



Ohjeita viestinnän suojaamiseen

Sisällysluettelo

Ohjeita viestinnän suojaamiseen	3
Luottamuksellisuus, eheys ja saatavuus	4
Hyvät käytännöt	6
Salasanan valinta	6
Mitä tietoa mihinkin palveluun?	6
Ohjelmistojen riittävä tietoturvaso	6
Luottamuksellisen tiedon suojaaminen	6
Varmuuskopiot ja niiden säilyttäminen	6
Yleisimmin käytetyt palvelut, niiden käyttöön liittyvät uhat ja niiltä suojautuminen	7
Puhelinpalvelut	7
Internetpalvelut	7
Internetyhteydet	11
Kodin langattomat internetyhteydet	11
Julkiset internetyhteydet	11
Mobiiliyhteydet	11
Älypuhelinten käyttö	12
Huomioi puhelimen käyttötarkoitus	12
Älypuhelimen käyttöönotosta	13
Viestintäpalveluiden käyttö ulkomailla	14

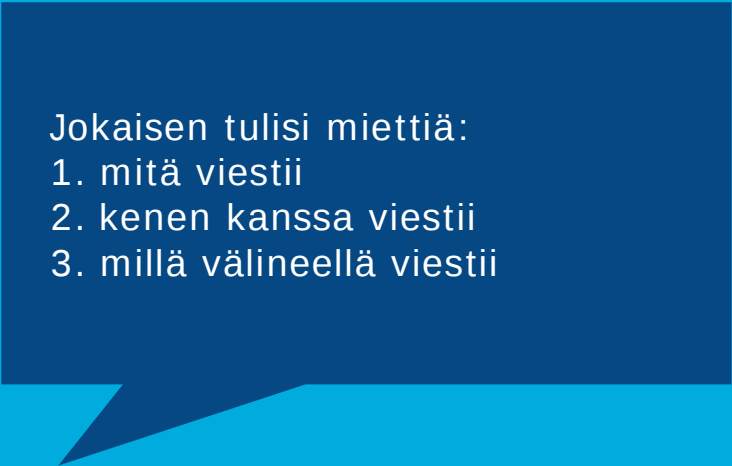
Ohjeita viestinnän suojaamiseen

Jokaisen internetiä käyttävän on syytä miettiä, missä määrin oma viestintä vaatii suojasta. Arviointia tehtäessä voi esimerkiksi pohtia, kuka voisi hyötyä viestinnän sisällöstä.

Luottamuksellista tietoa sisältävät viestit voi tarvittaessa salata. Ellei luottamuksellisia viestejä voi salata, kannattaa varmistaa, että tietoliikennetyhteys on suojattu. Ellei ole varma suojaustoimenpiteistä, kannattaa luottamukselliset keskustelut jättää käymättä.

On hyvä muistaa, että Suomen lainsäädäntö suojaa suomalaisissa tietoverkoissa välitettävien viestien luottamuksellisuuden, mutta se ei voi taata luottamuksellisuuden säilymistä ulkomaisissa viestintäpalveluissa tai Suomen rajojen ulkopuolella. Se, että palvelun käyttökieli on suomi, ei takaa, että palvelu on toteutettu Suomessa tai että tietojen käsittelyssä noudatettaisiin Suomen lainsäädäntöä.

Tässä ohjeessa kerrotaan tarkemmin internetin ja myös puhelimen käyttöön liittyvistä uhista luottamuksellisessa viestinnässä ja annetaan ohjeita viestinnän salaamiseen.



Jokaisen tulisi miettiä:

1. mitä viestii
2. kenen kanssa viestii
3. millä välineellä viestii

Luottamuksellisuus, eheys ja saatavuus

Sähköisen viestinnän turvaamisessa on syytä pohtia asioita tiedon luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta. Luottamuksellisuudella tarkoitetaan sitä, että viestejä pääsevät näkemään vain ne, joilla on siihen oikeutus. Eheydellä tarkoitetaan viestin sisällön oikeudettoman muuttumattomuuden varmistamista ja sitä, että viestintään käytetyt järjestelmät toimivat siten kuin niiden on tarkoitettu toimivan. Saatavuudella tarkoitetaan sitä, että tieto tai palvelu on saatavilla silloin, kun sitä tarvitaan.

Luottamuksellisuus on tärkein asia esimerkiksi henkilötietoja sisältävien tietojen välittämisessä tai yrityssalaisuuksien käsittelemisessä viestintäjärjestelmissä.

Verkkopankkiasioinnissa tärkein ominaisuus on **eheys**: käyttäjä voi luottaa siihen, että verkkopankkisivusto on aito ja asiointi on turvallista. Katso lisää: [Opas turvalliseen ostamiseen verkossa](#).

Julkisessa viestinnässä voi **saatavuus** olla tärkein asia, eli viesti on helposti kaikkien saatavilla. Viestinnän salaaminen parantaa tiedon luottamuksellisuutta, mutta saattaa heikentää viestinnän saatavuutta. Viestinnän suojaamista mietittäessä pitäisikin pohtia, mitkä näistä kolmesta asiasta ovat tärkeimmät ja valita suojauskeinot niiden mukaan. Alla on lueteltu esimerkinomaisesti suojauskeinoja ja esitetty niiden avulla saatettavaa suojaa luottamuksellisuuden, eheyden ja saatavuuden kannalta.

Toimenpide	Luottamuksellisuus	Eheys	Saatavuus
Sähköpostin salaus	Parantaa	Ei vaikutusta	Heikentää
Sähköinen allekirjoitus	Ei vaikutusta	Parantaa	Ei vaikutusta
Hyvän salasanan käyttö/ PIN-koodit	Parantaa	Ei vaikutusta	Heikentää
Ohjelmistojen ajantasaiset päivitykset	Parantaa	Parantaa	Parantaa
WLAN-verkon avoimuus	Heikentää	Heikentää	Parantaa
Tiedon tai koko kovale- vyn/muistitikun salaaminen	Parantaa	Ei vaikutusta	Heikentää
Yleisimpien pilvipalveluiden käyttö	Heikentää	Ei vaikutusta	Parantaa
WLAN-verkon WPA 2 salaus	Parantaa	Ei vaikutusta	Ei vaikutusta

Arvioi suojaamisen tarve:

1. Mieti, mitä tietoja lähetät, tallennat tai jaat käyttämissäsi palveluissa.
2. Pohdi tietojen arkaluonteisuuden perusteella, onko niiden suojaaminen tarpeen. Joskus tärkeämpää voi olla tiedon helppo saatavuus ja jakaminen, jolloin vahvojen suojausmenetelmien käyttö voi vaikeuttaa sujuvaa tiedon jakamista.
3. Valitse tai tarkista käytetyn palvelun mukaan sopiva suojausmenetelmä, mikäli tiedon suojaaminen on tarpeen. Eritasoisia suojausmenetelmiä on lukuisia eri tarkoituksiin.
4. Ulkopuolista voivat kiinnostaa esimerkiksi:
 - paikkatiedot
 - henkilötiedot
 - kontakti- ja viestintätiedot
 - pankkitiedot
 - kuvat
 - tiedostot
 - työmateriaali
 - käytetyt ohjelmistot ja laitteet
 - käyttäjätunnukset ja salasanat
 - verkkoselailu.

Hyvät käytännöt

Salasanan valinta

Eri palveluissa kannattaa käyttää eri salasanoja. Tärkeiden palvelujen käyttäjätunnusten ja salasanoiden valintaan ja säilytykseen on syytä kiinnittää erityistä huomiota. Palvelun tarjoama mahdollista lisävarmennusta kannattaa hyödyntää. Tällöin palveluun kirjautuminen vaatii salasanan lisäksi esimerkiksi matkapuhelimeen lähetetyn vahvistuskoodin. Itsellesi vähemmän tärkeiden palvelujen salasanoiden tallentamiseen voi käyttää salasanapalvelua tai -ohjelmistoa.

[Ohjeita hyvän salasanan valintaan](#)

Mitä tietoa mihinkin palveluun?

Harkitse tarkkaan, mitä tietoja on tarpeen antaa itsestäsi palveluun. Suojaustarvetta mietittäessä on hyvä olettaa, että kaikkiin järjestelmiin voidaan tunkeutua tai niistä voi löytyä hyväksikäytettäviä haavoittuvuuksia. Kerran paljastuneet tiedot voi olla mahdotonta saada pois internetistä.

Ohjelmistojen riittävä tietoturvaso

Pidä huolta tietokoneen ja matkapuhelimen ohjelmistojen ajantasaisuudesta. Käyttäjätunnukset ja salasanat päätyvät usein väärin käsiin haittaohjelman välityksellä. Asenna tietokoneeseesi ja matkapuhelimeesi vain ohjelmia, joita tarvitset. Suosi tunnettuja jakelukanavia ja valmistajan kotisivuja. Jotkut sivustot ehdottavat ohjelmistojen asentamista. Älä hyväksy asentamista, jos et tarvitse ohjelmaa.

Luottamuksellisen tiedon suojaaminen

Laitteen häviämisen varalta kannattaa tietokoneen kovalevy salata ja käyttää matkapuhelimessa suojakoodeja. Kovalevyn salaukseen voi käyttää esimerkiksi TrueCrypt-ohjelmistoa. Tiedostojen ja sähköpostiviestien salaukseen voi käyttää GPG/PGP-ohjelmistoja. Toinen vaihtoehto on käyttää erillistä salaavaa tallennusvälinettä, esimerkiksi usb-tikkua.

[Kansallisen tietoturvaviranomaisen NCSA-FI:n hyväksymiä salausratkaisuja](#)

Uudemmissa matkapuhelimissa on usein mahdollisuus ottaa käyttöön

tietojen salaus. Salaus saattaa olla päällä myös automaattisesti, jos

matkapuhelimen suojakoodit on otettu käyttöön. Matkapuhelimen tietojen tyhjennys etänä kannattaa myös ottaa käyttöön.

Varmuuskopiot ja niiden säilyttäminen

Laitteen häviämisen ja rikkoutumisen varalta kannattaa tiedoista ottaa säännöllisesti varmuuskopioita. Säilytyspaikka on harkittava tarkkaan. Varmuuskopiot kannattaa salata erityisesti, jos niitä säilytetään tai siirretään internetissä.

Yleisimmin käytetyt palvelut, niiden käyttöön liittyvät uhat ja niiltä suojautuminen

Puhelinpalvelut

Matkapuhelin (puhe, sms, MMS)

Matkaviestinverkon puheliikenne kulkee Suomessa, kun soittajalla ja vastaanottajalla on suomalaiset liittymät ja molemmat ovat puhelun aikana Suomessa. Tällöin viestinnässä noudatetaan Suomen lakeja. Soitettaessa ulkomaille, puhelun toisen osapuolen ollessa vierailulla ulkomailla tai toisen osapuolen käyttäessä ulkomaista liittymää voidaan soveltaa myös puhelun kohde- ja kauttakulkumaiden lakeja.

Tekstiviestit ja multimediaviestit reitittyvät Suomen sisäisesti, kun viestin lähettäjä ja vastaanottaja ovat Suomessa.

Uhat: Arkaluontoisten asioiden viestintään ei matkapuhelinta voi suositella ilman käyttäjän erityistoimia. Puhelin- ja tekstiviestiliikennettä sekä puhelimen sijaintia on mahdollista seurata matkapuhelimeen asennetun haittaohjelman avulla, teleyritysten välisen sanomavälitysliikenteen (SS7) tietoturvan heikkouksia hyödyntämällä tai matkapuhelinverkon tukiasemaksi naamioituvan valetukiaseman avulla. Hyökkäysten toteuttaminen vaatii tietotaitoa ja resursseja, joten ne ovat tyypillisesti tarkkaan johonkin henkilöön tai organisaatioon kohdennettuja. Näiden uhkien johdosta luottamuksellisia asioita ei kannata viestiä puhelimessa.

Viestintäviraston NCSA-toiminto on hyväksynyt salausratkaisuja eri tavoilla luokitellun tiedon välittämiseen.

[Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut](#) [pdf, 683 KB]

Yhteyden salaus: Matkaviestinverkon puhelut ovat salattuja puhelimen ja tukiaseman välillä.

Numeron salaus: Oman puhelinnumeron voi määrittää salaiseksi, jolloin puhelinnumero ei välity puhelun vastaanottajalle. Teksti- ja multimediaviestien yhteydessä myös salattu numero näytetään viestin lähettäjä tiedoissa.

Internetpalvelut

Internetissä tarjottavia palveluja voi käyttää niin kiinteän laajakaistaverkon kuin langattoman matkaviestinverkon datayhteyksien kautta. Verkon rakenteellinen toteutus on Suomessa, mutta verkkopalvelujen ja sivustojen tuottamiseen liittyvät palvelimet voivat sijaita Suomen rajojen ulkopuolella.

Verkkoselailu

Esimerkiksi: Uutispalvelut, hakukoneet

Verkossa asioidessa jää sivustolle jälki kävijästä ja kävijöiden syöttämistä tiedoista. Tallentuvia tietoja ovat esimerkiksi hakusanat, katsotut sivut ja sivujen selailuhistoria. Lisäksi useat verkkosivut pyytävät selainta tallentamaan muistiin evästeitä käyttäjän syöttämistä tiedoista, jotta sivustolla selailu on käyttäjälle sujuvampaa.

Verkkoliikenteen kansainvälisyys: Suomessa tietoja ei saa tallentaa käyttäjäkohtaisesti ilman henkilön suostumusta, mutta yleistilastot sivuvierailuista ja syötetyistä tiedoista ovat sallittuja. On huomioitava, että merkittävä osa palveluista on toteutettu Suomen rajojen ulkopuolella, jolloin noudatetaan palveluntarjoajan kotimaan lakeja. Palvelun tarjoaminen suomen kielellä ei takaa, että palvelu on tuotettu Suomessa.

Verkkosivuilla vierailun aikana tallennettuja tietoja voidaan käyttää sivuston käyttäjien kiinnostuksen määrittämiseen, sivustojen suunnitteluun ja käyttäjäprofiilien muodostamiseen mainostarkoituksessa.

Yhteiskäyttölaitteet: Selaushistoria ja evästeet kannattaa tyhjentää käytön jälkeen laitteesta, joka on muidenkin henkilöiden käytössä. Sivuhistorian tallentamisen voi myös estää selainasetuksista. Myös evästeiden käytön voi kieltää, mutta se voi hankaloittaa tai jopa estää joidenkin sivustojen katselua.

Kartta- ja navigaatiopalvelut

Esimerkiksi: Google Maps, Nokia Here Maps

Kartta- ja navigaatiopalvelut ovat sijaintitiedoille räätälöityjä palveluja, joissa käyttäjä haluaa tietää jonkin kohteen sijainnin, oman sijaintinsa tai reitin haluamiensa kohteiden välityksellä. Tiedot sijaintihauista jäävät palveluntarjoajan tietoon. Myös useat muut verkkosivustot ja -palvelut pyytävät sivulatauksen yhteydessä käyttäjän sijaintitietoja, jotta sivustolla voidaan esittää aluekohtaisia tietoja, kuten sääennustuksia sekä tietoja alueen tapahtumista ja palveluista.

Sijaintitietojen rajoittaminen: Käyttäjä voi määrittää palvelun ja laitteen asetuksista, että sijaintitietoja ei luovuteta automaattisesti. Navigaatiopalveluja käytettäessä sijaintitietojen lähettämisen voi estää lataamalla kartastot laitteeseen. Tällöin tiedot on päivitettävä itse säännöllisesti.

Sosiaalinen media

Esimerkiksi: Facebook, Twitter, Instagram, keskustelufoorumit

Sosiaalisen median palvelujen tietosuojakäytäntöihin on hyvä tutustua ennen palvelun ja suojausta vaativan viestinnän käyttöä. On muistettava, että kerran julkaistua tietoa on usein mahdotonta poistaa kokonaisuudessaan. Palveluissa on käytettävä hyviä salasanoja identiteetin suojaamiseksi. Tietoja syöttäessä on hyvä muistaa, että palveluun syötetyt tiedot voivat olla muidenkin kuin kohderyhmän saatavilla. Sosiaalisen median palvelut eivät pääsääntöisesti sovellu luottamuksellisen tiedon välitykseen.

Pikaviestimet

Esimerkiksi: Skype, Messenger

Pikaviestimet mahdollistavat reaaliaikaisen viestinnän kahden tai useamman henkilön välillä. Jos et ole varma, käytetäänkö pikaviestinohjelmassa salausta tai keille lähettämäsi viesti näkyy, luottamuksellisia tietoja ei kannata lähettää.

Sähköpostipalvelut

Esimerkiksi: Gmail, Hotmail, Luukku, Yahoo, Suomi24, laajakaistaliittymän mukana tulevat sähköpostipalvelut

Sähköpostiviestinnässä on huomioitava yhteyden suojaaminen. Lisäksi luottamuksellista tietoa sisältävät viestit tai liitetiedostot kannattaa tarvittaessa salata. Tietoa viestin vastaanottajasta ei voi salata, sillä sitä käytetään verkossa viestin siirtämiseksi vastaanottajalle. Palvelun tietosuojakäytäntöihin on hyvä tutustua ennen palvelun käyttöä ja ne kannattaa tarkistaa suojausta vaativassa viestinnässä.

Yhteyden suojaaminen: Käytä sähköpostiohjelmassasi suojattua yhteyttä sähköpostipalveluntarjoajan ohjeiden mukaisesti. Suojattu yhteys määritellään sähköpostiohjelman yhteysasetuksissa. Suojattu yhteys suojaa tietokoneen ja sähköpostipalvelimen välisen yhteyden salakuuntelulta.

Selainsähköpostia (esim. webmail-palvelut, Gmail, Google) käyttäessä tarkista, että käytössä on SSL-suojaus. SSL-suojaus salaa tietokoneesi ja nettisivun palvelimen välisen liikenteen sisällön ja auttaa sivuston aitouden varmistamisessa. Sivustolla käytetään SSL-suojausta, jos siitä kertova lukko on kiinni ja osoitteen alku on https://.



Sisällön suojaaminen: Sähköpostiviestin sisällön voi salata käyttämällä erillistä salaustenmenetelmää. Käytettävästä salaamistavasta täytyy sopia vastaanottajan kanssa. Useimmiten vastaanottajan täytyy käyttää samaa salaushjelmaa viestin salauksen purkamiseen tai tietää salaamiseen käytetty salasana. Viestin sisällön salaamiseen voi käyttää esimerkiksi sähköpostin suojaamiseen tarkoitettuja ohjelmistoja, kuten PGP (Pretty Good Privacy).

Pilvipalvelut

Esimerkiksi: Dropbox, Skydrive

Pilvipalveluja käytetään tyypillisesti tiedon, esimerkiksi varmuuskopioiden säilyttämiseen ja suurten tietomäärien, esimerkiksi valokuva-albumien sujuvaan jakamiseen.

Pilvipalvelujen käytössä on hyvä kiinnittää huomiota salasanan valintaan, suojattuun yhteyteen ja luottamukselliseksi tai arkaluonteiseksi arvioidun sisällön suojaamiseen.

Sisällön suojaaminen: Pilvipalveluun tallennettavat luottamukselliset tiedostot (kuvat, videot, dokumentit) voi ennen tiedostojen siirtoa salata turvallisuuden lisäämiseksi.

Verkkokaupat ja -pankit

Esimerkiksi: Amazon, Ebay

Verkkopalvelujen maksuliikenteen välityksessä ja kirjautumistiedoissa välitetään usein maksuväline- ja henkilötietoja, jotka kannattaa lähettää vain suojatun internetyhteyden kautta.

Suojattu yhteys: Tarkista aina ennen luottamuksellisten tietojen syöttämistä, että sivustolla käytetään SSL-suojausta. SSL-suojaus salaa tietokoneesi ja nettisivun palvelimen välisen liikenteen sisällön ja auttaa sivuston aitouden varmistamisessa. Sivus-

tolla käytetään SSL-suojausta, jos siitä kertova lukko on kiinni ja osoitteen alku on https://.



Näpäyttämällä lukkoa saat selainohjelmassa näkyviin sivun aitouden todentamiseen liittyvät tiedot. Tiedoissa näkyvän verkko-osoitteen pitää vastata selaimen osoiterivillä näkyvää verkko-osoitetta.



Internetyhteydet

Langalliset yhteydet ovat lähtökohtaisesti aina turvallisempia kuin langattomat yhteydet. Näin ollen erityisesti kotikäytössä langallisten yhteyksien käyttö on suositeltavaa. Monet laitteet voidaan liittää internetiin kuitenkin vain langattomien yhteyksien yli.

Kodin langattomat internetyhteydet

Kodin internetyhteys on yleisimmin toteutettu laajakaistatyypillisellä ADSL- tai kaapeliyhteydellä. Näissä yhteystyypeissä on yleistä, että yhteys jaetaan langattomasti WLAN-tukiasemalla esimerkiksi koko kodin käyttöön.

Oman WLAN-tukiaseman kautta tapahtuva liikennöinti on muistettava suojata siten, että:

1. sen kautta kulkevaa liikennettä ei voida suoraan salakuunnella ja
2. siihen ei voida liittyä ilman salasanaa. Tällä hetkellä suositellaan käytettäväksi WPA2-salausta (Wi-Fi Protected Access 2).

[Ohje langattomien verkkojen tietoturvasta](#)

Julkiset internetyhteydet

Yleisimpiä julkisia internetyhteyksiä ovat ns. avoimet WLAN-verkot, joissa yhteys on salaamaton. Avoimia verkkoja on esimerkiksi lentoasemilla, kahviloissa, kauppakeskuksissa ja muissa julkisissa tiloissa.

Avoimeen WLAN-verkkoon voi kytkeytyä kuka tahansa, jolloin yhteyden kautta siirrettävä tietoliikenne on helposti kenen tahansa sivullisen kuunneltavissa ja tallennettavissa, jos käytettävät sovellukset eivät salakirjoita liikennettä. Yleisin esimerkki sovelluksen käyttämästä salauksesta on verkkopankkien käyttämä https.

Monet julkiset avoimet WLAN-verkot vaativat erillisen kirjautumisen verkkosivun kautta ennen yhteyden muodostumista. Kirjautuminen avoimeen verkkoon ei kuitenkaan salaa liikennettä.

Avoimen WLAN-verkon käyttäjien on syytä varmistaa verkon tarjoajalta käytettävän verkon tiedot ja käyttöehdot.

Mobiiliyhteydet

Matkapuhelinverkoissa tapahtuva tiedonsiirto tukiaseman ja mobiililaitteen välillä on salattua Suomessa.

Älypuhelinien käyttö

Älypuhelinia käytetään puheluihin sekä internetpalvelujen hyödyntämiseen. Viestinnän yleisasetukset määrittävät käyttöönottovaiheessa. Palveluja käytetään pääasiassa älypuhelimelle ladattujen sovellusten avulla. Suurin osa sovelluksista edellyttää käyttäjän hyväksynnän esimerkiksi verkkoliikenteen tai sijaintitietojen käyttöön. Useat sovellukset käyttävät pilvipalveluita sovellusten tietojen tallentamiseen tai varmuuskopiointiin.

Yleisiä periaatteita

- Käyttäjä voi puhelimen käyttöönottovaiheessa määrittää puhelimen käyttöjärjestelmän yleisoikeuksia viestintään.
- Käyttäjä voi muuttaa määrityksiä myöhemmin.
- Sovelluksen asennusvaiheessa käyttäjä hyväksyy tai hylkää sovelluksen oikeudet viestintään.
- Osa sovelluksista ei toimi tai kaikki sovelluksen ominaisuudet eivät ole käytävissä, jos käyttäjä ei hyväksy sovelluksen vaatimia käyttöoikeuksia.

Huomioi puhelimen käyttötarkoitus

Älypuhelimien käyttöjärjestelmän ja sovellusten välittämien tietojen käyttöoikeudet kannattaa pohtia puhelimen käytön ja sillä käsiteltävän tiedon arkaluontoisuuden perusteella. Esimerkiksi työtehtävien vuoksi voi olla syytä rajoittaa puhelimen välittämää verkkoliikennettä tai sijaintitietoja. Rajoitukset voivat kuitenkin vähentää peruskäytössä olevan älypuhelimien käyttömahdollisuuksia. Esimerkiksi seuraavanlaiset sovellukset tarvitsevat toimiakseen tiettyjä käyttöoikeuksia:

- Puhelimen läheisyydessä olevista palveluista kertovat sovellukset tarvitsevat toimiakseen käyttäjän sijaintitiedon.
- Yhteydenpitoon tarkoitetut sovellukset voivat hyödyntää puhelinluettelon yhteystietoja, eikä niitä tarvitse tallentaa sovelluskohtaisesti.

On kuitenkin huomioitava mahdollisuus, että sijaintitiedot tai puhelinluettelo välittyvät ja tallentuvat myös sovelluksen ylläpitäjän palvelimille. Työnantajien on syytä pohtia asiaa ja opastaa henkilöstöä työkäytössä olevien älypuhelinien käytössä. Työnantajat voivat muun muassa laatia ohjeet puhelimen käyttöönottovaiheen asetuksista organisaation tietoturvapoliittikan mukaisesti sekä opastaa puhelimen käytön periaatteista.

Välitettävistä tiedoista kannattaa kiinnittää huomiota seuraaviin:

- Sijaintitiedot/Paikannustiedot
- Varmuuskopiointi
- Yhteystiedot
- Kalenteri

Lisäksi älypuhelimet voivat pyytää hyväksyntää seuraaviin tarkoituksiin:

- Mainosseurannan tietojen siirto
- Näppäimistö- tai käyttökokemuksen tietojen siirto palvelun parantamiseksi
- WLAN-tukiasematietojen lähettäminen
- Matkapuhelinverkon tukiasematietojen lähettäminen
- Automaattiset päivitykset

Älypuhelimien käyttöönotosta

Älypuhelimien käyttö edellyttää käyttäjätilin avaamista puhelimen ohjelmistovalmistajan palveluun. Tiliä käytetään puhelimen päivitysten ja sovellusten lataamiseen valmistajan sovelluskaupasta. Sama tili voi olla liitetty myös muihin palveluihin, kuten sähköpostiin. Palveluntarjoajalla on mahdollisuus yhdistää omassa palvelussaan samalta tililtä saatuja tietoja muihin saman palveluntarjoajan palveluiden tietoihin. Käyttäjätiliin kirjautumisen lisävarmennustoimenpiteet kannattaa aktivoida. Salasanan valinnasta löytyy lisätietoa ohjeen osiossa Hyvät käytännöt.

Älypuhelimien käyttöönoton yhteydessä on mahdollista ottaa käyttöön paikantamiseen liittyviä palveluita, kuten esimerkiksi puhelimen etäpaikannus varkaustapauksissa. Näiden palveluiden tietoturvariskit kannattaa arvioida tapauskohtaisesti.

Ohjelmistopäivitykset kannattaa aktivoida automaattisiksi, huomioiden mahdollisesti tarvittava päivitysten esto käytettäessä älypuhelimta ulkomaisissa matkaviestinverkoissa (roaming-kustannukset).

Sovellusten käytöstä on lisätietoa osiossa Yleisimmin käytetyt palvelut, niiden käyttöön liittyvät uhat ja niiltä suojautuminen.

Viestintäpalveluiden käyttö ulkomailla

Suomalaisten viestintäpalvelujen, kuten sähköpostipalvelujen tarjoajien on huolehdittava viestintäpalvelujensa luottamuksellisuudesta, eheydestä ja saatavuudesta. Kaikissa maissa lainsäädäntö ei takaa sähköiselle viestinnälle yhtä ehdotonta suojaa kuin Suomessa. Suomalaiset viranomaiset eivät voi taata ulkomaisen teleyrityksen tarjoamien viestintäpalveluiden tietoturvaa tai toiminnan luotettavuutta.

Esimerkiksi matkapuhelimella soittaminen ulkomailla ei takaa viestinnän luottamuksellisuutta, vaikka puhelimeen olisi asennettu suomalaisen teleyrityksen SIM-kortti. Sama koskee myös suomalaisen teleyrityksen tarjoaman sähköpostipalvelun käyttöä ulkomailla, koska tällöin käytetään ulkomaisen teleyrityksen tarjoamaa internetyhteyttä.

Yhteystiedot

PL 313

Itämerenkatu 3A

00181 Helsinki

Puh: 0295 390 100

Faksi: 0295 390 270

www.viestintävirasto.fi