Kuidas avastada mobiilist viiruseid ja kuidas neist hoiduda?

9 aastat tagasi - 28.07.2016 Autor: AM

Mobiilides avatakse samuti lisandeid ja käiakse kahtlastes veebides, mis tähendab, et väga levinud mobiiliplatvormides võib sattuda juba ka erinevate pahalaste ja viiruste peael. Kuidas neist hoiduda? Kuidas neid avastada? Samsungi tooteekspert Henry Tiitus annab nõu.

Iga arvutikasutaja soovib hoolitseda oma seadme turvalisuse eest ja tagada selle parimat funktsionaalsust. Seetõttu ollakse harjumuspäraselt ettevaatlik erinevate tundmatute veebiaadresside avamisel ning kaitstakse oma arvutit viirusetõrjeprogrammidega. Ent miskipärast pööratakse palju vähem tähelepanu meie igapäevase abimehe – mobiiltelefonide – turvalisusele, ehkki keskmiselt kasutavad inimesed oma nutiseadmeid vähemalt sama sageli või isegi sagedamini kui arvutit.

Nagu ka arvutite puhul, ohustab nutiseadmeid pahavara. Pahavara võib sattuda seadmesse kas SMS-i teel, Bluetoothi teel või siis läbi alla laetud rakenduse. Pahavara võib varastada seadme mälus olevaid andmeid, teha pangakonto tühjaks, helistada või saata sõnumeid tasulistele numbritele, muuta seadme spämm-botiks või lihtsalt muuta seadme kasutuskõlbmatuks. Sellest, kuidas oma Android mobiilseadet ohtude eest kaitsta ning viiruste ja pahavaraga nakatumist ennetada, jagab kasulikke nõuandeid Samsungi tooteekspert Henry Tiitus.

Märgid, et mobiilseade võib olla nakatunud

Sõltuvalt pahavara või viiruse tüübist võivad seadmel esineda sümptomid, mis annavad märku sellest, et telefoniga on midagi lahti. Näiteks võib märgata seadmes vaba ruumi hulga järsku vähenemist olgugi, et hiljuti pole midagi suuremahulist seadmele paigaldatud. Teiseks sagedaseks tundemärgiks on see, et seade on muutunud oluliselt aeglasemaks. Seda tuleb eelkõige silmas pidada uuemate seadmete puhul, kuna vanemate telefonide puhul võib seadme töö kiirust oluliselt mõjutada ka vanus. Veel üks märkidest, et seade võib olla viirusega nakatunud, on aku kiirem tühjenemine, kuna pahavara töötab seadmes pidevalt ja kulutab seeläbi akut.

Üks lihtsamatest nippidest, kuidas selgitada välja, kas telefon on nakatunud viirusega või on lihtsalt ülekoormatud, on algseadete taastamine. Kui nutiseade on muutunud liiga aeglaseks, on soovitatav varundada pildid ning muu tähtis informatsioon, kopeerides selle teisele seadmele ning teostada tehase seadmete taastamine. See eemaldab kolmandate osapoolte rakendused ning võimalikud probleemid, mis võivad taustal töötades muuta näiteks telefoni aeglasemaks, akuaega lühemaks jne. Kui pärast telefoni suurpuhastust ja algseadete taastamist jätkuvad endised probleemid, on tõenäoliselt tegu pahavaraga.

Sarnaselt arvutitega tuleb ka nutitelefonidega turvaliselt ümber käia ning arvestada kõiksugu pahavara ja viirustega. Tuleb meeles pidada, et oleme oma nutitelefoni siiski talletanud suurema osa personaalset informatsiooni alustades pangakonto andmetest lõpetades isiklike sõnumite ja fotodega, mille kuritarvitamist ja kahjustumist ilmselt mitte keegi ei soovi. Seetõttu on soovitatav nutiseadme igapäevasel kasutamisel järgida erinevaid pahavara ja viiruste ennetamise viise, sest vastasel juhul võib olla juba liiga hilja.

Lae rakendusi Google Play lehelt ning veendu äpi turvalisuses

Üks sagedasem viiruste tee nutitelefonisse kulgeb rakenduste ja mängude ebaturvalistelt lehekülgedelt laadimise tulemusel. Seetõttu on soovitatav rakendusi oma Androidi telefoni laadida üksnes Google Play lehelt, ent sealgi tuleb tähelepanelik olla – ka Google’i lehele võib sattuda pahavaralise koodiga äppe. Seetõttu tuleb nutitelefoni kasutajal olla tähelepanelik iga rakenduse allalaadimisel ning veenduda rakenduse turvalisuses: kontrollides rakenduse loojat, uurides kasutajate hinnanguid ja tagasiside-kommentaare. Mida populaarsem on rakendus ja mida rohkem positiivseid hinnanguid on antud, seda kindlam võib olla, et tegu on turvalise rakendusega. Lisaks tuleb rakenduste allalaadimisel üle vaadata ka rakenduse küsitavad permission'id ehk load – nii näiteks ei tohiks tavaline mäng kindlasti küsida õigust telefonikõnede salvestamiseks.

Ava üksnes turvalisi linke

Läbi mobiilse seadme ei ole soovitatav avada linke ei internetis surfates ega e-mailis, mille turvalisuses kasutaja pole veendunud. See kehtib ka WhatsAppi ja Facebook messengeri vahendusel jagatud linkide puhul, sest võib juhtuda, et hoopiski sõbra mobiilseade on pahavaraga nakatunud ning viirus proovib edasi levida. Samuti levib palju viirusi SMS-i ja MMS-i teel spämm-kirjade näol, mis sisaldavad endas viirusi. Sageli lisatakse SMS-i link veebiaadressiga, mis tundub pealtnäha usaldusväärne, ent klikates leheküljele nakatub seade hoopiski

viirusega.

Kasuta turvalisi wifi-võrke ja veendu Bluetoothi teel edastavate failide turvalisuses

Hoidu üldkasutatavate vabade wifi-võrkude kasutamisest – neid võrke kasutades on pahavara ründamise risk suurem. Mõned rakendused vajavad oma tööks Bluetoothi, aga võib juhtuda, et rakendustes on turvaaugud, mille kaudu saavad häkkerid kontrolli rakenduse üle ja omakorda seadme üle. Samuti on soovitatav mitte vastu võtta Bluetoothi kaudu saadetud faile, mille saatjas ja turvalisuses ei olda kindel.

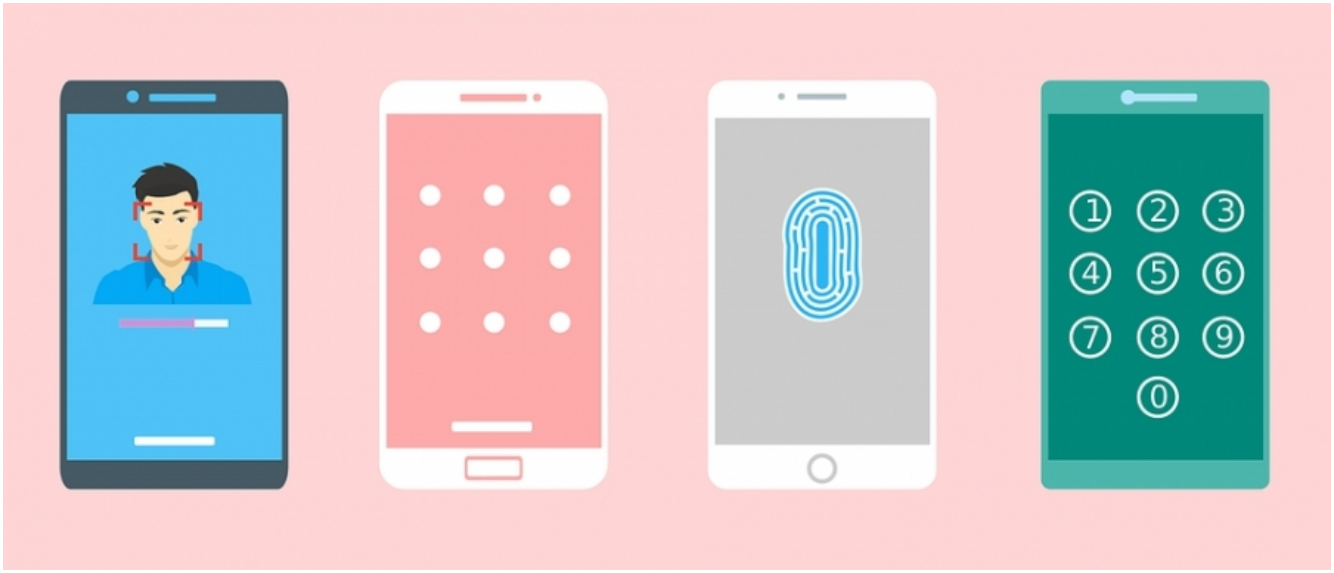
Tugevda kaitset viirusetõrjeprogrammiga

Google’i rakendused ja teenused turvavad igapäevaselt sinu seadet ja hoiatavad ohtlike rakenduste eest ning annavad märku potentsiaalsest ohust mobiilseadmele. Ent oma telefonis tasuks kasutada ka viirusetõrjeprogrammi, nagu näiteks tasuline AVG Antivirus või tasuta allalaaditav Avast, mis pakuvad lisaks viirusekaitsele erinevaid võimalusi oma telefoni turvalisuse häälestamiseks. Seejuures tuleb muidugi silmas pidada, et viirusetõrjeprogramm ei saa tagada telefoni 100%-list turvalisust ja äärmiselt oluline on ka kasutajapoolne hoolsus. Seetõttu on soovitatav lisaks ka kõiki eelnevaid nõuandeid täita ning olla oma nutitelefoni kasutades tähelepanelik ja hoiduda kõikvõimalikest kimbutavatest ohtudest. Samuti on hea teada, et mõned uuemad telefonid on viirusetõrjega juba varustatud. Näiteks on Samsung Galaxy S7 nutitelefonides eelinstallitud McAfee viirusetõrjeprogramm.

- Lahendused

- Mobiiltelefonid
- Turvalisus

Pilt


1 2 3
4 5 6
7 8 9
0