

Rotary



# Rotarin tietoturva...

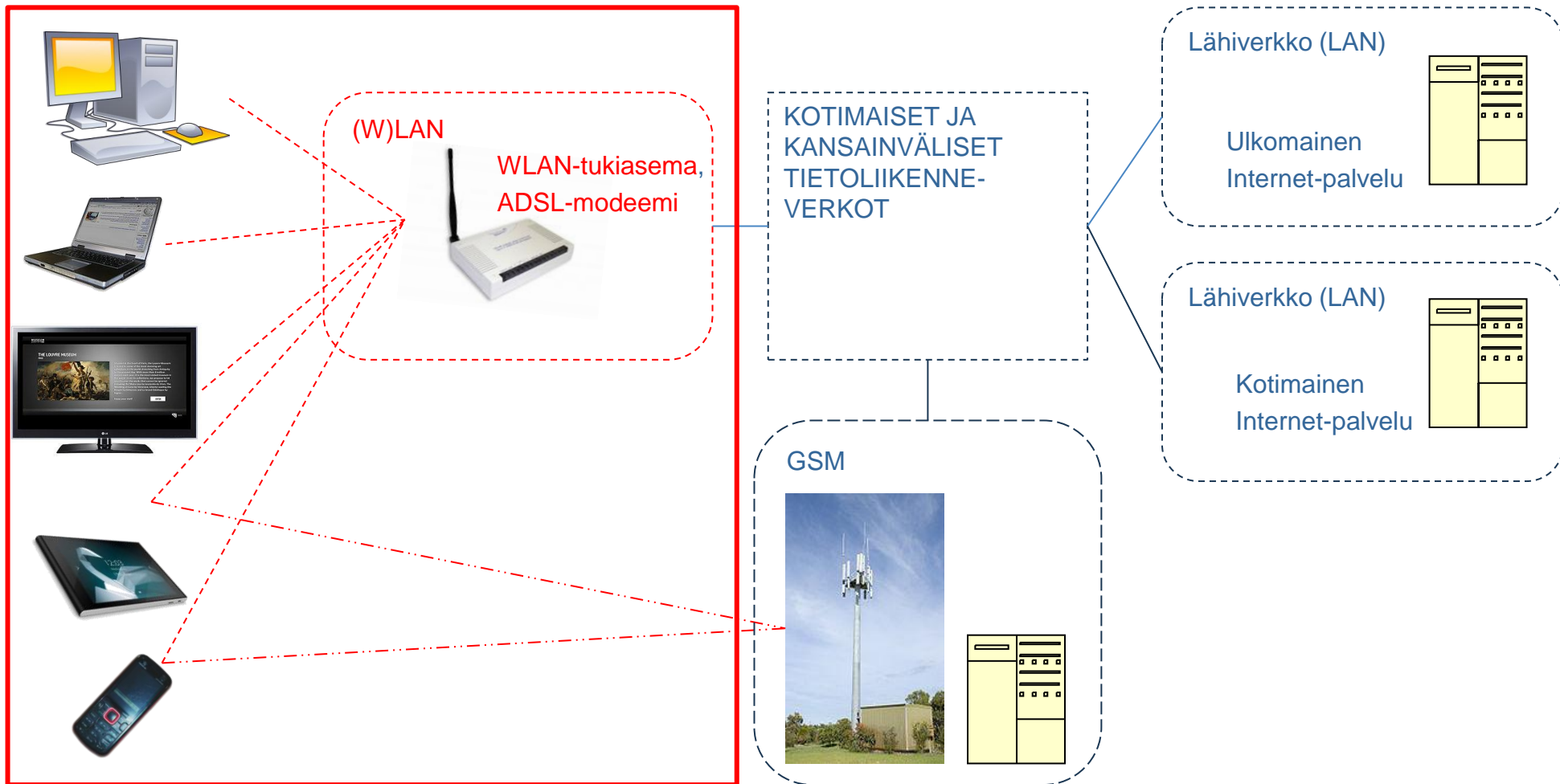
Veikko Brax

29.10.2015

Ylivieskan Rotaryklubi



# ... lähinnä ihmisen ja päätelaitteen näkökulmasta





## ... lähinnä ihmisen ja päätelaitteen näkökulmasta



Tietoliikenne-  
verkkojen  
(puhelinverkot,  
matkapuhelin-  
verkot,  
Internet,...)  
tietoturva

Ulkomaisen  
verkko-  
palvelun  
rotary.org,...)  
tietoturva

Kotimaisen  
verkko-  
palvelun  
(rotary.fi,  
ylivieskanrot  
ary.net,...)  
tietoturva

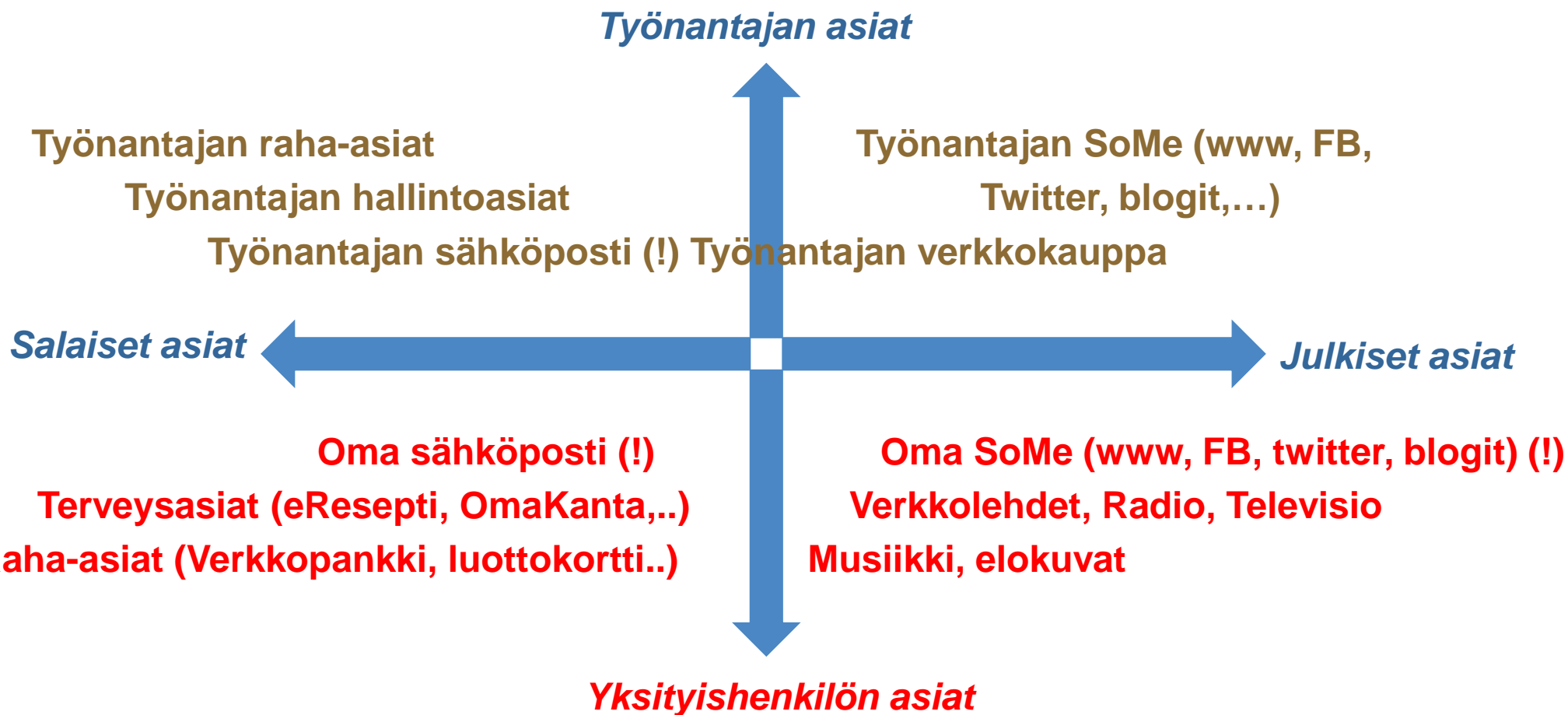


## Ihminen toimii lainsäädännön puitteissa...

- ✓ Valtion ja kunnan julkisten palveluiden ja oman hallinnon tietoturvasta määrää Laki.
- ✓ Yritys saa hoitaa tietoturvansa parhaaksi katsomallaan tavalla. Yritys nauttii suojaa ja vastaa tekemisistään rikosoikeuden tasolla.
- ✓ Työntekijä on työssään työnantajansa edustaja, ja muualla omissa asioissaan toimiessaan kansalainen. (vapaa-aika, ruokatunti,...)
- ✓ Kansalaiselle tietoturvan suoja ja vaatimuksia on upotettu Lakeihin, kuten Tekijänoikeus, Yksityisyys, Sananvapaus, Viestinnän vapaus,...
- ✓ Kansalaisen pitää voida käyttää sähköisiä julkisia palveluita tavallisella tietokoneella.
  - *Mutta hänen täytyy itse huolehtia omasta tietoturvastaan, ja vastata itse huolimattomuudestaan.*
  - *Tietämättömyys ei ole puolustus, kun aiheutettua vahinkoa arvioidaan oikeusistuimessa.*

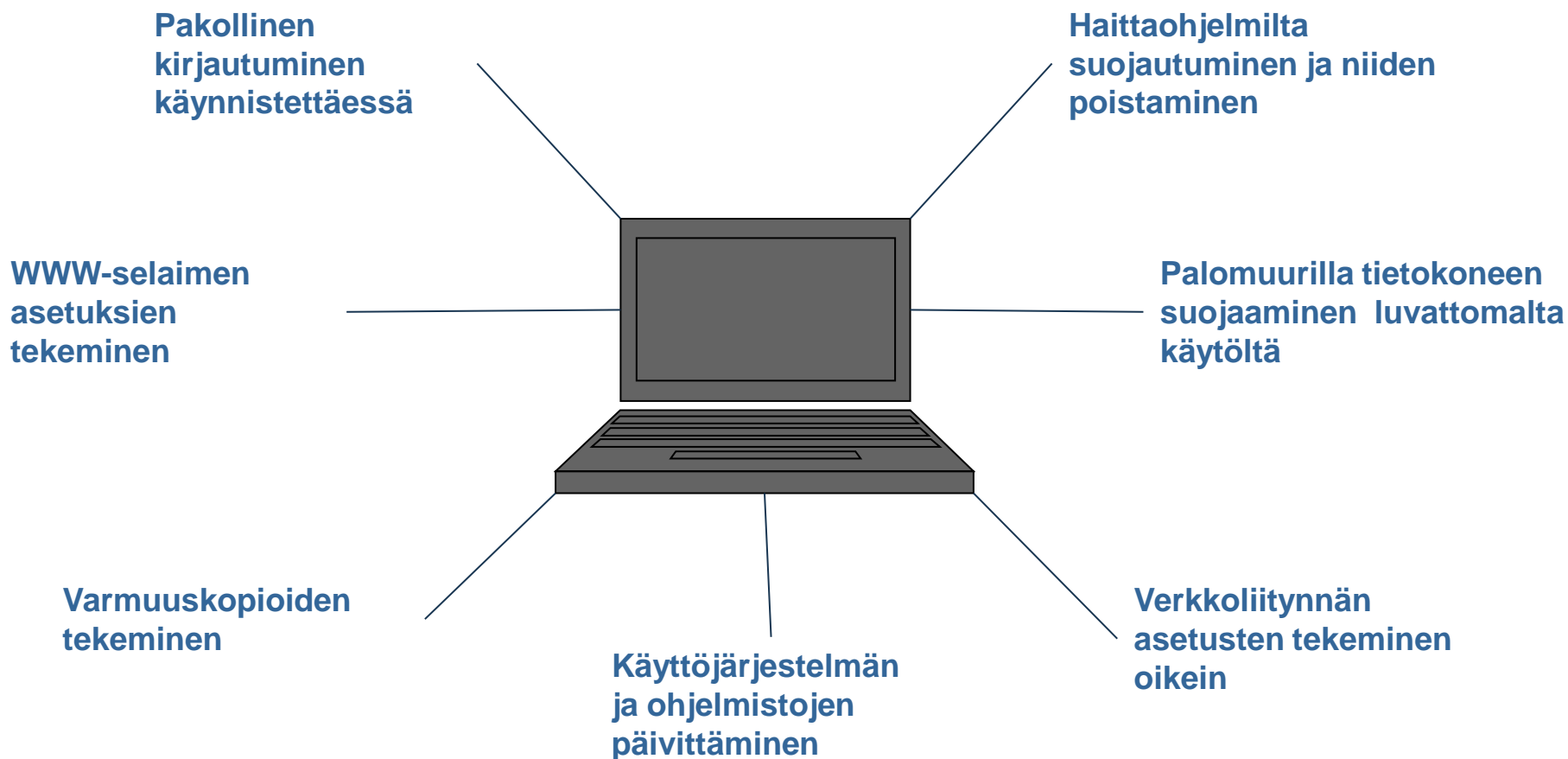


# ihminen työntekijän ja yksityishenkilön roolissa...





## Mitä rotarin tulisi tietää ja osata?





## Tietokoneen voi helposti tehdä turvallisemmaksi...

- ✓ Asenna vain luotettavia ohjelmia tietokoneeseesi.
- ✓ Aseta käyttöjärjestelmä ja sovellukset päivittymään automaattisesti - kotona.
- ✓ Tee varmuuskopioita (muistitikulle, DVD:lle, mutta ei pilveen (ainakaan vain))
  - Käyttöjärjestelmän ja sovellusohjelmien asennustiedostot.
  - Omat tiedostot
- ✓ Asenna virusten ja muiden haittaohjelmien torjuntaohjelma. Aseta se sitten tekemään pikatarkastuksia ja päivittymään automaattisesti. Suorita tarpeen vaatiessa ja toisinaan muutenkin täystarkastus, vaikka se kestää kauan.
  - Windowsiin upotettu Defender (tai Security)
  - Kaupallinen sovellus (F-Prot, G Data, Trend Micro, Comodo,...)
- ✓ **Asenna tietokoneesi palomuri (firewall) toimimaan**
  - Estää tietokoneen ja ohjelmiston luvattoman käytön - esim. ulkomailta Internet-liitynnän kautta
  - Usein se on virustorjuntaohjelmaan upotettu toiminto.
- ✓ **Aseta Internet-liityntä turvallisemmaksi:**
  - Aseta WLAN-tukiaseman radiotien salaus päälle.
  - Muuta ADSL-modeemin oletus-KT/SS omaksesi. Oletus-KT/SS on tarkoitettu vain siihen.
  - Asenna VPN yhteyden päästä-päähän salaamiseksi, jos mahdollista



## WWW-sivujen selailun voi tehdä turvallisemmaksi ...

- ✓ **Katsele vain luotettavia sivuja... tai vältä taatusti epäluotettavia sivuja**
- ✓ **Lue huolellisesti ja ajatuksella, ennen kuin annat suostumuksesi johonkin.**
  - Esim. joku ohjelma voi kysyä, saako se käyttää yhteystietojasi tai valokuviasi? Jos vastaat Kyllä, laiton saattoikin muuttua lailliseksi.
- ✓ **Keksi kunnolliset salasanat ja pidä ne turvallisessa tallessa.**
  - Käytä eri KT/SS eri palveluissa, älä käytä esim. Facebook-tunnuksia muihin palveluihin
    - Tietokoneen käynnistykseen esim. Microsoft-tilin KT/SS, kasvojen valokuvan tai sormenjäljen tunnistus,
    - Muita ohjelmistoja käynnistettäessä kullakin oma KT/SS, jos ne eivät kuulu tiliin.
  - KT/SS tallentaminen, omassa kalenterissa tai luotettavalla ohjelmalla kuten esimerkiksi Password Safe, LastPass, KeePass. Tee vielä tikulle varmuuskopio tiedostosta. Hyvä ohjelma tallentaa tiedoston luotettavalla tavalla salattuna.
- ✓ **Aseta www-selaimen toiminnot kohdalleen**
  - Aseta Do Not Track rajoitus päälle. Se ehkä estää sinun käyttäytymisen seuraamisen.
  - Aseta mainosten rajoitus päälle, esim. AdBlock, AdBlock Plus tai uBlock, jos niin haluat.
  - Rajoita tietojesi näkymistä vieraille esim. Facebookin kaltaisissa palveluissa





## Esimerkki Windows-tilin salasanan murtamisesta... joku voi haluta sen vaikka etäkäyttääkseen Windows- tietokonettasi...

LM configuration #0

Merkistö : [ABCDEFGHIJKLMNOPQRSTUVWXYZ]

Salasanataulukon koko : 8353082582

Salasanataulukon koko : 610 MB

Salasanan murtamisen onnistuminen : 99,04 %

- Taulukolla voi murtaa 14 merkin pituisen salasanan 99,05% todennäköisyydellä.
- Yksi tietokone murtaa salasanan parissa tunnissa, monta tietokonetta yhdessä muutamassa sekunnissa.

LM configuration #5

Merkistö: [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#\$%^&\*()-\_+= ]

Salasanojen lukumäärä: 915358891407 (2<sup>^</sup>39.7)

Salasanataulukon koko: 24 GB

Salasanan murtamisen onnistuminen: 99,9 %

- Taulukolla voi murtaa 14 merkin pituisen salasanan 99,9% todennäköisyydellä.
- Yksi tietokone murtaa salasanan parissa vuodessa, monta tietokonetta yhdessä muutamassa minuutissa.

Esimerkki, helposti arvattavien salasanojen salatut muodot tallennetaan salasana-taulukoiksi.:

joeuser:"":E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C:::

averageguy:"":299CCF964D9A359BAAD3B435B51404EE:A5C07214487C87B584E8877DE72DCA0B:::

Johtopäätös: Käytä pitkiä ja vaikeasti arvattavia salasanoja, ja tallenna ne luotettavalla tavalla itse.

Lähde: [www.ethicalhacker.net/columns/gates/tutorial-rainbow-tables-and-rainbowcrack](http://www.ethicalhacker.net/columns/gates/tutorial-rainbow-tables-and-rainbowcrack))



# Älykännykän voi helposti tehdä turvallisemmaksi...

## ✓ Älykännykkä käyttöön otettaessa

- Kirjoita puhelimesi laitenumero IMEI muistiin siltä varalta, että haluat esimerkiksi estää kadonneen puhelimesi käytön. Se löytyy puhelimen akun alta, tai sen saa näkyviin näytölle kirjoittamalla puhelinnäppäimillä \*#06# (Joku esimerkiksi varastaa puhelimesi, soittaa maksulliseen palveluunsa, ja jättää sinulle 1000€ puhelinlaskun maksettavaksi.)
- Aseta puhelimesi käynnistyessään kysymään Pääsykoodi (PIN), joka ei ole 0000, 1111,...
- Tallenna sitten PUK-koodi varmaan paikkaan, se löytyy liittymäsopimuksesta. Se löytyy myös liittymäsi verkkosivulta. Tarvitset sitä, jos unohdat PIN-koodin,
- Asenna puhelimesi virustorjuntaohjelma, etenkin jos käytät sillä verkkopankkia.
- Aseta käyttöjärjestelmä ja sovellukset päivittämään automaattisesti kotona WLANista.

## ✓ Asenna sovelluksia vain puhelimen valmistajan e-kaupasta.

## ✓ Liity langattomaan verkkoon oikein

- Asenna puhelimesi EI-LIITTYMÄÄN automaattisesti ja kysymättä vapaisiin WiFi-verkkoihin.
- Liity vain luotettaviksi arvioimiisi WiFi-verkkoihin.

## ✓ Varaudu puhelimesi katoamiseen

- Asenna toimintaan puhelimen paikannus, jotta voisit etsiä kännykkääsi toisella laitteellasi.

## ✓ Jos kuitenkin kadotat puhelimesi tai se varastetaan

- Lopeta verkkopankin ja sen luottokorttipalvelut, jos käytit niitä kännykällä.
- Pyydä puhelinoperaattoria estämään puhelimen (IMEI) pääsy mihinkään GSM-verkkoon.
- Jos puhelimesi on varastettu, tee rikosilmoitus poliisille.



## Esimerkki: Jos minun vanha puhelimeni olisi kadonnut... avaan Microsoft-tilini [microsoft.com/myphone](https://microsoft.com/myphone) ja...

Paikanna puhelin



Windows Phone  
Lumia 1020  
[358445501722 Päivitys](https://microsoft.com/myphone)

Viimeksi havaittu 15/11/2015 14:03:21 sijainnissa Ylivieska, P  
[Päivitä](#)

Soita

Vaikka puhelimesi ääni olisi mykistetty, se soi ääneen, jotta voit löytää sen.

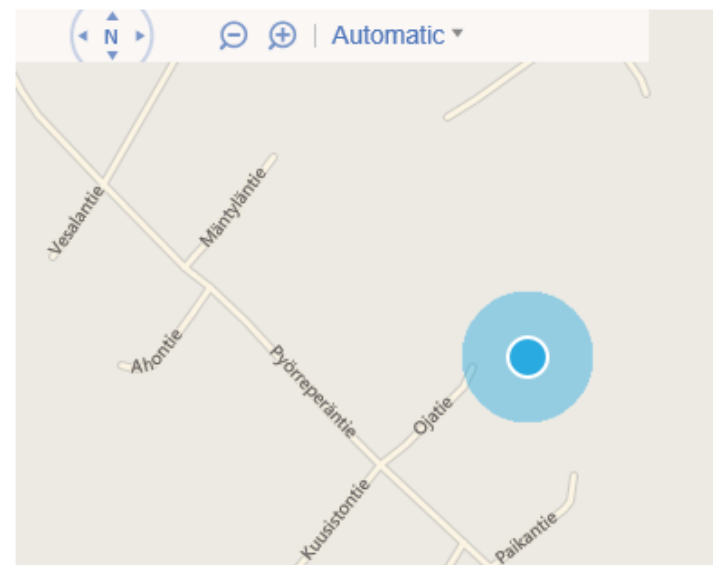
Lukitse

Jätitkö sen paikkaan, josta se voi lähteä jonkun matkaan? Lukitse toiset ihmiset ulos ja lisää näyttöön mukautettu viesti.

Tyhjennä

Jos puhelimesi on varastettu, siinä olevat henkilökohtaiset tiedot kannattaa tyhjentää.

Tekstiviestit voivat olla maksullisia.





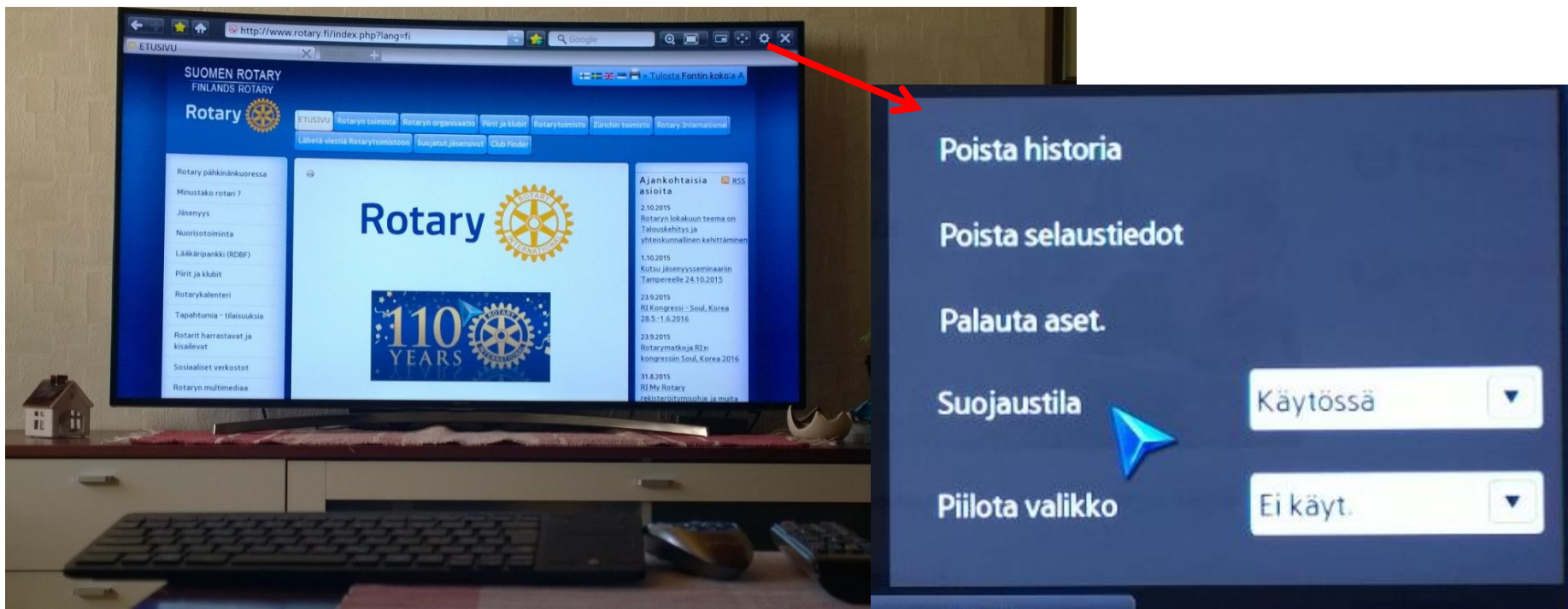
## Tabletin myös helposti tehdä turvalliseksi ...

- ✓ **Samat ohjeet kuin tietokoneelle aiemmin.**
  - Käytä vain luotettavia ohjelmistoja
  - Aseta ohjelmistot ja käyttöjärjestelmä päivittymään automaattisesti - kotona
  - Käytä virustentorjuntaohjelmaa
  - Varmuuskopioi tiedostosi
- ✓ **Aseta oman WLAN-tukiasemasi salaus päälle ja muuta sen KT/SS.**
- ✓ **Aseta tabletti ei-liittymään automaattisesti vapaisiin WiFi-verkkoihin.**
- ✓ **Liitä tablettisi vain luotettavaan WiFi-verkkoon.**
- ✓ **Asenna tablettiisi VPN päästä-päähän salaus, ja olet paremmassa suojassa liityttyäsi esimerkiksi hotellin WiFi-verkkoon.**
- ✓ **Asenna tablettiisi paikannusohjelma, jolla voit toisella laitteellasi ehkä löytää tablettisi, jos se häviää tai varastetaan.**



## Mahtaako Smart-TV olla turvallinen selaimena...

- ✓ Smart-TV sisältää tietokoneen, joka liittyy Internetiin erilaisilla selaimilla. Siihen voi myös asentaa viihteellisiä ohjelmia valmistajan palvelusta.
- ✓ Haittaohjelmien torjunta ja selaimen tietoturva ovat valmistajan toteuttamia ja ylläpitämiä ominaisuuksia.
- ✓ Valmistaja päivittää ne antennin tai Internetin kautta automaattisesti...





## Luottokorttia on helppo käyttää turvallisemmin...

- ✓ **Luottokortti on verkkokaupassa maksettaessa verkkopankkia turvallisempi – etenkin kiistatapauksissa.**
  - Verkkokaupassa kannattaa käyttää luottokorttia, joka ei ole omaan säästötiliin liitetty, vaan käyttötiliin jolla on vähemmän rahaa ja pienet käyttörajat. Epäselvässä kaupassa, jossa sinä et ollut syyllinen, menetetyt rahat saattavat jäädä luottoyhtiön vahingoksi.
  - Tutustu luottokortin ominaisuuksiin ja käyttötapoihin.
- ✓ **Asetuksilla voit määritellä luottokorttisi käyttötavan:**
  - Voit estää luottokorttisi käytön Internetissä kokonaan, jos niin haluat.
  - Aseta luottokortillesi sopivan pienet Euro-määräiset osto- ja nostorajat
  - Voit rajoittaa luottokorttisi maantieteellistä käyttöaluetta, niin että voit maksaa Suomesta Internet-ostoksia, mutta sillä ei voi maksaa ulkomailta. Joku ulkomailta voi anastaa sen tiedot.
- ✓ **Huolehdi sitten luottokortistasi, kuten omasta lompakosta**
  - Luottokorttia ei kannata jättää esim. pöydälle, työpaikalle tai hotellihuoneeseen.
  - Luottokortin avainlukulista kannattaa säilyttää omassa lukitussa tilassaan.
  - Jos kuitenkin kadotat luottokorttisi tai se on varastettu, se kannattaa sulkea heti. Sulkeminen kannattaa opetella jo etukäteen. Sinulle lähetetään aikanaan uusi luottokortti varsin kohtuullisilla korvauksilla, verrattuna mahdolliseen vahinkoon.



# Kiitos...