

# OUCH!

## ŠIAME LEIDINYJE...

- Planšetės apsauga
- Saugumo išlaikymas

## Jūsų naujos planšetės apsauga

### Apžvalga

Sveikiname įsigijus naują planšetę! Ši technologija tai efektyvus ir patogus būdas, suteikiantis galimybę bendrauti su kitais, pirkti internetu, žiūrėti filmus, žaisti žaidimus ir atlikti daugybę kitokių veiksmų. Kadangi jūsų planšetė greičiausiai taps svarbia jūsų gyvenimo dalimi, o gal net pakeis jūsų stacionarų kompiuterį, pateikiame keletą pagrindinių patarimų, kuriais galėtumėte apsaugoti ne tik savo planšetę, bet ir joje esančią informaciją.

### Kviestinė redaktorė

Lori Rosenberg yra sukaupusi nemažai patirties, kurdama mokomąją medžiagą apie informacijos saugumą ir vesdama mokymus darbuotojams bei klientams. Be to, jai labai patinka ieškoti naujų ir įdomių būdų, leidžiančių tomis žiniomis pasidalinti. Lori galite rasti Twitter paskyroje įvedę [@InfoSecLori](#).

### Planšetės

Galbūt nustebsite sužinoję, jog didžiausią riziką jūsų planšetei kelia ne programišiai, bet jūs patys. Tikėtina, jog planšetė greičiau kur nors bus pamesta, užmiršta arba pavogta, negu kas nors į ją įsilauš. Pirmas dalykas, kurį turėtumėte padaryti norėdami apsaugoti savo planšetę yra įjungti automatinį ekrano užsirakinimą. Tai reiškia, kad kaskart norėdami pasinaudoti planšetiniu kompiuteriu, pirmiausiai turėsite atrakinti jo ekraną, įvesdami patikimą skaitmeninį kodą, nubraižydami raštą arba nuskaitydami savo piršto antspaudą. Taip užtikrinama, jog pametus ar pavogus kompiuterį, niekas negalės prie jo prisijungti. Be to, taip apsaugosite visą savo asmeninę informaciją, mobiliąsias programėles ir kitą jo turinį. Įjungę automatinį ekrano užsirakinimą, galite pasinaudoti dar keletu papildomų patarimų, kuriais apsaugotumėte savo naująją planšetę:

1. Įdiekite arba įjunkite programinę įrangą, leidžiančią internetu, nuotoliniu būdu sekti savo planšetę. Tokiu būdu, pametus arba pavogus, galėsite prie jos prisijungti internetu ir nustatyti jos buvimo vietą, o blogiausiu atveju, nuotoliniu būdu ištrinti visą joje esančią informaciją.
2. Atnaujinkite savo įrenginį ir įjunkite automatinį atnaujinimą, kad jame visada būtų įdiegta naujausia operacinės sistemos versija. Nusikaltėliai programinėje įrangoje visada ieško naujų trūkumų, o pardavėjai nuolatos išleidinėja naujus atnaujinimus ir jų pataisas. Įdiegus naujausią operacinės sistemos ir mobiliųjų programėlių versiją, į jūsų planšetinį kompiuterį įsilaužti taps žymiai sudėtingiau.

## Jūsų naujos planšetės apsauga

3. Būkite atidūs pirmą kartą konfigūruodami savo planšetinio kompiuterio nustatymus, ypač susijusius su privatumo nuostatomis. Vienas iš didžiausių planšetinio kompiuterio privatumo trūkumų yra leidimas kitiems stebėti ir žinoti jūsų buvimo vietą. Rekomenduojame vietos nustatymą visur išjungti ir įjungti tik tose programėlėse, kuriose jums tikrai to reikia. To gali prireikti naudojant kai kurias programėles, kuriomis stebima jūsų buvimo vieta, pavyzdžiui, žemėlapių programinėje įrangoje arba bandant rasti vietinį restoraną, tačiau daugumoje programėlių naudoti tikrąsias vietas informacijos jums nereikės.
4. Dauguma planšetinių kompiuterių ir programėlių jūsų informaciją saugo debesijoje. Todėl įsitikinkite, jog suprantate, kur ir kaip yra saugomi jūsų duomenys. Juk mažiausiai norite, kad kas nors internetu su pasauliu pasidalintų jūsų asmeninėmis nuotraukomis, kuriose būtų pažymėta geografinė vietos informacija. Numatytuose nustatymuose išjunkite bet kokį informacijos dalinimąsi debesijoje ir įjunkite jį tik tada, kai norėsite pasidalinti kažkuo konkrečiu.
5. Planšetiniai kompiuteriai sinchronizuoja jūsų programėles su kitais įrenginiais, tokiais kaip išmanusis telefonas arba nešiojamasis kompiuteris. Sinchronizavimas gali būti naudinga funkcija, tačiau atidžiai stebėkite kokias programas ar funkcijas sinchronizujete. Jei esate įjungę sinchronizavimą, nenustebkite darbo naršyklėje išvydę savo planšetiniame kompiuteryje lankytas svetaines ir sukurtas korteles.



*Pagrindiniai veiksmai norint apsaugoti savo planšetę yra ekrano užrakimo funkcijos įjungimas, privatumo nuostatų peržiūra ir užtikrinimas, kad visada įdiegiami programiniai naujinimai.*

## Saugumo išlaikymas

Kartą apsaugoję savo planšetę, turėtumėte būti tikri, jog viskas taip ir liks. Pateikiame keletą veiksmy, kuriuos atlikę ilgainiui apsaugosite savo planšetę.

- Niekada nebandykite įsilaužti į savo paties planšetinį kompiuterį arba nulaužti jo sistemą. Taip galima apeiti daugybę saugumo kontrolės priemonių, kurios taps neveiksmingomis, todėl jūsų planšetinis kompiuteris taps neatsparus įsilaužimams.

## Jūsų naujos planšetės apsauga

- Parsisiųskite tik tas programėles, kurių jums iš tiesų reikia ir tik iš patikimų šaltinių. Programėles iPad planšetiniam kompiuteriui parsisiųskite naudodami iTunes. Prieš išleidžiant šias programėles, jas nuskenuoja Apple įmonė. Besinaudojantiems Google paslaugomis, rekomenduojame programėles parsisiųsti iš Google Play, o Amazon planšetinių kompiuterių vartotojai gali apsilankyti Amazon Appstore. Programėles galite parsisiųsti ir iš kitų svetainių, tačiau jos nėra tikrinamos, todėl gali būti užkrėstos. Galiausiai, nepriklausomai nuo to, iš kur gaunate programėlę, rekomenduojame ją ištrinti iš planšetinio kompiuterio, kai jums jos jau nebereikės arba kai jos aktyviai nebenaudosite.
- Įdiegdami naują programėlę, įsitikinkite, jog peržiūrėjote ir nustatėte privatumo nustatymus, kaip tai įprastai darote konfigūruodami pradinius savo naujojo planšetinio kompiuterio nustatymus. Atidžiai stebėkite, prie ko leidžiate jungtis kiekvienai programėlei. Pavyzdžiui, ar jūsų parsisiųstai programėlei tikrai reikia gauti prieigą prie jūsų draugų ir kontaktinės informacijos? Jei jums nepatinka programėlės leidimų reikalavimai, paieškokite kitokios programėlės, kuri tenkintų visus jūsų poreikius. Be to, reguliariai tikrinkite ar nepasikeitė nustatyti leidimai.

Jūsų planšetė yra galinga priemonė, todėl norime, kad mėgautumėtės jos naudojimu. Tiesiog prisiminkite, kad šie keli paprasti veiksmai ilgai saugos ne tik jus, bet ir jūsų naująją planšetę.

## SUŽINOKITE DAUGIAU

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

### Šaltiniai

- Saugus mobilių aplikacijų naudojimas: <https://www.securingthehuman.org/ouch/2015#january2015>
- Slaptafrazės: <https://www.securingthehuman.org/ouch/2015#april2015>
- Saugus Debesijos naudojimas: <https://www.securingthehuman.org/ouch/2014#september2014>
- Mobilaus įrenginio naudojimo pabaiga: <https://www.securingthehuman.org/ouch/2014#june2014>
- SANS dienos saugumo patarimas: [https://www.sans.org/tip\\_of\\_the\\_day.php](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](mailto:ouch@securingthehuman.org).

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



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/securethehuman](https://securethehuman)



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



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