Matkapuhelimen turvallinen käyttö

24.11.2020



Tänä päivänä moni osaa jo suojata tietokoneensa mm. viruksilta virustorjuntaohjelmalla, mutta matkapuhelin tai älypuhelin voi olla huonommin suojattu. Matkapuhelimen suojaaminen on yhtä tärkeää kuin tietokoneen, koska se sisältää nykyään omistajansa henkilökohtaisen elämän pienoiskoossa:

- sähköpostit
- puhelu- ja sijaintitiedot
- ystävien ja työkavereiden yhteystiedot
- teksti- ym. viestit
- kalenterimerkinnät
- jopa palveluiden salasanat

Näiden tietojen joutuminen vieraisiin käsiin aiheuttaa paljon harmia ja voi johtaa jopa huomattaviin taloudellisiin menetyksiin. Tietokoneesta poiketen matkapuhelimella voidaan aiheuttaa suuria taloudellisia menetyksiä puhelinlaskun kautta; jos puhelin on kaapattu haltuun ja sillä soitetaan maksullisiin numeroihin, yleensä ulkomaalaisiin numeroihin, saadaan aikaan suuri puhelinlasku. Sovelluskaupan kautta voi myös saada aikaan suuren luottokorttilaskun, jos sieltä tilataan maksullisia sovelluksia tai tehdään verkkokauppaostoksia.

Haittaohjelman, joka kaappaa puhelimen, voi saada, jos klikkaa puhelimeen tulleen multimediaviestin tai muun viestin kautta tullutta linkkiä. Kaappausohjelma voi olla naamioitunut myös vaikka pelisovellukseksi, jonka on ladannut Internetistä tai liitetiedostoksi. Haittaohjelman tai viruksen voi saada myös vierailemalla haittaohjelmaksi rakennetulla Internet-sivulla.

Miten voisin parantaa omaa ja puhelimeni tietoturvaa? Tässä pätevät suurelta osin samat keinot kuin tietokoneenkin suhteen. Tärkein tietoturvatekijä on puhelimen käyttäjä itse.

Sovellusten lataaminen

Lataa sovelluksia vain puhelimen omasta sovelluskaupasta: Android-puhelimella *Googlen Play*-sovelluskaupasta ja iPhonella Applen *App Storesta*. Näiden kauppojen ylläpitäjät yleensä poistavat niihin pyrkivät haittaohjelmat, mutta aina välillä niihinkin pääsee livahtamaan mukaan haittaohjelmia. Ennen latausta kannattaa katsoa sovelluksen lataus- ja arvostelumäärät. Jos ne ovat kovin pienet voi olla, että kyseessä juuri kauppaan ujutettu haittasovellus. Android-puhelimissa on Play Protect-sovellus, joka tarkastaa ladattavat sovellukset ennen latausta ja varoittaa epäilyttävistä sovelluksista.

Tarkasta sovellusten käyttöoikeudet

Sovelluksen asennuksen jälkeen on hyvä tarkastaa mitä käyttöoikeuksia sovelluksella on puhelimeen. Jos sovelluksella on oikeus vaikka puhelimen kameraan, mikrofoniin, sijaintiin ja kalenteriin, se voi kerätä paljon tietoa käyttäjän toimista ja vakoilla näin käyttäjää.

Liitetiedostot ja linkit

Avaa vain sellaisia liitetiedostoja, joiden alkuperästä olet tietoinen. Oudolta lähettäjältä tulleita liitteitä ei kannata avata. Joskus voi haitallinen liite tulla myös tutusta osoitteesta, lähettäjän väärentäminen ei ole kovin vaikea asia. Aina voi asian tarkastaa soittamalla lähettäjälle. Viestinä tulleisiin linkkeihin tulee myös suhtautua varauksella ja jättää klikkaamatta, koska niiden kautta voi asentaa puhelimeensa haittaohjelman. Ensin kannattaa lukea, mitä linkissä lukee ja jos se viittaa johonkin epämääräiseen, osoitteeseen ei pidä klikata. Ainakin Postin ja K-kaupan nimissä on lähetty huijauslinkkejä, jotka ovat johtaneet aivan muualle kuin näiden yritysten sivuille ja kyselevät sähköpostisoitteita ja salasanoja.

Varmuuskopiot

Mikäli puhelin rikkoontuu, menee hukkaan tai varastetaan, menetämme paljon tietoja. Siksi on hyvä olla varmuuskopiot tiedoista, esim. yhteystiedoista ja kalenterimerkinnöistä sekä valokuvista. Android-puhelimissa voidaan yhteystiedot ja kalenterimerkinnät varmuuskopioida Google-tilille. Puhelimen asetuksista voi käydä varmistamassa, että varmuuskopiointi on päällä: *Asetukset –> Järjestelmä –> Varmuuskopiointi ja palautus*. Google Photos -sovellus kopioi kuvat Googlen pilvipalveluun. Tämän voi tarkastaa avaamalla *kuvat-sovelluksen* ja sieltä oikeasta yläkulmassa olevan kirjaimen kohdasta pääsee kohtaan *asetukset.*

Applen iPhone käyttää varmuuskopiointipaikkana iCloudia. Tämän voi tarkastaa avaamalla *Asetukset* ja yläreunasta *oman nimen kohdasta* painamalla aukeaa valikko, jossa ylimpänä sovelluksena on iCloud. Tätä koskettamalla avautuu uusi valikko, josta selaamalla löytyy *iCloud-varmuuskopio.* Tästä voi tarkastaa, että

siinä kohdassa lukee *päällä*.

Päivitykset

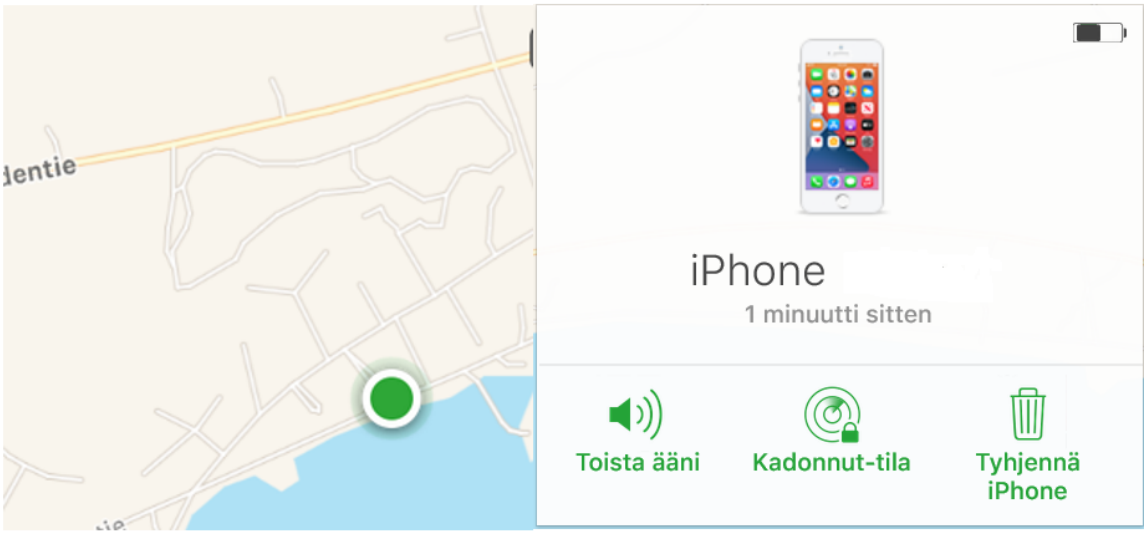
Käyttöjärjestelmän ja sovellusten päivityksien tarkoituksena on korjata mahdollisia tietoturva-aukkoja ja parantaa laitteen käyttöä. Päivitysasetuksissa tulisi olla automaattinen päivitys päällä, jolloin uudet päivitykset asennetaan automaattisesti. Android-puhelimissa tämän voi tarkastaa avaamalla *Asetukset* ja sieltä kohdan *Järjestelmä*. iCloud-puhelimissa puolestaan avaamalla *Asetukset* ja sieltä hakemalla kohdan *Yleiset,* jonka alla näkyy kohta *Ohjelmistopäivitys*.

Näytön lukitus ja SIM-kortin PIN-koodi

Näytön lukitus kannattaa ottaa käyttöön – jos puhelimen hukkaa, ei löytäjä pääse suoraan käsiksi puhelimen tietoihin. Näytön lukitustapa riippuu paljon puhelimen mallista, se voi olla joko numerosarja tai kuvio tai jopa sormenjälkeen perustuva. SIM-kortin PIN-koodi pitää vaihtaa, ettei puhelimen löytäjä voi käyttää SIM-korttia jossain toisessa puhelimessa.

Kadonneen puhelimen paikannus

Kadonneen puhelimen löytäminen onnistuu, tietokoneen tai toisen puhelimen selaimen avulla, jos puhelimessa on virta päällä. Android-puhelimissa paikannus löytyy Google-tilin kautta. Etukäteen on hyvä harjoitella puhelimen etsimistä kirjautumalla tietokoneella Google-tillille ja hakemalla sieltä kohta *Tietoturva* ja klikkaamalla *Laitteesi*-kohdasta puhelimen kuvaa sekä sieltä kohtaa *Etsi laite*. Täältä pystyy myös lähettämään puhelimeen äänimerkin tai näytölle tulevan viestin sekä puhelinnumeron johon puhelimen löytäjä voi soittaa. Äänimerkistä on silloin hyötyä, jos puhelimen on hukannut vaikka metsäretkellä. Myös puhelin tyhjentäminen on tätä kautta mahdollista. iPhonessa vastaavat toiminnot löytyvät, kun kirjautuu tietokoneella iCloud-palveluun ja siellä klikkaa kuvakkeesta *Etsi iPhoneni*. Kun puhelimen sijaintipiste näkyy kartalle pisteenä niin tätä pistettä klikkaamalla voi lähettää puhelimeen äänimerkin tai sen voi lukita ja tyhjentää.



Kuva 1.Puhelin on paikannettu selaimella iCloud-tilin kautta. Vihreää pistettä klikkaamalla avautuu valikko *Kadonnut-tila,* jota klikkaamalla pääsee lähettämään puhelimeen viestin, joka näkyy ruudulla.

Tietoturvasovellukset

Yleisesti iPhonea ja sen käyttöjärjestelmää pidetään tietoturvallisempana kuin Android-puhelimia. Android-puhelimissa voi harkita esim. operaattoreiden tarjoamia tietoturvapalveluita, mutta tärkein tietoturvatekijä on puhelimen käyttäjä itse.

Alpo Anttonen
Lehtori, Tietotekniikka
SeAMK Tekniikka