

# Kuidas hoida oma kontosid ja seadmeid turvalisena

6 years tagasi Autor: [Marko Habicht](#)

Internetiturvalisus ja oma seadmete ning kontode kaitsemine on muutunud üha aktuaalsemaks. Veebi vahendusel jagatakse tänapäeval väga palju tundlikku informatsiooni ning on äärmiselt oluline seda kõike teha turvaliselt.

Eilse järjekordse paroolide lekkimise teate valguses annab Tele2 Eesti klienditeenindusdirektor Sirli Seliov kolm nõuannet, kuidas oma kontosid turvaliselt hallata ja hoida.

## **Vali tugev parool ning vaheta seda regulaarselt**

- Mida tugevam on parool, seda raskem on seda suvalise genereerimise abil lahti murda. Kindlasti tuleks parooli panemisel järgida seda, et see poleks lihtsasti äraarvatav numbrikombinatsioon nagu 1234 või 1111.
- Samuti ära kasuta parooliks andmeid, mida teistel võib olla lihtne ära arvata. Selle alla kuuluvad nii sünnipäev, lähedase nimi kui ka tuntud tähekombinatsioonid klaviatuuril.
- „Üldiselt peetakse tugevaks parooliks 12-15 numbrite ja tähtede kombinatsiooni, mis sisaldab nii suuri kui väikseid tähi ning mitte kõrvuti asetsevaid numbreid,“ soovitas Seliov.
- Kaval lahendus on kasutada nõ sõnalist koodi. Selleks tuleb valida meeldejääv sõna – konkreetset sõna on lihtsam meeles pidada kui suvalist numbrikombinatsiooni. Näiteks sõnale “koer” vastavad mobiiltelefoni klaviatuuris numbrid 5(jkl) 6(mno) 3(def) 7(pqrs). Seega tuleb PIN koodiks 5637 ja seda on alati lihtne märksõna abil meelde tuletada.

## **Kõige olulisem on aga parooli lihtsalt regulaarselt vahetada. See on üks lihtsamaid võimalusi, millega hoida oma kontod kaitstud.**

- Ära kirjuta oma parooli arvutile või kanna neid kaasas rahakotis
- See käib nii arvuti, erinevate kontode, pangakaartide, telefoni kui ID-kaardi ja mobiili-ID kohta. Eriti viimase kahe, sest nende abil võib pahatahtlik inimene ellu viia erinevaid identifitseerimist vajavaid tehinguid ilma sinu teadmata.
- „Siin ei ole muud lahendust, kui õppida paroolid lihtsalt pähe,“ rääkis Seliov. Samuti soovitas Tele2 klienditeeninduse direktor kasutajale võtta ka seadmete ja kontode endi poolt pakutavad mitmeastmelised tuvastamise võimalused. „On mitmeid seadmeid, kus saab lisaks paroolile kasutada sõrmejälge või näotuvastust ning veebilehti, mis võimaldavad salasõnale lisaks seadistada mobiili abil teostatava sisselogimise.“

## **Ära jaga faile avalikus WiFis**

- Kui oled avalikus WiFi võrgus, siis lülita andmete jagamine ja AirDrop välja. Kui sa aga parasjagu interneti oma seadmes ei vaja, siis parem oleks WiFi üldse välja lülitada.

Seliovi sõnul ei pea avalikus WiFis olemist ei pea paaniliselt kartma. Küll aga ei soovita selle kaudu jagada tundlikku informatsiooni või tähtsaid faile.

## **Arvutimaailma toimetuse kommentaar**

- Parool peab olema selline, mis jääb meelde! Näiteks lemmik laulu värsike "Pagari posi piparkook1", "Juuli kuus lumi on maas83" Paljud kohad soovivad ja genereerivad suvalisi kombinatsioone, kuid neid on keeruline meelde jätta ning seda enam jõuavad need paberitükkidele. Osad soovivad suuri ja väikseid tähti ning numbreid, mis meie pakutud paroolis on täidetud. Ainus mis võib probleemiks esineda on tühikud, mida osad portaalid ei toeta.
- Kasuta erinevaid parooli. Sarnaselt eelmisele punktile on võimalik luua palju erinevaid parooli, neid endale mugavalt seostada ning paremini meelde jätta. Parooli lekete peamine probleem ei tulene mitte paroolide lihtsusest või keerukusest vaid sellest et sama parooli ja kasutajanime kasutatakse mitmes kohas. Kui igal pool on erinev parool, siis ühest kohast lekkimisel ei ole tarvis muretseda teiste kohtade turvalisuse pärast.

Eilse paroolide lekkimise kohta saad lugeda Geeniusest. <https://geenius.ee/uudis/215-000-eesi-kasutaja-parooliga-andmebaas-on-nuud-netis-avalatud-ja-otsitav/>

Geeniuse reastas ka kõige populaarsemad paroolid.

1. 123456 (1123 kontot kasutas seda parooli)
2. parool (311)
3. qwerty (298)
4. LZhan1689 (295)
5. 123456789 (218)
6. 12345 (158)
7. lammas (156)
8. minaise (137)
9. maasikas (135)
10. kallid (116)
11. killer (112)
12. samsung (110)


13. 123123 (109)
14. armastus (108)
15. lollakas (105)
16. teretere (103)
17. 12345678 (99)
18. asdasd (96)
19. lilleke (95)
20. 1234 (88)

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

Pilt

*Search through 1.4 billion leaked accounts*

# Gotcha?



**Is your password stolen?**

Linkedin, Yahoo, Dropbox and [many others](#) got hacked, and a list of 1.4 billion accounts is diligently copied around the Internet. Now it is time to check what they have got on you — and change your passwords today. Search for a **full email address** or a **domain name**.

See the [Estonia](#) numbers. Or try, for example, these organizations:

- [Postimees](#)
- [Eesti Rahvusringhääling](#)
- [Swedbank](#)
- [Tallinna Tehnikaülikool](#)
- [Justiitsministeerium](#)
- [Kaitseväge](#)
- [NATO Cyber Defence](#)