

Viis nippi, kuidas enda kasutajakontosid häkkimise eest kaitsta

5. august 2019 - 13:33 Autor: [AM](#)



Peame regulaarselt kandma hoolt selle eest, et nutiseadmete turvalisus oleks tagatud. Viiest nipist, kuidas enda kasutajakontosid pahalaste eest kaitsta, kirjutab Tele2 klienditeenindusdirektor Sirli Selio.

1. Vaheta kord kvartalis paroole

Tihti kasutame mugavuse tõttu paljude erinevate kontode puhul ühte ja sama salasõna. Kui aga kasvõi ühe sellise konto kasutajanimi ja parool lekkima peaks, on häkkeritel lihtne sisse pääseda ka kõigile teistele kontodele, kus sama parooli kasutanud oled. Seega uuenda enda paroole regulaarselt ning ürita iga konto puhul erinevat kasutada. Kui paroolide meeles pidamine tundub liiga keeruline, siis võid kasutada rakendusi, mis aitavad uusi ja turvalisi salasõnasid luua ning neid meeles pidada, näiteks äppe LastPass ja KeePass.

2. Tutvu salvestatud rakenduste õigustega

Uusi rakendusi alla laadides saad nii Google Play kui ka App Store'i rakendusepoes tutvuda infoga, millele äpp ligipääsu küsib. Kuigi kasutamistingimustega tutvumine on pealtnäha tüütu samm, mis sageli vahele jäetakse, tasub seejuures siiski tähelepanelik olla ning küsitav info hoolikalt läbi lugeda. Kahtlane on näiteks see, kui taskulambirakendus küsib ligipääsu sinu kontaktidele – tegemist võib olla nuhkvara-äpiga, mis kogub sinu isiklikke andmeid või nakatab telefoni pahavaraga. Kui tahad kontrollida, millisele infole sinu telefonis rakendustel ligipääs on, saad seda teha telefoni seadete alt.

3. Kontrolli seadmeid, kuhu oled sisse logitud

Kui oled kasutanud sotsiaalmeediat või lugenud meile seadmete kaudu, mis ei ole sinu enda telefon, arvuti või tahvelarvuti, tasub aeg-ajalt kontrollida, kuhu parasjagu sisse logitud oled. Seda saad teha näiteks enda Facebooki, Google'i või Instagrami konto turvalisuse (*security*) seadete alt ning seekaudu ka soovimatutest kohtadest ennast välja logida.

4. Uuenda regulaarselt tarkvara

Tarkvara pideva täiendamisega parandatakse turvaauke ja võimalikke vigasid. Seega on regulaarne tarkvarauendus üks lihtsamaid viise enda seadmeid "vaktsineerida" ning häkkimise eest kaitsta. Veendu, et automaatsed uuendused on sisse lülitatud nii sinu operatsioonisüsteemil kui ka rakendustel. Kindlasti pea meeles ka kodust ruuterit, mis on esimene pahalaste ja viiruste eest kaitsev filter.

5. Väldi avalikke WiFi võrke

Kuigi avalik ja tasuta WiFi muudab elu mugavamaks, kaasneb sellega alati turvarisk ning võimalus, et jagad tahtmatult oma andmeid

kellegagi, kes neid kurjasti ära kasutab. Eriti ettevaatlik peab seejuures olema rakenduste puhul, mis ei krüpteeri andmeid piisavalt – näiteks äpi kaudu mobiilipanka kasutades või krediitkaadiga oste tehes. Seega võiks avalikes kohtades pigem kasutada telefoni andmesideühendust ehk 3G või 4G võrku ning VPN ühendust (näiteks Private Internet Access või TorGuard).

- [Lahendused](#)
- [Turvalisus](#)