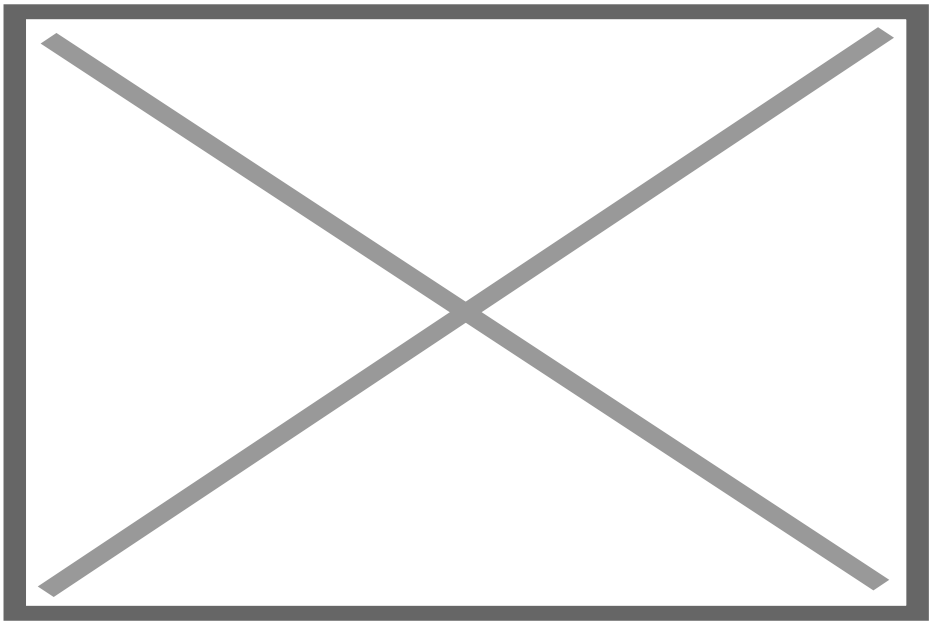
Metsa minnes pane ka ümbrust tähele ehk nutiseadme turvalisuse 12 sammu

12 aastat tagasi - 27.10.2014 Autor: Rica Williams



Kas oled see, kellele vanemad ja sõbrad helistavad, kui arvutiga midagi juhtub? Kui oled IT-spetsialist või IT-huviline, siis on üsna tõenäoline, et lähendaste jaoks oled ka kasutajatugi. Ning kui juba probleeme lahendad, siis tasub kindlasti rääkida ka nutiseadmete turvalise kasutamise soovitustest. Nii saab edaspidi loodetvasti vähem kõnesid, kus palutakse sinu abi.

Kujutame nüüd ette, et inimene on saanud just uue nutitelefoni. Ta võtab selle karbist välja… selle tundmaõppimine võtab oma aja. Ning olgem ausad, et taustapiltide, helitoonide valimine ja lahedate äppide allalaadimine on sageli lihtsam ja tähtsam kui näiteks nutiseadmele viirusetõrje tarkvara valimine ning erinevate kasutajakontode seadistamine.

IT-asjatundjad teavad väga hästi, miks nutiturvalisus on oluline, kuid kuidas seda teistele lihtsalt seletada?

Kõige lihtsam viis oma lähedasi aidata on selgitada, et nutiseadmed (nutitelefonid ja tahvelarvutid) on pigem võimsad arvutid. Mida rohkem me nutiseadmetes andmeid ja fotosid salvestame, suhtleme ja raha liigutame, seda rohkem tuleb ka turvalisusele tähelepanu pöörata. Täielikku turvalisust pole mõtet lubada, küll aga tasub küsida lähedastelt, kui oluline nutiseadmete sisu neile on? Sest mida

tähtsam see on, seda hoolikamad peame nende kasutamisel olema.

Julgus vs konservatiivsus

Eestis oleme uudsed tehnoloogiad ja uued IT-seadmed pigem julgelt vastu võtnud. Tasuta WiFi levib paljudes kohtades - bussidest parkide ja metsadeni, arvutid ja internet on väga paljudele meist igapäevased abimehed ja sõbrad. Viimastel aastatel on massidesse jõudnud nutiseadmed. Eestis just eelkõige nutitelefonid, kuid ka tahvelarvutite müük on tõusuteel.

Kõik see näitab justkui julgust - võtame uued asjad kasutusele ja saame hakkama! Samas on alati küsimus, kus tõmmata piir julguse ning oma võimete õigesti hindamise vahele.

IT turvalisus kui seenelkäik

Metsaski eksime ära sageli just siis, kui oleme julgelt seeni otsides edasi marssinud, panemata tähele ümbrust või ilmamuutusi.

IT-maailmas tähendab see, et oleme ametis näiteks ägedate äppide kasutamisega, kuid muu jaoks pole meil enam aega ega tähelepanuvõimet jätkunud.

Muidugi ei eksi just iga metsamineja ära ning niisamuti ei satu ka iga internetikasutaja küberkuritegijate küüsi… kuid küsimus on selles, kui tõenäoline see on või kui suured on meie kahjud, kui see nii juhtub.

Seda riski peab igaüks oskama enda jaoks hinnata ja teadma vajalikke samme selle vältimiseks.

Nutiseadmete turvalise kasutamise 12 sammu

1. Pane nutiseadmetele ekraanilukk peale (kas kood, muster või sõrmejälg).
2. Kasuta automaatset lukku (lukk läheb automaatselt peale näiteks 1 minuti jooksul, kui seadet ei kasutata)
3. Paigalda nutiseadmetele viirusetõrje tarkvara (uuri näiteks tootjatelt, kelle viirusetõrjet oma arvutis kasutad).
4. Uuenda pidevalt nutiseadme ja rakenduste tarkvara (kasuta uusimaid tarkvaraversioone).
5. Kontrolli enne rakenduste (äppide) allalaadimist nende tausta (vajadusel otsi internetist taustainfot, loe teiste arvamusi)
6. Proovi vältida rakendustes jäta-mind-meelde” võimaluse kasutamist (see teeb võimalikule kurjategijale sinu andmete ligipääsu väga lihtsaks).

7. Kasuta erinevate rakenduste puhul erinevaid ligipääsuparoole.
8. Loo tahvelarvutis erinevatele kasutajatele oma kasutajakontod (näiteks endale ja lapsele).
9. Kasuta Mobiil-ID võimalusi nutiseadmetes e-teenustesse sisselogimisel ja digiallkirja andmisel, nagu arvutis kasutad ID-kaarti, sest see on kõige turvalisem viis. (Mobiil-ID SIM-kaardi saad oma mobiilioperaatorilt).
10. Nutiseadet müües või vahetades kustuta kõik sinna salvestatud andmed. (Vajadusel küsi abi oma mobiilioperaatorilt).
11. Mõtle läbi, millised teavitusi soovid näha lukustatud ekraanil? Kui telefon on järelvalveta, siis näevad teised neid.
12. Ära jäta nutiseadmeid avalikes kohtades (kohvikus, kinod jne) järelvalveta.

RICA WILLIAMS
Nutikaitse 2017

FOTO: KAIDO EINAMA

- Lahendused
- Turvalisus