei ir apsipirkinėjimui, sumažinsite galimybę įrenginį užkrėsti virusais.

Kaip saugiai apsipirkti internetu?

- Visada įdiekite naujausius atnaujinimus ir naudokite naujausią antivirusinę programinę įrangą. Taip kibernetiniam nusikaltėliui bus žymiai sudėtingiau užkrėsti jūsų įrenginį.

Jūsų kredito kortelė

Reguliariai peržiūrėkite savo kredito kortelės ataskaitas, siekdami nustatyti ar nėra nuskaitomi kokie nors įtartini mokesčiai, ypač daugybę kartų atsiskaičius kortelėmis perkant internetu arba pasinaudojus nauja interneto svetaine. Kai kurie kredito kortelių tiekėjai suteikia galimybę kiekvieną kartą, atsiskaičius kortele arba viršijus numatytą sumą, apie tai gauti pranešimą el. paštu arba SMS žinute. Kitas būdas yra pirkimui internetu naudoti tik vieną kredito kortelę. Tokiu būdu, kilus pavojui, galėsite kortelę lengvai pasikeisti, nedarydami jokios įtakos kitiems mokėjimo būdams. Jei manote, kad buvo įvykdyta sukčiavimo veikla, nedelsdami paskambinkite kredito kortelę išdavusiai įmonei. Dėl šios priežasties pirkimui internetu turėtumėte naudoti kredito korteles, o debeto kortelėmis vengti naudotis, kai tik tai yra įmanoma. Naudojant debeto korteles, pinigai yra nuskaitomi tiesiai nuo jūsų banko sąskaitos, todėl nukentėjus nuo sukčiavimo, atgauti pinigus gali būti žymiai sudėtingiau. Galiausiai, naudoti kredito korteles turėtumėte todėl, kad kiekvienam internetiniam pirkiniui, dovanų kortelėms ar gerai žinomoms mokėjimo paslaugoms, tokioms kaip „PayPal“, jos sugeneruoja po unikalų kortelės numerį, todėl pardavėjui neturite atskleisti tikrojo savo kredito kortelės numerio.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę securingthehuman.sans.org/ouch/archives.

Šaltiniai

Socialinė inžinerija:	https://securingthehuman.sans.org/ouch/2017#january2017
Keturi būdai, padedantys likti saugiems:	https://securingthehuman.sans.org/ouch/2016#october2016
Jūsų namų tinklo apsauga:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS instituto dienos patarimas apie saugą:	https://www.sans.org/tip_of_the_day.php

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.