

# OUCH!

## ŠIAME LEIDINYJE...

- Atidumas
- Slaptažodžiai
- Naujinimas
- Atsarginės kopijos

## Kibernetiniai nusikaltėliai: kokie būdai padės nuo jų apsisaugoti?

### Apžvalga

Technologijoms tampa vis svarbesne mūsų gyvenimo dalimi, kartu jos tampa ir vis sudėtingesnės. Žinant, kaip greitai jos keičiasi, vadovautis saugumo patarimais gali būti painu. Atrodo, kad atsiranda vis naujesnių ir naujesnių patarimų apie tai, kaip turėtumėte ar neturėtumėte elgtis. Nors laikui einant duomenys, nurodantys, kaip apsisaugoti gali keistis, yra keletas pagrindinių dalykų, kuriuos galite nuolat daryti norėdami apsisaugoti. Nepriklausomai nuo to,

kokiomis technologijomis, kaip ir kur jomis naudojate, rekomenduojame vadovautis toliau pateiktais pagrindiniais keturiais būdais. Norėdami sužinoti daugiau informacijos apie bet kurį iš žemiau pateiktų būdų, pasinaudokite šio naujienlaiškio pabaigoje pateiktais Šaltinių adresais.

### Kviestinė redaktorė

Ryan Johnson tikslas yra užtikrinti, kad organizacijos būtų pasiruošusios reaguoti į neišvengiamus pažeidimus. Be to, SANS institute jis dėsto paskaitas apie „Pažangią tinklo ekspertizę“ ir aktyviai dalyvauja Twitter paskyroje adresu [@ForensicRJ](https://twitter.com/ForensicRJ).

- 1. Atidumas.** Visų pirma, turėkite omenyje, kad vien tik technologijos jūsų patikimai neapsaugos. Nusikaltėliai suvokia, jog paprasčiausias būdas apeiti pačias pažangiausias apsaugos technologijas yra pasinaudoti jumis. Jei reikia sužinoti slaptažodį, kredito kortelės ar asmeninius duomenis, lengviausias būdas tai padaryti yra jus įtikinti šią informaciją jiems pateikti. Pavyzdžiui, jie gali apsimesti „Microsoft“ techninę pagalbą teikiančiais darbuotojais, pranešančiais, kad jūsų kompiuteris – užkrėstas. Tuo tarpu realybėje tai yra paprasčiausi kibernetiniai nusikaltėliai, norintys gauti prieigą prie jūsų kompiuterio. Taip pat jie gali jums atsiųsti el. laišką, kuriame bus parašyta, kad jūsų pakuotė negali būti pristatyta, todėl turite paspausti laiške pateiktą nuorodą ir patvirtinti savo pašto adresą. Tuo tarpu realybėje jie bando jus įtikinti apsilankyti kenkėjiškoje svetainėje, kurią naudodami jie įsilauš į jūsų kompiuterį. Štai kaip prasideda puolimas išpirkos reikalaujančiomis programomis ar sukčiavimas apsimitant įmonės vadovu. Galiausiai, geriausia gynybos priemonė nuo nusikaltėlių esate jūs patys. Būkite įtarūs. Naudodamiesi sveiku protu galite pastebėti ir sustabdyti daugumą puolimų.
- 2. Slaptažodžiai.** Kitas žingsnis, padedantis apsisaugoti, yra kiekviename iš savo įrenginių ir internetinių paskyrų naudoti patikimą bei unikalų slaptažodį. Pagrindiniai žodžiai čia yra patikimas ir unikalus. Patikimas slaptažodis reiškia

## Kibernetiniai nusikaltėliai: kokie būdai padės nuo jų apsisaugoti?

tokį, kurio programišiai ar jų automatizuotos programos negalėtų lengvai atspėti. Pavargote nuo sudėtingų slaptažodžių, kuriuos sudėtinga prisiminti ir įvesti? Pabandykite naudoti slaptafrazes. Vietoj pavienio žodžio, naudokite frazes, kurias lengva prisiminti, pavyzdžiui, „Kur yra mano kava?“. Kuo ilgesnė slaptafrazė, tuo ji patikimesnė. Unikalus slaptažodis reiškia, kad kiekviename įrenginyje ir internetinėje paskyroje yra naudojamas skirtingas slaptažodis. Tokiu būdu, jei bus atspėtas vienas slaptažodis, visos kitos jūsų paskyros ir įrenginiai liks saugūs. Negalite prisiminti visų patikimų ir unikalių slaptažodžių? Nesijaudinkite, nes to padaryti negalime ir mes. Štai kodėl rekomenduojame naudoti slaptažodžių tvarkytuvę. Tai yra specializuota išmaniajam telefonui ar kompiuteriui skirta programa, galinti užšifruotu formatu saugiai laikyti jūsų slaptažodžius.



*Vadovaudamiesi šiais keturiais žingsniais ne tik apsisaugosite, bet ir neatsiliksite nuo naujausių technologijų.*

Galiausiai, vienas iš svarbiausių veiksnių, kurių galite imtis, siekdami apsaugoti bet kokią paskyrą, yra įjungti dviejų etapų tapatybės patvirtinimą. Vien slaptažodžių nebepakanka, siekiant apsaugoti savo paskyras, todėl visi turime naudoti kai ką patikimesnio. Dviejų etapų tapatybės patvirtinimas yra žymiai patikimesnis. Šiuo būdu naudojate savo slaptažodį ir antrą papildomą apsaugos priemonę, pavyzdžiui, kokią nors savo fizinę savybę (biometrija) arba kokį nors turimą dalyką (pavyzdžiui, į išmanųjį telefoną atsiųstą kodą ar kodus generuojančią išmaniojo telefono programą). Jei tik įmanoma, įjunkite šią parinktį kiekvienoje savo paskyroje, kurioje tik galite tai padaryti, įskaitant savo slaptažodžių tvarkytuvę. Dviejų etapų tapatybės patvirtinimas tikriausiai yra vienintelis ir svarbiausias būdas, kurį galite naudoti, siekdami apsisaugoti. Be to, jį naudoti yra žymiai paprasčiau nei įsivaizduojate.

- 3. Naujinimas.** Įsitinkite, kad jūsų kompiuteriuose, mobiliuosiuose įrenginiuose, programose ir kituose prietaisuose, prijungtuose prie interneto, yra įdiegta naujausia programinės įrangos versija. Kibernetiniai nusikaltėliai jūsų naudojamų įrenginių programinėje įrangoje nuolat ieško naujų pažeidimų. Juos aptikę, jie, naudodami specialias programas, šiais pažeidimais pasinaudoja ir įsilaužia į jūsų naudojamus įrenginius. Tuo tarpu šių įrenginių programinę įrangą sukūrusios įmonės sunkiai dirba, siekdamos šias problemas išspręsti ir leidamos naujinius. Įsitinkdami, kad jūsų kompiuteriuose ir mobiliuosiuose įrenginiuose yra įdiegti šie naujinimai, jūs užsitikinate, jog į juos kažkam bus žymiai sudėtingiau

## Kibernetiniai nusikaltėliai: kokie būdai padės nuo jų apsisaugoti?

įsilaužti. Norėdami, kad jūsų sistemos versija būtų pati naujausia, kai tik įmanoma, įjunkite automatinį naujinimą. Ši taisyklė taikoma beveik bet kuriai prie tinklo prijungtai technologijai, įskaitant prie interneto prijungtus televizorius, kūdikių stebėjimo įrenginius, namuose esančius maršruto parinktuvus, žaidimų pultus, o kada nors ateityje, galbūt, net jūsų automobilį. Jei jūsų operacinės sistemos arba įrenginiai yra seni ir jiems nebekuriami apsaugos naujiniai, rekomenduojame šiuos įrenginius pakeisti naujais, kuriems teikiama ši paslauga.

4. **Atsarginės kopijos.** Nesvarbu, kokie atsargūs bebūtumėte, kartais kas nors vis tiek gali įsilaužti į jūsų įrenginius. Jei taip įvyko, dažniausiai vienintelis būdas, leidžiantis įsitikinti, kad jūsų kompiuteryje ar mobiliajame įrenginyje nebeliko kenkimo programos, yra visiškai ištrinti kompiuterio sistemą ir iš naujo ją atkurti. Nusikaltėlis net gali uždrausti prieigą prie jūsų asmeninių failų, nuotraukų ir kitos, įsilaužtoje sistemoje esančios, informacijos. Dažniausiai vienintelis jums likęs būdas atkurti visą savo asmeninę informaciją yra pasinaudoti atsarginėmis kopijomis. Įsitinkite, kad reguliariai darote bet kokios svarbios informacijos atsargines kopijas ir patikrinkite ar šiuos duomenis įmanoma atkurti. Dauguma operacinių sistemų ir mobiliųjų įrenginių atsargines kopijas daro automatiškai. Be to, siekiant kas apsaugoti nuo kibernetinių nusikaltėlių, rekomenduojame laikyti Debesijoje arba ne internete.

## SUŽINOKITE DAUGIAU

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

### Šaltiniai

Sukčiavimas:	<a href="https://securingthehuman.sans.org/ouch/2015#december2015">https://securingthehuman.sans.org/ouch/2015#december2015</a>
Slaptažodžių tvarkytuvės:	<a href="https://securingthehuman.sans.org/ouch/2015#october2015">https://securingthehuman.sans.org/ouch/2015#october2015</a>
Dviejų etapų tapatybės patikrinimas:	<a href="https://securingthehuman.sans.org/ouch/2015#september2015">https://securingthehuman.sans.org/ouch/2015#september2015</a>
Slaptafrazės:	<a href="https://securingthehuman.sans.org/ouch/2015#april2015">https://securingthehuman.sans.org/ouch/2015#april2015</a>
Atsarginės kopijos:	<a href="https://securingthehuman.sans.org/ouch/2015#august2015">https://securingthehuman.sans.org/ouch/2015#august2015</a>

### 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](mailto:ouch@securingthehuman.org).

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



[securingthehuman.sans.org/blog](https://securingthehuman.sans.org/blog)



[/securethehuman](https://securethehuman)



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



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