4.

APSAUGOKITE SAVO VIRTUALIAS VERTYBES

Panašiai kaip jūs rūpinatės savo vertingais daiktais namuose, jūs turėtumėte tą patį daryti ir su savo virtualiai saugoma informacija, ar tai būtų jūsų finansiniai įrašai, jūsų paso skenuotos nuotraukos ar netgi jūsų adresas ir telefono numeris. Visuomet verta pagalvoti, kur jūs saugosite vertingą asmeninę informaciją ir kaip jūs galite ją apsaugoti.

Ištrinti kažką nedidelio yra labai patogu, jei gerdami kavą jūs tiesiog norite padaryti keletą greitų patobulinimų. Susirasti konkrečią informaciją, kuri guli jūsų elektroninio pašto ar kitose paskyrose ir po to ją ištrinti: nuskenuota jūsų tapatybės kortelė, banko duomenys ar jūsų sveikatos draudimo informacija, t.t. Jei šių duomenų jums reikės vėliau, jūs visuomet galite juos parsisiųsti arba atsispausdinti prieš ištrindami juos iš savo elektroninio pašto paskyros.

Giluminis valymas yra kruopštesnis procesas. Jis turėtų būti atliekams maždaug kartą per metus. Suarchyvuokite viską, ką turite sukaupę savo elektroninio pašto ar socialinų tinklų paskyroje, parsisiųskite visa tai į savo kompiuterį ir ištrinkite savo paskyros turinį, kad vėl galėtumėte „pradėti viską iš naujo“.

Patarimas: Vien ištrinti nepakanka – jūs dar turite ištuštinti šiukšliadėžę ir pažalinti laikinus failus!

Jūs patys turite nuspręsti, ar norite turėti savo archyvo ir dokumentų atsarginę kopiją debesyje, išsaugoti visa tai išoriniame kietajame diske ar USB atmintuke. Nepriklausomai nuo to kaip jūs tai saugosite, įsitikinkite, kad viso to neprarasite, kad pasirinkote stiprų slaptažodį, kuris jums kažką reiškia.

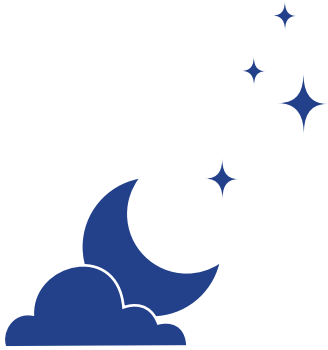
5.

PERDUOKITE TAI KITIEMS

Nors apie tai dažnai užmirštame, žiniatinklis (angl. web) taip yra pavadintas ne be pagrindo. **Mus visus internete jungia** įvairūs tinklai. Esame ne vien tik „draugai“ socialiniuose tinkluose, bet taip pat esame susieti ir per kontaktus mūsų elektroninio pašto paskyrose bei per nuotraukas, kuriomis dalijamės.

Kai imsite valyti savo elektroninio pašto ir socialinių tinklų paskyras, pagalvokite, ką dar jūs galėtumėte parsisiųsti ir po to ištrinti, siekiant padėti jūsų draugams ir bendradarbiams. Pvz., jūsų sesers banko duomenis, užrakto kodą patekimui į jūsų biurą, galbūt jūsų sūnaus paso skenuotą nuotrauką, – visa tai yra tik keletas pavyzdžių, kas galėtų sukelti tikrą galvos skausmą, jei netikėtai patektų į blogas rankas.

Perduokite tai kitiems! Jūsų skaitmenį saugumą galima sustiprinti tesiog atliekant keletą paprastų pagrindinių veiksmų. Pasidalinkite šiuo Duomenų detoksikacijos (Data Detox) patarimų rinkiniu su savo draugais, šeimos nariais, kolegomis. Galbūt tai padės jiems pakeisti savo įpročius taip, kaip tai jiems atrodo prasminga.



DATA DETOX KIT

PAKEISKITE NUSTATYMUS

kad apsaugotumėte savo nuomenis

Jei internetas būtų vien tik vieta, kur žmonės keičiasi šunų, vilkinčių dinozaurų kostiumus, nuotraukomis, slaptažodžių poreikis nelabai būtų ir juntamas. Tačiau internetas yra ta vieta, kur jūs apmokate sąskaitas, kur patalpinami jūsų vaistų receptai ir kur jūs registruojatės rengdamiesi balsuoti rinkimuose.

Gerai pagalvojus apie visas jūsų „virtualias vertybes“, kurios pasiekiamos interneto pagalba ir kurias jūs saugote savo įrenginiuose – **argi jūs neturėtumėte jų laikyti taip pat saugiai kaip ir savo piniginės ar raktų?**

Vienas ir paprastų būdų užkirsti kelią kitiems lengvai pasiekti jūsų virtualias vertybes – **tai neleisti jiems lengvai nuspėti jūsų slaptažodžių**. Daugybei žmonių net nereikia specialių techninių įgūdžių, kad patektų į jūsų paskyras – jie tiesiog pamėgina keletą kartų atspėti jūsų slaptažodžius ar paleidžia automatinę programą.

Kuomet jie jau gali patekti į jūsų paskyrą, jie gali pamėginti panaudoti tą kompromisinį slaptažodį ir kitoms paskyroms, surinkti infomaciją apie jus ir jūsų įpročius, perimti jūsų sąskaitas ar netgi pasinaudoti jūsų skaitmenine tapatybe.

Analizuodami šiuo Duomenų detoksikacijos (angl. Data Detox) rinkiniu jūs išmoksite praktinių veiksmų savo saugumui internete sustiprinti.

Taigi pradėkime!

A product of TACTICAL TECH

Supported by Firefox

Lietuvos bibliotekininkų draugija

datadetoxkit.org
#datadetox

1.

UŽRAKINKITE SAVO SKAITMENINES DURIS

Ekrano užraktai: slaptažodis, derinys, piršto antspaudas ar veido atpažinimo funkcija, kuria jūs naudojatės norėdami patekti į savo įrenginį, yra tam tikra **geriausia jūsų apsauga** nuo tų, kurie galėtų būti suinteresuoti patekti į jūsų įrenginį. Tačiau šių priemonių yra daugybė ir kartais gali būti sunku išsirinkti, kuri jums yra tinkamiausia.

Bet koks jūsų telefono, planšetės ar kompiuterio užraktas suteikia tam tikrą apsaugą ir yra geriau negu nieko. Panašiai, kaip ir durų spynų atveju, **kai kurie ekrano užraktai yra stipresni už kitus.**

Iš visų čia paminėtų užraktų ilgi, unikalūs slaptažodžiai yra stipriusi. Tai reiškia, kad, jeigu jūs naudojate slaptažodį savo įrenginiui atrakinti, jis turi susidėti iš raidžių, skaičių ir specialių simbolių.

Sakykime, jūs savo telefoną atidarote tiesiog perbraukdami per ekraną. Jūs galite padidinti jo saugumą nustatydami ilgą slaptažodį. Ar galbūt jūs naudojate kažkokį derinį? Galbūt tuomet vertėtų jį prailginti? Jūsų slaptažodis yra 1234? Gal tuomet tiesiog vertėtų mesti kauliuką septynis kartus ir įsiminti tą slaptažodį?

2.

ĮSILEISKITE TINKAMĄ

Sukurti puikų slaptažodį yra lengva. Jums tiesiog reikia laikytis keleto pagrindinių principų. Jūsų sklaptažodžiai turėtų būti:

Ilgi: **jie turi susidėti iš ne mažiau kaip aštuonių simbolių. Dar geriau būtų 16-20 simbolių.**

Unikalūs: **kiekvienai svetainei naudojami slaptažodžiai turėtų būti skirtingi.**

Parenkami atsitiktinai: **jūsų slaptažodžiai neturėtų būti kažkokie loginiai deriniai, kuriuos lengva nuspėti. Čia jums gali labai padėti slaptažodžių generatorius (angl. password manager).**

Stipriausiuose slaptažodžiuose naudojamos raidžių, skaičių ir specialių simbolių kombinacijos. Šis laiko išbandytas patarimas padeda sukurti stipresnius, sunkiau nuspėjamus slaptažodžius. Tenka apgailestauti, kad kai kurios slaptažodžių sistemos neleidžia naudoti tam tikrų specialių simbolių (pavyzdžiui, @#$%-=+), tačiau ilga raidžių ir skaičių kombinacija vistiek yra geriau nei trumpa.

Idealiu atveju jūs turėtumėte naudoti **slaptažodžių generatorių**, kuris jums sugeneruos slaptažodžius ir visus juos saugos. Slaptažodžių generatoriai, tokie kaip 1Password ir KeePassXC, rekomenduojami saugos ekspertų, iš esmės yra programėlė, kurios vienintelis tikslas yra apsaugoti jūsų kredencialus ir kitus jautrius duomenis.

3.

PRIDĖKITE ANTRĄ UŽRAKTĄ

Dviejų veiksnių atpažinimo (2FA) arba daugialypio atpažinimo (MFA) sistemos nustatymas reiškia, kad net jei kažkas ir suras jūsų slaptažodį, **jie greičiausiai neturės reikiamo papildomo veiksnio, kad galėtų patekti į įrenginį.**

Pmėginkite pasižiūrėti į jūsų dažniausiai naudojamos svetainės saugumo nustatymus ir programėles, ar nėra galimybės sukurti tokį papildomą užraktą. Pradėkite nuo pačių svarbiausių – finansinių programėlių ar paslaugų, tokių kaip elektroninis paštas, kurias jūs naudojate norėdami atkurti kitas savo paskyras.

Google:
Sign in to: myaccount.google.com →
Security →
2-Step Verification →
Get Started

Facebook:
Menu →
Settings →
Security and Login →
Use Two-factor Authentication

Patarimas: Kuriant kitą patikrinimo sluoksnį, jums reikės rasti būdą patvirtinti, kad tai jūs. Venkite naudoti SMS (į jūsų telefono numerį atsiunčiamas teksto žinutes) kaip antrąjį veiksnį, jei netikėtai pamestumėte savo telefoną. El.paštas paprastai yra patikimesnis variantas.