Lähteet: Ny Teknik 4. 3. 2015, F-Secure/Jarno Niemelä, Colourbox, Karttakeskus.

10 tapaa suojautua älykännykän urkinnalta

Älypuhelin on Suomessa jo kuudella aikuisella kymmenestä ja lähes kaikilla teineillä. Se kulkee päivisin aina mukana, ja yöllä se lepää sängyn vieressä. Siksi se tarjoaa monia keinoja tarkkailla käyttäjäänsä.

Mitä enemmän hankimme puhelimeen ominaisuuksia, sitä haavoittuvampi se on. Oheen on listattu tapoja, joilla älypuhelinta voi vakoilla sekä keinoja suojautumiseen.

1. Langaton verkko, wifi

Wifin avulla voit liittyä automaattisesti langattomaan verkkoon. Urkkija voi tuoda julkiseen tilaan valetukiaseman. Se on julkisen verkon näköinen.

Kännykkä voi yhdistää välitukiasemaan suoraan käyttäjältä kysymättä. Näin käy yleisimmin lentokentillä, hotelleissa, rautatieasemilla ja ostoskeskuksissa.

Urkkija tarvitsee valetukiasemaan vain tietokoneen ja muutaman halvan laitteen.

SUOJAUS: Vältä langatonta yhteyttä julkisilla paikoilla. Puhelimen voi suojata vpn-yhteydellä eli salatulla erillisverkolla, jossa viestit kulkevat kuin tunnelissa. Vpn:n voi hankkia verkkosuojauksia tarjoavilta yhtiöiltä.

Julkisenkin verkon tulisi olla salasanan takana.

2. Sovellukset eli appsit

Sovelluksia eli appseja on tarjolla puhelimiin satoja tuhansia. Monet niistä ovat ilmaisia.

Jotta sovellus toimisi, palvelun tekijä pyytää usein käyttöönsä tiedon siitä, mitä puhelimesi tekee ja missä se on. Osa ohjelmistotaloista myy saamaansa tietoa eteenpäin.

"Ilmaista lounasta ei ole. Palvelun tarjoajan on jotenkin hyödyttävä siitä, että hankit ohjelman", sanoo tietoturvayhtiö F-Securen asiantuntija Jarno Niemelä.

SUOJAUS: Tietoturvayhtiöt tarkkailevat suosituimpia ilmaisohjelmia. Tarkista sovelluksen tuottajan tausta verkosta. Ohjelmaa hankkiessa varo antamasta liikaa henkilötietoja.

3. Evästeet eli cookiet

Evästeen avulla palvelun tarjoaja kerää sinusta tietoa, kun käyt palvelun nettisivuilla.

Evästeellä palvelu voi rekisteröidä, kuinka pitkään viivyt verkossa, mitä ostat tai aiot ostaa. Se voi mitata, mikä kiinnostaa sinua eniten. Tietoja käytetään esimerkiksi kohdistetussa mainonnassa.

SUOJAUS: Evästeiden käytön voi estää. Ilman evästeitä on kuitenkin vaikea käyttää verkkoa.

Puhelimella voi mennä selaimiin yksityisessä tilassa. Sellainen on saatavilla Firefoxiin, Googlen Chromeen ja Internet Exploreriiin.

Tietoturvayhtiöiden tarjoamassa vpn:ssä on yksityisyysominaisuus. Se sallii välttämättömät evästeet, mutta suodattaa evästeiden seurannan.

4. Haittaohjelmat

Sähköposti tai tekstiviesti voi tuoda linkin, josta puhelimeen latautuu haittaohjelma. Se voi esimerkiksi valjastaa puhelimesi lähettämään maksullisia tekstiviestejä. Myös verkkosivu voi huijata käyttäjän asentamaan haittaohjelman.

SUOJAUS: Haittaohjelmia vastaan auttavat tietoturvaohjelmat. Ohjelmia ladatessa ei kannata aina luottaa suosituksiin. Viiden tähden suosituksia saattavat tehtailla pientä korvausta vastaan ohjelmayhtiön palkkaamat henkilöt.

5. Operaattorin tiedot

Puhelinoperaattori joutuu keräämään puhelusta dataa, jotta puhelu yleensä menee perille.

Suomessa operaattorin pitää säilyttää puhelun datatietoja muutamia kuukausia. Poliisi saa käyttää näin koottua dataa tai kuunnella puhelinta, jos puhelimen käyttäjää epäillään rikoksesta.

Saksassa poliisi voi lähettää tekstiviestejä haamuina. Niiden avulla voi paikantaa epäillyn huomaamatta.

SUOJAUS: Yritä vaikuttaa kansalliseen lainsäädäntöön. Operaattorien pitäisi luovuttaa dataa vain vakavien rikosten selvittämiseen.

6. Pilvipalvelut

Pilvipalvelu tallentaa tietoa datakeskuksiin. Niitä pitävät yllä esimerkiksi hakukoneet ja yhteisöpalvelut.

Pilvipalvelun yksityisyyteen kannattaa suhtautua samoin kuin Facebookiin. Pilven kotimaan lainsäädäntö vaikuttaa siihen, mikä on yksityistä.

Googlea ja muita ulkomaisia yhtiöitä ei kiinnosta, mitä Suomen laki sanoo tietoturvasta.

SUOJAUS: Lue pilvipalveluiden ehdot huolellisesti.

Suomalaisen kannattaa käyttää suomalaista palvelua, sillä täällä tiedon luovuttaminen eteenpäin on laitonta. Tietoturvayhtiöt tarjoavat myös tiedon salaamista eli kryptausta.

7. Paikannuspalvelut

Agps tarkoittaa data-avusteista satelliittipaikannusta. Se määrittää puhelimesi paikan metrin tarkkuudella.

Yleensä käyttäjä suostuu siihen, että hänen puhelimensa voi paikantaa. Niinpä Google, Microsoft tai Apple tietää, missä olet.

Paikannuspalvelulla on hyvätkin puolensa. Se löytää sinut onnettomuuden sattuessa.

SUOJAUS: Agps:n voi laittaa pois päältä. Älypuhelinta voi käyttää ilman paikannusta, mutta silloin monet palvelut eivät toimi yhtä hyvin.

Googlen palveluissa paikkahistorian voi tyhjentää ja paikkatiedon keräämisen sammuttaa.

8. Bluetooth-verkot

Bluetooth luo langattoman radioyhteyden kännykästä toiseen kännykkään, tietokoneeseen, hiireen tai tulostimeen. Julkisessa tilassa joku voi ohjata kännykkäsi

Bluetooth-yhteyden omaan tietokoneeseensa. Saatat viestiä väärän laitteen kanssa huomaamatta eroa.

SUOJAUS: Kännykän asetuksia voi muuttaa niin, että se toimii vain 3G- tai 4G-verkoissa. Niitä on kallista ja työlästä väärentää.

Uusissa älykännyköissä Bluetooth-yhteyskin on hyvin suojattu.

9. Signaalintiedustelu

Kaikki data, joka liikkuu valokuiduissa ja kaapeleissa, voidaan kerätä talteen.

Turvallisuus- ja tiedustelupalvelut, kuten yhdysvaltalainen NSA, brittiläinen GCHQ ja venäläinen FSB, voivat vakoilla tietojasi kaapelista, kun data kulkee Suomen ulkopuolelle.

Suomalaiset käyttävät paljon esimerkiksi Googlen, Facebookin, Amazonin ja Applen palveluja. Ne ovat yhdysvaltalaisia yrityksiä, joten viestimme ovat periaatteessa seurannassa.

SUOJAUS: Viestit kannattaa suojata usealla eri tekniikalla. Jos yksi pettää, voi toinen paikata. Lyhenne https verkko-osoitteen alussa tarkoittaa SSL-salattua yhteyttä.

Matkoilla kannattaa käyttää vpn-yhteyttä, jos aikoo käyttää verkkopankkia tai tekee puhelimella muuta arkaluontoista. Skype-yhteys voi olla turvallisempi kuin tavallinen kännykkäpuhelu. Yritysten kannattaa käyttää omaa It-palvelua.

10. Vakoiluohjelmat

Esimerkiksi epäilevä vaimo tai aviomies voi asentaa vakoilutyökalun puolison puhelimeen. Näin hän pääsee seuraamaan, mitä puhelimella tehdään.

SUOJAUS: Tietoturvaohjelmat löytävät vakoiluohjelmat. Kännykän lukkokoodi estää ohjelmien asentamisen puhelimeen omistajan tietämättä.