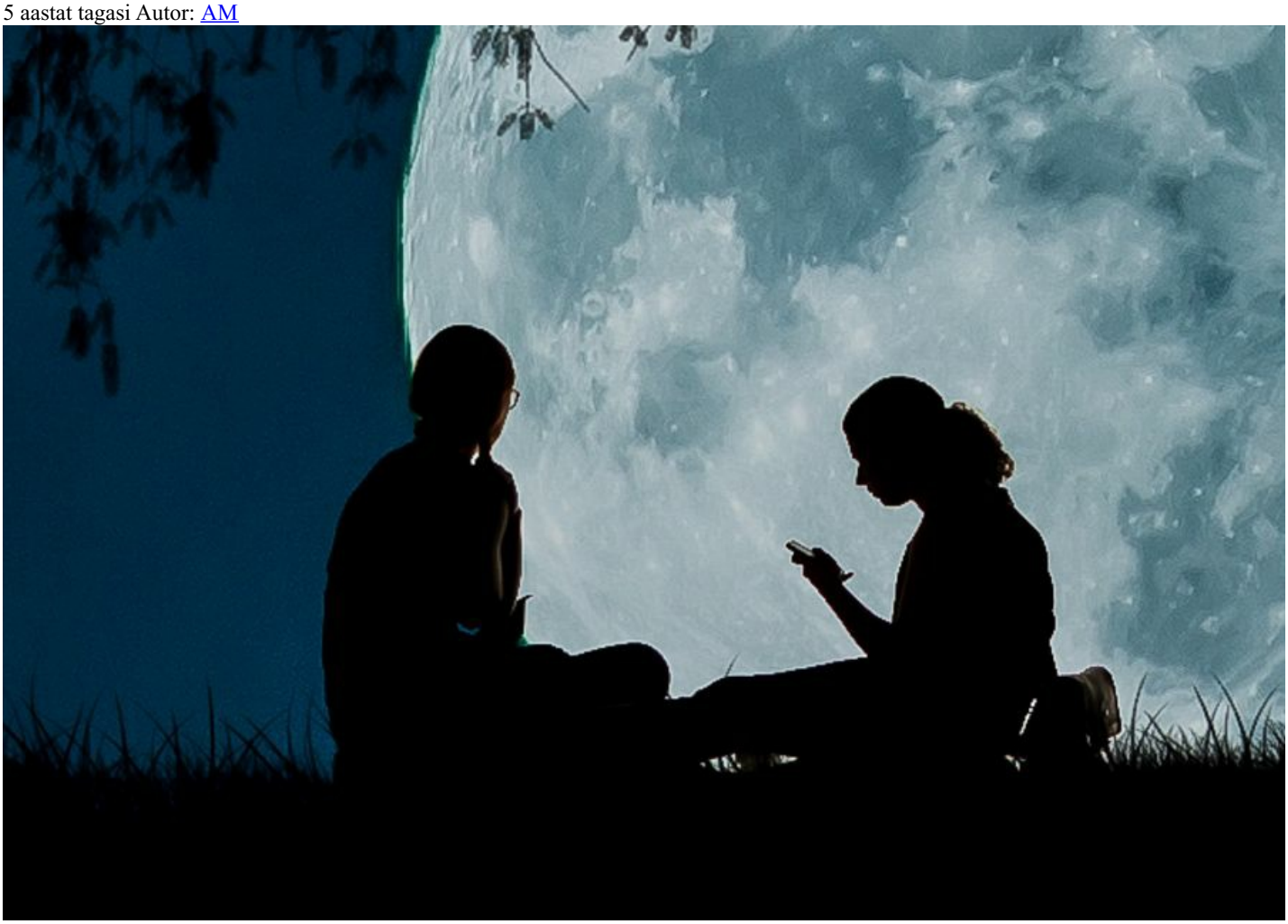
5 nõuannet digitaalse armuelu elamiseks

5 aastat tagasi Autor: AM



Kui oled lugenud Sir Arthur Conan Doyle'i Sherlock Holmesi detektiivilugusid või näinud BBC telesarju, siis on selge, et andekal detektiivil kulub vaid mõni hetk, et mõne inimese kohta üsna palju üksikasju detailide põhjal teada saada. Tänapäeval piisab mõnest sekundist ka inimestele, kes pole sellise kutsealaga seotud — Internetis on võimalik avastada kõike ja uppuda lõputusse infovoogu, mida me avalikult jagame. Me kipume olema liiga avameelsed, milles on teatavad riskid, eriti just isikliku elu paljastamisel.

Kaspersky piirkondliku uuringu andmetel, mis oli osa kampaaniast "Digitaalne pohmelus", on 31 protsendil Eesti vastajatest Facebookis avalik profiil. Risk kasvab, kui võtame arvesse, et keskmiselt 39% vastanutest möönab, et nad jagavad aeg-ajalt ka asukohti, kus nad on viibinud.

"Kui jagame avalikult juurdepääsu oma digitaalsele elule, jätame maha digitaalse jalajälje ja avaldame kogu oma intiimsuse. Seda saab võrrelda tänaval alasti kõndimisega ilma mingit kaitset omamata ja võimaldades mitte ainult oma tuttavatel, vaid ka tundmatutel inimestel, halbade kavatsustega ja emotsionaalselt ebastabiilsetel inimestel meie isiklikele asjadele juurdepääsu. See seab meid ohtu ja kutsub esile olukordi, millel võivad tekitada meie elus raskeid olukordi," selgitas Kaspersky piirkondlik esindaja Baltimaades Andis Steinmanis.

Liiga rohke isikliku teabe avaldamine Internetis võib olla vägagi ohtlik. 34% eestlastest tunnistab, et nad tavaliselt ei mõistagi, et asukoht on märgitud avalikuks ilma nende nõusolekuta, kui nad on midagi postitanud.

Selle stsenaariumi korral soovitab Kaspersky oma digitaal- ja armuelu turvamiseks järgida neid nõuandeid, mis aitavad hoolitseda oma intiimsuse eest Internetis ja vältida liigset eksponeerimist:

1. **Hoia oma sotsiaalmeedia profiilid privaatsetena** ja ära ole liiga avameelne. Hoidu postitamast oma profiilidesse liiga palju isikuandmeid. Enda postitatavad andmed võivad tunduda tähtsusetud, kuid see võib aidata kurjategijatel varastada identiteeti või luua külastatavate kohtade põhjal seaduspärasusi. Veelgi parem, kui juurdepääs piirdub väikese sõpraderühmaga.
2. **Lülita välja automaatsed asukoha määramise teenused.** Mobiilikaamera, fotoredaktor, mitmesugused digiteenused, mida kasutad foto postitamiseks, koondavad tänapäeval palju infot näiteks kohast, kus foto tehti.
3. **Pööra suuremat tähelepanu kompromiteerivate fotode ja videote hoidmisele.** Meie maine eraisikute ja paaridena on Internetis väga oluline. Sellepärast olge ettevaatlik fotode talletamisel, eriti kui need on kompromiteerivad. Pidage mõlemad meeles, et teie piltide ja videote kasutamisel võivad olla negatiivsed tagajärjed, kui need satuvad halbade kavatsustega inimeste kätte.
4. **Suhtu WiFi ühenduse kasutamisse ettevaatlikumalt.** Kui lood ühenduse traadita võrkudega, siis veendu, et kogu info oleks kaitstud. VPN-i kasutamise korral on kogu võrguliilus "toru otsteni" üle avaliku võrgu kaitstud.
5. **Kasuta usaldusväärseid turvalahendusi.** Installi vajadusel ka oma mobiilseadmesse viirusetõrjetarkvara, mis suudab kaitsta võimalike rünnakute eest.

- Uudised

- Lahendused
- Turvalisus