Täna on turvalise Interneti päev: kuus soovitust nutitelefoni turvalisemaks kasutamiseks

5. veebruar 2019 - 16:45 Autor: AM

Täna tähistatakse rahvusvahelist turvalise Interneti päeva üleskutsega olla nutivahendite kasutamisel veelgi nutikam. Isikuandmete väärkasutamine ja isikupärastatud reklaamid on vaid mõned riskidest, millest tasuks mobiiliomanikel teadlik olla.

„Küberhügieen on teadlikkus riskidest internetis ja oma digiseadmetes, mis on saanud meie igapäevaelu lahutamatuks osaks. See ei erine tavahügieenist: tuleb leida sobivad tooted, mis puhastavad ja kaitsevad ning kasutada ja vahetada neid regulaarselt," lausus Samsung Electronicsi Digi Pass programmi juht Baltikumis Egle Tamelyte.

E-postiga saadetud viirused, parooli lahtimurdmine, andmepüük ja muud petuskeemid on Tamelyte sõnul vaid mõned näited küberriskidest, mis käivad igapäevaselt nutitelefoniga taskus kaasas. Ta tõi välja kuus praktilist nõuannet, mis võimaldavad internetti turvalisemalt kasutada.

1. Kaitse oma privaatsust

Mõtle läbi, milliseid andmeid soovid erinevate rakenduste ja veebiteenuste jaoks jagada, ning kindlasti ära kasuta automaatseid eelvalikuid. Kui allalaaditud rakendus vajab ligipääsu andmetele, mida sa ei soovi jagada, siis keela juurdepääs. Sama reegel kehtib sotsiaalmeedias: mõtle hoolega, milliseid andmeid kellega soovid jagada, ning kas sinu puhkusefotod peavad olema kõigile avalikud ja jagatavad.

2. Tule digimullist välja

Inimesi, kes tarbivad uudiseid peamiselt sotsiaalvõrgustike kaudu, varitseb suurem oht sattuda n-ö digitaalsesse mulli. Selle põhjuseks on algoritmid, mis analüüsivad kasutaja tegevust ja määravad, millist sisu ja reklaame tulevikus ette sööta. Algoritmide tõttu näeb kõige sagedamini neid uudiste allikaid, mida oled varem soovinud tarbida ja meeldivaks märkinud. Tarbida tasuks võimalikult mitmesuguseid informatsiooniallikaid, et saada tasakaalustatud teavet ja mitte jääda ühekülgse, puuduliku informatsiooni tarbijaks.

3. Halda oma paroole

Paroolide nõrkus pole sageli nende vähene keerukus, vaid see, et paljud kasutavad samu paroole mitme või isegi kõigi kontode jaoks. Turvalisem on kasutada erinevaid paroole, eriti kõige väärtuslikumate kontode puhul. Soovitatav on kasutada paroolihalduse programme või kirjutada salasõnad paberile, nii et mitmete paroolide haldamine ja meelespidamine poleks peavalu. Tarbetu on ilmselt meenutada, et paberil paroolinimekirja ei tohiks mingil juhul hoida rahakotis.

4. Kasuta kaheastmelist autentimist

Kaheastmeline autentimine aitab tähtsaimate kontode turvalisust veelgi suurendada, olgu siis tegu sotsiaalmeedia konto või e-postkastiga. Autentimissüsteemid saadavad telefonile tekstisõnumi, mis nõuab sisselogimisel kuuekohalise koodi sisestamist.

5. Kustuta rakendused, mida ei kasuta

Rakendused on võimelised täpselt ära näitama nutitelefoni asukoha ja edastama need andmed reklaami- ja turundusettevõtetele. Kõik, mida pead väärtuslike andmete tasuta äraandmiseks tegema, on vaid oma telefoni taskus kaasas kandma. Ettevõtted teavad, kuhu lähed ja kui kaua seal viibid, ning saavad hinnata kasutaja vanust, sugu ja muud isiklikku teavet. Seega, kui rakendust enam ei kasutata, tasub see oma telefonist kustutada. Kui seda on uuesti vaja, saab selle kiiresti alla laadida.

6. Uuenda äppe

Arvutid ja nutiseadmed on küberkurjategijatele võrdselt atraktiivsed sihtmärgid, sest neis on kaasas kasutaja tundlikud isikuandmed. Nutiseadmete kaitsmiseks küberrünnakute eest tuleb regulaarselt uuendada nii tarkvara kui operatsioonisüsteemi. Samuti tuleb meeles pidada, et rakendusi ei tasu alla laadida kahtlastest allikatest.

- Uudised
- Lahendused

- Mobiiltelefonid