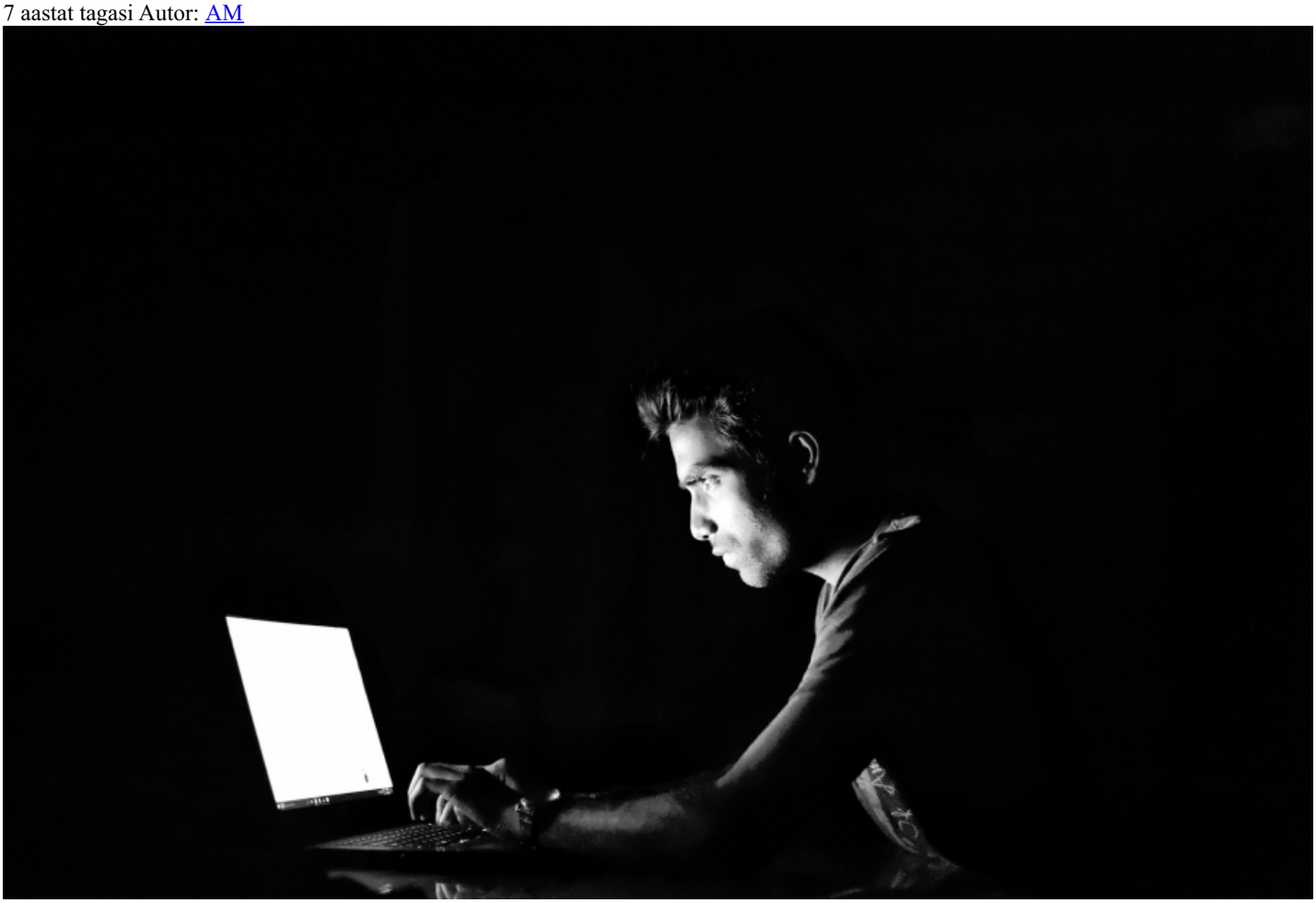
Selgita välja, kas keegi on su kontole sisse häkkinud

7 aastat tagasi Autor: AM



Oktoobris läbi viidud uuringu kohaselt on 18 protsenti eestlastest oma kaaslase telefonis nuhkinud. Peale koduste spioonide mõtlevad internetis liikuvad pahalased andmetele ligipääsemiseks välja järjest nutikamaid skeeme. Kuidas saada teada, kas võõrad silmad käivad Sinu kontodel?

Tele2 tootedirektori Katrin Aroni sõnul saab kõige lihtsamini kontrollida, kas inimese kontode andmed on lekkinud veebilehelt „Have I Been Pwned?“ - sellest lehest oleme ka AM-is juba mõned korrad kirjutanud, kui suurem häkkimistelaine ees oli.

“Samuti tasub aeg-ajalt kontrollida, kes ja millisest arvutist sinu kontol käib. Nii, nagu laseme korrapäraselt hooldada oma autot, koristame kodu või käime arsti juures, nõnda tuleks tähelepanu pöörata ka oma küberhügieenile,” ütles Aron ja tõi välja kuus võimalust oma privaatsuse kaitsmiseks.

1. Vaheta kord kuus paroole. Kui mõne olulisema konto kasutajanimi ja parool peaksid lekkima, siis võid jääda ilma nii oma rahast kui isiklikest materjalidest. Kui paroolide meelespidamine tundub keeruline, siis on olemas paroolihaldamise tarkvarad nagu LastPass ja KeePass. Need lahendused aitavad turvalisi paroole regulaarselt luua ja meeles pidada.

2. Kontrollige kontol ja seadmes toimuvat. Facebookil, Twitteril ja Google’il on võimalused hiljutiste kontoga seotud toimingute kontrollimiseks. Turvaseadete alt näeb loetelu viimastest sisselogimiskordadest ja seadmetest, millega kontole on sisenetud. Lisaks näete, millistel rakendustel on õigus teie konto infot kasutada ning neid õigusi saab ka piirata. Üldjuhul võimaldavad sotsiaalmeediakontod tellida SMSi või e-posti teel hoiatusteateid, kui keegi tundmatu proovib teie kontole siseneda või kui sisselogimiseks kasutatakse uut seadet.

3. Kontrollige salvestatud rakenduste õigusi. Nii Google Play kui ka App Store’i rakendusepoes on välja toodud, millisele infole äpp ligipääsu küsib. Tasub olla tähelepanelik, kui näiteks taskulambi-rakendus küsib ligipääsu teie kontaktidele, sest aeg-ajalt satub rakendusepoodi ka nuhkvaraäppe. Eriti hoolikas tuleb olla kolmandate tootjate rakendustega, mis ei ole saadaval ametlikes rakendusepoodides. Androidi seadmes tuleb rakenduste õiguste nägemiseks avada menüüst Settings (Seaded) ® Apps (Rakendused) ja seejärel valida soovitud rakendus ja Permissions (Load). iOSi puhul Settings ® Privacy, kust saab kontrollida igale rakendusele antud õigusi.

4. Veendu, mis programmid arvutis jooksevad. Kindlasti tasub arvutisse tarkvara laadides ja installeerides olla ettevaatlik. Aeg-ajalt peaks kontrollima, mis programmid arvutis taustal töötavad ja vaadata ka üle veebilehitseja laiendid. Loetelu parajasti aktiivsetest programmidest leiab Windowsi operatsioonisüsteemis Task Manageris ja Apple seadete puhul Activity Monitoris. Kui töötav rakendus on tundmatu, tasuks selle kohta teha veebiotsinguga kiire taustakontroll. Sarnaselt tuleks toimida ka kõigi veebilehitseja lisamoodulite ja lisanditega, mille installimist te kas ei mäleta või enam ei vaja. Näiteks Facebooki erinevad testid või aktiivsusäpid.

5. Tee ära tarkvarauuendused. Veendu, et automaatsed uuendused on sisse lülitatud nii operatsioonisüsteemil kui ka rakendustel.

Tähelepanuta ei tasuks jätta ka kodust ruuterit, kuna see on esimene filter, mis kaitseb viiruste ja pahalaste eest.

6. Kontrolli, kes on Sinu WiFi-ga ühendatud. Veebiühenduste jälgimine on lihtne ja ühendatud seadmete loetelu vaatamiseks tuleb sisse logida oma ruuteri seadistusse. Aeg-ajalt tasub muuta ka WiFi parooli (sealhulgas ka vaikimisi kehtivat ruuterisse sisselogimise administraatori salasõna). Hotellides või kohvikutes võiks avatud WiFi asemel kasutada VPN-ühendust või mobiilset internetti.

- Uudised
- Turvalisus