Nutinõu: 5 olulist sammu, et end ja oma nutitelefoni küberpättide eest kaitsta

2 aastat tagasi - 29.05.2024 Autor: AM

Pilt: Lora mudel, Realistic Vision V6.0 B1, Stable Diffusion

Küberpettuste ja küberkuritegude hulk on viimaste aastate jooksul järsult tõusnud ning tihti saavad kurjategijad rahale ja andmetele ligi just kasutajate nutitelefonide kaudu. Täielikku kaitset pole küll võimalik saavutada, kuid paari ohutusmeedet rakendades on võimalik ohvriks sattumise tõenäosust oluliselt langetada. Elisa infoturbejuht Mai Kraft selgitab, mida tasub silmas pidada ja kuidas end kaitsta.

“Möödunud aastal pidi eestlaste internetikasutust turvav Elisa Netivalvuri teenus reageerima enam kui 9 miljonil korral, mis viitab, et olukord küberruumis ei ole kiita. Enda ja oma lähedaste kaitsmisele peaksid seetõttu mõtlema kõik,” lausus ta, “kui arvutis viirusetõrje kasutamine ja üldiste küberhügieeni põhimõtete järgmine on juba midagi, millest paljud teavad, siis jäetakse tihti aga nutitelefonidega seotud ohukohad tähelepanuta.”

Selleks, et end kaitsta, soovitab Kraft tähelepanu pöörata viiele suuremale teemale.

1. Uuenda alati tarkvara

On raske leida kedagi, kes poleks juba kolmandat korda telefoni operatsioonisüsteemi uuendust edasi lükanud või vältinud mõne rakenduse värskendamist. Kuigi see võib tunduda kui lihtsalt millegi tüütu edasi lükkamine, siis märgib Kraft, et iga uuendus lastakse välja asja pärast ning tihti on uuenduse suurimaks võiduks paranenud turvalisus. Lükates uuendusi edasi seatakse end ohtu, sest ka kurjategijad on teadlikud eelnevates versioonides avastatud turvavigadest.

“Hea praktika on võimaldada seadmel automaatsed uuendused ära teha niipea, kui need tekivad. Enamikel seadmetel on võimalik uuendused lasta ära teha öösel, siis kui kasutaja magab. Mida kiiremini viimased turvaparandused paigaldatud saavad, seda väiksem on tõenäosus, et küberpätt pääseb seadmesse näiteks mõnda rakendusse sattunud turvaaugu abil,” rääkis ta.

2. Vali hoolega rakendusi ja jälgi nende õigusi

Ilma rakendusteta ei kujutaks keegi nutiseadet ette ning kuigi need on pea alati kasulikud, kujutab iga äpp endast ka potentsiaalset ohtu – turvaauguga rakendus võib avada tee ülejäänud seadmesse, niisamuti võib tekkida oht siis, kui alla laetakse mõne äpi libaversioon. Seetõttu soovitab Kraft rakendusi alati alla laadida vaid ametlikest äpipoodidest ning ka siis rakendada ettevaatlikkust: lugeda äpi arvustusi ning vajadusel isegi otsingumootorite abil uurida, kas tegu on millegi ohutuga.

“Rakenduse alla laadimisega kõik tegelikult ei piirdu – peale paigaldamist tahavad äpid enamasti igasugu õigusi. Lihtsalt kõigele “jah” vajutamise asemel võiks võtta hetke ja päriselt süveneda, millele äpp ligipääsu soovib ja miks tal seda vaja on. Kui näiteks pilditöötlusäpp tahab ligipääsu sinu klaviatuurile, kontaktidele, meilile ja brauseri ajaloole, siis võib tegemist olla millegi kahtlasega. Ühtlasi võiks aeg-ajalt üle vaadata oma olemasolevate rakenduste õigused ja kustutada ära need äpid, mida tegelikult vaja ei ole,” lisas ta.

3. Paigalda ka oma nutiseadmesse viirusetõrje

Kui arvutites viirusetõrje kasutamine on saanud millekski tavapäraseks, siis nutitelefoni puhul seda tihti ei tehta. Samas rõhutab Kraft, et viirused võivad nakatada ka telefone ja seetõttu tasub kaitsemüürid üles laduda ka seal. Selle kõrval tasuks kasutusele võtta ka täiendavad turvateenused – näiteks Netivalvuri – mis suudavad millegi ohtliku eest hoiatada ka siis, kui midagi veel päriselt alla laadima ei hakata.

“Hea viirusetõrje ning ettevaatlikkus internetis toimetades on kaks suurimat abimeest, mis aitavad turvalisust tagada. Alati saab teha rohkem, kuid neid kaht teemat ei tohiks mitte kunagi tähelepanuta jätta,” lausus ta.

4. Lülita välja kõik ebavajalik

Selleks, et kaitsta oma seadet võõraste eest, tasub välja lülitatuna hoida ka kõik see, mida parasjagu ei kasutata. Näiteks tasub iPhone’i omanikel AirDrop sisse lülitada vaid siis, kui päriselt faile saadetakse ning Bluetooth ja Wi-Fi võiks olla sisse lülitatud vaid siis, kui neid päriselt tarvis läheb. Mida vähem on viise kellelgi võõral seadmega ühendus luua, seda turvalisem lõpuks kõik on.

5. Ettevaatust kõnede ja sõnumitega

Viimaste aastate jooksul on küberrünnete kõrval järsult suurenenud ka petukõnede ja -sõnumite hulk, mistõttu tasuks Krafti sõnul kõigil nende osas ettevaatlik olla. Täna on kõige levinumateks petuskeemideks kõned pankadelt, investeerimispettused ning paki saabumisest teavitavad võltssõnumid.

“See on valdkond, kus parima kaitse tagab ülim skeptilisus – tea, et pangatöötajad ei küsi kunagi su sisselogimisandmeid ning pakifirmad ei vaja, et sa andmeid üle kinnitaksid. Kui midagi tundub natukenegi kahtlane, tasub korraks samm tagasi astuda ja mõelda. Suure tõenäosusega on kõhutundel õigus ning pettus on juba ukselävel,” lisas ta.

- Lahendused
- Turvalisus

Pilt