4 soovitust laste ja noorte nutiseadmete turvalisuse tõstmiseks

12. märts 2021 - 15:18 Autor: AM

Nutiseadmed mängivad meie laste elus aina olulisemat rolli, tahame või ei taha. Huawei ekspert Vitali Donskoi pani kokku neli soovitust, mida iga lapsevanem peaks järgima, kui soovib, et tema järeltulijal oleks mobiilse nutiseadmega internetis võimalikult turvaline tegutseda.

Eesti mobiilside operaatorite andmetel saavad lapsed esimese päris oma telefoni kooli minnes ja järjest sagedamini on selleks mõni odavam nutitelefon. Mida vanemaks laps saab, seda suuremat rolli nutitelefon tema elus mängib suhtlemiskanalina. Kui väikemate laste mobiilikasutusest vanematel enamasti päris hea ülevaade, siis alates teisme-east läheb lapse nutikasutuse kontrollimine järjest keerulisemaks ja lapse enda huvid laiemaks.

Nutitelefonile kulutatava aja piiramine ja lapse tegevuste jälgimine on vajalik, kuid kooliealisele lapsele ekraaniaja täielik keelamine tähendab ühe omaealistega sotsiaalse suhtlemise võimaluse ära võtmist. Seetõttu on järjest suuremas hulgas kodudes lahenduseks selged nutikasutuse reeglid ja nutikasutusega seotud ohtude võimalikult väikeseks viimine, samuti laste õpetamine internetis varitsevatest ohtudest.

Vaadake, et seade ise ja olulisemad kontod oleks turvalise parooliga kaitstud

Vaadake koos lapsega üle, et kõik valikud paroolid ja PIN-koodid oleks sisse lülitatud ja turvalised. Kõige esmasem viis turvalisust suurendada on tagada, et seadmel oleks sisse lülitatud ja parooliga kaitstud ekraanilukk. See on vajalik seadme kaotuse või varguse korral, aga eriti teismeliste puhul ka näiteks pahatahtlike sõprade vastu. Donskoi kirjeldab üht ebameeldivat juhtumit: „Minu tutvusringkonnas juhtus hiljuti lugu, kus sõbra telefoni oma kätte saanud teismeline marakratt postitas sõbra telefonist erinevatesse vestlusgruppidesse sõnumeid, mis telefoniomanikku häbistasid. Mõtlematu nali tegi telefoniomanikule palju haiget ja paigutub ilmselt üheks küberkiusamise vormiks.“ Samuti on oluline üle vaadata lapse olulisemate kasutajakontode paroolid ning kus võimaik, võtta kasutusele kaheastmeline autentimine.

"Vaadates ka Eestit puudutavaid suuremaid paroolide lekkeid näeme kui paljud inimesed vaatavad tänase päevani turvalistele paroolidele läbi sõrmede. Sageli vallivad isegi täiskasvanud omale lihtsasti äraarvatava parooli, näiteks numbrijada 123456 või mingid väga levinud sõnad,“ selgitas Donskoi.

Ka lastele on vaja rõhutada juba varakult paroolituгbe olulisust - tuletada meelde, et paroole ei tohiks paljastada isegi lähedastele sõpradele, kanda rahakotis, seljakotis või telefoniümbrisesse kirjutatuna. Kui paroole on palju või on raskusi nende meeles pidamisega, siis saab salvestada need spetsiaalsetesse rakendustesse, nagu näiteks Google Playst või ka Huawei App Gallery valikust leitav „NordPass“ või „Password safe“.

"Uuemates telefonides on hea kasutada biomeetrilisi andmeid - näotuvastust või sõrmejälge. Need andmed on salvestatud telefoni kiibile, mistõttu on need turvalised isegi siis kui telefon on nakatunud viirusega. Seetõttu peetakse seda tüüpi lukke eriti ohutuks,” ütles Donskoi.

Kontrolli seadme sisemisi turva- ja privaatsus-seadeid

Sõltumata seadme mudelist on igal nutitelefonil tehases peale pandud turvaseaded, mis aitavad kontrollida, kellel ja millal on juurdepääs telefonikasutaja andmetele. „Telefoni seadetes saate vaadata üle kõige sagedamini kasutatavad rakendused lastele ja kontrollida nende privaatsusseadeid, näiteks juurdepääsu lubamine kaamerale ja mikrofonile, asukohateave või rakendusesiseste ostude keelamine. Nii võite olla kindel, et lapsed, kes kogemata või uudishimulikult telefonis midagi vajutavad, ei tekita tõelist kahju, ”selgitas Huawei ekspert.

Samuti on kõigil enim levinud mobiiliplatvormidel võimalik aktiveerida topelt-autentimise funktsioon, et vanemad saavad kõik olulisemad uuendused, ostud või protsessid enne nende tegemist kinnitada. „See aitab tagada, et laps ei tõmba oma telefoni mingeid sobimatuid äppe, aga ka tagab kontrolli internetist tehtud ostude üle, et kaardimaksetest ei peituks ootamatuid üllatusi, ”ütles Donskoi.

Laadige alla ja lülitage sisse erinevad lisaturvalisuse võimalused

Lisaks mobiiliseadme operatsioonisüsteemi sisse ehitatud turvaseadetele saab telefonidesse installida täiendavaid turvalisust suurendavaid äppe. Näiteks vanemad leiavad Google Play või ka Huawei App Gallery äpipoest rakenduse nimega Screentime, mis võimaldab vaadata lapse telefoni kasutamise ja veebis surfamise ajaloo aruannet, määrata aja, millal telefon ei tööta või lukustada teatud rakendused. Sarnaseid lahendusi on saadaval ka kõigile mobiiliplatvormidele.

Samuti on kasulik installida oma telefoni viirusetõrjeprogramm, mis aitab ennetab pahavara, ohtlike linkide, rünnakute või soovimatute kõnede ja sõnumite korral, näiteks Avira Antivirus, mis aitab seadmeid tõhusalt rünnakute eest kaitsta. See mitte ainult ei blokeeri kahtlasi reklaame ja lehti ning võimalda kontrollida andmetele juurdepääsu, vaid sellel on ka seadme skaneerimisfunktsioon, mis tuvastab ja eemaldab pahavara.

Selgitage lastele internetiga seotud ohte

Nii laste kui ka täiskasvanute puhul on suurim turvaoht enamasti ikka kasutaja ise. Kuigi laste puhul on näha, et internetist varitsevatest ohtudest räägitakse neile järjest enam ka koolis, siis kipuvad kõige elementaarsemad teadmised ikkagi vahel ununema ja vajavad kodus üle rääkimist. Ehkki eelpool toodud tehnoloogia-alased näpunäited aitavad ka passiivselt suurendada laste digitaalset turvalisust, on oluline see kõik koos lapsega ka läbi arutada, et ta ka mõistaks vajadust ise oma turvalisuse suurendamiseks. Kõige olulisem on siiski mobiiliseadme kasutaja enda soov ohte ennetada ning oskus pettusi varakult ära tunda.

- Lahendused

- Androidiblog
- Mobiiltelefonid
- Turvalisus