Jälle müüdi sinu andmed maha? Ekspert soovitab, kuidas enda andmetega internetis turvaliselt ümber käia

8 aastat tagasi - 10.04.2018 Autor: AM

Andmed lekivad isegi Zukerbergi firmast. Kas üldse on võimalik midagi teha? Isiklike andmete eest hoolitsemine on tänapäeval olulisem kui kunagi varem ja äsja avalikkust raputanud sotsiaalmeediamaastikul aset leidnud andmeskandaalpole esimene, selliseid jamasid on olnud ka ka minevikus. Kuidas saab siis tavaline inimene lihtsasti enda andmed kaitsta ning mida üldse on mõistlik enda kohta avaldada? Samsung Eesti tootekoolitaja Riho Kopso toob välja kõige olulisemad reeglid, mida internetiavarustes surfates järgida tasuks.

Vaata üle kasutajasätted sotsiaalmeedias

Et sotsiaalmeedias enda andmeid paremini hallata, tasub kriitilise pilguga üle käia kõik võrgustiku privaatsussätted. Sotsiaalmeediakontodel tuleks igal juhul üle vaadata, kellega täpselt enda informatsiooni jagada.

„Kõik sotsiaalvõrgustiku kasutajad ei pea ilmselt teadma, milline on inimese perekonnaseis või mis on tema telefoninumber," ütles Kopso. "Iga info, mis välja anda, on oluline teave kõikvõimalikele firmadele, kes võivad seda teile teadmata turunduseks ära kasutada."

Näiteks salvestab sõnumirakendused kasutajate kõnede ajalugu ning saadetud SMS sõnumeid juhul, kui kasutaja on selleks rakendusse esmasel sisselogimisel nõusoleku andnud.

„Kuigi kasutajad annavad selleks enda telefoninumbri sisestamisega ise nõusoleku, siis tasub taaskord kaaluda, kas sellist informatsiooni on kindlasti tarvis sotsiaalvõrgustiku kätte usaldada," soovitas Kopso.

Vali tugevad paroolid ja kaheastmeline autentimine

Selles nõustuvad absoluutselt kõik küberturvalisuse spetsialistid, et tugev parool ja selle regulaarne vahetamine on absoluutselt kõige parem viis, kuidas enda andmeid kaitsta.

„Parooli puhul tuleks valida fraas, mida on võimalikult keeruline ära arvata. Unustada tuleks kõigile tuntud väljend salasõna ning kasutada pigem salafraase ehk sõnade kogumeid, mis muudab parooli arvamise märkimisväärselt raskemaks," õpetas Kopso. "Kahjuks on viimase aja andmelekete ajal selgunud, et eestlased valivad tihtipeale parooliks klassikalise 123456, parool või qwerty. See on aga ülimalt ebaturvaline ning sama hea oleks parooli üldse mitte kasutada."

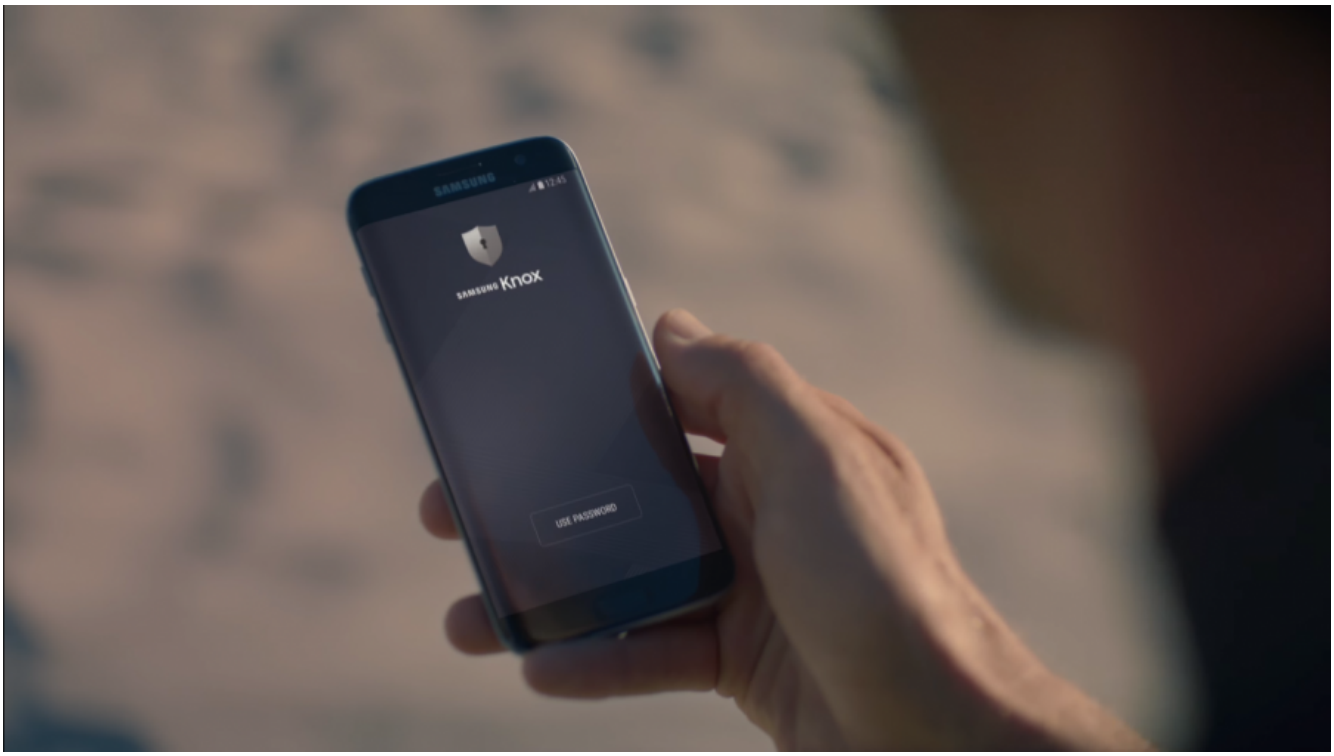
Lisaks salafraasi kasutamisele tasub selle sisu muuta võimalikult ettearvamatuks. Näiteks valides parooliks fraas „Minuparoolonvägakeeruline", siis oleks selle asemel üheks variandiks hoopis „M1nyPAr00l0Nv2gak33rul1ne". Fraas jääb samaks, kuid sellisel juhul on paroolis rohkelt numbreid ja suuri tähti, mis muudab selle murdmise keerukamaks.

Lisaks annab tõhusat lisakaitset kaheastmeline isikutuvastus. Tegu on lihtsa vahendiga, mis kaitseb kasutaja andmed isegi siis, kui parool on mõnele internetipahalasele teada.

Ära kliki ühtki tundmatut või kahtlase sisuga linki

Tundub uskumatu, aga inimesed on varmad klikkima kõiki linke, mis saabuvad e-kirjaga või hüpikakendega. Suur punane "Vajuta siia" peaks olema esimene häirekell selle kohta, et veebilehe turvalisust tasuks enne kontrollida. Sõbra e-posti aadressilt ainult lingiga tulnud e-kiri võib tunduda täiesti autentne, sest sõbrad saadavad ikka teineteisele naljakaid pilte ja videosid, aga kui kirjas ei ole sõber puhtas eesti keeles öelnud, et link on turvaline, siis seda avada ei tasu. Kui sõber telefonis kinnitab, et tema tõesti selle lingi saatis, siis võib juba ettevaatlikult piiluda.

"Ühe mõtlematu lingilevajutusega võite anda pahalastele kontrolli oma arvuti, selles leiduvate andmete, maksevõimaluste ja muu privaatse kohta," ütles Kopso.



Kasuta krüpteerituid turvalisi seadmeid

Lisaks ettevaatusele internetivõrgustikes tasub kriitilise pilguga üle vaadata seadmed, mida me igapäevaselt kasutame. Enamik meie nutiseadmeid on ühendatud internetiga ja toodavad andmeid, mis ka seadme omanikfirmale edastatakse.

Hiljuti sattusid mitmed telefonitootjad kriitika alla, nagu ei austaks nende seadmete toimimisloogika piisavalt inimeste privaatsust. Seega on nutiseadet valides oluline mõelda ka sellele, kes on seadme tootja ning kuidas see tootja inimese seadmest tulevate andmetega ümber käib.

„Samsungi telefonid kasutavad isiklike andmete kaitsmiseks Knox turvasüsteemi, mis laseb kasutajatel näiteks tööga seotud tundlikku infot hoida spetsiaalse parooliga kaitstud kaustades. 2014. aastal kinnitas ka Ameerika Ühendriikide Riiklik Julgeolekuagentuur (NSA), et Knox süsteemiga kaitstud seadmed on sobilikud riigiametnike tööl kasutamiseks," ütles Kopso.

Kas kõik, mida küsitakse, on avaldamiseks?

Nutiseadmeid kasutades on oluline meeles pidada, et sugugi mitte kõiki andmeid pole alati tarvis rakendusele anda.

„Ilmselt on paljud kohanud olukorda, kus mõnda rakendust või mobiilimängu kasutades küsib see ligipääsu kasutaja kontaktidele või asukohale. Kui see pole

rakenduse toimimise seisukohast oluline, siis võib selle ligipääsu julgelt ära keelata. Sellisel juhul on taaskord üks asi vähem, mille pärast muretseda,“ rääkis Kopso.

Paigaldades Google Mapsi on loogiline, et rakendus vajab infot kasutaja asukoha kohta, kuid mobiilimäng ilmselt mitte.

Kasuta viirusetõrjeid ja uuenda tarkvara koheselt

Viirusetõrje kasutamine ei ole ammugi enam mitte ainult arvutikasutajate pärusmaa, vaid häid viirusetõrjeprogramme on ka mobiilsetele platvormidele. Lisaks tasub koheselt paigaldada kõik tarkvarauuendused, sest aeg-ajalt leitakse süsteemidest turvaauke ning siis on oluline need koheselt ära lappida.

- Uudised
- Lahendused

- Turvalisus

Pilt

