5 olulist turvaviga, mida iga päev võrgus teed

8 aastat tagasi - 14.10.2017 Autor: AM

Suur hulk inimesi teeb igapäevaselt hooletusest ja teadmatusest nutiseadmeid kasutades ohtlikke turvavigu. Kui Sa ei taha, et Sinu paroolid, isiklikud pildid ja vara võõraste kätte satuvad, siis tuleks hoolitseda elementaarse küberhügieeni eest. Tele2 tootedirektor Katrin Aron toob välja viis levinumat turvaviga ja lahendust.

1. Pikka aega sama parooli kasutamine kõikjal

Ära kasuta ühte ja sama parooli mitmel kontol ja võimaluse korral vaheta parooli regulaarselt. Kuna paroole on keeruline meelde jätta, siis selle jaoks on loodud nutikaid rakendusi, näiteks LastPass ja KeePass. Sama parooli kasutamine kõikjal on võrreldav ühe võtme kasutamisega kodu, pangakonto ja auto avamiseks.

Paroolide häkkimistehnoloogia on teinud suure hüppe, pahalased kasutavad tihti näiteks sotsiaalmeedia kaudu levivat nuhkvara. Turvaline parool peaks sisaldama suuri ja väiksed tähti, numbrikombinatsioone ja soovitavalt ka sümboleid.

2. Nutitelefoni ebapiisav lukustus

Kui pahalane pääseb mööda telefoni ekraanilukust, siis on nende käes suur osa meie elust – alates isiklikest vestlustest kuni paroolide ja piltideni. Siiani ei kasuta pea 15% nutitelefonide kasutajatest mingisugust telefoni lukustamise viisi. Kuigi telefoni lukustamiseks saab valida paljude viiside vahel, on siiski klassikaline PIN-kood või parool üks turvalisemaid meetmeid. Et kaitsta telefoni sisu nuhkijate või üle õla piilujate eest võiks kasutada kuuekohalist PIN-koodi, sest seda on palju keerukam lahti muukida kui näiteks mustrilukku.

3. Kaheastmelise autentimise kasutamata jätmine

Kui paroolid ja kasutajatunnused võivad lekkida, siis kaheastmeline autentimine on tavalisest paroolist oluliselt turvalisem lahendus. Kõige tüüpilisem on juhuslikult genereeritud kood, mis saadetakse SMS-iga kinnitamiseks kasutaja telefonile. Suuremad teenusepakkujaid võimaldavad kaheastmelist autentimist, näiteks Facebook, Instagram, Twitter, Google, Apple, Microsoft, Amazon ja Dropbox.

4. Liigse info jagamine

Kogu informatsioon, mida sa internetis jagad, võib osutuda heaks abimaterjaliks häkkeritele. Nii võib sotsiaalmeediast leida vihjeid parooli lahtimuukimiseks kuni turvakontrolli küsimusele vastamiseks. Enne postitamist tasuks üle vaadata ka postituse sihtgrupp ehk kes sinu jagatud sisu näevad.

5. Avaliku WiFi-võrgu kasutamine

Häkkeritele ja pahalastele on avalikud WiFi-võrgud kullakaevandused, sest enamik inimesi ei kasuta turvameetmeid. Avaliku võrgu kasutamine on nutitelefonis ja sülearvutis asuvate andmetele turvarisk. Avalikus võrgus tuleks vältida panga- ja meilikontodele sisselogimist, isiklike failide jagamist, veebipoes ostlemist ja turvamata veebilehtede külastamist. Kindlasti ei tohiks automaatselt oma seadet ühendada võõraste seadmetega. Võimaluse korral tuleks kasutada VPN-ühendust ehk virtuaalset privaatvõrku või mobiilset internetti.

- Uudised

- Andmeside
- Mobiiltelefonid
- Turvalisus
- Võrguseadmed

Pilt