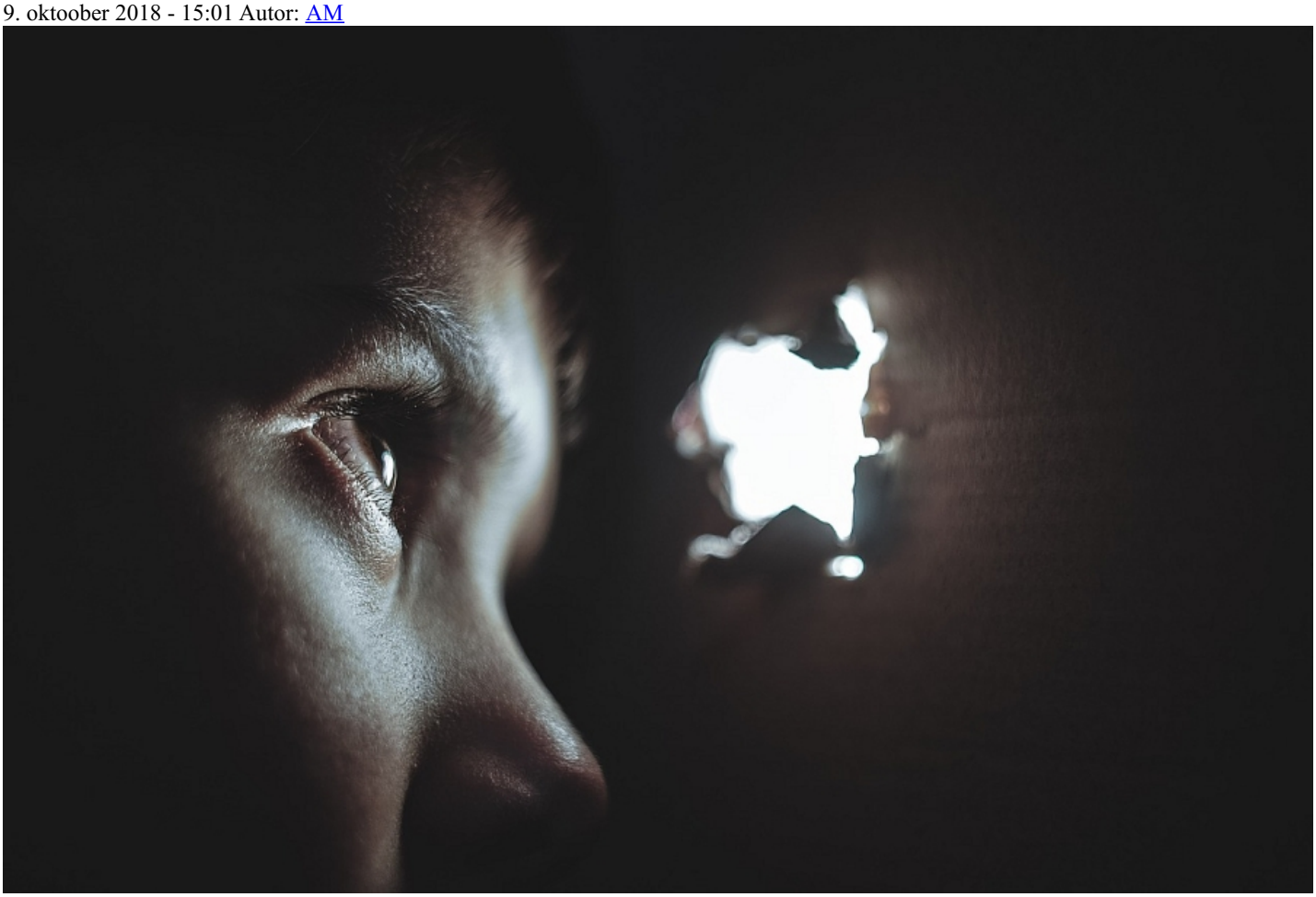
Ekspert annab nõu: kuidas end sextortion´i eest kaitsta

9. oktoober 2018 - 15:01 Autor: AM



Peaaegu keegi ei saa enam öelda, et tal pole midagi varjata. Nutitelefonidesse on salvestatud pea kogu inimese elu – paroolid, isiklikud pildid ja sõnumid. Praegu levib maailmas *sextortion*-tüüpi väljapressimiste laine, millega pahalased üritavad privaatseid pilte välja pettes või varastades raha välja pressida. Tele2 klienditeenindusdirektor Sirli Seliov selgitab lihtsaid meetodeid, kuidas oma telefon turvaliseks muuta ja sellega halvimast pääseda.

Tele2 klienditeenindusdirektori Sirli Seliovi sõnul lekivad isiklikud andmed peamiselt kahel viisil – kas inimene jagab neid ise või saab jaole pahalane: „Me anname oma nutiseadmele väga palju infot, jagades lahkelt oma asukohta, salvestades paroole ning laadides üles personaalset infot, arvestamata elementaarse turvalisusega.“

Lukusta ekraan ka lähikondsete eest

Kõige lihtsam viis oma telefoni sisu üle kontrolli kaotamiseks on ekraani lukustamata jätmine. Mullu Eestis läbiviidud uuringu kohaselt ei lukusta 38 protsenti inimestest oma telefoni ekraani ning seadme kaotuse puhul näevad kõik selle sisu.

Statistiliselt tuleb aga välja, et kõige agaramad nuhkijad on inimese enda lähedased. Elementaarseks andmekatiseks sobib seega kõik – numbriline ekraanilukk, visuaalne kombinatsioon, näotuvastus või sõrmejäljelugeja.

Kui telefon on aga kadunud või pahategija kätte sattunud, siis on julgematel võimalik ennetavalt määrata sisu kustutamine – kui telefoni püütakse vale parooliga liialt palju sisse logida või lähenetakse brutaalsema häkkimisega, siis telefon kustutab kogu oma sisu.

IPhone’il saab seda teha menüüst *Settings > Touch ID & Passcode > Erase Data*.

Androidile tuleks tõmmata selleks vastav äpp, näiteks Lost Android.

Ära jaga endast tundlikku materjali elektrooniliselt

Eestis läbiviidud küsitluse kohaselt saadavad noored endast agaralt alastipilte. Kuni 24-aastastest on seda teinud 26 protsenti ning 25-34-aastastest 12 protsenti.

“Kui suhe peaks inetult lõppema, siis võib sellisest materjalist saada kergelt kättemaksu või väljapressimise vahend,” hoiatas Seliov.

Lülita välja funktsioonid, mida sa parasjagu ei kasuta

Häkkerid on võimelised tegema asju, mida sa ettegi kujuta. Teoreetiliselt saab Bluetoothi, asukoha määramist, NFC-d, WiFit või mobiilset

andmesidet kasutada inimese tegemiste järgi nuhkimiseks või tema telefonist andmete varastamiseks.

Mõistagi me tegelikult ei lülita kõiki neid funktsioone igapäevaselt sisse-välja, aga vähemalt asukoha jagamise ja Bluetoothi osas võiks sellele tõsiselt mõelda.

Ära tõmba alla kahtlaseid äppe

Sarnaselt arvutile ei ole hea tõmmata ka telefoni tundmatuid äppe, mille sisu päris täpselt ei tea. Enne rakenduse laadimist tuleb alati kontrollida, kes on äpi looja ja arendaja. Näiteks pangaäppide puhul on loojaks pank ise ning kõikvõimalikke teisi versioone ei tohiks kindlasti alla laadida.

„Soovitan alati lugeda ka kommentaare ja jälgida rakenduse hinnangut. Näiteks on kahtlane alla tõmmata sellist Paypali laadset äppi, kus pole ühtegi tärni või kommentaari. Võimalus, et tegu on võltsäpiga, on siin väga suur," selgitas Seliov.

- Uudised

- Androidiblog
- Mobiiltelefonid
- Turvalisus