

## Uus turvatähelepanek: liiga tihti paroolide vahetamine on tegelikult halb

18. august 2016 - 0:22 Autor: [Kaido Einama](#)



Üks põhilisi mantraid, mida küberturvaekspertid on pidevalt korranud, kõlab nii: "...ja oma salasõna pead sa tihti ja regulaarselt vahetama." Uusimate tõdemuste järgi aga ei pea - selgub, et väga tihe vahetamine ja selle nõudmine muudab paroolid hoopis nõrgemaks.

USA Riikliku kaubanduskomisjoni "peatehnoloog" Lorrie Cranor esines hiljutisel turvakonverentsil Las Vegases, rääkides turvalistest salasõnadest ning soovitas hoopis vastupidist: mitte vahetada väga tihti oma salasõnasid. Põhjus on lihtne - kui nõuda paroolide pidevat vahetamist, hakkavad inimesed neid muutma mingi kindla (äraarvatava) skeemi järgi, sest iga kord millegi täiesti suvalise, raskesti meelde jääva tähekombinatsiooni väljamõtlemine on tavainimese jaoks võimatu. Selline parool ei jää meelde ja kui kasutatakse kõigi nõutud turvareeglite järgi, siis kirjutatakse see uus keeruline parool lihtsalt üles, mis on jälle turvarisk. Või luuakse kindel süsteem: muudetakse üht numbrit paroolis, üht tähte jne. Selline muster aga aitab häkkeril samamoodi tulevasi parooli lihtsalt ära arvata, isegi kui vana parool on lekkinud ja kasutaja on võtnud kasutusele uue, äraarvatava mustriga tuletatud väike tunnusõna.

FTC IT-juht ei pea enam heaks nõuandeks muuta salasõna iga 60 päeva järel. Loomulikult tuleb parooli muuta kohe, kui kuskil saidil on turvaleke ja kui sama parooli kasutati ka mujal sisselogimiseks, kuid liiga tihti pole vaja muutmist nõuda.

Lorrie Cranor [kirjeldab blogis](#), kui lihtne oli testi käigus kasutajate uusi parooli vana salasõna põhjal ära arvata:

- 17% kasutajatest tarvitasid selliseid lihtsaid skeeme, mille äraarvamiseks kulus vaid 5 proovimist
- 41% kontodest olid lahtimurtavad tuletamise teel uue parooli äraarvamise esimese kolme sekundi jooksul

### **Millal parooli vahetada?**

Cranor soovib: vaheta parooli nii harva kui võimalik. Niipea, kui tekib kahtlus, et parool võib olla lekkinud, tuleks see ära vahetada - sisselogitavas süsteemis ja igal pool mujal, kus on kasutusel sama või sarnane salasõna.

- Vaheta, kui oled seda jaganud oma sõbra või tuttavaga;
- Vaheta, kui keegi piilus parooli sisestamise ajal üle sinu õla;
- Vaheta, kui tundub, et sisestasid parooli kogemata valel leheküljel (nt võimalikult õngitsemis-saidil);
- Vaheta, kui tundub, et parool on liiga nõrk;

Igal juhul tasub mõelda sellele, kas ja kui tihti sundida kasutajaid oma salasõnu muutma ning alati on turvalisem leida mõistlik kompromiss. [Üks hea koomiks](#) illustreerib hästi, miks on raskesti meelde jääv salasõna teinekord kergesti masina poolt äraarvatav ja kuidas kergesti meelde jääv salasõna on praktiliselt lahtimurdmatu.

[Vaata lähemalt sellest bogist.](#)

- [Uudised](#)
- [Turvalisus](#)