

OUCH!

Tässä numerossa...

- Langaton kotiverkkosi
- Verkkosi kytketyt laitteet

Kotiverkkosi suojaaminen

Yleiskatsaus

Vuosia sitten kotiverkot olivat suhteellisen yksinkertaisia, parhaimmillaan vain pelkkiä yhteyspisteitä kodin tietokoneelta internettiin. Viime vuosina kotiverkoista on kuitenkin tullut huomattavan paljon monimutkaisempia, nykyisin lisäämme verkkoomme monia laitteita ja käytämme verkkoa myös muuhun kuin pelkkään internet-selailuun. Tässä uutiskirjeessä kerromme miten voit luoda turvallisen kotiverkon itsellesi ja perheellesi.

Vierastoimittaja

Cheryl Conley johtaa tietoturvatietoisuustiimiä Lockheed Martinilla. Hänen tietoturvatietoisuuskampanjansa on jalkautettu yli 100 000:lle työntekijälle, alihankkijalle ja yrityksen yhteistyökumppanille. Seuraa Cherylä [@conleychera](#).

Langaton kotiverkkosi

Lähes jokaisen kodin verkon perustana on langaton verkko (wifi tai wlan). Tämän avulla kodin laitteesi pystyvät kytkeytymään verkkoon langattomasti ilman johtoja. Suurinta osaa langattomista verkoista hallinnoidaan internet-reitittimellä, joka on joko palveluntoimittajasi tai itsesi asentama verkkolaite, joka kytkee kotiverkkosi ulkoverkkoon. Kotisi eri laitteet yhdistyvät langattomaan verkkosi tällä reitittimellä. Reitittimen kautta laitteet pystyvät keskustelemaan internettiin tai muiden kotisi laitteiden kanssa. Tämän vuoksi langattoman verkkosi turvallisuus on oleellinen osa kotisi suojaamista. Suosittelemme seuraavia toimenpiteitä langattoman verkkosi suojaamiseen.

- Vaihda reitittimen oletussalasanat, erityisesti hallinnointiin käytettävien tunnuksien osalta. Hallinnointiin käytettävä tunnus on tunnus, jolla kirjaudutaan laitteen hallinta-asetuksiin ja muutetaan laitteen asetuksia. Monet verkkolaitteet toimitetaan oletustunnuksien kanssa ja näiden tunnuksien salasanat ovat yleisesti tiedossa, jolloin laitetta pääsee halutessaan hallinnoimaan kuka vaan. Tämän vuoksi salasanat kannattaa vaihtaa pitkiksi, uniikkeiksi salasanoiksi, jotka vain sinä tiedät.
- Vaihda laitteesi asettama kotiverkkosi oletusnimi (SSID). Tämä on verkkotunnus, jonka laitteet näkevät etsiessään verkkoa. Anna verkollesi uniikki nimi, jonka tunnistat itse helposti, mutta varmista että nimessä ei ole mitään luottamuksellista tietoa, kuten osoitettasi tai nimeäsi. Verkkosi asettaminen piilotetuksi (tai niin että laite ei lähetä itse nimeään verkkoon) ei käytännössä tehosta tietoturvaa, koska modernit skannauslaitteet tai kokeneet hyökkääjät löytävät myös piilotetut verkot.

Kotiverkkosi suojaaminen

- Varmista, että vain luotetut henkilöt pystyvät liittymään langattomaan verkkoosi ja että kyseiset yhteydet ovat salattuja. Voit varmistua näistä asioista käyttämällä johtavia turvallisuuskäytäntöjä. Paras langattoman verkon suojaustapa on tällä hetkellä WPA2. Enabloimalla tämän käyttöön, langattomaan verkkoosi liittymisen vaatii aina salasanan ja kun salasana on syötetty, kaikki verkkoliikenne on salattua. Älä käytä vanhempia salaustapoja, kuten WEP tai jätä salausta kokonaan pois. Avoimet verkot mahdollistavat kenen tahansa liittymisen kotiverkkoosi.
- Varmista, että langattomaan verkkoosi kytkeytymiseen tarvittava salasana on tarpeeksi vahva ja eri kuin reitittimen pääkäyttäjäsalausana. Muista, että tämä salasana täytyy syöttää useimmiten vain kerran, liityttäessä verkkoon ensimmäistä kertaa ja tämän jälkeen laitteesi muistavat salasanan.
- Monet langattomat verkot tarjoavat vierasverkko-ominaisuutta. Tämän käyttö mahdollistaa vieraidesi internet-käytön, mutta pitää sen erillään muista verkkosi laitteista. Jos luot vierasverkon, muista noudattaa siinä samoja turvallisuusasetuksia kuin pääverkossa.
- Älä ota käyttöön "WiFi Protected Setup" tai muuta vastaavaa toiminnallisuutta, joka mahdollistaa uuden laitteen liittymisen verkkoosi ilman salasanaa.
- Jos sinusta tuntuu, että muista kaikkia eri salasanoja, suosittelemme salasanaohjelmiston käyttöönottoa.



Jos et ole varma miten saat edellä mainitut suositukset toteutettua reitittimelläsi, pyydä palvelutarjoajaltasi lisäohjeita, katso reitittimen mukana tulleista ohjeista tai etsi reitittintäsi koskevat ohjeet valmistajan kotisivuilta.

Verkkoosi kytketyt laitteet

Seuraava vaihe on tietää mitä laitteita langattomaan verkkoosi on kytketty ja varmistaa, että nämä laitteet ovat turvallisia. Ennen tämä oli suhteellisen vaivatonta, mutta koska nykyisin kotona voi olla niin monia laitteita ja lisäksi "aina verkossa" olevat laitteet, kuten televisio, vauvamonitori tai jopa termostaatti tarvitsevat verkkoa, tämä voi olla hankalaa. Helppo tapa tarkistaa langattomaan verkkoon kytketyt laitteet on käyttää yksinkertaista verkkoskanneria, kuten Fingiä. Näiden koneelle

Kotiverkkosi suojaaminen

tai mobiililaitteelle asennettavien sovellusten avulla voit skannata langattoman verkon ja tunnistaa jokaisen verkkoon kytketyn laitteen. Kun olet tunnistanut kaikki kytketyt laitteet, varmista että niiden turvallisuusasetukset ovat asianmukaiset. Varmista, että kaikissa laitteissa on viimeisimmät käyttöjärjestelmäpäivitykset ja että automaattiset päivitykset ovat kytketty päälle. Jos laitteesi mahdollistavat salasanan käytön, käytä aina mahdollisimman vahvaa ja uniikkia salasanaa. Kannattaa myös tutustua palveluntarjoajasi verkkosivuihin, siellä on usein neuvoja kotiverkkosi suojaamiseen.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-utiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa <http://www.securingthehuman.org>.

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2015#april2015
Salasananhallintasovellukset:	https://securingthehuman.sans.org/ouch/2015#october2015
Tablettisi suojaaminen:	https://securingthehuman.sans.org/ouch/2016#january2016
Kotiverkkosi skannaaminen:	http://l.rud.is/home-network-mapping

Lisenssi

OUCH! julkaisijana toimii "SANS Securing The Human"-organisaatio ja jakelu tapahtuu [Creative Commons BY-NC-ND 3.0 lisenssillä](#). Voit vapaasti jakaa tätä uutiskirjettä ja käyttää sitä osana tietoturvatietoisuusohjelmaasi kunhan et muokkaa uutiskirjettä. Käännös- ja lisätietoja varten, ota yhteys www.securingthehuman.org/ouch. Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy



securingthehuman.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.org/gplus