Kuidas tunda ära äpipoodides pesitsevaid ohtlikke peturakendusi?

5 aastat tagasi - 24.09.2021 Autor: AM

Iga mõne kuu tagant võib kuulda Google'i või Apple'i rakendustepoest leitud petu- ja võltsrakenduste kohta, mis varastavad kasutajate andmeid, nakatavad telefoni pahavaraga või kasutavad telefoni ilma kasutaja loata krüptorahade kaevandamiseks. Elisa infoturbe juht Mai Kraft selgitab, kuidas selliseid rakendusi ära tunda ja mida enda kaitsmiseks teha.

"Suuresti võib rakendustepoodidest leida kolme sorti ebasoositavaid rakendusi: kloonid, pahavaraga nakatunud rakendused ja spämmrakendused," lausus Elisa infoturbe juht Mai Kraft. Ta selgitas, et neist esimese puhul jäljendab rakendus mõnd muud edukat äppi ja pommitab allalaadimise järel kasutajat reklaamidega, varastab tema andmeid või nakatab telefoni muu nuhtlusega.

Pahavaraga nakatunud rakendused ning spämmrakendused on see-eest aga justkui päris äpid – taskulamp, märkmete tegemiseks mõeldud äpp, võidusõidumäng vms. Reaalse funktsionaalsuse pakkumise asemel on aga nende põhiliseks eesmärgiks pommitada kasutajat reklaamidega, varastada tema andmeid, kaevandada seadmega krüptorahasid või nakata telefon muu pahalasega.

"Google ja Apple võitlevad selliste äppide vastu küll püssi- ja ussirohuga, kuid on paratamatu, et mõni sarnane rakendus võib filtritest läbi lipsatada. Seepärast on oluline, et iga telefonikasutaja oskaks ka ise ohtlikke rakendusi ära tunda," ütles Kraft ning tõi välja peamised viisid, kuidas selliseid rakendusi tuvastada.

Vaata arvustusi

Nii Google kui ka Apple näitavad iga rakenduse juures arvustusi, mille abil on võrdlemisi lihtne selgeks teha, kas rakenduse näol on tegu asjaliku tööriistaga või hoopis millegi ohtlikumaga. Kui näed, et teised kasutajad kurdavad liigsete reklaamide üle, räägivad viirustest või on selgelt öelnud, et äpp teeb midagi väga väära, siis tasub sellest võimalusel pigem eemale hoida.

Loe kirjeldust ja vaata pilte

Kui keegi on kulutanud lugematu arvu tunde päriselt hea rakenduse tegemiseks, siis võid kindel olla, et ta kulutab ka mõned tunnid korralike piltide ja kirjelduse loomisele. Kui huvipakkuva rakenduse kirjeldus on täis vigu, puudub üldse või on illustreerivad pildid väga madala kvaliteediga ja väidetava funktsionaalsusega mitte seotud, siis on tegu selge ohumärgiga ning sellist äppi ei tasuks enda telefoni tõmmata.

Vaata allalaadimiste hulka

Populaarsetel rakendustel on tihti miljoneid või isegi miljardeid allalaadimisi, mis teeb originaaläppide leidmise üsnagi lihtsaks. Kui tahad alla laadida näiteks Instagrami äppi ja näed, et seda on alla tõmmatud vaid mõned tuhanded korrad, siis peaks see olema selgeks signaaliks, et tegu ei ole autentse rakendusega. Kui kahtled, siis suundu rakenduselooja kodulehele ja kliki sealt allalaadimislingile – see suunab sind otse äpipoe õige rakenduse juurde.

Mõtle õiguste peale

Rakendustepood näitab tihti juba enne allalaadimise alustamist seda, milliseid õiguseid äpp telefonis tahab. Kui neid seal ei märka, siis küsitakse õiguseid pärast installimist ja seega annab see võimaluse rakenduse iseloomu peale mõelda. Kui näiteks kalkulaator tahab ligipääsu su kontaktidele, kaamerale ja süsteemisätetele, siis võib üsnagi julgelt oletada, et rakenduse tegijal on kurjemad kavatsused.

Tee taustakontrolli

Kui kõige eelneva põhjal ei ole võimalik täie kindlusega öelda, kas rakendus on turvaline või ei, siis tuleb alati appi Google. Löö rakenduse nimi otsingumootorisse, sirvi läbi viimased uudised ja foorumipostitused. Kui tegu on võltsäpiga, siis võid üsnagi kindel olla, et keegi on sellest juba ka kirjutanud. Kui pärast kõike seda ütleb sisetunne endiselt, et asjad pole päris õiged, siis jäta äpp alla laadimata.

“Kõige lõpuks tasub meeles pidada, et parim viis ennast peturakenduste eest kaitsta on tõmmata alla vaid need äpid, mida sa vajad,” sõnas infoturbe juht. “Sul on telefonis juba kalkulaator ja taskulamp olemas, seega pole mõtet huvi pärast veel järgmist äpipoest alla laadida. Mida vähem ebavajalikku installida, seda lihtsamini saab ennast kaitsta.”

Niisamuti soovitab Kraft aeg-ajalt seadmes inventuuri teha ja kustutada ära need rakendused, mida sa pole lähiajal kasutanud. “Kui vaja, siis saad need alati hiljem

uuesti alla laadida. Seniks on aga mõistlikum talitada turvaliselt ja hoida telefonis vaid neid äppe, mida sa ka päriselt vajad,” ütles ta.

- Lahendused

- Androidiblog
- Mobiiltelefonid
- Turvalisus

Pilt

