Langattomasti, mutta turvallisesti

Langattomien lähiverkkojen tietoturvallisuudesta

Viestintävirasto
Kyberturvallisuuskeskus

Langattomasti, mutta turvallisesti

Tämä raportti on kooste Viestintäviraston Kyberturvallisuuskeskuksen syyskuussa 2014 julkaisemista langattomien lähiverkkojen tietoturvaa käsitelleistä artikkeleista.

Sisällys

1 Langaton lähiverkko — enemmän kuin silmä näkee

Langattomat lähiverkot eli WLAN:t ovat suosittu, halpa ja helppokäyttöinen tapa päästä tietokoneella tai älypuhelimella internetiin. Helppous ei kuitenkaan takaa turvallisuutta.

1.1 Mikä on langaton lähiverkko eli WLAN?

Langattomilla lähiverkoilla (englanniksi "wireless local area network", WLAN) tarkoitetaan yleensä IEEE 802.11 -ryhmässä määriteltyjä standardeja käyttäviä tietokoneiden liityntäverkkoja. Kauppanimi *Wi-Fi* viittaa nimenomaan kyseisiin standardeihin.

WLAN on maailmanlaajuinen standardi. WLAN-laitteet viestivät eri puolilla maailmaa käytännöllisesti katsoen samoilla 2,4 GHz- sekä 5 GHz -radiotaajuusalueilla. Taajuusalueet on standardeissa jaettu useiksi kanaviksi. Kanavat, joita saa käyttää, vaihtelevat maittain ja alueittain, mutta kaikki WLAN-tekniikkaa käyttävät laitteet toimivat kuitenkin kaikissa WLAN-verkoissa. Myös muunlaisia langattomia lähiverkkoja on olemassa, mutta niiden käyttö on huomattavasti vähäisempää kuin IEEE 802.11 -standardeihin perustuvien verkkojen, joten WLAN on käytännössä IEEE 802.11 -verkkojen synonyymi.

Langattomista lähiverkoista on tullut hyvin suosittuja niiden edullisuuden, käyttöönoton helppouden ja joustavuuden vuoksi. Langattoman lähiverkon kautta tarjotaan usein pääsyä internetiin. Helpoimmillaan se vaatii vain sähkövirran kytkemistä WLAN-tukiasemaan sekä laitteen liittämistä internetiin langallisen lähiverkon kautta. Tämän jälkeen WLAN:n käyttäjä tarkistaa esiasetetun verkon nimen tukiaseman käyttöoppaasta ja liittää tietokoneensa sen mukaiseen langattomaan verkkoon. Useimmissa uusissa kannettavissa tietokoneissa ja älypuhelimissa WLAN-asema on sisäänrakennettu.

1.2 WLAN:n heikkouksia

WLAN-tekniikan luonteeseen kuuluu, että langattomia verkkoja voi luoda melko vapaasti. Rajoitteena ovat radiotielle aiheutuvat häiriöt, joita syntyy vierekkäisten asemien päällekkäisistä kanavista ja sallittujen radiotaajuuksien rajallisesta määrästä.

Jotkin päätelaitteet kyselevät aktiivisesti ja käyttäjästä riippumatta, onko niiden muistamien verkkojen nimisiä verkkoja saatavilla. Hyökkääjä voi perustaa oman langattoman verkon, jonka nimi muistuttaa tai on sama kuin halutun verkon nimi. Samanniminen verkko voidaan myös luoda automaattisesti päätelaitteen tätä huhuillessa. Tämän vuoksi langaton yhteys kannattaa kytkeä pois päältä aina silloin, kun sitä ei tarvita.

Yleensä päätelaitteet pyrkivät automaattisesti käyttämään parasta radiosignaalia tuottavaa tukiasemaa, ja laite voi itsenäisesti yhdistää tai vaihtaa huomaamatta hyökkääjän verkkoon. Näin hyökkääjä voi kaapata käyttäjien liikennettä oman tukiasemansa kautta ja hyödyntää tai tallentaa haluamiaan tietoja.

Langattomassa verkossa myös muut käyttäjät voivat ottaa yhteyttä laitteeseen, ellei sitä ole estetty tukiasemassa (ns. langaton verkon erotus). Jos käyttäjien tunnistautuminen verkkoon on toteutettu ja säädetty huonosti, myös pahantahtoisten tahojen on mahdollista kytkeytyä siihen ja lähettää muille käyttäjille tai verkon laitteille haitallista liikennettä. Siksi on hyvä huolehtia myös päätelaitteiden turvallisuudesta.

1.3 Viestinnän salaus WLAN:ssa

WLAN-tekniikka perustuu vapaasti eteneviin radioaaltoihin samaan tapaan kuin radiopuhelimissa. Muut asemat voivat kuulla lähettävän aseman viestin, vaikka viesti olisi tarkoitettu vain jollekin tietylle asemalle. Siksi viestit on pystyttävä salakirjoittamaan.

WLAN:n radiorajapintaa varten on määritelty useita vaihtoehtoisia salausmenetelmiä. Niistä WEP- *(Wired Equivalent Privacy)* ja WPS-menetelmien *(Wi-Fi Protected Setup)* salakirjoitusalgoritmi on kuitenkin murrettu. WPA2+AES-salaus jaettua avainta (englanniksi "pre-shared key", PSK) käyttäen on kotikäyttäjälle hyvä ratkaisu, kunhan jaettu avain ei ole hyökkääjän helposti arvattavissa tai saatavissa.

Lähes kaikissa WLAN-tukiasemissa on mahdollisuus valita, näkyykö verkko kaikille vai ei. Tällä ei kuitenkaan ole mitään tekemistä salauksen kanssa. Verkon näkyvyysasetus vaikuttaa ainoastaan siihen, mainostaako tukiasema verkon olemassaoloa vai pitääkö siihen liittyvien päätelaitteiden tietää verkon nimi muuta kautta voidakseen lähettää viestejä verkkoon.

Tärkeää on myös muistaa, että WLAN-liikenteen salaus koskee vain radioliikenteen salausta. WLAN-tukiasema ei vaikuta siihen, onko siitä johtoa pitkin lähtevä liikenne salattu vai ei. Lisäksi pahantahtoinen taho voi päästä muokkaamaan tukiaseman kautta kulkevaa liikennettä, jolloin muutkin suojausmenetelmät voidaan murtaa. Sama pätee toki kaikkiin verkkoihin, mutta WLAN-verkoissa viestien väärentäminen on teknisesti helpompaa kuin muissa verkoissa.

Paras suojautumiskeino käytettäessä yleisiä WLAN-verkkoja on huolehtia, että käytettävä internet-palvelu (esimerkiksi pankki tai sähköposti) käyttää liikenteen päästä päähän ulottuvaa salausta tai jopa käyttää erillistä kokonaisvaltaista liikenteen salausta tarjoavaa palvelua. Salauksessa voi hyödyntää luotettavaa kaupallista tarjoajaa tai kodin tai työpaikan salakirjoitettua VPN-yhteyttä.

1.4 Tarkkana oman WLAN:n ylläpidossa

WLAN-tukiasemien turvallinen hallinta vaatii tarkkaavaisuutta. Hallintakäyttöliittymän oletussalasana, jota käyttäjä ei ole muuttanut, on väärinkäyttäjälle helppo ja huomaamaton tapa muokata verkon säädöt itselleen sopiviksi. Niin kuin aina, tehtaalla asetetut salasanat kannattaa muuttaa heti.

Vuodesta 2011 lähtien jonkun toisen suojaamattoman WLAN-verkon käyttämistä ei Suomen rikoslaissa ole enää katsottu luvattomaksi käytöksi, eikä se sinällään ole siis enää rangaistavaa (laki 190/2011 rikoslain muuttamisesta).

Suojaamaton langaton verkko tarkoittaa sellaista verkkoa, jonka radioliikennettä ei ole salakirjoitettu. Toiset jakavat tarkoituksella omaa internetyhteyttään ilmaiseksi WLAN:n yli kenelle tahansa tarvitsevalle naapuriavun hengessä. Toisaalta WLAN voi myös tahattomasti jäädä suojaamatta, jos omistaja ei osaa suojata sitä tai ymmärrä, mitä suojaaminen tai suojaamatta jättäminen tarkoittaa.

Jos joku WLAN:n käyttäjä törttöilee tai loukkaa tietoturvaa, tekijä itse on luonnollisesti vastuussa tekemisistään. Avoimen WLAN:n omistajan ongelmana on kuitenkin se, että verkon kautta tehtyjen tietoturvaloukkausten paljastuessa poliisi tulee luultavasti ensimmäisenä kyselemään tapahtuneesta verkon omistajalta. Poliisi voi tällöin esimerkiksi ottaa tekovälineiksi epäillyt laitteet ja tietokoneet haltuun todistusaineiston suojelemiseksi. Prosessiin joutuneelle verkon omistajalle voi aiheutua paljon

vaivaa, vaikka häntä ei epäiltäisikään rikoksesta.

1.5 Lisää aiheesta

Ohje 2/2011 Langattomien verkkojen tietoturvasta
https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeettulkinnatsuosituksetjaselvityksetjaohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22011langattomienverkkojentietoturvasta.html

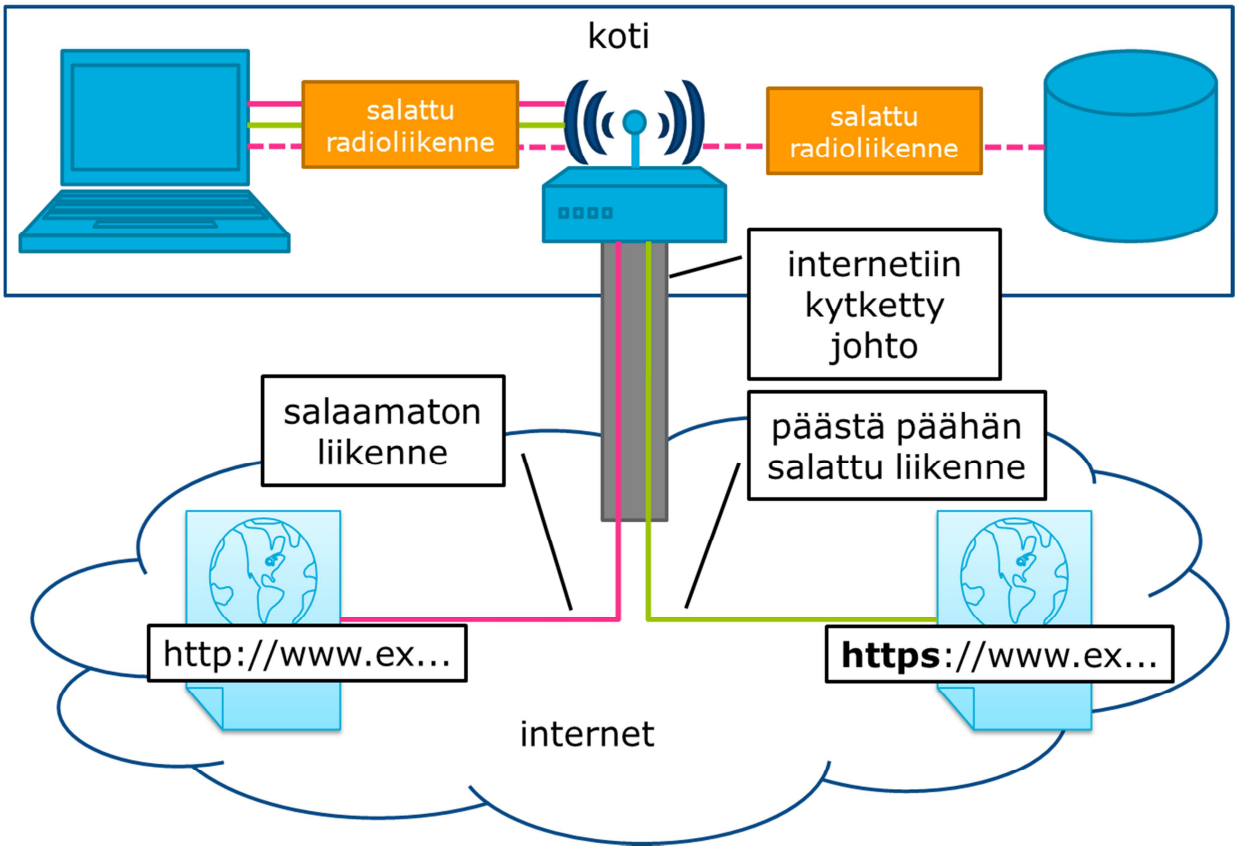
IEEE 802.11 Wireless Local Area Networks. The Working Group for WLAN Standards
http://grouper.ieee.org/groups/802/11/

2 WLAN-salaus koskee vain radioliikennettä

Salatun langattoman lähiverkon (WLAN) käyttö ei ole sen turvallisempaa kuin salaamattoman langallisen lähiverkon. Tietysti mikä tahansa WLAN:n salaus tarjoaa parempaa suojaa salakuuntelua ja harhautuksia vastaan kuin salauksen käyttämättä jättäminen.

2.1 Pitäisikö salata?

Koska WLAN-tekniikka perustuu vapaasti eteneviin radioaaltoihin, hyvissä oloissa signaali on kuultavissa yli sadan metrin etäisyydellä ja erikoisvälineillä viestintä onnistuu kilometrinkin päästä. Kuka tahansa voi lähettää oikeita tai väärennettyjä viestejä verkkoon.



Kuva 1 Langattoman lähiverkon salauksen vaikutus rajoittuu vain langattomaan tiedonsiirtoon. Langaton lähiverkko ei suojaa yhteyksiä esimerkiksi verkkosivuihin, vaan siihen pitää käyttää muita keinoja.

Tietoturvallisuuden takaamiseksi WLAN-käyttäjän pitäisi pystyä varmistumaan, että hänen laitteensa viestii tunnetun tukiaseman kanssa, ja että muut kuulolla olevat laitteet eivät pysty ymmärtämään hänen ja tukiaseman välistä liikennettä tai ujuttamaan sekaan valheellisia viestejä. Viestinnän luottamuksellisuuden vuoksi viestit on pystyttävä salakirjoittamaan ja niiden eheys varmistamaan.

Viestiliikenteen salaaminen vaatii päätelaitteissa ja tukiasemissa käytettäviä salaisia tietoja, kuten salakirjoitusavaimia. Salaisuuksien jakaminen voi joissakin tapauksissa olla työlästä ja joissakin harvinaisissa tilanteissa salauksen käytöstä voi olla enemmän haittaa kuin hyötyä.

2.2 WLAN:n salausmenetelmiä

WLAN:n radiorajapintaa varten on määritelty useita vaihtoehtoisia salausmenetelmiä. Nämä menetelmät salakirjoittavat päätelaitteen ja tukiaseman välillä kulkevat viestit niin, etteivät sivulliset pysty niitä helposti ymmärtämään tai muokkaamaan huomaamattomasti.

Salausmenetelmät myös tunnistavat tukiaseman käyttäjille niin, etteivät muut voi helposti esiintyä luotettuna tukiasemana. WLAN:n käyttäjiä ja päätelaitteita WLAN:n salauksella ei kuitenkaan pysty luotettavasti tunnistamaan.

Vanhin salausmenetelmä WEP *(Wired Equivalent Privacy)* on osoitettu monella tapaa haavoittuvaksi, eikä sitä suositella käytettäväksi, jos uudempia menetelmiä on saatavilla. WPA2 *(Wi-Fi Protected Access II)* on ollut Wi-Fi Alliancen hyväksymissä laitteissa tuettu vuodesta 2006 lähtien. Se täytyy kuitenkin osata ottaa käyttöön. Myös WPA-salaus saattaa olla käytettävissä. WPA-salaus oli välivaihe WLAN-standardien kehityksessä ennen kuin WPA2 saatiin valmiiksi.

Myös Wi-Fi Protected Setup- eli WPS-salaus on osoitettu haavoittuvaksi, eikä sitä suositella enää käytettäväksi. WPS-salaus oli tarkoitettu helppokäyttöiseksi vaihtoehdoksi WPA2:lle, mutta WPS:n suunnitteluvirheiden vuoksi hyökkääjä voi vähäisellä vaivalla arvata salausavaimen.

2.3 Suosituksia salaukseen

Kuluttajille suositellaan Advanced Encryption Standard -algoritmia käyttävää WPA2-salausmenetelmää ja siihen vahvaa (pitkä, monimutkainen ja vaikeasti arvattava) esijaettua salasanaa. Langattoman tukiaseman asetuksissa tämä valinta esiintyy yleensä merkintänä "WPA2+PSK (AES)" tai "WPA2-Personal". Vahvan 20-merkkisen salasanan laatiminen ei ole vaikeaa, eikä sitä tarvitse muistaa ulkoa, kun sen tallentaa päätelaitteen käyttöjärjestelmän muistiin verkon ensimmäisellä käyttökerralla.

Kotiverkon salasana voi olla turvallista kirjoittaa muistiin paperille, jota säilyttää kirjoituspöydän laatikossa. Jos joku hyökkääjä pystyy sen sieltä viemään, hän pystyy siitä riippumatta tekemään myös paljon ilkeämpiäkin asioita verkolle ja sen käyttäjille, joten kodin suojaaminen tehokkaasti tuo enemmän turvaa kuin verkon monimutkaisen salasanan opettelu ulkoa.

Lain mukaan yksinkertaisenkin salauksen murtaminen on Suomessa kiellettyä ja rangaistavaa. Kannattaa kuitenkin aina käyttää vahvaa salausta, sillä käyttämisen vaiva on kuitenkin suunnilleen yhtä suuri.

Jos motivoituneet salakuuntelijat arvioidaan varteenotettavaksi uhaksi, tulee muistaa, että jokainen, joka saa

WLAN:n esijaetun salasanan haltuunsa, pystyy purkamaan salauksen kaikesta kuulemastaan kyseisen WLAN:n liikenteestä. Tämä voi olla erityisen varteenotettava uhka yritysten tarjoamissa vierailijaverkoissa. Vaikka verkon tarjoava yritys olisi luotettava, kaikki verkossa vierailevat eivät välttämättä ole. Suojatun näennäisen yksityisverkon (engl. encrypted VPN) käyttö on suositeltavaa.

WLAN-verkon asetusten turvallisuudesta on yhteenveto alla olevassa taulukossa.

2.4 Lisää aiheesta

Ohje 2/2011 Langattomien verkkojen tietoturvasta
https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeettulkinnatsuosituksetjaselvitykset/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22011langattomienverkkojentietoturvasta.html

Asetus	Turvallisuus
ei salakirjoitusta	Ei ole turvallinen ilman erillistä salausta ja vastapuolen tunnistusta.
WEP-salaus	Ei suositella käytettäväksi, jos WPA- tai WPA2-salaus on käytettävissä. WEP-salaus on melko helposti murrettavissa.
WPA-salaus	Varsin turvallinen, mutta WPA2 on vieläkin turvallisempi.
WPA2-salaus	Suositeltu, vahvin saatavilla oleva salaus. Vanhat päätelaitteet eivät ehkä tue WPA2:a, mutta tukiasemat voi asettaa käyttämään WPA:ta ja WPA2:ta samanaikaisesti.
WPS-salaus	Ei suositella käytettäväksi, sillä on erittäin helposti murrettavissa. WPS-salaus kannattaa kytkeä pois päältä tukiasemasta.
piilotettu verkko (engl. disable SSID broadcast)	Ei suositella käytettäväksi, sillä asetus ei lisää yhtään tietoturvaa ja saa jotkin verkkoon kytketyt päätelaitteet lähettämään verkon nimeä silloin, kun ne eivät ole siihen yhteydessä.

3 Suojaamattoman WLAN:n käyttö

Avoimissa ja suojaamattomissa langattomissa lähiverkoissa tietoturvasta huolehtiminen jää pääasiassa käyttäjän vastuulle. Myös oman avoimen WLAN:n ylläpitäminen vaatii huolellisuutta.

3.1 Naapurin suojaamattoman WLAN:n käyttö

Langattoman lähiverkkoyhteyden voi pitää suojaamattomana, jolloin kuka tahansa voi käyttää sitä. WLAN-yhteys voidaan usein erityistoimenpiteillä säätää myös niin, ettei verkko näy ulkopuolisille (ns. hidden SSID, hidden WLAN tai "ei-mainostettu" WLAN). Se, että verkko ei näy ulkopuolisille, ei tarkoita, että verkko olisi suojattu. Verkon suojauksesta tulee tarvittaessa huolehtia erikseen.

Verkon suojaamisella tarkoitetaan sitä, että verkko on suojattu esimerkiksi salasanalla, jolloin ennalta määrittelemättömät henkilöt eivät pääse käyttämään verkkoa. Verkon suojaaminen salasanalla on suhteellisen varma keino estää

verkon luvaton käyttö sellaisilta ulkopuolisilta, jotka eivät ryhdy murtamaan suojausta. Jos verkon suojaus murretaan, kysymys voi olla rikoslain (39/1889) 38 luvun 8-8a §:ssä tarkoitetusta tietomurrosta.

Suomessa suojaamattoman langattoman tietoverkkoyhteyden kautta muodostettu internet-yhteyden käyttäminen ei ole rangaistava teko. Kun suojaamattoman verkon käyttöön ei liity riskiä syyllistyä rikokseen, avointen langattomien verkkojen tarjoaminen on mahdollista.

Internetiä saa siis käyttää avoimen WLAN:n kautta. Riitojen välttämiseksi toisten omistamien verkkojen käyttäminen kannattaa kuitenkin pitää kohtuullisena ja muutenkin välttää haitan aiheuttamista verkonkäytöllään. Esimerkiksi yhteyden muodostaminen suojaamattoman verkon kautta sisäverkon palvelimiin, toisen henkilön tietokoneelle tai erityisaloilla käytettyihin tietojärjestelmiin tai päätelaitteisiin voi olla rangaistavaa luvattomana käyttönä (rikoslaki (39/1889) 28 luku 7-9 §).

3.2 Viestinnän luottamuksellisuus

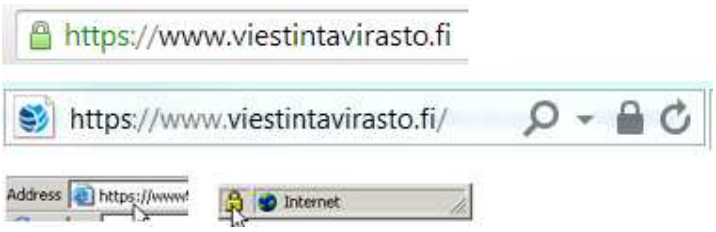
Viestintä suojaamattomassa WLAN:ssa on Suomen lain mukaan yhtä luottamuksellista kuin postikortissa: viestinnän salaisuus on rikkomaton. Käytännössä viestintäsalaisuuden rikkomista on kuitenkin kummassakin tapauksessa vaikea huomata tai osoittaa.

Oleellista on miettiä etukäteen, miten arvioida vieraiden verkkojen turvallisuutta ja verkkojen ylläpidon ammattimaisuutta sekä suhteuttaa vieraiden verkkojen käyttö niiden luotettavuuteen. Joissakin verkoissa esimerkiksi saattaa olla parempi käyttää nettiä vain nimettömästi, eikä kirjautua mihinkään sivustoille omilla käyttäjätunnuksilla. Edistyneemmille käyttäjille ja yritysten työntekijöille salakirjoitukseen perustuva näennäinen yksityisverkko eli kryptografinen VPN voi olla hyvä lisäturva.

Myös suojattujen www-sivujen käyttö suojaa hyvin salakuuntelulta ja viestien vääristelyltä. Suojatut www-sivut tunnistaa siitä, että niiden osoite alkaa protokollatunnisteella "**https**" ja selaimen osoiterivillä tai tilatiedoissa näkyy kiinni olevan lukon kuva. Myös muiden Transport Layer Security- (TLS) ja Secure Sockets Layer (SSL) -suojattujen palveluiden käyttö on varsin turvallista.

Langattoman lähiverkkotekniikan luonteeseen kuuluu, että väärennettyjen viestien lähettäminen on huomattavan helppoa. Langallisten verkkojen tilanteeseen nähden väärennettyjen viestien lähettäjän kiinnijäämisen riski on pieni.

Väärennetyillä viesteillä voi sotkea salakirjoitettujakin yhteyksiä, jopa siinä määrin, että uhri kuvittelee keskustelevansa luotetun palvelimen kanssa, vaikka hän oikeasti keskustelee hyökkääjän kanssa.



Kuva 2 Esimerkkejä verkkoselainten tavoista ilmoittaa www-yhteyden olevan salattu päästä päähän.

Avoimen WLAN:n käytössä korostuu tarve arvioida omasta päätelaitteesta verkkoon näkyviä palveluita. Esimerkiksi Windows-tietokoneissa käyttäjien on helppo jakaa tiettyjen tiedostokansioiden sisältöjä muille kotiverkon käyttäjille. Jaot näkyvät helposti myös liitettäessä tietokone vieraaseen verkkoon, ellei käyttäjä poista jakoja käytöstä tai säädä käyttöjärjestelmän ohjelmistopalomuuria estämään jakoihin liittyvä liikenne. Microsoftin Windows Vista- ja myöhemmissä Windowsin versioissa verkon sijainnin (engl. network location) valinta vaikuttaa automaattisesti muun muassa näihin suojausasetuksiin.

Jos suojattavat tiedot ovat hyvin arvokkaita (esimerkiksi yrityssalaisuuksia) ja todennäköiset hyökkääjät hyvin varustautuneita, on parasta olla käyttämättä suojaamattomia WLAN-verkkoja sellaisten tietojen käsittelyyn.

Laajakaistaiset kolmannen ja neljännen sukupolven matkaviestinverkot (3G ja 4G) ovat varteenotettava vaihtoehto vieraan WLAN:n käytölle. Niiden käyttö Suomessa suomalaisella liittymällä on kohtuullisen edullista. Ulkomailla mobiililaajakaistan käyttö voi kuitenkin olla huomattavasti kalliimpaa.

3.3 Tunnistautuminen

Salauksen puuttumisesta huolimatta langaton lähiverkko saattaa vaatia käyttäjältään tunnistautumista tai käyttöoikeuden osoittamista. Karkeimmillaan se tarkoittaa, että tukiasemaan on määritelty, mitkä päätelaitteet saavat käyttää sen palveluita.

Hienostuneempi tapa vaatia käyttäjien tunnistautumista on asettaa verkkoon tai tukiaseman yhteyteen palvelin, jolle pitää esittää esimerkiksi käyttöoikeuden todistava koodi. Käyttäjä voi saada koodin esimerkiksi paperilapulla hotellin vastaanottotiskiltä ilmaiseksi tai veloitusta vastaan. Tunnistautumista ja maksua voidaan vaatia myös edellyttämällä luottokorttitietojen syöttämistä tunnistautumispalvelimelle, joka sitten veloittaa luottokorttia automaattisesti.

Tunnistautumisen vaatiminen antaa epärehellisille toimijoille mahdollisuuden käyttää ihmisten antamia tietoja väärin. Jos verkon omistaja on epärehellinen, hän voi käyttää keräämiään tietoja toisin kuin mihin tiedot luovuttaneet ihmiset ovat ne tarkoittaneet. Epärehellinen kolmas osapuoli voi myös verkon omistajan tietämättä saada käyttäjä uskomaan, että tämän pitää antaa joitakin tietoja huijarin tekemän verkkosivun kautta. Suojaamattomassa langattomassa verkossa valesivun levittäminen ei ole vaikeaa.

Markkinoilla on saatavilla tietoja varastavia tukiasemia ja ohjelmistoja sellaisille rikollisille, jotka eivät halua itse räätälöidä välineistöään. Laitteet eivät välttämättä muistuta normaalia langatonta tukiasemaa ja ohjelmalliset versiot voivat toimia esimerkiksi älypuhelimessa.

WLAN-kirjautumissivujen ja liikenteen luotettavuutta tulisi suojaamattomissa verkoissa arvioida samalla tavalla kuin muussakin internetkäytössä: mitä tietoja kannattaa luovuttaa, miksi näitä kysytään ja näyttääkö kaikki normaalilta. Verkon omistajan edustajalta, kuten kahvilan tai hotellin henkilökunnalta kannattaa kysyä ohjeita ennen kuin menee luovuttamaan tietojaan. Hotellihuoneesta löytyy myös usein kirjalliset ohjeet verkon käyttöön.

3.4 Lisää aiheesta

Ohje 2/2011 Langattomien verkkojen tietoturvasta
https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeettulkinnatsuosituksetjaselvitykset/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22011langattomienverkkojentietoturvasta.html

Näin meitä huijataan! https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/07/ttn20140723140 8.html

Hallituksen esitys Eduskunnalle laiksi rikoslain 28 luvun 7 §:n muuttamisesta http://www.finlex.fi/fi/esitykset/he/2010/20100277

Microsoft: Verkkosijainnin valitseminen, Windows 7 http://windows.microsoft.com/fi-fi/windows/choosing-network-location#1TC=windows-7

4 Liikkuvan työntekijän WLAN-selviytymisopas

Langattomat lähiverkot tekevät työn tekemisestä tien päältä helppoa ja edullista. Työt voi tehdä myös tietoturvallisesti, kun noudattaa yrityksen tietoturvamääräyksiä ja kuluttajillekin tärkeää perushuolellisuutta ja varovaisuutta palveluiden käytössä.

4.1 Perusasiat kuntoon

Useilla työpaikolla on tarkat ohjeet ja määräykset siitä, miten työpaikan tietokoneita ja tietoteknisiä palveluita tulee käyttää työnantajan tilojen ulkopuolella. Liikkuvan työntekijän tulee osata ohjeet ja määräykset hyvin, sillä ne kuuluvat työnantajan työnjohto-oikeuden piiriin. Määräysten rikkominen voi pahimmillaan johtaa jopa työntekijän vahingonkorvausvastuuseen sekä työsuhteen purkuun.

Matkustavan työntekijän on hyvä huolehtia työvälineidensä tietoturvasta ja päivityksistä. Erityisesti kannattaa huolehtia sähköisten tunnistevälineiden (niin sanottu token tai toimikortti) turvallisesta säilytyksestä. Jo salatun VPN-yhteyden käyttöön tarvittava tunnistevälineen katoaminen voi altistaa työntekijän tietoturvauhalle. Jos työntekijä noudattaa työnantajan antamaa määräystä käyttää toimiston ulkopuolella VPN-yhteyttä, hän ei voi tunnistevälineen puuttuessa käyttää internetiä. Jos taas työntekijä ei noudata määräystä vaan käyttää internetiä kaikesta huolimatta, hänen verkkoliikennettään voi olla helppo salakuunnella.

Tietojen vakoilemiseen ei välttämättä tarvita tietotekniikkaa. Tietokoneen näytön katselu työntekijän selän takaa voi paljastaa paljon. Näyttöruutuun asetettavat tietoturvasuojakalvot vähentävät mahdollisuuksia asiattomaan kurkkimiseen, mutta täyttä suojaa eivät nekään anna.

4.2 Tarvitsetko varmasti WLAN:a?

Jo päätelaitteen WLAN-aseman päälle kytkeminen voi paljastaa hyökkääjille arvokkaita tietoja. Useimmat päätelaitteet nimittäin huhuilevat aktiivisesti, onko niiden tuntemia verkkoja saatavilla. Hyökkääjät saattavat odottaa paikoissa, joissa liikkuvia työntekijöitä vierailee usein, ja seurata, minkä nimisiä verkkoja laitteet kyselevät.

Laitteiden tekemien kyselyiden perusteella hyökkääjät voivat profiloida mahdollisia uhrejaan. Kysyttyjen verkkojen nimistä hyökkääjät saattavat päätellä, että jonkin tietyn laitteen käyttäjä on vieraillut jossakin hyökkääjiä kiinnostavassa verkossa ja on ehkä kiinnostavan yrityksen työntekijä. Tämän jälkeen hyökkääjät voivat kohdistaa uhriin valikoituja kyber- ja kineettisen maailman hyökkäyksiä sekä pyrkiä manipuloimaan tätä.

Hyökkääjät voivat myös tekaista samannimisen verkon, mitä käyttäjän laite on huhuillut. Monet laitteet kytkeytyvät automaattisesti ennestään tuntemiinsa verkkoihin. Jos alkuperäinen oikea verkko on ollut suojaamaton, kytkeytyminen onnistuu. Tällöin hyökkääjät voivat helposti salakuunnella uhrin liikennettä.

Siksi on hyvä kytkeä laitteen langaton lähiverkkotoiminto kokonaan pois käytöstä aina silloin, kun sitä ei tarvita. Joissakin laitteissa sen voi tehdä erityisellä katkaisimella, toisissa toimintoa ohjataan ohjelmallisesti.

Joka tapauksessa luottamus WLAN-verkon hyvään ylläpitoon pitää aina arvioida. Jos et luota verkon pääsynhallintaan, käyttäjien valitsemiseen, liikenteen erottamiseen tai verkon ylläpitäjään, älä käytä kyseistä verkkoa.

4.3 Käyttö ulkomailla

IEEE 802.11 -standardeihin perustuvat WLAN-laitteet käyttävät taajuuskaistoja, jotka on kansainvälisesti sovittu vapaasti käytettäviksi. Kanavat, joita kaistoilta saa käyttää, vaihtelevat maittain. Langattomat verkkolaitteet osaavat yleensä käyttää sallittuja kanavia, kunhan niille määritellään kulloinenkin sijaintimaa. Päätelaitteet yleensä tunnistavat maakoodin tukiasemien lähettämistä tiedotteista, eikä WLAN:n käyttäjän tarvitse huolehtia asiasta.

Ihmisten suhtautuminen langattomiin verkkoihin vaihtelee maittain ja tapahtumittain. Maissa, joissa alalla ei ole toimivaa lainsäädäntöä tai valvontaa, voi langaton verkko olla pahantahtoisten hakkereiden puuhakenttä. Erityisesti tietoturvakonferensseissa tai -koulutuksissa tarjottavat verkot mielletään usein hakkerityökalujen testausympäristöksi, vaikka niitä ei ole välttämättä sellaiseksi tarkoitettu.

Ulkomaiden langattomia lähiverkkoja koskeva lainsäädäntö voi muutenkin poiketa tuntuvasti suomalaisesta laista. Esimerkiksi Venäjällä on 8.8.2014 uutisoitu määräyksestä, jonka mukaan julkisten eli suojaamattomien WLAN:ien käyttäjien on rekisteröidyttävä verkkoa ylläpitävälle operaattorille, jonka puolestaan on pyydettäessä luovutettava kerätyt henkilötiedot viranomaisille.

4.4 Verkkojen kartoitus

Useat tietotekniikka-alan suuryritykset, kuten Microsoft ja Google, pyrkivät luomaan maailmanlaajuisia karttoja langattomien lähiverkkojen sijainneista. Langattomia lähiverkkoja käyttävät päätelaitteet, erityisesti älypuhelimet, saattavat lähettää yrityksille tietoja havaitsemistaan verkoista. Tietoja keräämällä yritykset pyrkivät muun muassa tarjoamaan nopeita, varmatoimisia ja tarkkoja paikannuspalveluita.

Joillekin käyttäjille ja organisaatioille tämä on tietoturva- ja tietosuojariski. Jotkin yritykset saattavat haluta pitää langattomien lähiverkkojensa nimet salassa. Verkon nimen mainostamisen esto WLAN-tukiasemassa (verkon "piilotus") saattaa paradoksaalisesti vaikeuttaa verkon salassapitoa, sillä jotkin päätelaitteet kutsuvat muuallakin ollessaan niitä piilotettuja verkkoja, joissa ne ovat vierailleet. Päätelaitteen ja sitä kantaneen ihmisen kulkeman reitin voi päätellä tarkkailemalla esimerkiksi metroasemilla tai muissa liikenteen solmukohdissa tietoja, joita päätelaite lähettää automaattisesti koskien sen tuntemia verkkoja.

Tietojen keräämisen ja lähettämisen voi kytkeä pois päältä päätelaitteissa. Esimerkiksi Nokian Lumia-puhelimissa sen voi tehdä WLAN-asetusvalikossa olevan WLAN-seurannan hallinnan asetuksilla.

4.5 Lisää aiheesta

Päätelaitteiden tietoturvaohje 5/2013 VAHTI
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20131210Paeaetel/name.jsp

Sisäverkko-ohje 3/2010 VAHTI
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/name.jsp

Microsoft: Non-broadcast Wireless Networks with Microsoft Windows; Why Non-broadcast Networks are not a Security Feature http://technet.microsoft.com/en-us/library/bb726942.aspx#EDAA

5 Tietoturva oman langattoman lähiverkon ylläpidossa

Yhteydenotto langattomaan lähiverkkoon käy huomaamattomasti. Tämä tarkoittaa sitä, että jos joku yrittää tehdä pahojaan verkossasi, asia paljastuu todennäköisesti vahinkojen jo tapahduttua. Tässä artikkelissa neuvomme, kuinka välttää vaaroja oman WLAN:n ylläpidossa.

5.1 Tukiaseman turvallisuus

Tukiaseman tietoturvallisuus on avain koko langattoman verkon tietoturvallisuuteen. Mikä tahansa IEEE 802.11 -standardin mukainen laite voi toimia WLAN:n tukiasemana. Yleensä tukiasemana käytetään siihen tarkoitettua laitetta, joka käytännössä on pieni erikoistunut tietokone.

Kuten minkä tahansa tietokoneen, myös WLAN-tukiaseman suojauksessa tulee huomioida sen fyysinen suojaus, sähköinen pääsynhallinta, tärkeiden tietojen varmuuskopiointi, tapahtumakirjanpito, ohjelmiston päivitykset sekä palveluiden kovennus.

Tukiaseman fyysisen suojauksen tarkoitus on havaita ja estää laitteen peukalointi asiaankuulumattomilta henkilöiltä. Kotioloissa riittää, että tukiasema suojataan kuten muukin kodin irtaimisto. Julkisissa tiloissa tukiasema voi olla syytä ruuvata kattoon ja sen johdotus koteloida. Sisäverkon ylläpitäjien kannattaa myös suodattaa kytkimillä muualta sisäverkosta langattomille tukiasemille menevää liikennettä esimerkiksi VLAN:eja (engl. virtual local area network) käyttäen.

Tukiaseman asetuksia hallitaan yleensä lähiverkon yli tukiaseman WWW-käyttöliittymällä. Monissa laitteissa pääsy hallintakäyttöliittymään on automaattisesti estetty laitteen langattomasta portista ja internetportista. Valitettavasti on sellaisiakin laitteita, joissa pääsy hallintakäyttöliittymään on suojattu vain salasanalla. Kannattaa valita laite, johon pääsyä voi säädellä.

Tukiaseman hallintakäyttöliittymässä on yleensä vain yksi käyttäjätunnus, esimerkiksi "admin". Sen salasana tulee valita huolella ja vaihtaa ajoittain. Jos laitteeseen on mahdollista luoda useita käyttäjätilejä, kannattaa luoda omansa eri käyttäjille ja käyttötarkoituksille.

Joissakin tukiasemamalleissa on viime aikoina paljastunut tietomurron mahdollistavia niin sanottuja takaportteja. Takaportti on huonosti dokumentoitu tai kokonaan dokumentoimaton ominaisuus, joka tyypillisesti mahdollistaa laitteen etähallinnan heikosti suojatulla tavalla. Käyttäjien kannattaa seurata asiaa koskevia tietoturvauutisia ja vaihtaa turvallisempaan laitteeseen, jos vanhasta laitemallista paljastuu takaportti. Myös muunlaiset korjaavat toimenpiteet voivat olla mahdollisia, mutta niiden suorittaminen vaatii usein erityistä tietoteknistä taitoa.

Tukiaseman tuottamia ja siinä säilytettäviä tärkeitä tietoja ovat lähinnä tukiaseman asetukset sekä tapahtumalokitiedot. Tiedot voidaan yleensä varmuuskopioida laitteen hallintakäyttöliittymän kautta. Tapahtumalokitiedot ovat tärkeitä vikatilanteiden ja tietoturvaloukkausten selvittämiseksi ja tulevien vahinkojen estämiseksi.

WLAN-tukiasemien ohjelmistot eivät yleensä päivity itsestään, vaan ylläpitäjän täytyy olla itse aktiivinen ja tarkastaa säännöllisesti, onko laitteille tarjolla päivityksiä. Tukiasemalaitteisiin saattaa olla liitettynä myös muita toimintoja kuin WLAN-tukiasemana toimiminen.

Muihin toimintoihin kannattaa tutustua ja sulkea kaikki ne, jotka ovat tarpeettomia itselle.

5.2 Radiohäiriöt

Tukiaseman radiolähettimen lähetystaajuudet ja -tehot vaikuttavat laitteen käytön tietoturvallisuuteen. Väärin lähettävä tukiasema voi aiheuttaa haitallisia häiriöitä muille radioaaltoja käyttäville laitteille ja näin estää palveluita. Suomessa WLAN-laitteille sallitut radiokaistat ja lähetystehot on lueteltu Viestintäviraston määräyksessä 15 laajakaistaisten datasiirtolaitteiden (WAS/RLAN) luokassa (ks. kappale 5.6).

WLAN-laitteet valmistetaan usein niin, että niillä on kyky käyttää kaikkia IEEE 802.11 -standardiperheessä määriteltyjä taajuuksia. Se, mitä taajuuksia laite käytännössä käyttää ja millä lähetysteholla, määritellään yleensä laitteen hallintaohjelmistolla. Siksi WLAN-laitteiden asetusten määrittely, erityisesti maa-asetus, on käyttöönotossa tehtävä oikein.

Turvallisen WLAN-laitteen ostamiseen ja sen säätämiseen turvalliseksi saa neuvoja muun muassa laitteen myyjältä, Viestintäviraston tekemästä radiolaitteiden ostajan oppaasta (ks. kappale 5.6) sekä omalta telepalveluoperaattorilta.

5.3 Verkon turvallisuus

Langattoman lähiverkon tietoturvallisuudella tarkoitetaan tässä verkon käyttäjien suoraan kokemaa tietoturvallisuutta. Verkon käyttäjillä on heidän tarvitsemiensa tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen ja joskus myös verkossa tehtyjen toimenpiteiden kiistämättömyyteen liittyviä tarpeita.

Tukiaseman ja internetliittymän siirtonopeus on rajallinen. Jättäessään langattoman lähiverkon suojaamatta omistaja ottaa riskin jäädä itse vaille tarvitsemaansa palvelua, sillä ennalta rajaamaton käyttäjäjoukko saattaa käyttää liian paljon verkon kaistaa.

Vuoden 2009 jälkeen valmistetut tukiasemat pystyvät tyypillisesti välittämään liikennettä yli 100 Mbit/s, joten pullonkaulaksi muodostuu yleensä internetliittymän nopeus. Helppo tapa välttää tämä riski on suojata WLAN salasanalla ja antaa salasana vain niille, joiden luottaa käyttävän verkkoa kohtuullisesti.

Joissain tukiasemissa on mahdollista määritellä erillinen langaton lähiverkko satunnaisia vieraita varten. Vierasverkolle voi määritellä oman nimen ja salasanan. Vierasverkko on toiminnassa samanaikaisesti tukiaseman tavallisen langattoman verkon kanssa. Näin tavallisen verkon nimeä ja salasanaa ei tarvitse paljastaa vieraille, joihin ei ehkä täysin luota. Vierasverkon voi usein myös erottaa muusta sisäverkosta niin, että vierasverkon käyttäjät pääsevät ainoastaan internetiin.

Kaiken kaikkiaan radioliikenteen salaaminen ratkaisee useimmat langattoman lähiverkon turvallisuusuhat. Salausta on käsitelty tämän raportin luvussa 0.

Niin kuin kaikki muutkin salasanat, myös langattoman lähiverkon salasana kannattaa muuttaa ajoittain.

5.4 WLAN-"mokkulat" ja kännykän internetyhteyden jakaminen WLAN:lla

Markkinoilla on monia niin sanottuja WLAN-mokkuloita eli langattoman laajakaistaverkon (3G- tai 4G-matkapuhelinverkon) kautta internetiin kytkeytyviä laitteita, joita voi käyttää WLAN:n välityksellä. Nämä laitteet ovat WLAN-tukiasemia, jotka tyypillisesti saavat sähkövirtansa omasta akustaan. Myös useiden älypuhelinten internetyh-

teyttä on mahdollista jakaa WLAN:n välityksellä lähellä oleville laitteille. Tällöin älypuhelinkin toimii WLAN-tukiasemana.

Niiden käyttöön pätee kaikki, mitä edellä on sanottu muiden WLAN-tukiasemien ja -verkkojen ylläpidosta. Sekä WLAN-mokkuloissa että älypuhelimissa tukiaseman tietoturva-asetuksia voi kuitenkin olla vaikea tai jopa mahdoton muuttaa. Oletusasetukset ovat onneksi kohtuullisen turvalliset useimpiin käyttötilanteisiin, mutta oletusarvoiset salasanat pitää aina muuttaa ennen käyttöä.

Android-, iOS- (Apple) ja Windows Phone 8 -käyttöjärjestelmät (muiden muassa uudet ja päivitetyt Nokian Lumia-puhelimet) tukevat ilmarajapintasalausta suositelluin asetuksin (WPA2-PSK (AES)). Windows Phone 8:ssa salauksen asetuksia ei voi muuttaa eikä poistaa käytöstä. Android- ja iOS-käyttöjärjestelmissä asetuksia pystyy vaihtamaan myös turvattomampiin.

Markkinoilla olevat kuluttaja-asiakkaille tarjottavat WLAN-mokkulat tukevat niin ikään WPA2-PSK (AES) -salausta.

5.5 WLAN:n käyttö kännykällä

Monissa WLAN-toiminnolla varustetuissa älypuhelimissa on langattomien lähiverkkojen käyttöä helpottavia ominaisuuksia. Joissakin tilanteissa ominaisuuksien käyttö voi kuitenkin vaarantaa käyttäjän yksityisyyden ja tietoturvan.

Windows Phone 8.1 -käyttöjärjestelmää käyttävissä älypuhelimissa (esimerkiksi useat Nokia Lumia -puhelimet) on toiminto nimeltään WLAN-seuranta (engl. WiFi Sense). Kun toiminto on käytössä, puhelin kytkeytyy automaattisesti suojaamattomiin langattomiin lähiverkkoihin silloin, kun WLAN-toiminto ja puhelimen paikannustoiminto ovat päällä. Lisäksi toiminto paitsi hakee Microsoftilta tietoja lähistön langattomista lähiverkoista, myös jakaa Microsoftille puhelimen tallentamat salattujen verkkojen nimet ja salasanat.

Puhelimessa voi myös määritellä, salliiko käyttäjä Microsoftin jakaa verkkojen salasanat käyttäjän kavereiden Windows Phone 8.1 -puhelimille, joissa WLAN-seuranta on käytössä. Salasanoja ei näytetä kavereille, mutta käytännössä heidän puhelimensa saavat salasanat selväkielisinä. Puhelimen ensimmäisessä käyttöönotossa WLAN-seuranta tarjotaan oletusarvoisesti kytkettäväksi päälle. Käyttäjien kannattaa tutustua Windows Phone 8.1:n tietosuojatietoihin.

Android-käyttöjärjestelmällä toimivat älypuhelimet voi asettaa varmuuskopioimaan puhelimen asetukset, mukaan lukien tallennetut langattomien lähiverkkojen nimet ja salasanat, Googlen pilvipalveluun. Jos puhelin rikkoutuu, katoaa tai vaihdetaan uuteen, käyttäjä voi palauttaa tiedot pilvestä. Tiedot tallennetaan pilveen selväkielisinä ja vain käyttäjän Google-tilin salasanan suojaamina. Varmuuskopiointi on käytössä oletusarvoisesti, mutta käyttäjä voi kytkeä sen pois päältä. Käyttäjän kannattaa tutustua Googlen tietosuojatietoihin.

Myös Applen iOS-käyttöjärjestelmällä toimivissa laitteissa on varmuuskopiointitoiminto. Varmuuskopiot tallennetaan Applen pilveen käyttäjän iTunes-tilille. Langattomien lähiverkkojen salasanat varmuuskopioidaan vain, jos käyttäjä valitsee varmuuskopioiden salakirjoittamisen. Salakirjoituksessa käytettävää salasanaa laite ei tallenna minnekään, joten tiedot ovat varsin hyvässä turvassa niin kauan, kuin käyttäjä muistaa salasanan.

5.6 Lisää aiheesta

Ohje 2/2011 Langattomien verkkojen tietoturvasta
https://www.viestintavirasto.fi/ohjausja

valvonta/ohjeettulkinnatsuosituksetjaselvitykset/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22011langattomienverkkojentietoturvasta.html

Viestintäviraston määräys 15 luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä https://www.viestintavirasto.fi/ohjausjavalvonta/lainsaadanto/maaraykset/maarays15luvastavapaidenradiolahettimienyhteistaajuuksistajakaytosta.html

Luvasta vapautetut radiolaitteet https://www.viestintavirasto.fi/taajuudet/radiolaitteet/luvastavapaatlaitteet.html

Radiolaitteet. Ostajan opas. 6. uudistettu painos, Helsinki 12/2013 https://www.viestintavirasto.fi/attachments/Radiolaitteen_ostajan_opas.pdf

Ohjeita viestinnän suojaamiseen https://www.viestintavirasto.fi/attachments/Ohjeita_viestinnan_suojaamiseen.pdf

Microsoft: Yhteyksien muodostaminen WLAN-seurannalla http://www.windowsphone.com/fi-fi/how-to/wp8/connectivity/use-wi-fi-sense-to-get-connected

Android Central: Android's Wifi backup feature is neither new, unique nor dangerous http://www.androidcentral.com/android-s-wifi-backup-feature-neither-new-unique-nor-dangerous

Apple: iTunes: About iOS backups http://support.apple.com/kb/HT4946

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