7 võimalust oma nutitelefoni häkkimise eest targalt kaitsta

9 aastat tagasi - 30.05.2017 Autor: AM

Mais vallandus üle maailma küberrünnakute laine, mis tabas paljusid arvuteid. Samas inimesed oma nutitelefoni häkkimise eest eriti ei kaitse. Arvestades, kui palju jõuab uudistesse hirmutavaid pealkirju andmete ja identiteedivarguste kohta, on enamik inimesi paigaldanud oma koduarvutisse viirusetõrjetarkvara, installinud tulemüüri ning võtnud kasutusele keerulise parooli.

Tele2 klienditeeninduse direktori Sirli Seliovi sõnul inimesed üldjuhul oma nutitelefoni turvalisuse peale ei mõtle. „Paraku teevad seda väga usinalt küberkurjategijad. Nokia Threat Intelligence'i aruandest selgus, et 2016. aastal sagenes nutitelefonide nakatumine pahavaraga järsult. Võrreldes eelmise aastaga oli tõus 96% ja 71% telefonidest pole pahavara vastu turvafunktsioone," rääkis Seliov.

„Meie mobiilseadmed on väikesed digitaalsed abilised, mis sisaldavad sama palju või isegi rohkem väga isiklikke andmeid kui laua- või sülearvuti," ütles Seliov ja lisas, et kadunud, varastatud või häkitud telefon annab vargale hea võimaluse identiteedivarguseks või pangakonto tühjendamiseks. Ta tõi välja seitse lihtsalt viisi, mille abil saab oma telefoni häkkimise eest kaitsta.

1. **Värskendage oma operatsioonisüsteemi.** Teate ju küll neid tüütuid teadaandeid, mis hüppavad ekraanile ja annavad teada, et peaksite värskendama oma operatsioonisüsteemi. Üldjuhul lükkame selle edasi. Ärge tehke seda. Tavaliselt hõlmavad need värskendused vanas operatsioonisüsteemis leitud turvaprobleemide parandusi. Mida kauem ootate, seda lihtsam saak olete häkkeritele.
2. **Puhastage oma rakendused.** Võib-olla olete sõltuvuses Instagramist, Snapchatist või Pokemon GOst – meil kõigil on oma lemmikrakendused. Ometi on palju rakendusi viljakas pinnas viirustele. Kui häkkerid leiavad mõnest rakendusest turvaaugu, saavad nad seda kasutada juurdepääsuks teie isikuandmetele. Pole teada, millist teavet rakendus kogub ja kus seda levitatakse. Tehke telefonis korrapäraselt suurpuhastusi ja kustutage rakendused, mida te enam ei kasuta. Veenduge, et telefon värskendab ülejäänud rakendusi automaatselt, sest enamik uuendusi hõlmab turvaparandusi. See on lihtne: iPhone'iga avage seaded, kerige alla valikuni

„iTunes & App Store” ja kontrollige, kas värskendused on valitud automaatseks allalaadimiseks. Kui teil on Android, siis avage rakenduse Play Store menüüjaotises punkt „Settings” („Seaded”) ja kontrollige, kas funktsioon „Auto-update apps” („Värskenda rakendused automaatselt”) on sisse lülitatud. Laadige rakendusi alla ainult App Store’ist või Google Playst.

3. **Lukustage.** Jätta telefon lukustamata on sama, mis jätta uks vargale pärani lahti. Seega veenduge, et automaatlukustuse funktsioon aktiveeritakse kohe pärast seadme kasutamist, näiteks ühe minuti järel. Samuti võtke kasutusele häkkimiskindel parool. Kui telefon pakub võimalust valida neljakohalise parooli asemel kuuekohaline, siis tasub valida viimane variant. Hoiduge liiga lihtsatest kombinatsioonidest, nagu 0000, 1234 või oma sünnikuupäev ja eelistage kohandatud tähtarvkoodi, mida on raskem lahti murda.
4. **Ärge kasutage avalikku Wi-Fit.** Tasuta avalik Wi-Fi on ebaturvaline võrk. Sellise võrgu kasutamine teeb teie teabe kinnipüüdmise ja hõivamise häkkeritele väga lihtsaks. Avaliku Wi-Fi kasutamine veebiotsinguteks ja uudiste lugemiseks ei ole üldjuhul nii hull, kui mistahes paroolide või isiklike andmete sisestamine. Kui teil on vaja e-kirju lugeda, siis kasutage oma telefoni andmesidet, mis on palju turvalisem. Samal põhjusel lülitage välja Bluetooth, kui te seda aktiivselt ei kasuta. Üks moodus end kaitsta on kasutada virtuaalset privaatvõrku ehk VPNi. See on tarkvara, mis krüptib avaliku võrgu kaudu toimuva ühenduse sisu. VPN on üldjuhul sisse ehitatud tööalaseks kasutamiseks mõeldud seadmetesse. See on turvalisem kui parooliga Wi-Fi võrk.
5. **Kaitske end SMSi teel õngevõtmise eest.** Kas olete sellest varem kuulnud? Selle tekkelugu on järgmine: varaste jaoks on kõige tõhusam viis nutitelefoni häkkimiseks saata n-ö peibutussõnum, teiste sõnadega kasutada SMS-õngitsemist. Kui kasutaja klõpsab tekstis oleval lingil või vastab sõnumile, saavad küberkurjategijad installida seadmesse pahavara, mis salvestab teie andmed.
6. **Tühjendage kadunud või varastatud telefon andmetest.** Mobiiltelefoni kaotamine pole üksnes tohutu ebamugavus, mis võib tekitada eelarvesse augu. Kui te pole oma seadet turvanud, võib see jätta teid ka ründele avatuks. Aktiveerige enda kaitseks rakendus Find My iPhone või Android Device Manager, mis võimaldab teil jälgida oma telefoni asukohta ja kõik andmed kaugelt kustutada.
7. **Olge numbri avaldamisel ettevaatlik.** Te ju ei annaks oma numbrit suvalisele inimesele, kes seda küsib? Olge siis selle andmisel ettevaatlik ka siis, kui seda küsitakse veebis, näiteks veebisaidil registreerumisel või ostu sooritades. Mida sagedamini oma numbrit jagate, seda suurem on risk sattuda SMS-rünnete ja SIM-kaardi vahetuse pettuste ohvriks. Viimasel juhul

kasutavad häkkerid kaaperdatud numbrit, et saada sõnumite kaudu juurdepääs kahekordset autentimist kasutavatele kontodele.

- Uudised

- Andmeside
- Androidiblog
- Mobiiltelefonid
- Turvalisus

Pilt