5 modulis – 2 pamoka

**APSAUGOK SAVE SOCIALINIUOSE TINKLUOSE**

# *12 paprastų dalykų, kuriuos galite padaryti, kad būtumėte saugesni internete*

## **Neil J. Rubenking, Jill Duffy**

2021 metai, kovo mėnesio 19 diena

https://uk.pcmag.com/antivirus/94680/12-simple-things-you-can-do-to-be-more-secure-online

**1. Įdiek antivirusinę programą ir nuolat ją atnaujink**

Tokią programinę įrangą vadiname antivirusine, tačiau apsisaugojimas nuo tikrųjų kompiuterinių virusų yra tik nedidelė jos veiklos dalis. Vieni virusai užšifruoja tavo failus ir reikalauja sumokėti už jų atkūrimą. „Trojos arklių“ programos atrodo kaip tinkamos, tačiau slapta jos vagia tavo asmeninę informaciją. Veiksminga antivirusinė programa apsaugo nuo šių ir daugelio kitų rūšių kenkėjiškų programų.

Teoriškai gali nustatyti ir pamiršti antivirusinę apsaugą, leisti jai veikti fone, atsisiųsti atnaujinimus ir pan. Praktiškai turėtum kartkartėmis ją peržiūrėti. Dauguma antivirusinių programų rodo žalią banerį arba piktogramą, kai viskas gerai veikia. Jei atidarius programą pamatysi geltoną arba raudoną piktogramą, vadovaukis instrukcijomis, kad viskas vėl pradėtų veikti.

Nesvarbu, ar pasirinkai paprastą antivirusinę programą, ar visą saugumo priemonių rinkinį, kasmet turėsi jį atnaujinti. Geriausia, jei padarysi automatinė programos atnaujinimą. Naudojant kai kuriuos saugumo produktus, taip galima gauti garantiją, kad nebus kenkėjiškų programų. Vėliau visada gali atsisakyti, jei kiltų noras išbandyti kito gamintojo antivirusinę programą.

## **2. Kiekvienam prisijungimui naudok unikalius slaptažodžius**

Vienas iš lengviausių būdų, kaip įsilaužėliai pavogia informaciją, yra iš vieno šaltinio gautas naudotojo vardas ir slaptažodis. Vėliau gauta kombinacija yra išbandoma kituose šaltiniuose. Pavyzdžiui, įsilaužėliai gavo tavo vartotojo vardą ir slaptažodį ir įsilaužė į el. paštą. Jie gali bandyti prisijungti prie bankininkystės svetainių arba pagrindinių internetinių parduotuvių naudodami tą patį vartotojo vardo ir slaptažodžio derinį. Geriausias būdas užkirsti kelią vieno duomenų saugumo pažeidimo domino efektui - kiekvienai savo internetinei paskyrai naudoti stiprų, unikalų slaptažodį.

Sukurti unikalų ir stiprų slaptažodį kiekvienai paskyrai - ne žmogaus darbas. Todėl naudok slaptažodžių tvarkyklę. Keletas labai gerų slaptažodžių tvarkyklių yra nemokamos, o norint pradėti jomis naudotis, reikia nedaug laiko. Tačiau mokamos slaptažodžių tvarkyklės paprastai turi daugiau funkcijų.

Kai slaptažodžių tvarkyklė atrakinama, prisijungi prie savo interneto paskyras automatiškai. Tai ne tik padeda užtikrinti didesnį tavo saugumą, bet ir padidina efektyvumą bei produktyvumą. Daugiau nebegaiši laiko prisijungimams įvesti.

**3. Įsigyk VPN ir naudokis juo**

Kiekvieną kartą, kai jungiesi prie interneto naudodamasis tau nepriklausančiu "Wi-Fi" tinklu, turėtum naudoti virtualųjį privatųjį tinklą (VPN). Pavyzdžiui, nueini į kavinę ir prisijungi prie nemokamo "Wi-Fi" tinklo. Tu nieko nežinai apie to ryšio saugumą. Gali būti, kad kas nors kitas tame tinkle, tau nežinant, gali peržiūrėti arba pavogti tavo kompiuterio ar mobiliojo telefono siunčiamus failus ir duomenis. „Wi-Fi“ ryšio savininkas gali būti sukčius, kuris nemokamą prieigą naudoją apgaudinėjimams. VPN šifruoja tavo interneto srautą, nukreipdamas jį per VPN bendrovei priklausantį serverį. Tai reiškia, kad niekas, net nemokamo "Wi-Fi" tinklo savininkas, negali sužinoti tavo duomenų.

Naudojant VPN taip pat paslepiamas tavo IP adresas. Reklamuotojai ir sekimo programos, norinčios nustatyti tavo tapatybę arba geografinę vietą pagal šį IP adresą, vietoj to matys VPN bendrovės adresą. Savo buvimo vietos suklastojimas naudojant VPN serverį kitoje šalyje taip pat gali padėti atrakinti turinį, kuris nėra prieinamas tavo regione. Žvelgiant rimčiau, žurnalistai ir aktyvistai represinėse šalyse jau seniai naudoja VPN technologiją, kad galėtų saugiai bendrauti.

Taigi, jei jungiesi per "Wi-Fi" - nesvarbu, ar tai būtų nešiojamasis kompiuteris ar telefonas - tau tikrai reikia VPN. Jei niekada anksčiau nesi naudojęsi VPN arba ši technologija tau atrodo šiek tiek neįkandama, prieš prisijungdamas prie bet kokių svetainių palauk, kol prisijungsi prie saugaus ryšio.

**4. Naudok dviejų veiksnių autentifikavimą (jeigu jis siūlomas)**

Dviejų veiksnių autentifikavimas gali būti varginantis, tačiau dėl jo tavo paskyros tampa saugesnės. Dviejų veiksnių autentifikavimas reiškia tai, kad norint patekti į savo paskyras, reikia pereiti ne tik vartotojo vardą ir slaptažodį, bet ir kitą autentifikavimo lygį. Jei paskyroje esantys duomenys ar asmeninė informacija yra slapti ar vertingi ir paskyroje siūlomas dviejų veiksnių autentifikavimas, turėtum jį įjungti. "Gmail", "Evernote" ir "Dropbox" - keli internetiniai puslapiai, kuriose siūlomas dviejų veiksnių autentifikavimas.

**5. Naudok slaptažodžius, net jei jie neprivalomi**

Taikyk slaptažodžių užraktą visur, kur tik įmanoma, net jei jis neprivalomas. Pagalvok apie visus savo išmaniajame telefone esančius asmeninius duomenis ir ryšius. Būti be kodų užrakto sunkiai įsivaizduojama.

Daugelyje išmaniųjų telefonų numatytasis nustatymas - keturių skaitmenų PIN kodas. Neapsistok ties tuo. Naudok biometrinį autentifikavimą, kai tai įmanoma ir nustatyk stiprų prieigos kodą, o ne kvailą keturženklį PIN kodą. Nepamiršk, slaptažodis turi būti stiprus!

**6. Skirtingoms paskyroms naudok skirtingus el. pašto adresus**

Žmonės, kurie yra ir labai organizuoti, ir metodiški savo saugumo atžvilgiu, dažnai skirtingiems tikslams naudoja skirtingus el. pašto adresus, kad su jais susijusios internetinės tapatybės būtų atskirtos. Jei į paskyrą, kurią naudoji tik socialiniams tinklams, ateina apgaulingas el. laiškas, kuriame teigiama, kad jis yra iš tavo banko - jis netikras.

Daugelyje svetainių tavo el. pašto adresas prilyginamas tavo naudotojo vardui, tačiau kai kuriose gali pasirinkti savo naudotojo vardą. Apsvarstyk galimybę kaskart naudoti kitą naudotojo vardą - juk tavo slaptažodžių tvarkyklė jį įsimena! Dabar kiekvienas, bandantis patekti į tavo paskyrą, turi atspėti ir naudotojo vardą, ir slaptažodį.

**7. Išvalyk interneto talpyklą**

Niekada nenuvertink, kiek daug apie tave žino naršyklės talpykla. Išsaugoti slapukai, išsaugotos paieškos ir žiniatinklio istorija gali rodyti namų adresą, informaciją apie šeimą ir kitus asmeninius duomenis.

Norėdamas geriau apsaugoti šią informaciją, kuri gali slypėti jūsų žiniatinklio istorijoje, būtinai reguliariai ištrink naršyklės slapukus ir išvalyk naršyklės istoriją. Tai paprasta. "Chrome", "Edge", "Firefox", "Internet Explorer" arba "Opera" tiesiog paspausk Ctrl+Shift+Del, kad atsidarytų langas, kuriame galėsi pasirinkti, kuriuos naršyklės duomenų elementus nori išvalyti.

**8. Išjunk naršyklėse funkciją „Išsaugoti slaptažodį“**

Apskritai, ką apie tave gali žinoti naršyklė, daugumoje naršyklių yra integruotas slaptažodžių valdymo variantas. Tačiau mes, PCMag, jų nerekomenduojame. Manome, kad slaptažodžių apsaugą geriausia palikti slaptažodžių tvarkykles kuriantiems ekspertams.

Daugiau gali skaityti pateiktame straipsnyje :)