Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön

10/2014

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön 3

1 Ohjeita kaikille peruskäyttäjille 3

1.1 Käytä suojakoodia 3

1.2 Käytä automaattista lukitusta 3

1.3 Tee salasanoista riittävän monimutkaisia 3

1.4 Säädä näytölle tulevien ilmoitusten näkyvyyttä 4

1.5 Asenna tietoturvapäivitykset 4

1.6 Lataa sovelluksia vain luotettavista lähteistä 4

2 Ohjeita elinkaareen ja etähallintaan 4

2.1 Käytä pilvipalveluita harkiten 5

2.2 Pilvipalvelu auttaa etähallinnassa 5

2.3 Poista, tyhjennä ja palauta 5

2.4 Ole tarkkana, kun ostat käytetyn puhelimen 5

2.5 Puhelimissakin on haittaohjelmia 6

2.6 Älypuhelin ei ole ikuinen 6

3 Lisävinkit tehokäyttäjille parempaan tietoturvaan 6

3.1 Käytä massamuistin salausta 6

3.2 Poista käytöstä ylimääräiset langattomat yhteydet 7

3.3 Ota haittaohjelmatorjunta käyttöön 7

3.4 "Roottaa" vain, jos tiedät mitä teet 7

3.5 Suosi VPN-palvelua ulkomaan yhteyksissä ja avoimen WLAN:n käytössä 7

3.6 Hallitse keskitetysti yrityspuhelimia 7

Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön

Matkapuhelin ei ole enää pelkkä puhelin. Sillä kommunikoidaan monipuolisesti, siihen tallennetaan paljon henkilökohtaisia tietoja ja sitä käytetään yhä useammin maksuvälineenä. Niinpä matkapuhelimen käyttöön liittyvät tietoturvariskit ovat myös lisääntyneet. Tässä ohjeessa Kyberturvallisuuskeskus antaa vinkkejä matkapuhelimen tietoturvan ja yksityisyydensuojan parantamiseen.

Kännykän ominaisuuksien monipuolistuminen on tehnyt laitteesta yhä kiinnostavamman kohteen huijareille. Myös laitteen tietojen hallitseminen pilvipalveluissa tai laitteen yllättävä katoaminen voi aiheuttaa ongelmia käyttäjälle.

Kun huomioit seuraavat vinkit, varkaat eivät hyödy puhelimestasi, urkkijat eivät saa tietojasi ja yleisimmät haittaohjelmat kiertävät kännykkäsi. Vinkit on jaettu kolmeen osioon kohdistuen peruskäyttäjille, etähallintaan ja etäkaareen ja lopuksi lisäämään erityisesti matkapuhelinten tehokäyttäjien tietoturvaa.

Vinkit on julkaistu Viestintäviraston Kyberturvallisuuskeskuksen Tietoturva nyt! -artikkeleissa viikolla 43/2014.

1 Ohjeita kaikille peruskäyttäjille

Ensimmäiset perusvinkit ovat suunnattu kaikille matkapuhelinten käyttäjille parantamaan matkapuhelimen tietoturvaa ja yksityisyydensuojaa.

1.1 Käytä suojakoodia

Puhelimen käyttöliittymän lukitseva suojakoodi kannattaa asettaa päälle. Puhelimen merkki ja malli vaikuttavat siihen, onko suojakoodi numerosarja (suojakoodi), piirrettävä kuvio (suojakuvio) vai kirjoitettava salasana.

Muista suojauksen riittävä monimutkaisuus, jotta koodin arvaaminen ei ole liian helppoa. Kun avaat lukituksen, huomioi myös aika, paikka, tapa sekä muut silmäparit. Näin lukituksen suojaus ei paljastu ulkopuolisille.

1.2 Käytä automaattista lukitusta

Ota käyttöön puhelimen automaattinen lukitus järkevällä viiveajalla (esim. 1 minuutti). Tämä suojaa puhelintasi vahinkoklikkauksilta laukun- tai taskunpohjalla ja erityisesti, jos unohdat puhelimesi tai se varastetaan.

1.3 Tee salasanoista riittävän monimutkaisia

Puhelimen käytössä tarvitaan lukuisia PIN- ja suojakoodeja sekä palvelukohtaisia salasanoja. Kaikki edellä mainitut suojaukset kannattaa luoda riittävän monimutkaisiksi, jotta koodit ja salasanat eivät ole helposti arvattavissa tai sivusta silmäillessä tunnistettavissa.

Huomioi, että

- pilvipalveluihin kirjautuessa pääsytunnisteen muodolla ja pituudella on suuri merkitys, koska pilvessä oleviin tietoihin voi päästä käsiksi useiden eri päätelaitteiden avulla.
- erillisen salasanojen muistamiseen ja suojaamiseen tarkoitetun ohjelman salasanan muotoilussa on oltava erityisen tarkka.
- PIN-koodi voi olla pidempi kuin puhelimen vaatimat neljä numeroa.

1.4 Säädä näytölle tulevien ilmoitusten näkyvyyttä

Puhelimen näytölle voi lukittunakin tulla ilmoituksia esimerkiksi saapuneista teksti- tai pikaviesteistä tai uutisista, joissa näkyy viestin sisältöä.

Ilmoitusten näkyvyyttä voit säätää puhelimen asetuksista, jos et halua, että ilmoitus näyttää varsinaisen viestin sisältöä puhelimen ollessa lukittuna näkyvällä paikalla.

1.5 Asenna tietoturvapäivitykset

Ohjelmistojen ajantasaiset turvapäivitykset kannattaa aina asentaa. Lisäksi puhelimessa käytetyt sovellukset tulee päivittää säännöllisesti.

On hyvä huomioida, että jossain vaiheessa puhelimen käyttöjärjestelmä ja sovellukset tulevat elinkaarensa päähän ja niiden päivitykset lakkaavat. Tällöin puhelimesta tulee turvattomampi ja sen käyttäminen altistaa tietoturvauhille.

1.6 Lataa sovelluksia vain luotettavista lähteistä

Älypuhelimen käyttöä voi lisätä lataamalla puhelimeen uusia sovelluksia. Jos tallennat sovelluskauppaan luottokorttitietosi, niin käyttöön kannattaa ottaa vähintään ajoittainen ostosten vahvistaminen.

Lisäsovellukset kannattaa ladata vain luotetusta, ensisijaisesti puhelinvalmistajan tai käyttöjärjestelmän valmistajan sovelluskaupasta. Kolmannen osapuolen sovelluskauppaan on syytä suhtautua varoen. Räätälöidyt ohjelmat ja käyttöjärjestelmät (engl. firmware) eivät välttämättä ole sitä, mitä lupaavat. Ne saattavat sisältää jopa haittaohjelman.

Huomioithan, että myös luotetuista sovelluskaupoista voi löytyä haitallisia ohjelmia, sillä valmistajankaan seula ei ole täydellinen. Erityisesti lisäturvallisuutta lupaaviin sovelluksiin on syytä suhtautua kriittisesti ja ladata niitä vain tunnetuilta toimijoilta.

Sovellusten vaatimat oikeudet tulee tarkastaa ja suhteuttaa ne sovelluksen tarvitsemiin toimintoihin. Esimerkiksi askelmittarin ei pitäisi tarvita pääsyä yhteystietoihisi. Toisaalta yleisessä tiedossa jo on, että sovellukset vaativat toimiakseen internetyhteyden, jonka käyttölupaa ei enää ole tarpeen kysellä. Esimerkiksi Android Play Storen oikeuskyselyssä ei mainita nettiyhteyden käyttöoikeutta erikseen. Sovellusten saamista arvioista voit myös päätellä niiden luotettavuutta ja tietoturvallisuutta.

Lasten ja alaikäisten kanssa on hyvä sopia, miten asioidaan sovelluskaupoissa ja opastaa heitä, miten toimia, kun puhelimeen ladataan uusia sovelluksia. Ostoksiin voi myös asettaa hankintakohtaisen hyväksynnän, jotta voit välttyä yllättävän suurilta matkapuhelinlaskuilta.

2 Ohjeita puhelimen elinkaareen ja etähallintaan

Matkapuhelin varastoi lukuisia tietoja ja oletusyhteyksiä. Nämä tiedot voivat koitua omistajalleen haitaksi, etenkin jos puhelimen uusi omistaja päättää käyttää niitä väärin tai ulkopuolinen pääsee hyödyntämään etäyhteyksin pilvipalveluita. Matkapuhelin tulee myös aikanaan elinkaarensa päähän ja päivitystuen loputtua puhelin on alttiimpi tietoturvauhille.

Kun on perehtynyt puhelimensa käyttöön ja ominaisuuksiin, omat tiedot pysyvät helpommin vain omissa käsissä. Esimerkiksi pilvipalvelut ovat huolelliselle käyttäjälle suureksi hyödyksi.

2.1 Käytä pilvipalveluita harkiten

Pilvipalveluun on hyvä säilöä ajantasaiset varmuuskopiot puhelimen tiedoista. Pilven avulla puhelimen sisältämiä tietoja voi jakaa myös muille henkilöille ja päätelaitteille. Varomattomalla käytöllä pilvipalveluihin tallennetut tiedot saattavat kuitenkin päätyä tahattomasti myös ulkopuolisille.

Jos olet kirjautunut pilvipalveluun jonkun toisen henkilön laitteella, tietosi voivat jäädä tai yhdistyä tähän laitteeseen. Tällöin toisen laitteelta on jatkossakin mahdollista kirjautua pilvipalvelutilillesi.

Jos et halua, että tietosi leviävät ulkopuolisille pilvipalvelujen kautta, kaikkia puhelimen sisältämiä tietoja ei kannata tallentaa pilveen. Puhelimen yhteystiedotkin voivat riittää ja valokuvat voi halutessaan jättää pois.

Lisäksi puhelinta varten voi luoda erillisen pilvipalvelutilin, jonka ei tarvitse olla sidottu esimerkiksi sähköpostitiliin tai muihin palveluihin. Näin tietomurtojen yhteydessä haitta kohdistuisi vain yhteen palveluun.

Pilvipalveluissa on tärkeää käyttää riittävän monimutkaista salasanaa. Jos joku ulkopuolinen näkee salasanan, hän voi kirjautua palveluun toiselta päätelaiteelta. (ks. vinkki nro 1.3.)

2.2 Pilvipalvelu auttaa etähallinnassa

Pilvipalvelujen avulla voi ottaa käyttöön puhelimen etähallinnan. Se voi olla hyödyllinen, jos puhelin esimerkiksi katoaa tai se varastetaan. Puhelimen sijainti tallentuu pilvipalveluun, ja näin puhelin voidaan paikallistaa. Pilvipalvelujen etähallinnan avulla voi esimerkiksi

- asettaa puhelimen hälyttämään, jotta se löytyy paremmin
- lukita puhelimen, jotta ulkopuolinen ei voi sitä käyttää
- tyhjentää puhelimen, jotta ulkopuolinen ei saa haltuunsa sen tietoja.

Jos puhelin on kadonnut tai varastettu, operaattori voi estää liittymän käytön. Puhelin on kuitenkin etäpaikannettava ja -tyhjennettävä ennen kuin operaattori sulkee liittymän. Sulkemisen jälkeen pilvipalvelun etähallintaakaan ei enää voi käyttää.

Joidenkin valmistajien kautta voi myös estää puhelimen uudelleen aktivoinnin. Näin puhelin ei kuitenkaan palaudu alkuperäiselle omistajalleen, mutta ainakaan varas ei pysty hyötymään puhelimesta.

Jos pilvipalveluihin käytetty puhelin katoaa pysyvästi, palvelun salasanat pitää vaihtaa. Myös kadonnut päätelaite pitää poistaa pilvipalvelun laitelistalta. Näin puhelimen tietoihin tallentuneiden salasanojen avulla ei enää pääse käsiksi pilvipalveluun.

2.3 Poista, tyhjennä ja palauta

Jos myyt tai luovutat puhelimesi toiselle

- poista pilvipalveluissa käytetty puhelin pilvipalvelun laitelistalta
- tyhjennä puhelimen muisti ja tyhjennä tai poista erillinen muistikortti
- palauta puhelin tehdasasetuksiin.

Näin tietosi eivät päädy seuraavalle puhelimen käyttäjälle.

2.4 Ole tarkkana, kun ostat käytetyn puhelimen

Jos otat käyttöön toisella henkilöllä olleen puhelimen, se kannattaa palauttaa tehdasasetuksiin. Lisäksi on syytä tarkistaa, ettei puhelin ole liitetty sellaiseen pilvipalveluun, jonka kautta tallen-

tamasi tiedot saattaisivat ohjautua puhelimen entiselle omistajalle. Markkinoilla liikkuu myös käytettyjä, mutta varastettuja puhelimia. On syytä epäillä väärinkäytöstä, jos puhelin on erityisen halpa, se on lukittu, puhelimen pääsykoodia ei ole tallessa tai puhelin sisältää täysin tuntemattoman ihmisen tietoja. Tällaisissakin tilanteissa toisen henkilön tiedot ovat yksityisiä, ja niiden levittäminen ja käyttäminen on kiellettyä.

Lisäksi on hyvä ottaa huomioon, että käytetty puhelin voi koitua kalliiksi, mutta turhaksi hankinnaksi. Esimerkiksi jos puhelimen edellinen omistaja etälukitsee laitteen ja tekee siitä käyttökelvottoman.

2.5 Puhelimissakin on haittaohjelmia

Koska matkapuhelinta käytetään paljon verkossa asiointiin, sekin voi saada haittaohjelmatartunnan. Erityisesti verkkopankkien käytössä on syytä olla tarkkana. Haittaohjelmatartuntaa voit epäillä seuraavissa tapauksissa:

- Puhelimen käyttö hidastuu, eikä uudelleen käynnistys auta.
- Puhelimen käyttöjärjestelmä kaatuu tai pysähtelee.
- Akku alkaa yhtäkkiä kulua entistä nopeammin.
- Epätavallinen määrä verkkoliikennettä tai -aktiviteettia ilman, että olet itse muuttanut verkkokäyttäytymistäsi. Voit tarkistaa verkkoliikenteen määrän hallinta-asetuksista.
- Saat ylimääräisiä mainoksia tai ohjaudut väärille sivustoille.
- Saat roskapostia tai tuttavasi kertovat saavansa sinulta teksti- tai sähköpostiviestejä, joita et ole lähettänyt.

HUOM! Selatessasi internetissä voit saada varoituksen haittaohjelmatartunnasta, joka onkin huijaus. Suhtaudu tällaisiin varoituksiin aina varauksellisesti.

Jos matkapuhelimesi on saastunut, käytä puhdistamiseen hyväksi havaittuja antivirus-tuotteita, palauta puhelin tehdasasetuksille tai halutessasi asenna käyttöjärjestelmä uudestaan.

Puhelinvalmistajilta saat tarvittavat ohjeet ja työkalut, mutta tarvittaessa voit antaa puhelimesi myös luotettavan huoltoliikkeen puhdistettavaksi. Näiden toimenpiteiden seurauksena puhelimessa olevat tiedot valitettavasti usein menetetään, siksi puhelimen varmuuskopiointi on tärkeää.

2.6 Älypuhelin ei ole ikuinen

Jossakin vaiheessa puhelimen käyttöjärjestelmä tulee elinkaarensa päähän. Tällöin ohjelmistokehittäjä lopettaa puhelimen päivitykset eikä tietoturva-aukkoja enää korjata. Näin myös puhelimen käytöstä tulee turvatonta. Viimeistään tässä vaiheessa on syytä harkita uuden puhelimen hankintaa.

3 Lisävinkit tehokäyttäjille parempaan tietoturvaan

Viimeisen osan vihjeet on tarkoitettu niille, jotka käyttävät kännykkäänsä työ- ja raha-asioiden hoitamiseen ja hakevat selkeästi parempaa tietoturvaa. Vinkit hyödyntävät erityisesti niitä käyttäjiä, joiden tallennetut tiedot ja verkkoasiointi on syytä pysyä suojattuna kaikissa tilanteissa.

3.1 Käytä massamuistin salausta

Kun haluat salata puhelimeesi tallennetut tiedot, ota käyttöön massamuistin salaus. Muista myös salata muistikortti, sillä suuri osa tiedoista tallennetaan erilliselle muistikortille, puhelimen sisäisen muistin sijaan. Salauksen vahvuus

on suoraan riippuvainen käyttämäsi salasanan ja -koodin laadukkuudesta.

3.2 Poista käytöstä ylimääräiset langattomat yhteydet

Älypuhelimessa voi olla samanaikaisesti päällä lukuisia langattomia yhteyksiä, esimerkiksi WLAN, Bluetooth, NFC ja GPS. Ota ylimääräiset yhteydet käyttöön vain tarvittaessa ja poista ne välittömästi käytöstä, kun et niitä tarvitse.

Jatkuvasti päällä olevat tarpeettomat yhteydet kuluttavat akun virtaa ja saattavat yhdistää matkapuhelimen tuntemattomiin verkkoihin käyttäjän tietämättä. Kun kytket tarpeettomat yhteydet pois päältä, puhelimesi akku kestää pidempään ja yksityisyydensuojasi paranee.

3.3 Ota haittaohjelmatorjunta käyttöön

Tietokoneissa virustorjunta on jo arkipäivää, mutta myös matkapuhelimiin on saatavilla virustorjuntaohjelmistoja.

Etenkin jos käytät matkapuhelintasi usein työ- ja raha-asioittesi hoitamisessa, on syytä panostaa myös haittaohjelmatorjuntaan. Torjuntaohjelmistoja on saatavilla tunnetuilta ja luotetuilta palveluntarjoajilta.

3.4 "Roottaa" vain, jos tiedät mitä teet

Osa käyttäjistä haluaa nopeuttaa puhelimensa käyttöä tai lisätä sen ominaisuuksia muokkaamalla puhelimen alkuperäistä käyttöjärjestelmää tai vaihtamalla sen kokonaan uuteen kolmannen osapuolen käyttöjärjestelmään. Tätä kutsutaan puhelimen "roottaukseksi" (engl. rooting).

"Roottaus" voi kuitenkin avata puhelimen hyökkäyksille, jos valmistajan ylläpitämä ja päivittämä alusta altistetaan ulkopuolisille ja tuntemattomille tietoturva-aukoille.

Yleensä valmistajan takuu ei enää ole voimassa puhelimessa, jonka alkuperäisiä toiminnallisuuksia on muutettu. "Roottaus" onkin paikallaan vain osaavissa käsissä, kun se tulee aitoon tarpeeseen ja on puhelimen käytön kannalta välttämätöntä.

3.5 Suosi VPN-palvelua ulkomaan yhteyksissä ja avoimen WLAN:n käytössä

Jos käytät puhelintasi ulkomailla tai avoimissa WLAN-verkoissa, harkitse salatun yhteyden eli VPN:n käyttöä. Etenkin jos hoidat puhelimellasi päivittäisiä pankki- ja työasioitasi tai luet sähköpostiasi, VPN:n käyttö on suositeltavaa. VPN-yhteyden voit saada käyttöösi luotettavilta kaupallisilta toimijoilta.

3.6 Hallitse keskitetysti yrityspuhelimia

Yrityskäytössä olevien puhelimien yhteydenpitoa ja ylläpitoa varten kannattaa harkita keskitetyn hallintajärjestelmän MDM:n (Mobile Device Management) käyttöönottoa. Lisäksi yritysten olisi hyvä käyttää viestinnässään suojattuja yhteyksiä (VPN) ja salattuja sovellusyhteyksiä esimerkiksi sähköpostia luettaessa.

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi