

OUCH!

ŠIAME LEIDIME...

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

Saugus apsipirkimas internete

Sezonas, per kurį verta būti atsargiems

Artėja šventinis metas, todėl netrukus milijonai žmonių visame pasaulyje pradės ieškoti pačių geriausių dovanų. Daugelis mūsų, ieškodami puikių pasiūlymų ir siekdami išvengti ilgų eilių bei nekantrių žmonių minių, rinksis apsipirkimą internete. Deja, tai taip pat yra mėgstamiausias nusikaltėlių metų laikas, per kurį jie yra linkę internetu arba finansiškai sukčiauti. Šį mėnesį paaiškinsime apie pirkimo internetu pavojus ir patarsime, kaip galite nuo jų apsisaugoti.

Kviestinis redaktorius

Jonathan Homer (@JonathanLHomer) yra pripažintas lyderiu, aktyviai ugdančiu sąmoningumą apie kibernetinį saugumą tiek vyriausybės, tiek privačiame sektoriuose. Jis specializuojasi visuomenės įtraukimo į dalyvavimą ir pažangiausių jos mokymo metodų srityje.

Netikros internetinės parduotuvės

Nors dauguma internetinių parduotuvių yra legalios, kai kurios iš jų veikia neteisėtai – tokios yra nusikaltėlių sukurtos netikros svetainės. Nusikaltėliai šias netikras svetaines kuria kopijuodami gerai žinomų parduotuvių išvaizdą arba naudodami jų pavadinimą. Tuomet jie šias svetaines naudoja siekdami privilioti žmones, ieškančius geriausių pasiūlymų. Internete ieškodami pačių mažiausių kainų galite būti nukreipti į vieną iš tokių netikrų svetainių.

Rinkdamiesi svetainę produkto pirkimui, venkite svetainių siūlančių drastiškai žemesnes kainas, nei bet kur kitur arba siūlančių produktus, kurie yra išparduodami visos šalies mastu. Priežastis dėl kurios jų produktai yra tokie pigūs yra ta, kad jūsų gautas produktas bus nelegalus, suklastotas arba pavogtas, o kai kuriais atvejais jūs jo išvis negausite. Apsisaugokite imdamiesi toliau nurodytų veiksmų:

- Įsitikinkite, kad svetainė turi oficialų el. pašto adresą ir telefono numerį, kuriuo galite susisiekti pardavimų arba pagalbos klausimais. Jei svetainė atrodo įtartina, paskambinkite ir pasikalbėkite su jos atstovu.
- Atkreipkite dėmesį į akivaizdžius įspėjamuosius ženklus, tokius kaip prasta gramatika ar rašyba.
- Būkite itin atsargūs, jei svetainė atrodo kaip tiksliai gerai žinomos svetainės, kurią naudojote praeityje, kopija, kurios adresas arba parduotuvės pavadinimas nors truputį skiriasi. Pavyzdžiui, galbūt esate lankęsi adresu

Saugus apsipirkimas internete

<https://amazon.com>, norėdami apsipirkti „Amazon“ svetainėje. Būkite itin atsargūs, jei „Amazon“ svetainė apsimetančio tinklalapio adresas būtų <http://store-amazon.com>.

- Įveskite parduotuvės pavadinimą arba adresą paieškos sistemoje ir peržiūrėkite, ką apie šią svetainę praeityje yra rašę kiti žmonės. Atkreipkite dėmesį į tokias frazes kaip „apgaulingas laiškas“, „niekada daugiau“ arba „netikra“. Atsiliepimų trūkumas taip pat nėra geras ženklas, kadangi tai rodo, jog svetainė yra ganėtinai nauja.

Prisiminkite, jog vien todėl, kad svetainė atrodo profesionaliai, nereiškia, jog ji veikia teisėtai. Jei dėl svetainės kyla nors menkiausių abejonų, skirkite laiko jos patikrinimui. Jei dėl jos nesate tikri, nesinaudokite ja. Vietoj to, susiraskite gerai žinomą svetainę, kuria galite pasitikėti arba kuria saugiai naudojotės praeityje. Galbūt joje nerasite tokio gero pasiūlymo arba populiarios prekės, tačiau tikėtina, jog įsigysite legalų produktą ir jūsų banko išrašė atspindės tiksli informacija.

Jūsų kompiuteris / mobilusis įrenginys

Be apsipirkinėjimo teisėtai veikiančiose svetainėse, turite įsitikinti, jog jūsų kompiuteris arba mobilusis įrenginys yra saugus. Kibernetiniai nusikaltėliai bandys užkrėsti jūsų įrenginius tam, kad galėtų sužinoti jūsų banko duomenis, kredito kortelės informaciją ir jūsų slaptažodžius. Apsaugokite savo įrenginius imdamiesi toliau nurodytų veiksmų:

- Jei namuose yra vaikų, apsvastykite galimybę įsigyti du įrenginius – vieną vaikams, o kitą suaugusiems. Vaikai yra smalsūs ir puikiai moka naudotis technologijomis, todėl yra didesnė tikimybė, kad jų įrenginys bus užkrėstas. Vykdydami internetinius sandorius, tokius kaip naudojimas internetine bankininkyste ar pirkimas internetu, naudokite atskirą kompiuterį arba planšetę – taip sumažinsite galimybę įrenginį užkrėsti. Jei nėra galimybės turėti atskirų įrenginių, tuomet bendrame kompiuteryje susikurkite atskiras vartotojų paskyras ir įsitinkite, kad vaikams nėra suteiktos administratoriaus teisės.
- Vykdydami finansines operacijas, junkitės tik prie tų belaidžių tinklų, kuriuos valdote arba kuriais pasitikite, pavyzdžiui, savo namų tinklo. Viešas belaidis tinklas, pavyzdžiui, vietinėje kavinėje, gali puikiai tikti naujienu skaitymui, bet ne jungimuisi prie savo banko paskyros.



Apsaugokite savo informaciją pirkdami tik patikimose ir geros reputacijos internetinėse parduotuvėse.

Saugus apsipirkimas internete

- Visada įdiekite naujausius atnaujinimus ir naudokite naujausios versijos antivirusinę programą. Taip kibernetiniams nusikaltėliams bus žymiai sunkiau užkrėsti jūsų įrenginį.

Jūsų kredito kortelė

Sekite savo kredito kortelės išrašus, norėdami nustatyti ar jūsų pinigai nėra nuskaitomi įtartiniems tikslams. Išrašus turėtumėte peržiūrėti reguliariai, bent jau kartą per mėnesį. Kai kurie kredito kortelių teikėjai suteikia galimybę būti informuotiems el. paštu arba SMS žinute kaskart nuskaičius pinigus arba kai yra pasiekama tam tikra nuskaitytų pinigų suma. Kitas variantas yra pirkimui internetu turėti atskirą kredito kortelę, tokiu būdu į ją patekus, galėsite kortelę lengvai pakeisti neįtakodami jokios kitos mokėjimo veiklos. Jei manote, kad buvo sukčiauta, nedelsdami paskambinkite kredito kortelę išdavusiai įmonei ir paaiškinkite situaciją. Dėl šios priežasties kredito kortelės yra žymiai tinkamesnės pirkimui internetu, nei debeto kortelės. Naudojantis debeto kortelėmis pinigai yra nuskaičiuojami tiesiogiai nuo jūsų banko sąskaitos, todėl patekus į sukčių pinkles gali būti žymiai sunkiau atgauti savo pinigus.

Galiausiai, yra sukurta nauja technologija, leidžianti apmokėti neatskleidžiant savo kredito kortelės numerio. Pamąstykite apie kredito korteles, kurios kaskart perkant internetu sugeneruoja naują unikalų kortelės numerį, arba naudokitės gerai žinomomis mokėjimo svetainėmis, tokiomis kaip PayPal, kurios nereikalauja pardavėjui atskleisti savo kredito kortelės numerio.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę <http://www.securingthehuman.org>.

Šaltiniai

5 žingsniai išliktu saugiu:	https://www.securingthehuman.org/ouch/2014#october2014
Jūsų namų tinklo apsauga:	https://www.securingthehuman.org/ouch/2014#january2014
Jūsų planšetės apsauga:	https://www.securingthehuman.org/ouch/2013#december2013
SANS dienos saugumo patarimas:	https://www.sans.org/tip_of_the_day.php

Licencija

OUCH! Yra leidžiamas SANS Securing The Human instituto ir platinamas pagal [Creative Commons BY-NC-ND 3.0 licencija](https://creativecommons.org/licenses/by-nc-nd/3.0/). Jums leidžiama naudoti ir platinti šį naujienlaiškį su sąlyga, kad niekas nebus keičiama. Norėdami gauti daugiau informacijos susisiekite su mumis ouch@securingthehuman.org.

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.



securingthehuman.org/blog



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](https://www.securingthehuman.org/gplus)