

## **Uskallatko käyttää kännykkääsi?**

### **Älypuhelin ja tablettien turvallisuus kuluttajan kannalta**

Olli Moisiola

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2014





<b>Tekijä tai tekijät</b> Olli Moisiola	<b>Ryhmätunnus tai aloitusvuosi</b> HETIK13M
<b>Raportin nimi</b> Uskallatko käyttää kännykkääsi? Älypuhelinien ja tablettien turvallisuus kuluttajan kannalta	<b>Sivu- ja liitesivumäärä</b> 25 ja 4
<b>Opettajat tai ohjaajat</b> Outi Valkki	
<p>Tämän opinnäytetyön tarkoitus on tutkia älypuhelinien ja samoja käyttöjärjestelmiä käyttävien tablettien turvallisuutta tavallisen kuluttajan näkökulmasta. Työn tavoitteena on esittää helposti ymmärrettävässä muodossa mobiililaitteisiin kohdistuvat riskit ja miten näitä riskejä voi välttää. Tässä työssä käsitellään kolmea Suomessa suosituinta käyttöjärjestelmää: Androidia, iOSia ja Windows Phonea, sekä niitä käyttäviä älypuhelimia ja tabletteja. Muut mobiililaitteet on rajattu pois tästä tutkimuksesta. Aineisto tutkimukseen koottiin tietoturvyhtiöiden ja Euroopan kyberturvallisuuskeskuksen raporteista, Viestintäviraston ja valmistajien tiedotteista ja ohjeista sekä alan lehtien artikkeleista.</p> <p>Opinnäytetyössä käytiin läpi yleisimmät kuluttajaa koskevat uhat ja mistä ne tulevat. Tutkittiin ilmaisohjelmien ansaintalogiikkaa pyrkien ymmärtämään niiden riskit, tarkasteltiin WLAN -verkkojen riskejä ja käyttöoikeussopimuksia sekä pohdittiin tulevaisuutta tietoturva-alan julkaisemien ennustusten valossa. Lisäksi perehdyttiin lyhyesti käyttöjärjestelmiin ja niiden eroihin ja yhtäläisyyksiin.</p> <p>Tuotokseksi syntyi pieni opas muistutukseksi perussäännöistä joilla turvata älylaitteensa turvallisuus ja yksityisyys verkossa toimiessa. Aihetta olisi mahdollista jatkaa kehittämällä verkkosivu, jossa turvallisuusohjeet olisivat yhteenkoottuina ja helposti löydettävänä sekä ajantasainen päivitys eri käyttöjärjestelmiin ja laitteisiin liittyvistä uhista ja ehdotuksia toimista näiden uhkien välttämiseksi.</p>	
<b>Asiasanat</b> Tietoturva, älypuhelimet, tabletit, haittaohjelmat, langaton viestintä, mobiilisovellukset	

<p><b>Authors</b></p> <p>Olli Moisiola</p>	<p><b>Group or year of entry</b></p> <p>HETIK13M</p>
<p><b>The title of thesis</b></p> <p>Do you dare to use your smartphone? Smartphone and tablet computer information security from the consumer's point of view</p>	<p><b>Number of pages and appendices</b></p> <p>25 + 4</p>
<p><b>Supervisor(s)</b></p> <p>Outi Valkki</p>	
<p>The aim of this thesis was to study from the consumer's point of view the safety of smartphones and tablets that use the same operating systems. The idea was to explain in an accessible manner the risks associated with mobile devices and how to avoid these risks. This thesis studies the three most popular operating systems in Finland: Android, iOS and Windows Phone, as well as the smartphones and tablets using them. Other mobile devices were left outside the scope of the study. The material was collected from the reports of data security companies and the European Union Agency for Network and Information Security, communications by the Finnish Communications Regulatory Authority and manufacturers, as well as from articles in related magazines.</p> <p>This study lists the most common threats concerning the consumer and their origins. Furthermore this study discusses the revenue logic of freeware trying to understand their risks, examines the risks associated with WLAN and license agreements and looks into the future in the light of the forecasts published by the data security industry. Finally, the study briefly describes the various operating systems and their differences and similarities.</p> <p>As a result, a short guidebook is created about the basic rules of how to guarantee the data security and privacy of your smart device on the internet. The next step after this study would be to develop a website where these security instructions would be easily accessible with updated information about the threats concerning various operating systems and devices, as well as suggestions of how to avoid these threats.</p>	
<p><b>Key words</b></p> <p>Information security, smartphones, tablet computer, malware, wireless communication, mobile applications</p>	

# Sisällys

1 Johdanto.....	1
2 Turvallisuusuhat.....	2
2.1 Fyysiset riskit.....	3
2.2 Haittaohjelmat.....	4
2.3 Ilmaisohjelmat.....	8
2.4 Wi-Fi-yhteyksien riskit.....	10
2.5 Tulevaisuus .....	13
3 Käyttöjärjestelmät.....	16
3.1 Android.....	17
3.2 iOS .....	19
3.3 Windows Phone.....	22
4 Yhteenveto ja pohdinta .....	24
Lähteet.....	26
Liite 1 .....	37
Liite 2.....	40

# 1 Johdanto

Opinnäytetyössä pyritään selvittämään, millaisia tietoturvaohjeita kohdistuu älypuhelimien ja tablettitietokoneisiin sekä miten kuluttajan pitäisi niihin suhtautua. Tavoitteena on esittää mobiililaitteisiin kohdistuvat riskit ja niitä pienentävät toimenpiteet niin, että asiaan perehtymätönkin henkilökin ne ymmärtää. Työstä on rajattu pois työkäytössä olevat mobiililaitteet, koska niiden tietoturva-vaatimukset ovat toisenlaisia ja ansaitsevat oman tutkimuksensa. Tutkimuskysymykseni on, mitä jokaisen kuluttajan tulisi tietää älylaitteen tietoturvasta. Lisäksi kysyn mitä jokaisen tulisi tehdä ottaessaan käyttöön uuden älylaitteen. Halusin myös luoda tiiviin oppaan, jossa selkeästi tulee ilmi perustoimenpiteet jotka auttavat turvaamaan laitteen ja käyttäjän yksityisyyden.

Langaton viestintä on kätevää ja nopeaa, mikä on tehnyt meistä myös riippuvaisia siitä. Mobiililaitteen kadotessa, rikkoutuessa tai joutuessa haittaohjelman hyökkäyksen kohteeksi muuttuu elämä hankalaksi. Yhteystietojen katoaminen, yhteydenpidon vaikeutuminen, liiketoiminnan pyörittämisen ongelmat ja monet muut asiat vievät ihmisen epämukavuusalueelle. Vaikka suurin riski on laitteen rikkoutuminen, on tietoturvan ja yksityisyyden vaarantuminen nousemassa koko ajan tärkeämmäksi aiheeksi.

Lisäksi tutkimuksessa yritetään selvittää, milloin turvautua suojausohjelmiin ja milloin asetuksissa olevat ominaisuudet ovat riittävät. Tutkitaan haittaohjelmia, langattoman verkon riskejä ja tapoja miten haitakkeet pääsevät laitteisiin. Tehdään katsaus siitä, mitä tietoturvayhtiöt ajattelevat tulevaisuudesta sekä käydään lyhyesti läpi suosituimpien käyttöjärjestelmien historiaa ja tekniikkaa. Aiheesta oleva tieto on hajanaista ja osin pahasti vanhentunutta, mikä johtuu alan nopeasta kehityksestä. Aiheesta on tehty vain vähän opinnäytteitä. Kirjoissa aihetta yleensä sivutaan ohimennen tai keskitytään fyysiseen uhkaan, jota sitäkään ei tule väheksyä.

Mobiililaitteita ovat myös erilaiset kannettavat tietokoneet ja useat muut laitteet, jotka ovat yhteydessä verkkoon joko Wi-Fi-yhteydellä tai SIM-kortilla, kuten mokaajat, älykellot, kämmentietokoneet, korttipäätteet, navigaattorit ja GPS-paikantimet. Tämä opinnäytetyö keskittyy älypuhelimien ja tabletteihin sekä niiden kolmeen Suomessa yleisimpään käyttöjärjestelmään.

## 2 Turvallisuusuhat

Kuluttajat ovat enenevässä määrin siirtymässä mobiileihin laitteisiin, älypuhelimiin ja tabletteihin, mutta eivät suojaa niitä kuten perinteisiä tietokoneita. Laitteiden määrän kasvaessa rikolliset ja luvattomat käyttäjät alkavat hyödyntämään tietämättömyydestä ja piittaamattomuudesta syntyviä haavoittuvuuksia yhä enemmän. Älypuhelin on silti tois- taiseksi melko turvallinen väline surffailuun, sillä uhat tulevat muualta kuin verkko- sivuilta. Vaarat vaanivat sovelluksissa ja etenkin niiden mainoksissa. Älylaitteiden etu on se, että sovellukset kysyvät, saavatko ne käyttää haluamiaan oikeuksia ja käyttäjän täytyy päättää, ovatko oikeudet hyväksyttävissä ja saako ohjelma asentua. (Kärkkäinen, 2013.)

Mobiililaitteissa, Android-käyttöjärjestelmää lukuunottamatta, ei ole vahvistettu niin sanottua drive-by-hyökkäystä eli haittaohjelman tunkeutumista suoraan verkkosivulta (ENISA Cyber Threat Landscape report, 2012). Android-laitteet ovat suurin kohde erilaisille haittaohjelmille: vuoden 2014 ensimmäisellä neljänneksellä Androidiin löytyi 275 ja iOSiin ja Symbianiin molempiin yksi uusi haittaohjelmavariantti tai -perhe. (F-Secure, Mobile Threat Report Q1 2014, 2). Aivan tuoreena uhkana löytyi tietoturva- aukko Androidin ytimessä olevassa Binderissä, joka hallitsee kaikkea sovellusten vies- tinvälitystä. Tätä aukkoa ei ole vielä käytetty hyväksi, ja aukon löytäneet tietoturva- yhtiö Check Pointin tutkijat toivovat sovelluskehittäjien huomioivan riskin ja sulkevan mah- dollisuudet väärinkäyttöön. (Check Point, 2014.) Älypuhelimien selainten ongelma on ettei koko URL-verkko-osoite mahdu aina näyttöön, jolloin ei voi olla varma onko osoite oikea, tästä hyötyvät tietojen kalastajat, samat jotka PC- ja Mac-maailmassakin yrittävät huijata väärille verkkosivuille (Dwivedi, H., Clark, C. & Thiel, D., 2010, 7).

Riskien välttäminen vaatii jonkun verran vaivaa ja ajatustyötä, joten mukavuudenhalui- nen käyttäjä voi helposti jättää perusturvallisuuden huomiotta. Älylaitteiden käyttö työssä voi hämärtää työ- ja viihdekäytön välistä rajaa ja näin tuoda liiketoiminnalle ris- kejä, joita on vaikea ennakoida. Vain 26 % älypuhelimien käyttäjistä on ladannut jonkun turvaohjelmiston (Norton Report 2013, 5). Nortonin mukaan yksi kymmenestä vakoi- lee tai tutkii luvatta kumppaniensa tai ystäviensä sähköposti- tai sosiaalisen median so-

vellusten tilejä syystä tai toisesta, joten laitteen lukitus on tärkeää (Norton Report 2013, 23).

Omanlaisensa riskin tuo viranomaistahojen suorittama tarkkailu, kuten Snowden-paljastusten kertoma NSA:n ja muiden virastojen tekemä tietojen massiivinen kokoaminen, joka vaarantaa ainakin yksityisyyden suojan vaikkei tietorvaa vaarantaisikaan. Lisäksi laitteen valmistaja saattaa tarkkailla laitetta ja kerätä tietoja tuotekehityksen nimissä. Tietojen kalastelu eri tavoin - sähköpostilla, tekstiviestein, soitoin ja korruptoituneiden verkkosivujen kautta - on arkipäivää mobiililaitteissakin. Vähänkin epäilyttäviin yhteydenottoihin tulee suhtautua hyvin varovasti. Mikään tietojen luovuttaminen ei ole viisasta, etenkin eri tunnusten ja puhelinnumeron luovuttaminen, salasanoista puhumattakaan, voi koitua kalliiksi ja työlääksi ongelmaksi. (security.intuit.com.) Erilaisten haittaohjelmien, tietokaappausten ja -urkinnan ohella suuri vaara on laitteen fyysinen rikkoutuminen, katoaminen tai varkaus.

## **2.1 Fyysiset riskit**

Tietoturvayhtiö Symantecin julkaisemassa Norton Report 2013:ssa kerrotaan, että 27 % aikuisista mobiililaitteen käyttäjistä on kadottanut laitteensa tai se on varastettu tutkimusta edeltäneen vuoden aikana (Norton Report 2013, 7). Tämä kertoo, ettei älypuhelimia ja tabletteja käsitellä kovinkaan huolellisesti. F-Securen Mikko Hyppösen mielestä suurimmat riskit ovat älylaitteen hukkaaminen, varkaus tai kastuminen, neljäntenä lapsen tietämättömyyttään tekemät satojen eurojen sovellusostokset eli hyvin jokapäiväiseen elämään liittyvät riskit. (Hyppönen, M. 27.11.2014).

Viime vuonna Helsingin Sanomat kertoi älypuhelimien varkauksien kasvaneen voimakkaasti, Varkauksiin liittyi kuitenkin lähes aina myös omaa huolimattomuutta, laite oli pöydällä tai muuten näkyvillä. Näihin varkauksiin oli myös pääsyynä ulkomaalainen varasjoukko. (Salonen, 2013.) Älypuhelimet ja tabletit ovat varmasti varkaiden haluamia, mutta toivottavasti kehittyvät etähallinnan keinot jarruttavat intoa, kuten jäljitys ja laitteen sulkeminen sekä tietojen poisto. Kadonneen laitteen IMEI-koodin ilmoittaminen operaattorille ja sieltä kansainväliseen CEIR-rekisteriin tekee laitteen käytöstä mahdollonta jo useimmissa maissa (Mobiiliasiantuntijat, 2014). Tosin rikollisten intoa kehittää

teknisiä keinoja erilaisten suojausten ja lukitusten ohittamiseksi ei pidä aliarvioida, se on vähintään yhtä tehokasta kuin uusien suojauskeinojen kehittäminen. Riskinsä on myös jos luovuttaa puhelimensa tuntemattomalle vain pientä soittoa varten. Nopea soitto kalliiseen palvelunumeroon ja yhtä nopea soittotietojen poisto ja mahdolliset kymmenien eurojen laskut ovat jo matkalla. Vikkeläsorminen voi soiton sijasta jopa ladata haittaohjelman puhelimeen ilman, että omistaja huomaa mitään. Puhelinnumeron luovuttaminen epäilyttävään palveluun tai outoon numeroon takaisinsoittaminen voivat myös kostautua kalliisti. (Mobiiliasiantuntijat, 2014). Lisäksi irrottautuminen hämäräperäisestä palvelusta voi olla hyvinkin vaivalloista.

Puhelimet putoavat vahingossa veteen, asvaltille, wc-pönttöön ja mitä kummallisimpiin paikkoihin, eivätkä nykyaikaisten laitteiden näytöt ja osat aina kestä kovia iskuja tai kosteutta. Avuksi kömpelyyden tai huonon tuurin aiheuttamiin laitteen rikkoutumisiin ei juuri muuta voi kuin yrittää olla huolellinen. Pientä lisäturvaa toisi silikoninen tai kumiseosta oleva tarvikekuori. Kovin harva näitä kuitenkaan näyttää käyttävän, liekö syyinä käsittelytuntuman muuttuminen kömpelömmäksi. Parin kymppin sijoitus lisäkuoreen usean sadan euron puhelimessa olisi aika pieni investointi. On myös olemassa muutamia iskuja kestäviä malleja, mutta ne ovat yleensä suositumpia ulkotöissä työskentelevillä. (verkkokauppa.com). Näytön kestävyyttä parantaa jonkin verran näyttöön kiinnitettävä kalvo, joka auttaa myös puhtaanapidossa. Eri merkeillä on monentyyppisiä näyttöjä, joista parhaimpien sanotaan kestävän naarmutusta ruuvimeisselillä ja jopa tylpän esineen iskuja. (Gorilla Glass, 2014).

## 2.2 Haittaohjelmat

Haittaohjelmia (malware) on monia eri tyyppisiä erilaisiin tarkoituksiin. Mobiililaitteissa yleisimmät ovat troijalaiset, takaovisovellukset ja madot, sekä niin sanotut PUA-sovellukset eli mahdollisesti ei-toivotut sovellukset (Potentially Unwanted Applications). Eri haittaohjelmatyypit tavoittelevat eri asioita, huonomaineisimpina ne jotka vahingoittavat laitteen tietoja ja/tai varastavat ne. Luottokortti- ja salasana-tietojen vienti aiheuttaa suurimmat vahingot uhrille, joskin yritysten tietojen päätyminen väärin käsiin voi myös aiheuttaa suuria ongelmia. Valtaosa haittaohjelmista on vakoiluohjelmia, jotka haluavat eteenpäin myytävää tietoa jalostettavaksi kaupallisiin tarkoituksiin,



eikä niiden tarkoitus ole aiheuttaa näkyvää haittaa. Haittaa syntyy, kun haitake käyttää laitteen muistitilaa ja hidastaa tietoja lähettäessään uhrin omaa yhteydenpitoa ja tietoliikennettä. (Viestintävirasto, 2014a; F-Secure MTR Q1 2013.) Vaikka tietoturvaa ei näennäisesti olisikaan rikottu, on yksityisyyden suoja mennyttä henkilökohtaisten tietojen vuodettua ulkopuolisiin käsiin ilman, että niiden käyttöä voi itse kontrolloida. Haittaohjelmia on koottu Taulukoon 1.

**Taulukko 1.** Haittaohjelmat (F-Secure MTR Q1 2013, 4).

<p><b>Haittaohjelmia (Malware)</b> Sovellus, joka aiheuttaa merkittävän turvallisuusrisikin käyttäjän järjestelmälle ja/tai datalle.</p>	
	<p><b>Trojialainen (Trojan)</b> Yleisin ja monipuolisin haittaohjelmista. Nimi tulee siitä, että sovellus tekeytyy hyötyohjelmaksi, mutta taustalla tekee jotain muuta. Yleensä houkuttelee itsensä ladattavaksi ilmaisohjelmana. Saatetaan liittää laillisiin sovelluksiin ja tarjota sovelluskaupoissa. Ei normaalisti kopioitu.</p>
	<p><b>Takaovi (Backdoor)</b> Antaa mahdollisuuden laitteen etähallintaan.</p>
	<p><b>Mato (Worm)</b> Pyrkii levittämään itsestään mahdollisimman paljon kopioita. Kantaa mukanaan erilaisia laitteita vahingoittavia tai hyödyntäviä sovelluksia. Esiintyy joskus yhdessä Trojialaisen kanssa.</p>
<p><b>PUA – Mahdollisesti ei-toivottu sovellus (Potentially Unwanted Application)</b> Tarkoittaa sinänsä laillista ohjelmaa, jolla voi olla ei-toivottuja tai tunkeilevia ominaisuuksia. Se voi toimia kyseenalaisella tavalla sekä vahingossa aiheuttaa turvallisuusrisikin.</p>	
	<p><b>Mainosohjelma (Adware)</b> Sinänsä lailliseen ja harmittomaan mainossovellukseen piilotettu sovellus, joka voi seurata ja raportoida käyttäjän toimista. Voi haitata laitetta hidastamalla toimintaa. Aggressiivisemmat versiot voivat muuttaa laitteen asetuksia ja pyrkiä ohjaamaan turvattomille tai kyseenalaisille verkkosivuille.</p>
	<p><b>Vakoiluohjelma (Spyware)</b> Kerää dataa käyttäjän toiminnasta, kuten selaushistoriasta tms. Varastoi tiedon joko laitteeseen tai lähettää sen ulkoiselle palvelimelle.</p>
	<p><b>Jäljitysohjelma (Trackware)</b> Kerää tietoja käyttäjän ja/tai laitteen tunnistamiseksi kolmannelle osapuolelle.</p>

Älylaitteet sisältävät paljon tietoja, joita eri tahot voivat käyttää hyväkseen. Tietoa on laitteen käyttäjästä, puhelimesta ja sen ominaisuuksista, paikannustietoja ja tieto laitteen liikkumissuunnasta ja -nopeudesta. Laitteen ominaisuuksia ja tietoja käyttävät sovellukset ja pelit löytääkseen niille mahdollisimman hyvät toiminnallisuudet. Tietoja käyttävät ohjelmien kehittäjät ja/tai palveluntarjoajat sekä kolmannet osapuolet, kuten mainostajat. Sovellukset siis saattavat pyytää laajoja oikeuksia mainoskirjaston toiminnan takaamiseksi, eikä suinkaan ohjelman toiminnan varmistamiseksi. (Viestintävirasto, 2014a). Tietojen kerääminen ja niillä rahastaminen ilmaissovellusten siivellä on (yleensä) laitteen toiminnan kannalta melko harmitonta puuhaa, mutta jos tarkastellaan haittaohjelmien levittämisen perimmäisiä motiiveja, löytyy sieltä aina raha. F-Securen mukaan uusien haittaohjelma-perheiden ja varianttien määrästä 81 - 88 % on tähdätty vain suoraan rahastamiseen, ja todennäköisesti loppuillakin pyritään tavalla tai toisella rahastamaan jotakuta. Hupi tai ilkeys mielessä tehtyjä haittaohjelmia lienee sangen vähän (F-Secure Mobile Threat Report Q1, 2, 2014.) Haittaohjelmien määrä on huima, vuonna 2013 tietoturvayhtiö McAfee keräsi 2,47 miljoonaa uutta mobiilihaittaohjelmanäytettä (McAfee Labs Threats Report Q4 2013, 12).

Ilmaisohjelmien liitteenä olevat mainosbannerit ovat joskus ongelmallisia, jos niiden mainossisältö on vaihtuvaa, sillä mainos saattaa olla yleensä harmiton, mutta välillä viedä korruptoituneelle verkkosivulle tai sisältää haittaohjelman. Jäljitysohjelmien tarkoitus on kerätä luvatta laitteesta sijaintitietoja, joilla laite ja/tai henkilö voidaan yhdistää muihin tietoihin. Vakoiluohjelmat ovat astetta aggressiivisempia. Ne pyrkivät myös henkilökohtaisiin tietoihin, sivuhistoriaan ja yhteystietoihin sekä laitteen IMEI-koodin, mallin, käyttöjärjestelmäversion ja muiden teknisten tietojen lähettämiseen. (Viestintävirasto, 2014a.) Nykyään vakoiluohjelmia käytetään myös kohdistetusti yritysten ja organisaatioiden vakoiluun, kuten Suomessa ulkoministeriöön vuonna 2013. Ohjelmia yritetään ujuttaa kohteeseen suoran hyökkäyksen lisäksi useita reittejä, kuten alihankkijoiden ja yksityisten henkilöiden järjestelmiin istuttamalla. (Viestintävirasto, 2014b.) Vakoilu- ja jäljitysohjelmien lähteeksi, ilmaisohjelmien lisäksi, mainitaan usein aikuisviihdesivut sekä vertaisverkon MP3-musiikkitiedostoja ja sovelluksia jakavat sivut. (F-Secure Threat report H2, 2013; virukset.fi).

Trojialaisia on haittaohjelmista lähteestä tai laskutavasta riippuen 75 - 90 %, tämä arvio on kooste F-Securen, Nortonin ja McAfeen arvioista. Määrittely on hankalaa, koska eri

haittaohjelmatyypeillä on paljon samoja ominaisuuksia ja toimintoja. Taulukossa 2. on yleisimpiä esimerkkejä Troijalaisten toiminnoista.

**Taulukko 2.** Esimerkkejä Troijalaisten toiminnoista (F-Secure Mobile Threat Report Q1, 2014, 2)

<b>Mitä Troijalainen voi tehdä?</b>	
<b>Lähetää tekstiviestejä</b>	Huomaamatta lähettää tekstiviestejä kalliisiin palvelunumeroihin ja/tai tilaa tekstiviestipalveluita.
<b>Lataa tiedostoja tai sovelluksia</b>	Lataa ja asentaa ei-toivottuja tiedostoja tai sovelluksia laiteelle.
<b>Jäljittää sijaintia</b>	Jäljittää ja tallentaa laitteen sijaintitietoja ja/tai käyttää kameraa ja/tai mikrofonia käyttäjän tarkkailuun.
<b>Skannaa puhelinta</b>	Teeskentelee tietoturvaohjelmaa ”skannaamalla” laitetta, mutta ei todellisuudessa tee mitään hyödyllistä. Yleensä kerää tietoja ja lähettää niitä kolmannelle osapuolelle.
<b>Klikkailee linkkejä</b>	Ottaa taustalla yhteyttä eri verkkosivuihin kasvattaakseen niiden kävijämääriä.
<b>Varastaa tietoja</b>	Varastaa henkilökohtaisia ja/tai yrityksen tiedostoja, yhteystietoja, valokuvia, kalenteritietoja ja muuta laitteeseen tallennettua informaatiota.
<b>Laskuttaa sinua</b>	Kolmas osapuoli yrittää laskuttaa ilmaisen ja laillisen sovelluksen asennuksesta, käytöstä tai päivityksestä.
Tässä esitellyt ominaisuudet ovat yleisimpiä esimerkkejä Troijalaisten käytöstä. Räätelöityjä versioita lienee tuhansittain. Yhdessä Troijalaisessa voi olla myös useampia ominaisuuksia.	

PC-tietokoneista tuttu ransomware on haittaohjelmatyyppi, joka on uutena tulokkaana siirtymässä mobiililaitteisiin. Se ottaa tietokoneen ”panttivangiksi” ja vaatii lunnaita tiedostojen vapauttamiseksi. Tätä tyyppiä on tavattu mobiililaitteissa, mutta ne eivät ole

toistaiseksi pystyneet lukitsemaan laitteiden tiedostoja tai muutakaan osaa. Kesäkuussa 2014 kuitenkin löytyi Androidille haittaohjelma nimeltään Slocker, joka pystyy tähän (F-Secure Threat Report H1 2014, 12). Se leviää kolmannen osapuolen Android-kauppojen kautta. Tälle kiristysohjelmalle tyypillisesti lunnaiden maksu tuskin auttaa ja käytetty salausta on niin hyvä, että sitä on erittäin vaikea poistaa. Paras suoja on ennaltava-rautuminen ajantasaisilla suojausohjelmistolla ja päivitetyllä käyttöjärjestelmällä. (Jason, 2014.)

Eräs uusi uhka mobiililaitteille on bot, haittaohjelmatyyppi, jota hyökkääjä voi käyttää tartutetun laitteen hallintaan. Kun bot-ohjelma on asentunut laitteelle, se ottaa yhteyttä c&c-palvelimeen (command-and-control), joka voi hallita laiteta ja asentaa sinne uusia haittaohjelmia, määrätä lähettämään roskapostia tai suorittamaan palvelunestohyökkäyksiä osana muita saastutettujen laitteiden verkkoa, botnettä. (F-Secure Labs.) F-Securen raporttien mukaan hieman alle 20 % haittaohjelmista on botnet-tyyppisiä (F-Secure Mobile Threat Report Q1, 2014).

Suojaamaton pc-kone tai palvelin saattaa olla suuri riski älypuhelimelle, jos konetta käytetään synkronointiin ja/tai puhelimen lataukseen, voi haittaohjelma ujuttautua puhelimeen tai viedä tiedot varmuuskopion kautta. Pc-koneella oleva haittaohjelma, jolla on riittävät oikeudet, voi päästä tietoihin bluetoothin tai usb-kaapelin kautta, vaikka synkronointia ei käynnistä. Tietoja on viety Android-, iOS- ja Blackberry-laitteista, sanoo Kim Westerlund tietoturvayhtiö Nixusta. Hän ei kuitenkaan pidä riskiä laajamittaiseen vakoiluun suurena, koska pc:lle on saatava pääsy. Ja tämä tarkoittaa kiinnostusta tiettyyn käyttäjään, rikollisilla ei taas ole väliä kuka uhri on. Westerlund uskoo, että sama uhka on myös Windows-puhelimilla. (Lehto, 2013.) Toisaalta Windows-puhelimien kehittäjänä Microsoftilla työskentelevä Vesa-Matti Paananen kertoo blogissaan Windows 7 ja 8 puhelinten arkkitehtuurin estävän tämän kaltaiset murtautumiset käyttöjärjestelmään (Paananen, 2012).

### **2.3 Ilmaisohjelmat**

Ilmaiset mobiilisovellukset ovat houkuttelevia, mutta onko niitä oikeasti olemassa? Kannattaa ymmärtää jonkun verran verkkomailman ansaintalogiikoita, jotta hahmot-

taa mahdollisia riskejä ja mitä ilmaisen tuotteen vastikkeeksi joutuu antamaan. Seuraavassa muutamia tapoja rahoittaa ilmaissovelluksia.

**Mainosrahoitus** yleinen ja laillinen tapa rahoittaa tuotetta, tuotteen myyjä saa rahaa mainostajalta. Jolleivät mainokset ärsytä, tämä on ihan hyvä tapa hankkia sovellus. Pienenä riskinä on mainosten mahdollisesti sisältämät haittaohjelmat, jotka voivat olla korruptoituneita sovelluksen tuottajan tietämättä. Mainosta täytyy klikata ennen kuin mahdollinen haittaohjelma voi yrittää latautua. (Albrecht, 2014.)

**Käyttäjän profilointi** on mainosrahoituksen seuraava taso. Yhtiöt kuten Facebook ja Google keräävät käyttäjäprofiileista suuret määrät tietoa, jota käytetään markkinointitarkoituksiin. Tämä saattaa aiheuttaa suuriakin yksityisyysoongelmia, koska käyttäjällä ei ole mahdollisuuksia kontrolloida, mitä dataa kerätään ja miten sitä käytetään. Myös tiedustelupalvelut ovat kiinnostuneita tiedoista. On vaikea tietää, mikä on tämän tyyppisen ”ilmaisen” palvelun tai tuotteen todellinen hinta ja ovatko riskit yksityisyyden menettämisestä liian suuret. (Albrecht, 2014.)

**Harrastus ja ideologia** ovat monien sovellusten synnyn takana. Harrastuksen hauskuuden osa on nähdä muiden käyttävän sovelluksia. Joskus motiivina on ideologia, kuten suuryritysten dominoinnin vastustaminen, turvallisuuden lisääminen jne. Nämä ovat rehellisesti ilmaisia, eikä näihin tuotteisiin sisälly piilotettuja kustannuksia. Riskinä on harrastajamaisuuden vuoksi sovellusten turvataso ja käytettävyys saattaa olla heikompi kuin kaupallisissa tuotteissa. Myös tuki saattaa olla olematonta ja päivitykset harvinaisia. (Albrecht, 2014.)

**Lahjoituksilla rahoittaminen** on muunnelma edellisestä, jotkin ilmaissovellusten toimittajat pyytävät avoimesti lahjoituksia. Monet käyttävät sovelluksia ilmaiseksi, mutta monet maksavat pienen summan kattaakseen valmistajan kustannuksia. Tästä esimerkkinä Wikipedia, jonne sijoitettu raha tuo varmasti hyvän katteen. (Albrecht, 2014.)

**Verorahoitteiset** sovellukset ovat yleensä kulttuurilaitosten tai virastojen palveluportaaleja. Laatu voi vaihdella paljonkin, turvallisuus on yleensä hyvä. Esimerkkejä ovat mm. HSL Aikataulu- ja Reittipalvelu. (Albrecht, 2014.)

**Palvelumaksut** tai **upselling** ovat tapoja, joissa saat perustuotteen tai palvelun ilmaiseksi, mutta maksamalla saat lisää toiminnallisuutta tai kapasiteettia. Tämä on hyvä tapa houkutella asiakkaita kokeilemaan tuotetta. Joissain tapauksissa tuote on ilmainen, ja ansainta tapahtuu tukipalveluita myymällä. Hyvä tapa hankkia tuote, kunhan toimittaja on luotettava, esimerkkinä useimmat pilvipalvelut kuten F-Securen younited ja Dropbox sekä mobiilipelit kuten Clash of the Clans. (Albrecht, 2014.)

**Kaupanpäällinen** tai **kimputus** vaikuttaa siltä, että saat jotain ilmaiseksi kun ostat jotain muuta. Ilmaisten tuotteiden hinta on varmasti laskettu kokonaishintaan mukaan. Esimerkkinä ovat mobiilipelit, joiden mukana saa yhden tai useamman ilmaisen pelin. (Albrecht, 2014.)

**Piraattituotteita** saatetaan tarjota ilmaiseksi, mutta tarjoajalla ei ole oikeutta jaella sitä. Tämä on maasta riippuen enemmän tai vähemmän laitonta. Tarjoaja voi olla rikollinen verkkokauppa tai vertaisverkon kautta saatava ilmaisohjelma ja tuotteet onkin kyllästetty haittaohjelmilla. Kannattaa tutkia, kuka on sovelluksen alkuperäinen myyjä tai tuottaja ja ladata sovellus sieltä, ja samalla välttää haittaohjelman riski. (Albrecht, 2014.)

Huijaukset ja haittaohjelmat ovat usein piiloutuneet ilmaisohjelmiin. Kannattaa olla erittäin varovainen kun älylaitteeseen ilmestyy tarjouksia ilmaisesta palvelusta tai tuotteesta. Puhelinnumero on maksuväline, ja väärään paikkaan päätynyt numero voi tulla kalliiksi. Kivaksi, hyödylliseksi ja hyväksi luultu ohjelma voi paljastua hyvin ikäväksi haittaohjelmaksi. Jos tarjous on liian hyvä ollakseen totta, se ei yleensä ole totta, vaan vain keino istuttaa haittaohjelma laitteellesi. (Albrecht, 2014.)

## 2.4 Wi-Fi-yhteyksien riskit

Kun kulkee ympäri kaupunkia, maata ja maailmaa on mukavaa löytää ilmaisia Wi-Fi-hotspotteja. Ne usein ovat nopeampia ja ulkomailla edullisempiäkin kuin puhelimen 3G/4G-yhteydet ja niihin on helppo kirjautua. Vaara vaanii näissäkin houkutuksissa, etenkin jos yhteys mainostaa itseään ”Totally Free Internet” tai samankaltaisilla vauhdikkaan kuuloisilla lauseilla. Nämä voivat olla rikollisten paikallisesti, esimerkiksi vain

kannettavalla tietokoneella ylläpitämiä hotspotteja, joiden tarkoitus on tietojenkalastelu tai jokin muu epäilyttävä toiminto. (Gallagher, 2014.) Yhdysvalloissa on löydetty ainakin 17 matkapuhelinmastoa, joista vakoillaan matkapuhelimia. Vakoilu paljastui ESD America -yhtiön asiakkaiden havaittua CryptoPhone-turva-puhelimiensa vuotavan dataa. Sitä, kuka näiden vakoilumastojen taustalla on, ei vielä tiedetä (Popular Science, 2014). Useimmat hotspotit ovat isojen operaattoreiden tarjoamia palveluja ja niitä on tuhansittain asemilla, kahviloissa ja ravintoloissa. Niissä ei periaatteessa ole mitään vikaa (eräästä hienoisesta ongelmasta jäljempänä), mutta ne tarjoavat tunkeilijalle mahdollisuuden vaivihkaa vakoilla nettiliikennettäsi ja kaapata tietojasi vihamielisin tarkoituksin. Tähän on syynä älylaitteiden asetuksissa oletuksena oleva automaattinen kirjautuminen tunnistettuun Wi-Fi-verkkoon. Tämä tarkoittaa sitä, että jos joku on rakentanut haitallisen Wi-Fi-yhteyden samalle verkkonimelle jolla uhri on ollut aikaisemmin yhteydessä verkkoon, pääsee hyökkääjä uhrin ja verkon väliin huomaamatta ja ilman salasanoja. Puhelimen langattoman WLAN-yhteyden ollessa päällä laite pyrkii yhdistämään itsensä aina verkkoon, ja koska yhteydenotto pyyntö tulee puhelimesta tunnettuun verkkoon päin, ei salasanaa tai vahvistusta kysytä. Useimmissa laitteissa tämän ominaisuuden pystyy ottamaan pois päältä, mutta osasta vanhempia Android-laitteita tämä mahdollisuus puuttuu. Tällaisen hyökkäyksen pystyy toteuttamaan missä tahansa missä on normaalistikin avoimia verkkoja. (Gallagher, 2014.) Jopa 39 % käyttäjistä ei tee mitään suojaustoimia käyttäessään avoimia Wi-fi-verkkoja (Norton Report 2013, 22). Aikaisemmin mainittu ongelma on näissä ilmaisten verkkoyhteyksien toimitusehdoissa, joita kukaan ei yleensä lue. F-Securen Sean Sullivan teki poikkeuksen ja luki ne ollessaan matkalla Lontoossa Heathrow Expressissä. Yllätys oli melkoinen, tässä suora lainaus Heathrow Express Wi-Fi -käyttöehdoista (Terms of Use):

CONSENT TO MONITORING. HEX RESERVES THE RIGHT TO, AND YOU ACKNOWLEDGE AND CONSENT THAT HEX MAY (BUT IS NOT REQUIRED TO) MONITOR YOUR COMMUNICATIONS AND ACTIVITIES VIA THIS SERVICE (INCLUDING THEIR CONTENT) DURING TRANSMISSION AND IN CONNECTION WITH USE OF THIS SERVICE, AND MAY DISCLOSE ANY SUCH INFORMATION FOR PURPOSES OF ENSURING YOUR COMPLIANCE WITH THIS AGREEMENT, APPLICABLE LAW, COOPERATING WITH LEGAL AUTHORITIES, AND OTHERWISE PROTECTING HEX'S RIGHTS, PROPERTY AND INTERESTS. (Sullivan, 2014a.)

Kun otat käyttöön HEXin langattoman verkon, hyväksyt mahdollisuuden että yhteyttäsi tarkkaillaan, mukaan luettuna sisältö. Tuskin yksityisyyttään voi enää selkeämmin luovuttaa ulkopuolisten tarkasteltavaksi. Ja HEX vielä korostaa toisessa lainauksessa, että vastuu yksityisyydestä ja turvallisuudesta on sinun vastuullasi:

YOU ARE RESPONSIBLE FOR YOUR SECURITY AND PRIVACY. Although privacy and security are important to HEX, you understand and agree that you shall have no expectation of privacy or security in your use of this Service. There are privacy and security risks associated with wireless communications and the Internet generally.

You acknowledge that HEX makes no assurance that your communications or activities will be or will remain private or secure, and agree that HEX assumes no responsibility in that regard. You agree that you, and not HEX, are solely responsible for your own privacy and security in using this Service, and for implementing any protections you deem to be appropriate to protect and secure your privacy, and your activities, hardware, software and systems. (Sullivan, 2014a.)

Lisäksi HEX sanoutuu irti liki kaikesta vastuusta tietojen katoamisesta haitallisiin verkkosivuihin. Ilmainen verkkosivu on hyvin suhteellinen käsite. (Sullivan, 2014a)  
Toinen esimerkki turvallisuudesta ilmaisen verkon ehdoissa on Yhdysvalloista, AT&T:n ilmaisverkosta Starbucks-kahvilaketjussa:

#### SECURITY WARNING

The unsecured nature and ease of connection to public Wi-Fi hotspots increases the risk that unauthorized persons can access your phone, laptop or other device or your communications over the Wi-Fi network. Wi-Fi customers should take precautions to lower the security risks. If you have VPN, AT&T recommends that you connect through it for optimum security. AT&T also encourages its users to observe standard security practices. You should ensure that computer hard drives are not shared; that laptops have firewall protection; and that security software is installed, functional and updated on your device. AT&T recommends that you avoid transmitting or accessing sensitive personal information over the Wi-Fi network, and that you only connect to known Wi-Fi hotspots. (Sullivan, 2014b.)

Käyttöehdoissa sanotaan sängen suoraan, että yhteyden käyttö on turvatonta ja suositellaan parempia käytäntöjä. Lieneekö monikaan lukenut käyttöehtoja. Ilmainen on houkuttelevaa, mutta onko se loppujen lopuksi ensinkään ilmaista. (Sullivan, 2014b)



F-Secure teki Lontoossa testin perustamalla 200 eurolla pienen Wi-Fi -verkon ja laittamalla käyttöehtoihin kohdan, jossa hyväksyjä luopuu esikoisestaan vastineeksi verkon käytöstä. Kuusi henkilöä hyväksyi ehdon ennen sivun poistamista. Verkkoa käytti puolen tunnin aikana 250 laitetta, pääsääntöisesti ilman omistajansa hyväksyntää. (F-Secure, 2014.)

## 2.5 Tulevaisuus

Mitä on tulevaisuudessa edessä? Tietoturvyhtiöiden ennusteet eivät ole kovin valoisaa luettavaa, sillä haittaohjelmien kehittäminen mobiiliympäristöön jatkuu kiihtyvällä tahdilla. McAfeen mukaan uusien mobiilihaittaohjelmien kasvu, joka on lähes yksinomaan Android-ympäristöön kohdistuva, oli jo vuonna 2013 suurempi kuin PC-ympäristöön kehitettyjen haittaohjelmien määrä. PC:n haittaohjelmien määrän kasvu on lähes pysähtynyt, uusien Android-haittaohjelmien määrä kasvoi 33 %. McAfee Labs odottaa tämän trendin myös jatkuvan vuonna 2014. Yhtiö myös odottaa kokonaan uuden tyyppisten hyökkäysten kohdistuvan Androidiin. Esimerkiksi ransomware-hyökkäyksiä jotka kohdistetaan suoraan mobiililaitteisiin ja jotka kykenevät avaamaan laitteen perustiedot ja lukitsemaan ne. Lunnat maksetaan normaalilla valuutalla tai virtuaalivaluutta Bitcoinilla tunkeutujalle. Muita uusia taktikoita voivat olla NFC-järjestelmien haavoittuvuuksia hyväksikäyttävät hyökkäykset, joissa yritetään saada maksulaite hallintaan. Myös kasvavassa BYOD eli tuo-oma-laitteesi-trendissä on riskinsä, yritysten infrastruktuuria urkimaan kehitettyjen haittaohjelmien ujuttaminen puhelimiin odottamaan yhdistämistä yritysverkkoon tekee kattavasta laitteistonhallinnasta hyvin haastavaa. (McAfee Threats Predictions 2014, 2013.)

Japanilaisen tietoturvyhtiö Trend Micron mukaan tulevaisuudessa kyberrikolliset parantavat haittakoodien piilottamista ja salausta, mikä vaikeuttaa haittaohjelmien etsimistä ja analysointia. Yhtiö myös uskoo Android-haittaohjelmien kehittämisen kasvavan ja teollistuvan. Mobiili-botnettien markkinoiden kasvua yhtiö pitää todennäköisenä lähitulevaisuudessa. Botnet-hyökkäyksissä ei yksittäisen laitteen laskuteholta vaadita paljoa, joten älylaitteet soveltuvat kaapattavaksi tähän käyttöön hyvin. Yritys uskoo myös tiettyjä kohderyhmiä vastaan kodistettujen hyökkäysten yleistyvän, kuten tiettyihin vähemmistöihin tai kansallisuuksiin jo kohdistuneet hyökkäykset Koreassa ja Kiinassa.

(Trend Micro, Monthly Mobile Review, 2014.) Haittaohjelmien määrän kasvamisen ja laadun paranemisen ohella Trend Microssa ollaan huolestuneita järjestelmäriippumattomien haittaohjelmien tulemisesta ja yleistymisestä. Nämä sovellukset liikkuvat sujuvasti eri käyttöjärjestelmien välillä ja suorittavat joko samoja tehtäviä tai mukauttavat toimintojaan alustan mukaan. Esimerkkinä ANDROIDOS\_USBATTACK.A, haittasovellus, joka teeskentelee olevansa Android-laitteen puhdistusohjelma. Todellisuudessa se varastaa tietoja laitteelta ja asentaa laitteessa olevalle SD-kortille automaattisesti latautuvan haittaohjelman, joka tarttuu Windows PC:hen kun laite yhdistetään siihen synkronointia tai latausta varten. Sovellus käyttää PC:n mikrofonia käyttäjän salakuunteluun. (Trend Micro, Monthly Mobile Review, 2014.)

Eräs toinen haittaohjelma toimii toisinpäin, tarttumalla PC-koneesta Android-laitteeseen pyrkien urkkimaan pankkitietoja. Järjestelmäriippumattomia haittaohjelmia voidaan käyttää tehokkaasti ujuttautumisessa suurten yritysten ja hallitusten virastojen järjestelmiin, toisaalta myös tiedustelupalvelut voivat käyttää niitä omiin tarkoituksiinsa. Tunnetaan jo sovellus, joka on vakoillut yritystä ja levinnyt yritysverkon kautta älypuheliiniin vakoilemaan henkilön tietoja. Ohjelmassa oli myös kauko-ohjausominaisuus, jolla voitiin ladata ja asentaa toisia haittaohjelmia. On mahdollista, että haittaohjelmat pyrkivät murtautumaan erilaisiin kodin ja teollisuuden automaatiojärjestelmiin. Jos hyökkäys esimerkiksi kohdistuisi kodin turvajärjestelmään, voisi rikollinen tutkia, onko joku paikalla ja ohittaa hälytysjärjestelmän murtautuessaan asuntoon. Teollisuudessa voitaisiin häiritä tai keskeyttää yrityksen tuotantoa. Tällaisen järjestelmäriippumattoman haittaohjelman tekee erityisen vaaralliseksi juuri sen kyky siirtyä laitteesta toiseen ja mahdollisuus ladata muita haittasovelluksia käyttäjän tietämättä. Ei tarvita kuin yksi infektoitunut laite ketjureaktion alottamiseen. (Trend Micro, Monthly Mobile Review, 2014.) Kooste tietoturvyhtiöiden ja ENISAn uhkaennustuksista on liitteessä 2.

Yksi suojautumiskeino on salatun VPN-yhteyden (Virtual Private Network) käyttö. Kannettavissa tietokoneissa yritysmaailmassa tuttu toiminto on saatavilla Android- ja iOS-käyttöjärjestelmiin ainakin F-Securen Freedom- ja Avastin Secure Line – tuotteissa. Windows Phone 8.1-käyttöohjeista päätellen VPN on mahdollinen vain yrityskäytössä (Windows Phone VPN). Freedom ja Secure Line avaavat yhteyden palveluntarjoajan pilvipalveluun, ja tätä kautta haluttuun kohteeseen. Nämä palvelut eivät

kerää lokitietoja käyttäjistä. Ohjelmien toimintoihin kuuluu haitallisten sovellusten ja sivustojen esto, salaus WLAN-verkoissa, tietojenurkinnan esto ja seurannan esto. Ominaisuuksiin kuuluu myös maan vaihdon mahdollisuus eli verkkosivu luulee yhteydenoton tulevan esim. Yhdysvalloista, vaikka se tulisi Suomesta. (F-Secure, 2014, Freedom.) VPN-palvelut herättävät Yhdysvaltain viranomaisissa kuumia tunteita ja ainakin FBI on hakenut laajempia valtuuksia murtautua näihin verkkoihin. (Vänskä, 2014). Palvelut ovat tulleet mobiililaitteissa käyttöön kevään ja alkukesän 2014 aikana, eikä niistä ole juuri löydettävissä käyttäjien arvosteluja tai käyttökokemuksia, joten niiden toimivuutta ei voi vielä arvioida. Twitterissä, F-Securen tilissä, käyttäjät tosin kiittelevät Freedom –palvelua (Twitter.com).

Rik Ferguson, Trend Micron tutkimusjohtaja, on pessimistinen tulevaisuuden suhteen, hän uskoo tulevan vuoden aikana ilmaantuvan murtotyökalun (exploit kit), jolla voidaan murtautua älylaitteisiin suoraan verkkosivulta. Tällaisia drive-by-hyökkäyksiä on jo joihinkin puhelimiin onnistuttu tekemään. Näissä hyökkäyksissä on laite jailbreikattu eli ohjelmiston lukitus on avattu, tällöin tunkeutuja saa laitteen hallintaansa ja pystyy asentamaan siihen sovelluksia ja käyttämään sitä esimerkiksi palvelunestohyökkäyksissä. (Kärkkäinen, 2014.)

Lohdullista on se, että vaikka haittaohjelmia on liikkeellä paljon, mahdollisuus saada tartunta Suomessa sängen pieni, vain 0-2 torjuttua haitaketta kymmentä tuhatta käyttäjää kohti. Isossa Britanniassa määrä on selvästi suurempi, 15-20 kymmentä tuhatta kohditi. Hyökkäysten ja onnistumisten määrä kasvaa vääjäämättä haittaohjelmien kehittyessä ja käyttäjämäärän kasvaessa. (F-Secure Mobile Threat Report Q1, 2014, 3.)

### 3 Käyttöjärjestelmät

Älypuhelimien käyttöjärjestelmissä ylivoimainen on Android. Edes Applen iOS ei yllä lähellekään sen myyntilukemia, ja kaikki muut käyttöjärjestelmät ovat marginaalissa. Suomessa suosittu Windows Phone ei maailmanlaajuisesti yllä kuin 2,5% markkinaosuuteen ja muut yhteensä alle puoleen tästä. Valmistajista Samsung on menettänyt osuuttaan pienemmille valmistajille, mutta on silti suurin vajaan kolmanneksen osuudellaan. Muiden käyttöjärjestelmien romahduksen takana on BlackBerryn vaikeudet ja Symbianin poistuminen markkinoilta. (IDC Worldwide Mobile Phone Tracker, 2014.) Tableteissa johdossa on yhä Applen iPad reilun neljänneksen osuudellaan, Samsung tiukasti kannoillaan, mutta molemmat ovat menettäneet markkinaosuuksiaan pienemmille valmistajille. (IDC Worldwide Quarterly Tablet Tracker, 2014).

Taulukko 3, Älypuhelimien ja tablettien markkinaosuudet tammi-kesäkuu 2014 (IDC Worldwide Mobile Phone Tracker ja IDC Worldwide Quarterly Tablet Tracker).

	2014		2013		2013/2014
	Tammi-Kesäkuu		Tammi-Kesäkuu		
Älypuhelimien käyttöjärjestelmä	Määrä (milj. kpl)	Markkinaosuus%	Määrä (milj. kpl)	Markkinaosuus%	Kasvu
Android	255,3	84,7%	191,5	79,6%	33,3%
iOS	35,2	11,7%	31,2	13,0%	12,7%
Windows Phone	7,4	2,5%	8,2	3,4%	-9,4%
Muut	3,4	1,1%	9,6	2,8%	-60,7%
Yhteensä	301,3	100%	240,5	100%	25,3%
Tabletin valmistaja	Määrä (milj. kpl)	Markkinaosuus%	Määrä (milj. kpl)	Markkinaosuus%	Kasvu
Apple	13,3	26,9%	14,6	33,0%	-9,3%
Samsung	8,5	17,2%	8,4	18,8%	1,6%
Lenovo	2,4	4,9%	1,5	3,3%	64,7%
ASUS	2,3	4,6%	2,0	4,5%	13,1%
Acer Group	1,0	2,0%	1,5	3,4%	-36,3%
Muut	21,9	44,4%	16,4	37,0%	33,4%
Yhteensä	49,3	100%	44,4	100%	11,0%

Nämä kolme käyttöjärjestelmää ovat perusidealtaan melko samankaltaisia, mutta liikkellä eri strategioilla: Android (lähes) avoimella koodilla ja kymmenillä valmistajilla, Windows Phone suljetulla lähdekoodilla ja useilla valmistajilla (mm. Microsoft, HTC, LG ja Samsung), ja Apple suljetulla koodilla, tarkasti valvotuilla sovelluksilla ja vain omilla tuotteillaan. Windowsin Surface- ja Lumia-tableteissa on Windows RT 8.1-käyttöjärjestelmä, joka on lähempänä tietokoneiden Windows 8.1-käyttöjärjestelmää kuin Windows Phone-järjestelmää. (Windows.microsoft.com). Kaikki kolme käyttöjärjestelmää ovat hiekkalaatikko- (sandbox) tyyppisiä. Hiekkalaatikkoympäristössä sovellukset suoritetaan omalla alueellaan, jossa on mm. tallennusalueet ja muut toiminnot. Sovellukset eivät pääse toistensa alueille, eivätkä voi vaikuttaa toisiinsa tai käyttöjärjestelmän toimintaan. Android eroaa tässä siinä, että sovellukset pyytävät asennusvaiheessa lupaa käyttää laitteen eri resursseja ja jos sovelluksessa on haittaohjelma, pääsee se käsi samoihin pyydettyihin tietoihin kuin isäntäohjelma, ja voi lähettää niitä kolmannelle osapuolelle. Windows Phone ja iOS taas eivät salli hiekkalaatikon ulkopuolista toimintaa. (Android sandbox; Apple sandbox; Windows Phone sandbox; Krishnan, Campagna & Iyer, 2011, 17)

### 3.1 Android

Android Inc. perustettiin lokakuussa 2003 ja tarkoitus oli kehittää digikameroita, mutta markkinoita ei pidetty tarpeeksi suurina ja päätettiin keskittyä älypuhelin käyttöjärjestelmiin. Vuonna 2005 Google osti yhtiön ja 5.11.2007 ilmoitti kehittävänsä Android-nimistä käyttöjärjestelmää. Päivää pidetään Androidin syntymäpäivänä. Syyskuussa 2008 ensimmäinen Android-puhelin, T-Mobile G1/HTC Dream, näki päivänvalon. Huhtikuussa 2008 tuli ensimmäinen leivosten ja makeisten mukaan nimetty versio, Android 1.5 Cupcake, tämä nimeämiskäytäntö on voimissaan vieläkin. Syyskesällä 2010 Android-laitteet ohittivat myynnissä Applen iOS-laitteet, eikä kasvu tunnu pysähtyvän vieläkään. (Startapp, 2014.) Versio 4.4 Kitkat julkaistiin lokakuussa 2013 ja uusin Lollipop-niminen versio ilmestyi 15.10.2014. Eri valmistajien laitteisiin päivitykset tulevat hiukan eri aikaan, koska järjestelmän muokkaus kullekin laitteelle ja mallille vie aikansa.(android.com.) Androidin kehittämistä hallinnoi nykyään Googlen vetämä, 2007 perustettu Open Handset Alliance (OHA). Tässä yhteenliittymässä on 84 valmistaja-, operaattori- ja ohjelmointiyritystä (Open Handset Alliance, FAQ).

Android perustuu Linux-käyttöjärjestelmätimeen, jonka Google on muokannut mobiilikäyttöön ja Java-ohjelmointikieleen perustuvaan Dalvik-virtuaalikoneeseen jonka päällä Android-sovellukset toimivat. Sovelluskehitys tehdään Java-kielellä, joka käännetään erikseen Dalvikin käyttämään muotoon.(Linux.fi/Android.) Käyttöjärjestelmä koostuu neljästä kerroksesta; sovellukset, sovelluskehys, ohjelmakirjastot ja Linux-ydin. Laitteen ydinohjelmia ja kolmannen osapuolen ohjelmia ei eritellä, vaan ne ovat tasa-arvoisia sovelluksia resurssien käytössä. (Open Handset Alliance, FAQ.) Jos selaimen tulee haitallinen sovellus, se ei pääse käsiksi muihin sovelluksiin tai käyttöjärjestelmän ytimeen. Kuitenkin hyväksytty haitallinen sovellus pääsee kaikkialle minne selainkin pääsee. (symantec.com, 2011, 11.) Ladattavat sovellukset pyytävät hyväksynnän ja ilmoittavat mitä oikeuksia haluavat, tosin kaikki pyydetty oikeudet täytyy hyväksyä tai sovellus ei lataudu. (support.google.com; symantec.com, 2011, 12). Joten täytyy tarkasti miettiä, suostuuko kompromissiin tietoturvan ja yksityisyyden suhteen ladatessaan sovelluksen.



Kuva 1. Yksinkertaistettu kuva Android arkkitehtuurista (source.android.com).

Androidin hyviä puolia on näytönlukitus, jossa on useita hyviä vaihtoehtoja, joita kannattaa myös käyttää luvattoman käytön estämiseksi. Lukitusvaihtoehdot ovat: liu'utus,

kasvotunnistus (face unlock), kuvio, PIN-koodi ja salasana. Suositeltava on vähintään PIN-koodi ja siinä enemmän kuin neljä numeroa. Paras vaihtoehto on salasana joka tehdään isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä käyttäen. (support.google.com, b.) Uusimmassa Lollipop-versiossa on myös mahdollisuus parittaa laitteita, esimerkiksi puhelin tai tabletti älykellon kanssa, jolloin laitteen tunnistaessa kellon, sen lukitus muuttuu kevyemmäksi, esimerkiksi salasanasta kuvioksi, tai lukitus aukeaa. (Laakso, 2014).

Android-laitteet ovat erittäin monipuolisia ja tehokkaita älypuhelimia ja tabletteja, jotka taipuvat lähes kaikkeen mitä pystyy keksimään. Niiden peruskäyttö on melko yksinkertaista oppia ja taitojen karttuessa niitä voi hyödyntää niin harrastuksissa, kuin ammattikäytössäkin. Eri valmistajien versiot vaihtelevat jonkun verran, mutta se ei ole yleensä haitannut käyttöä. Erittäin tärkeää on pitää mielessä Androidin tietoturva, järjestelmään yritetään istuttaa erilaisia haitakkeita useita eri reittejä. Riskejä kasvattaa ns. roottaus eli ohjelmistolukituksen poisto, tällöin alkuperäinen ohjelmisto korvataan toisella tai laitteen ominaisuuksia muutellaan. Nämä muutokset yleensä kasvattavat haittaohjelmien vaaroja. (androidsuomi.fi, 2011.) Ajantasaisen turvaohjelman käyttö ja sovellusten lataaminen vain laillisista sovelluskaupoista kuitenkin minimoii riskejä ja tekee Android-laitteista turvallisia käyttää.

### **3.2 iOS**

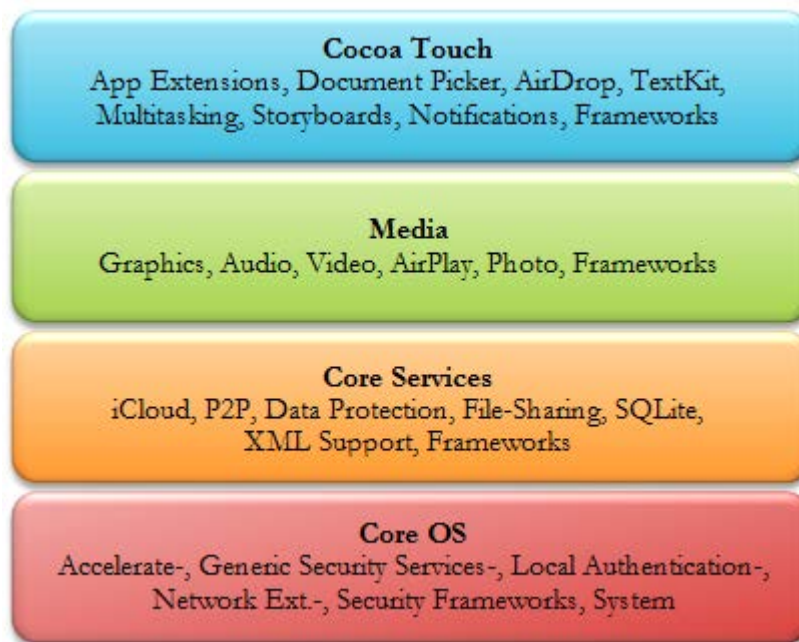
Apple esitteli iPhone 9. tammikuuta vuonna 2007, eikä maailma ollut enää entisensä. Puhelin muutti ihmisten tapaa käyttää laitteitaan ja sai ihmiset vaatimaan laitteiltaan enemmän. iPhone perustuu OS X-käyttöjärjestelmään ja sitä kutsuttiin ensimmäisessä laitteessa nimellä iPhone OS. Nimitys muuttui kesäkuussa 2010, kun versio iOS 4 julkaistiin. Jos ensimmäistä iPhonea vertaa nykyisiin, oli se hyvin alkeellinen, silti siinä oli useita uusia ominaisuuksia, erityisesti kolme vallankumouksellista ominaisuutta: kapasitiivinen kosketusnäyttö, Mobile Safari-verkkoselain ja iPod-soitin. Kapasitiivinen näyttö oli ensimmäinen sormilla toimiva kosketusnäyttö, joka lisäksi mahdollisti nipistämällä tehtävän zoomauksen. Uusi näyttö mahdollisti myös fyysisten painikkeiden poiston. Mobile Safari oli ensimmäinen mobiililaitteelle suunniteltu selain ja se oli lähes yhtä tehokas kuin pöytäkoneissa. Yhdessä kosketusnäytön kanssa se mahdollisti aivan uuden

käyttömukavuuden verkossa surffailuun. iPod-soitin oli sovelluksena ensimmäisessä iPhonessa ja mullisti musiikin kuuntelun tavat helppokäyttöisyydellään. Syyskuussa 2007 tuli ensimmäinen päivitys, jonka merkityksellisin asia oli iTunes musiikkikauppa, josta sai ladattua musiikkia suoraan puhelimeen. Puhelin sai nopeassa tahdissa uusia päivityksiä jotka paransivat vanhoja ominaisuuksia ja toivat uusia. (The Verge, 2013.)

Huhtikuussa 2010 tuli päivitys 3.2 ja seuraava suuri mullistus, iPad. Tabletti toi uusia, isolle näytölle sopivia ominaisuuksia ja paransi netin käyttöä. Vaikka sitä arvosteltiin vain isoksi iPhoneksi, se oli menestys. Saman vuoden heinäkuussa tuli jo seuraava versio, iOS 4, jossa oli runsaasti parannuksia, kuten moniajo, etukamera videopuheluita varten ja tarkka Retina-näyttö. Ominaisuuksia tuli versio versiolta lisää ja versiossa 5 esiteltiin Siri, virtuaaliassistentti, joka kommunikoi äänellä ja osasi vastata mitä erilaisimpiin kysymyksiin. iOS versioissa 6 ja 7 tuli yhä lisää uusia erilaisia ominaisuuksia ja entisiä paranneltiin, syyskuussa 2014 tuli iOS 8 kahdessa uudessa puhelimessa iPhone 6 ja iPhone 6 Plus. iPhone 6 Plus on suurella näytöllä varustettu phablet-tyyppinen laite, puhelimen ja tabletin välimuoto. iOS on käytössä iPhone-, iPad-laitteiden lisäksi iPod Touch- ja Apple TV-laitteissa. (The Verge, 2013.)

iOS-käyttöjärjestelmä on kerroksittainen, kuten muutkin käsiteltävät käyttöjärjestelmät. Sovellukset kommunikoivat iOSin teknologian järjestelmärajapintojen (frameworks) kautta, jotka toimivat ajureiden kanssa. Tämä rakenne suojaa laitteistoa muutoksilta ja mahdollisilta haittaohjelmilta. (iOS Tech Overview, 2014, 8.)





Kuva 2. iOS –arkkitehtuurin kerrokset ja esimerkkejä sisällöstä. (iOS Tech Overview, 2014, 8).

Kuvassa 2 näkyvällä Cocoa Touch-tasolla ovat tärkeimmät kirjastot sovellusten kehittämiseen. Sen ominaisuuksiin kuuluu mm. kosketusnäytön hallinta, käyttäjätiedot, kalenterin ja yhteystietojen tuki. Se tarjoaa välineet sovellusten visuaalisten käyttöliittymien toteuttamiseen. (iOS Tech Overview, 2014, 11.) Media-tason kirjastot ja palvelut mahdollistavat grafiikan, äänen ja videon esittämisen sovelluksissa sujuvasti. (iOS Tech Overview, 2014, 22.) Core Services –kerros on järjestelmäpalveluiden kerros, se sisältää SQLite tietokantakirjaston, paikannusominaisuudet, iCloudin ja Core Foundation –rakenteen, jossa on työkaluja esimerkiksi asetusten hallintaan, aika ja päivämäärä, kielet ja merkkijonot. (iOS Tech Overview, 2014, 35.) Core OS –taso on perusta jolle muut tasot tukeutuvat, sovellukset käyttävät vähintäänkin epäsuorasti tämän tason ominaisuuksia muiden tasojen rajapintojen kautta. (iOS Tech Overview, 2014, 48).

iPhone ja iPad ovat hyvin suosittuja laitteita, eikä syyttä. Niiden käyttö on melko helppoa, ominaisuudet hyviä ja sovelluksia saatavana käytännössä mihin tarkoitukseen hyvänsä. Tietoturvan kannalta ne ovat erittäin turvallisia laitteita, suurin riski on ns. jailbreikatulla laitteilla, jailbreak on Androidin roottausta vastaava tekniikka, jolla ohjelmisto joko vaihdetaan tai sitä muokataan. Lopputuloksena laitteen alkuperäinen suojaus häviää ja se on altis ulkopuolisten hyökkäyksille. (Cassavoy, L. 2014.) Joidenkin mie-

lestä jailbreikkaus on ollut eduksi iPhoneen kehittämiseksi, uusien mallien nopea murtaaminen löytää käyttöjärjestelmien haavoittuvuudet, joita Apple pääsee korjaamaan ennen kuin ne aiheuttavat ongelmia kuluttajille (Bergman, N., Stanfield, M., Rouse, J. & Scambray, J. 2013, 53). iOS-käyttöjärjestelmään on esiintynyt uhkia PDF-dokumenttien kautta, yleensä käyttäjä on houkuteltu lataamaan korruptoitu dokumentti, mikä asentaa jailbreak-ohjelman ja pystyy sen jälkeen asentamaan haittaohjelmia, Apple on tietävästi korjannut tämän haavoittuvuuden. (Sullivan, S. 2010; Hyppönen, M. 2010). Vaikka iOS-laitteet ovat säilyneet merkittävältä turvauhkilta, ei tämä tilanne tule olemaan ikuisen, tämän vuoden alussa on havaittu iPhoneen varta vasten suunniteltu haittaohjelma (F-Secure Mobile Threat Report Q1, 2014, 2). Tämä haitake vahtii SSL-yhteyksiä varastakseen Apple ID:n ja salasanoja (F-Secure Threat Report H1, 2014, 3). Laitteista on myös löytynyt paljon erilaisia haavoittuvuuksia, joko laitteiden vanhenemisen myötä tai uusien laitteiden hiukan keskeneräisten järjestelmien takia, nämä voivat altistaa erilaisille hyökkäyksille (Viestintävirasto, 2014c). Marraskuussa tietoturvayhtiö Palo Alto Networks kertoi iOS-laitteiden haittaohjelmaperheestä, WireLurkerista, joka pystyy tunkeutumaan murtamattomaan iPhoneen. Tunkeutuminen tapahtuu saastuneen Mac-tietokoneen kautta, löytö tapahtui Kiinassa. (Palo Alto Networks, 2014.) Apple kertoo torjuneensa hyökkäyksen tunneissa sen jälkeen kun se oli löytynyt. Yhtiö myös vakuuttaa ettei haitakkeesta ole vaaraa, jollei tarkoituksella poista laitteiden suojausta ja manuaalisesti lataa ohittaen laitteiden turvavarmistusta. (Dilger, 2014.)

### 3.3 Windows Phone

Windows-puhelinten historia alkaa vuodesta 2000, Pocket PC 2000 –käyttöjärjestelmästä, joka pohjautui Windows CE 3.0 alustalle. Se muistutti ja toimi kuten Windows 98-käyttöjärjestelmä. Järjestelmää käytettiin Pocket PC-laitteissa ja sen 2002-versio oli ensimmäinen jota kutsuttiin älypuhelimeksi. Vuoden 2003 versio oli nimeltään Windows Mobile 2003 ja seuraava Windows Mobile 5, vuonna 2005. (Amy, 2010.) Windows Phone –nimiseksi järjestelmä muuttui 2010, version 7 myötä ja samana vuonna julkaistiin ensimmäiset Windows –puhelimet, joita valmistivat mm. HTC, LG ja Samsung. Seuraavana vuonna julkaistiin versio 7.5 ”Mango” ja Nokia ilmoitti ottavansa Windows Phonon ensisijaiseksi käyttöjärjestelmäkseen. Kun Nokia sai lopulta ensimmäiset Lumia –puhelimet, oli kilpailu jo kovaa, iPhone ja eri Android-mallit olivat löytäneet asiakas-

kunnan ja Lumioille ei tuntunut löytyvän tilaa. Windows Phone 8 julkaistiin 2012 ja esitteli useita parannuksia ja yhden munauksen, virheenä pidettiin sitä ettei versio 7.x ollut päivitettävissä versioon 8. Parannuksia olivat SD-korttipaikka, NFC, HD-näyttö ja suurempi tallennustila. Lisäksi toisiin malleihin tuli erittäin tarkkoja kuvia ottavia kame- roita joissa on hyvin valovoimainen optiikka. Kehityksestä huolimatta ei käyttöjärjes- telmä yltänyt siihen mitä Microsoft ja Nokia toivoivat. Tähän toi kehitystä keväällä 2014 julkaistu Windows Phone 8.1, joka paransi käyttökokemusta ja toi paranneltuja ominaisuuksia näyttöön, näppäimistöön ja langattomaan yhteyteen. (Allison, M. 2014.) Suomessa Windows –puhelimet ovat olleet suosittuja Nokia -yhteyden takia ja erittäin menestyneitä yrityspuhelimita, jopa yli 80 % yrityskäytössä olevista laitteista on Lumi- oita, syy lienee yhteensopivuudessa muiden Windows –laitteiden kanssa, Office –tuessa ja hyvässä tietoturvassa (Nygren, T. 2013).

Windows Phonen arkkitehtuuri muistuttaa muiden käyttöjärjestelmien arkkitehtuuria, se on kerroksittainen ja sisältävät likipitään samat toiminnot. Käyttöjärjestelmän ajatuk- sena on ettei sovelluksilla ole pääsyä toistensa suoritusympäristöihin, puhelimeen voi- daan siirtää tietoja vain sovelluksen omilla toiminnoilla tai hallintaohjelmistolla, eikä laitteen muistia voi käyttää suoraan USB-yhteydellä. Näillä keinoilla pyritään tilantee- seen jossa puhelimeen ei pääse mitään haittaohjelmia, eikä siis tarvita torjuntaohjelmia. Jokainen soitto tai tekstiviesti on käyttäjän hyväksyttävä ennen kuin ne lähtevät, toisin kuin Androidissa. Tämä tekee alustasta hyvin turvallisen. (mrwpf.wordpress.com, 2012.)

Windows Phone on ainoa käyttöjärjestelmä jolle ei ole löytynyt yhtään haittaohjelmaa, eikä siten sille ole tehty mitään suojausohjelmia (F-Secure Mobile Threat Report Q1, 2014, 2). Tulevaisuudessa on hyvin todennäköistä että joku keksii murtautumistavan myös Windows Phone –käyttöjärjestelmään, mikään tietojärjestelmä ei ole loputtoman turvallinen. Windows -käyttöjärjestelmään on kuitenkin mahdollista ladata Windows Storesta F-Securen ilmainen Safe Browser –selain, se onko turvaselain tarpeen, jää käyt- täjän päätettäväksi. Selaimen liittäminen puhelimen lapsiasetuksiin voi olla toimiva aja- tus, jos laite on alaikäisten käytössä. (windowsphone.com, 2014.) Windows Phone – puhelimit ovat tietoturvan kannalta turvallisimmat älypuhelimet ja muilta ominaisuuksil- taankin kilpailukykyiset muiden käyttöjärjestelmien laitteiden kanssa.

## 4 Yhteenveto ja pohdinta

Idea aiheesta syntyi, kun lähipiiriin alkoi ilmestyä tabletteja ja älypuhelimia, pian kuulin ilmaan heitettyjä kysymyksiä siitä, onko laitteilla turvallista surffata ja asioida pankissa. Hankittuani oman älypuhelimien, kysymys tietoturvasta ja muista riskeistä arvokkaalle laitteelle konkretisoitui. Yritettyäni verkossa selvittää vastausta kysymyksiin kävi nopeasti ilmi, ettei vastauksen löytäminen ollutkaan yksinkertaista, vinkkejä toki löytyi, mutta vasta pitkähkön kaivelemisen jälkeen. Materiaalia oli paljon, mutta se oli hajallaan eri instanssien verkkosivuilla, tietoturvayhtiöt, viranomaiset, yliopistot ja alan lehtien verkkosivut sisälsivät paljon vinkkejä. Vastaukset olivat kuitenkin sangen pintapuolisia, ”tee näin – älä tee noin”-tyyppiset vastaukset eivät kertoneet miksi niin kannattaa tai ei kannata tehdä. Asian selvittely jalostui opinnäytetyön aiheeksi sangen nopeasti. Ensin ajatuksena oli luoda kattava opas aiheesta ja sitä tukemaan verkkosivu, jossa olisi ajantasainen tieto koottuna yhteen paikkaan ja joka päivittyisi säännöllisesti. Nopeasti kävi selväksi, että tämä vaihtoehto ei ole aikataulullisesti mahdollinen, joten se jää jatkoprojektiksi. Liitteeksi kuitenkin syntyi pieni opas josta voi tarkistaa perustoimet älylaitteen turvalliseen käyttöön, toki kannattaa käydä läpi myös laitteen käyttöohjeen turvasetuksetkin, laitteilla on omat persoonalliset piirteensä jotka on syytä huomioida.

Tutkimuskysymykseksi rajautui kysymys: Mitä jokaisen kuluttajan tulisi tietää älylaitteensa tietoturvasta. Matti ja Maija Meikäläisen kannattaa jotakin tietää aiheesta suojatakseen satojen eurojen investointiaan. Tutkimuksessa kävi ilmi, että suurin riski on rikkoontuminen, katoaminen tai kastuminen, noin joka kolmas käyttäjä törmää näihin ongelmiin. Niihin ei oikeastaan löydy muuta apua kuin laitteen huolellinen käsittely. Haittaohjelmien kanssa tekee Suomessa tuttavuutta alle 0,5 % (promillea) käyttäjistä, mutta riski on kasvamassa ja sen seuraukset voivat pahimmillaan olla kalliimmat kuin laitteen rikkoutuessa. Uudet laitteistoriippumattomat haittasovellukset saattavat levitä puhelimen kautta yrityksen järjestelmään, jolloin vahinkoja voi vain arvuutella. Vaikka uhka on pieni, tulee se huomioida, tavallisen kuluttajankin. Tutkimuksessa yritettiin myös selvittää miten haitakkeet voivat päästä laitteelle ja mitä kannattaa huomioida la-datessaan sovelluksia laitteelleen. Tähän sopii vastaukseksi vanha sanonta – jos jokin

on liian hyvää ollakseen totta, yleensä se ei ole totta. Tavallisesti on kyseessä halpa hinta, ilmaisuus tai piraattituote kun haittaohjelma saastuttaa laitteen.

Suoranaisten tietoturvaohjelmien lisäksi kuluttajia uhkaa vaarantunut yksityisyys, meidän tietojamme keräävät ja säilyttävät useat tahot joiden toimintaan emme voi vaikuttaa, emmekä tiedä mihin tietojamme käytetään. Haittaohjelmat keräävät näitä tietoja kaupallisiin tarkoituksiin ja eri maiden valtiolliset elimet tietoyhteyksien vakoilulla. Vuodet 2013 ja 2014 ovat olleet alalla varsinaiset hullut vuodet, uusia väärinkäytöksiä on paljastunut tätäkin yhteenvettoa kirjoitettaessa ja epäilemättä lisää paljastuu. Kun lainsäädäntö vielä laahaa pitkällä teknisen kehityksen jäljessä, ei yksityisyyden suojele tule olemaan mikään yksinkertainen asia.

Opinnäytettä tehdessäni kävin läpi erittäin suuren määrän materiaalia, joka olisi antanut aiheen useampaankin tutkimukseen: mobiililaitteet työelämässä, haittaohjelmien teknisempi tutkimus ja millaisia ovat torjuntaohjelmat, ainakin nämä ansaitsisivat tarkempaa tutkimusta. Minulle jäi älylaitteiden riskeistä ja kuinka niiden kanssa tulisi toimia, sangen hyvä kuva ja aion jatkaa aiheen seuraamista tulevaisuudessakin. Opinnäytetyö oli hiukan katkonainen prosessi, idea perustui Projektimoduulin Tutkimussuunnitelmatyöhön, jonka tein syksyllä 2013. Kun toinen opinnäyteidea meni myttyyn keväällä 2014, palasin älylaitteen turvaongelmiin ja toukokuussa asia varmistui aiheeksi. Huomattava osa tiedonkeruusta ja työn rungon kirjoittaminen tapahtui kesä-heinäkuussa noin kolmen viikon aikana ja loppukesänä käytin päivän tai kaksi työn kokoamiseen. Syksyllä käytin aikaa mahdollisuuksien mukaan myös työn päivittämiseen, vaikka olin tietoinen älylaitteiden ja niiden uhkien nopeasta kehityksestä, hämmästytti tapahtumien vauhti. Syksyllä tuli laitteista ja käyttöjärjestelmistä uusia versioita, joille välittömästi paljastui uusia uhkia, puhumattakaan uusista uhista vanhoille käyttöjärjestelmille. Uusimmat tiedot tässä työssä ovat joulukuun alusta ja aihetta voisi päivittää loputtomiin. Työ oli erittäin hyvää harjoitusta tietojen etsimiselle ja oleellisen tiedon erottamiselle, kävin työssä läpi mm. liki 50 tietoturvayhtiön verkkosivut. Koko opinnäytetyöprosessi oli muiden koulutehtävien ja nopean Fast Track –opiskelun vuoksi hetkittäin kiireistä, mutta opetti tehokkaasti projektinhallintaa. Työ oli kaikenkaikkiaan antoisaa ja erittäin kiinnostavaa, aikaa hiomiseen olisi käyttänyt kauemminkin.

## Lähteet

Allison, M. 2014, wmpoweruser.com, A history of Windows Phone – The road to treshold

Luettavissa: <http://wmpoweruser.com/a-history-of-windows-phone-the-road-to-threshold/>

Luettu 25.11.2014

Amy, 2010, notebook.com, A brief history of Windows Mobile

Luettavissa: <http://notebooks.com/2010/04/12/a-brief-history-of-windows-mobile/>

Luettu 24.11.2014

android.com, 2014

Luettavissa: <http://www.android.com/versions/lollipop-5-0/>

Luettu 16.10.2014

Android sandbox

Luettavissa: <https://source.android.com/devices/tech/security/#the-application-sandbox>

Luettu 20.10.2014

androidsuomi.fi, 2011

Luettavissa: [http://wiki.androidsuomi.fi/Mit%C3%A4\\_roottaminen\\_tarkoittaa](http://wiki.androidsuomi.fi/Mit%C3%A4_roottaminen_tarkoittaa)

Luettu 30.11.2014

Apple sandbox

Luettavissa:

<https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html>

Luettu 20.10.2014

Bergman, N., Stanfield, M., Rouse, J. & Scambray, J. 2013, 53  
Hacking Exposed: Mobile Security Secrets and Solutions  
McGraw-Hill Education, New York

Cassavoy, L. 2014, cellphones.about.com, What does it mean to jailbreak an iPhone?  
Luettavissa: [http://cellphones.about.com/od/glossary/f/jailbreak\\_faq.htm](http://cellphones.about.com/od/glossary/f/jailbreak_faq.htm)  
Luettu 30.11.2014

Check Point, 2014  
Luettavissa: <http://www.checkpoint.com/press/2014/media-alert-check-point-researchers-uncover-potential-next-generation-android-attacks.html>  
Luettu 17.10.2014

Dilger, E D. Apple Insider, 2014, WireLurker, Masque Attack malware only a threat  
for users who disable Apple's iOS, OS X security  
Luettavissa: <http://appleinsider.com/articles/14/11/10/wirelurker-masque-attack-malware-only-a-threat-for-users-who-disable-apples-ios-os-x-security>  
Luettu 12.11.2014

Dwivedi, H., Clark, C. & Thiel, D., 2010, 7  
Mobile application security  
McGrawHill Companies, New York

ENISA Threat Landscape 2012  
Luettavissa: <http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISAThreatLandscape>  
Luettu 14.7.2014

F-Secure, 2014, Freedom  
Luettavissa: [https://www.f-secure.com/fi\\_FI/web/home\\_fi/freedome](https://www.f-secure.com/fi_FI/web/home_fi/freedome)  
Luettu 15.10.2014

F-Secure Labs

Luettavissa: [https://www.f-secure.com/en/web/labs\\_global/botnets](https://www.f-secure.com/en/web/labs_global/botnets)

Luettu 6.10.2014

F-Secure, 2014, lehdistötiedote

Luettavissa: [http://www2.f-secure.com/fi/web/corporation\\_fi/news-info/product-](http://www2.f-secure.com/fi/web/corporation_fi/news-info/product-news-offers/view/story/1620787/F-Secu-)

Secu-

ren%20testi%20osoittaa%20ihmisten%20k%C3%A4ytt%C3%A4v%C3%A4n%20lang  
attomia%20verkkoja%20huolettomasti

Luettu 5.10.2014

F-Secure Mobile Threat Report Q1, 2013, 4.

Luettavissa: [https://www2.f-secure.com/en/web/labs\\_global/whitepapers](https://www2.f-secure.com/en/web/labs_global/whitepapers)

Luettu 27.6.2014

F-Secure Mobile Threat Report Q1, 2014, 2

Luettavissa: [https://www2.f-secure.com/en/web/labs\\_global/whitepapers](https://www2.f-secure.com/en/web/labs_global/whitepapers)

Luettu 3.7.2014

F-Secure Mobile Threat Report Q1, 2014, 3

Luettavissa: [https://www2.f-secure.com/en/web/labs\\_global/whitepapers](https://www2.f-secure.com/en/web/labs_global/whitepapers)

Luettu 3.7.2014

F-Secure Threat Report H1, 2014, 3

Luettavissa: [http://www2.f-secure.com/en/web/labs\\_global/whitepapers](http://www2.f-secure.com/en/web/labs_global/whitepapers)

Luettu 10.9.2014

F-Secure Threat Report H1 2014, 12

Luettavissa: [http://www2.f-secure.com/en/web/labs\\_global/whitepapers](http://www2.f-secure.com/en/web/labs_global/whitepapers)

Luettu 9.9.2014



F-Secure Threat report H2, 2013

Luettavissa: [http://www.f-secure.com/documents/996508/1030743/Threat\\_Report\\_H2\\_2013.pdf](http://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2013.pdf)

Luettu 27.6.2014

Gallagher, S. Ars Technica, 2014

Luettavissa: <http://arstechnica.com/security/2014/06/free-wi-fi-from-xfinity-and-att-also-frees-you-to-be-hacked/>

Luettu 14.7.2014

Gorilla Glass

Luettavissa: <http://www.corninggorillaglass.com/>

Luettu 20.10.2014

Hyppönen, M. 2010

Luettavissa: <https://www.f-secure.com/weblog/archives/00002004.html>

Luettu 30.11.2014

Hyppönen, M. 27.11. 2014. Tutkimusjohtaja. F-Secure. Sähköposti.

IDC Worldwide Mobile Phone Tracker, 2014

Luettavissa: <http://www.idc.com/getdoc.jsp?containerId=prUS25037214>

Luettu 14.10.2014

IDC Worldwide Quarterly Tablet Tracker, 2014

Luettavissa: <http://www.idc.com/getdoc.jsp?containerId=prUS25008314>

Luettu 14.10.2014

iOS Tech Overview, 2014, 8

Luettavissa:

<https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iOSTechOverview.pdf>

Luettu 25.11.2014

Kilpailu- ja kuluttajavirasto, 2014

Luettavissa: <http://www.kkv.fi/Tietoa-ja-ohjeita/Ostaminen-myyminen-ja-sopimukset/huijaukset/henkilötietojen-kalastelu/>

Luettu 20.10.2014

Krishnan, A., Campagna, R. & Iyer, S. 2011

Mobile Device Security For Dummies

John Wiley & Sons Inc., New York

Kärkkäinen, H. IT-Viikko, 2014, Seuraavan 12 kuukauden aikana tulee murtotyökalu, joka muuttaa kaiken

Luettavissa: <http://www.itviikko.fi/tietoturva/2014/11/26/seuraavan-12-kuukauden-aikana-tulee-murtotyokalu-joka-muuttaa-kaiken/201416335/>

Luettu 27.11.2014

Kärkkäinen H., IT-Viikko, 2013, Älypuhelin on epämääräisilläkin sivuilla turvallinen – vielä hetken

Luettavissa: <http://www.itviikko.fi/tietoturva/2013/03/19/lypuhelin-on-epamaaraisillakin-sivuilla-turvallinen--viela-hetken/20134083/7>

Luettu 25.6.2014

Laakso, J. mobiili.fi, 2014, Uusi Android on nimeltään Lollipop

Luettavissa: <http://mobiili.fi/2014/10/15/uusi-android-on-nimeltaan-lollipop/>

Luettu 16.10.2014

Lehto T., 3T, 2013, Näin urkinta onnistuu, puhelimen synkronoinnissa piilee riski

Luettavissa:

[http://www.3t.fi/artikkeli/uutiset/teknologia/nain\\_urkinta\\_onnistuu\\_puhelimen\\_synkronoinnissa\\_piilee\\_riski](http://www.3t.fi/artikkeli/uutiset/teknologia/nain_urkinta_onnistuu_puhelimen_synkronoinnissa_piilee_riski)

Luettu 27.6.2014

Linux.fi/Android

Luettavissa: <http://linux.fi/wiki/Android>

Luettu 13.10.2014

McAfee Labs Threats Report Q4 2013, 12

Luettavissa: <http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2013.pdf>

Luettu 2.7.2014

McAfee Threats Predictions 2013

Luettavissa: <http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2013.pdf>

Luettu 10.7.2014

McAfee Threats Predictions 2014

Luettavissa: <http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2014.pdf>

Luettu 10.7.2014

Mobiiliasiantuntijat, 2014, Mobiilitietoturvavinkkejä kuluttajille ja pienille organisaatioille

Luettavissa: <http://www.mobiiliasiantuntijat.fi/mobiilitietoturvavinkit.html>

Luettu 26.6.2014

mrwpf.wordpress.com, 2012, Windows Phone, haittaohjelmat, virustorjunta ja palomuuuri

Luettavissa: <http://mrwpf.wordpress.com/2012/04/27/windows-phone-haittaohjelmat-virustorjunta-ja-palomuuri/>

Luettu 20.7.2014

Norton Report 2013, 17.

Luettavissa: <http://go.symantec.com/norton-report-2013>

Luettu 14.7.2014

Norton Report 2013, 7.

Luettavissa: <http://go.symantec.com/norton-report-2013>

Luettu 14.7.2014

Nyrgen, T. 2013, Marketvisio

Luettavissa: <http://www.marketvisio.fi/fi/ajankohtaista/uutiset-marketvisio/1838-nokia-lumia-suosituin-yritysten-puhelinmalli>

Luettu 1.12.2014

Open Handset Alliance, FAQ

Luettavissa: [http://www.openhandsetalliance.com/oha\\_faq.html](http://www.openhandsetalliance.com/oha_faq.html)

Luettu 13.10.2014

Paananen, V. Mr Windows Phone Finland-blogi, 2012, Windows Phone, haittaohjelmat, virustorjunta ja palomuuri

Luettavissa: <http://mrwpf.wordpress.com/2012/04/27/windows-phone-haittaohjelmat-virustorjunta-ja-palomuuri/>

Luettu 27.6.2014

Palo Alto Networks, Unit 42, 2014

Luettavissa: <https://www.paloaltonetworks.com/company/press/2014/palo-alto-networks-reveals-discovery-of-unprecedented-ios-and-os-x-malware.html>

Luettu 10.11.2014

Popular Science, 2014, Mysterious phony cell towers could be intercepting your calls

Luettavissa: <http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls>

Luettu 8.9.2014

Jason, SafeandSavvy-blogi, F-Secure, 2014

Luettavissa: [http://safeandsavvy.f-secure.com/2014/06/24/5-things-you-need-to-know-about-malware-that-takes-your-files-hostage/#.VA9cScJ\\_s8o](http://safeandsavvy.f-secure.com/2014/06/24/5-things-you-need-to-know-about-malware-that-takes-your-files-hostage/#.VA9cScJ_s8o)

Luettu 26.6.2014

Albrecht, M. SafeandSavvy blogi, F-Secure, 2014

Luettavissa: [http://safeandsavvy.f-secure.com/2014/01/10/free-good-or-bad/#.VA9ja8J\\_s8p](http://safeandsavvy.f-secure.com/2014/01/10/free-good-or-bad/#.VA9ja8J_s8p)

Luettu 8.7.2014

Salonen, J. Helsingissä älypuhelinien varkausaalto – samalla kikalla viety 30 000 euron arvosta puhelimia, HS, 23.5.2013.

Luettavissa:

<http://www.hs.fi/kaupunki/Helsingiss%C3%A4+%C3%A4lypuhelinien+varkausaalt+o++samalla+kikalla+viety+30+000+euron+arvosta+puhelimia+/a1369198649594>

Luettu 25.6.2014

security.intuit.com, Phising, pharming, vishing and smishing

Luettavissa: <https://security.intuit.com/phishing.html>

Luettu 20.10.2014

source.android.com

Luettavissa: <https://source.android.com/devices/tech/security/>

Luettu 13.10.2014

Startapp, History of Android

Luettavissa: <http://www.startapp.com/infographics/history-of-android.aspx>

Luettu 13.10.2014

Sullivan, S. 2010

Luettavissa: <https://www.f-secure.com/weblog/archives/00002003.html>

Luettu 30.11.2014

Sullivan, S. F-Secure, 2014a

Luettavissa: <http://www.f-secure.com/weblog/archives/00002719.html>

Luettu 14.7.2014

Sullivan, S. F-Secure, 2014b

Luettavissa: <http://www.f-secure.com/weblog/archives/00002724.html>

Luettu 14.7.2014

support.google.com.a

Luettavissa: <https://support.google.com/googleplay/answer/6014972?hl=fi>

Luettu 14.10.2014

support.google.com.b

Luettavissa: <https://support.google.com/android/?hl=fi>

Luettu 17.10.2014

symantec.com, 2011, 12

Luettavissa:

[http://www.symantec.com/content/en/us/about/media/pdfs/symc\\_mobile\\_device\\_security\\_june2011.pdf](http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf)

Luettu 15.10.2014

symantec.com, 2011, 11

Luettavissa:

[http://www.symantec.com/content/en/us/about/media/pdfs/symc\\_mobile\\_device\\_security\\_june2011.pdf](http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf)

Luettu 15.10.2014

Twitter.com

Luettavissa: <https://twitter.com/FSecure>

Luettu 27.11.2014

The Verge, 2013, iOS: A visual history

Luettavissa: <http://www.theverge.com/2011/12/13/2612736/ios-history-iphone-ipad>

Luettu 14.10.2014

verkkokauppa.com, 2014

Luettavissa: <http://www.verkkokauppa.com/fi/product/52246/fcnxg/Caterpillar-Cat-S50-4G-matkapuhelin-musta>

Luettu 20.10.2014

Viestintävirasto, 2014a

Luettavissa:

<https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/alypuhelintientietoturva.html>

Luettu 8.7.2014

Viestintävirasto, 2014b

Luettavissa:

<https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/kohdistetuthaittaohjelmatovatnykyvakoilunarkipaivaa.html>

Luettu 20.8.2014

Viestintävirasto, 2014c

Luettavissa:

<https://www.viestintavirasto.fi/tietoturva/haavoittuvuudet/2014/haavoittuvuus-2014-105.html>

Luettu 1.12.2014

Windows.microsoft.com

Luettavissa: <http://windows.microsoft.com/fi-fi/windows/windows-rt-faq>

Luettu 5.11.2014

windowsphone.com, 2014

Luettavissa: <http://www.windowsphone.com/en-us/store/app/f-secure-safe/5f87cacf-564b-484a-8ab6-646fc1d18c7a>

Luettu 30.11.2014

Windows Phone sandbox

Luettavissa: <http://msdn.microsoft.com/en-us/library/windows/apps/xaml/dn263232.aspx>

Luettu 20.10.2014

Window Phone VPN

Luettavissa: <http://www.windowsphone.com/fi-fi/how-to/wp8/connectivity/use-a-vpn-connection>

Luettu 8.8.2014

virukset.fi

Luettavissa: <http://virukset.fi/tietoa-meista/>

Luettu 4.11.2014

Vänskä, O. MicroPC, 2014, Tor ja vpnkäyttäjistä tulee vapaata riistaa FBille jos lakialoite menee läpi

Luettavissa:

[http://www.mpc.fi/kaikki\\_uutiset/tor+ja+vpnkayttajista+tulee+vapaata+riistaa+fbille+jos+lakialoite+menee+lapi/a1013270](http://www.mpc.fi/kaikki_uutiset/tor+ja+vpnkayttajista+tulee+vapaata+riistaa+fbille+jos+lakialoite+menee+lapi/a1013270)

Luettu 1.10.2014



# Liite 1

## Tietoturvaohjeita

Olen tähän kerännyt koosteen vinkeistä joilla suojata älypuhelimesi tai tablettisi. Lista saattaa näyttää pitkältä, mutta kun sen kerran käy laitteensa kanssa läpi, voi elää melko huolettomana laitteensa kanssa. Suurin riski Matti ja Maija Meikäläiselle on laitteen rikkoontuminen tai katoaminen, joten kannattaa opetella huolellinen tapa käsitellä laitetta. Rahan menetyksen lisäksi vaivaa voi tulla tietojen palauttamisessa. Kun käyttää tervettä maalaisjärkeä, eivät uhat älylaitteille kasva merkittäviksi. Opettele käyttämään laitettasi ja sen sovelluksia, niin niistä saatava ilo ja hyöty vain kasvaa. Lue myös laitteesi käyttöohjeet, sillä jokaisella laitteella on omat ominaisuutensa.

## Fyysinen turvallisuus

- Älä jätä laitettasi näkyviin pöydälle tms. tai avonaiseen laukkuun/reppuun.
- Pidä laitteen IMEI-koodi tallessa ja saatavilla.
- Huolehdi laitteen varmuuskopioinnista.
- Älä lainaa laitettasi tuntemattomalle.
- Suojaa SIM-kortti ja näytönavaus salasanoilla, muuta esiasetetut PIN-koodit (myös vastaajan). Luo niin vahvat salasanat kuin laitteella on mahdollista.
- Ota laitteen paikannus käyttöön jos sellainen on (voit asentaa myös tietoturvayhtiöitten varkaudenesto-ohjelman) ja laitteen kadotessa yritä paikannusta heti kun mahdollista.
- Soita kadonneeseen puhelimeesi heti kun pystyt.
- Ilmoita operaattorille katoamisesta/varkaudesta ja kerro IMEI-koodi.
- Ilmoita varkaus poliisille ja kerro IMEI-koodi.
- Tee soiton- ja viestinsiirrot kadonneesta puhelimesta jos on mahdollista.
- Sulje puhelin etänä ja poista laitteesta tiedostot, etenkin jos se sisältää yritystietoa tai henkilökohtaisesti arkaluontoista tietoa.
- Kiinnitä laitteeseen yhteystietosi, sähköposti tai toinen puhelinnumero, esimerkiksi tarralla tai laita ne aloitusnäyttöön.
- Suojaa laitetta iskuilta suojakuorella tai kotelolla.

- Pidä näyttö puhtaana, tuhruisesta näytöstä voi pystyä päättelemään pin-koodin tai lukituskuvion.

## **Haittaohjelmilta suojautuminen**

### **1. Sovellusten asentaminen**

- Varmista sen sivuston tai sovelluskaupan luotettavuus jolta olet tuotetta tai palvelua lataamassa.
- Älä lataa piraattiohjelmiä.
- Tarkista, mitä oikeuksia sovellus pyytää.
- Tarkista sovelluksen julkaisijan tiedot.
- Vältä lataamista vertaisverkosta.
- Noudata erityistä varovaisuutta ilmaisten ja mainosrahoitettujen ohjelmien ja niiden sisältämien mainosten kanssa.
- Maksullisen ohjelman tarjoaminen ilmaiseksi tarkoittaa lähes varmasti haittaohjelmaa.
- Tarvitseeko sovellus paikkatietoasi? Sen avulla voi yhdistää muita sinusta kerättyjä tietoja.
- Laitteen valmistajan ja käyttöjärjestelmän toimittajan sovelluskaupat ovat turvallisempia kuin kolmasien osapuolten sovelluskaupat.

### **2. Haittaohjelmien torjunta**

- Käytä Android-laitteissa tietoturvaohjelmistoa, Apple- ja Windows-mobiililaitteissa se ei toistaiseksi ole ajankohtaista (eikä oikeastaan mahdollistakaan).
- VPN-yhteys suojaa haittaohjelmilta, jäljitykseltä ja yksityisyytesi pysyy turvassa.
- Pidä oman tietokoneesi tietosuojan ajan tasalla ja käytä mieluiten vain sitä laitteiden synkronoinnissa.
- Älä kytke puhelintasi tai tablettiasi tuntemattomaan tietokoneeseen.
- Varmuuskopioi laitteesi tiedot.
- Vältä sovellusten mainosten klikkaamista. Jos haluat tutustua mainoksen tuotteeseen tai palveluun, katso niitä suojatulta tietokoneelta.

- Älä säilytä tärkeitä tai arkaluonteisia - omia tai yrityksen - tietoja laitteella, ellei se ole aivan välttämätöntä.
- Käytä tietojen salausohjelmaa, jos säilytät arkaluonteisia tietoja laitteella.
- Käytä salasanojen suojausohjelmaa, jos säilytät salasanoja laitteella.
- Pidä Bluetooth-yhteys oletusarvoisesti pois päältä.
- Lue laitteen käyttöohjeet ja erityisesti suojausasetukset.
- Älä avaa tuntemattomista lähteistä tai numeroista tulevia linkkejä tai liitteitä. Ole varovainen myös tutusta lähteestä tulevien linkkien ja liitteiden kanssa, jos ne poikkeavat normaaleista. Älä anna salasanoja, käyttäjätunnuksia tai puhelinnumeroasi.
- Suojaa myös sähköposti- ja muut tilisi, joita käytät mobiililaitteen kautta.
- Älä avaa tuntemattomasta lähteestä tullutta MMS-viestiä.

### 3. Verkkoturvallisuus

- Käytä julkisia ja avoimia Wi-Fi-verkkoja harkiten, älä kirjaudu niihin jos ne pyytävät henkilökohtaista tietoa, kuten puhelinnumeroa, nimeä, sähköpostiosoitetta, tunnussanoja, tms.
- Älä pidä laitteen automaattista verkkokirjautumista oletusarvoisesti päällä.
- Käytä VPN-yhteyttä turvaamaan yksityisyyttäsi, jos laite sen sallii.
- Noudata samoja tietoturvaperiaatteita älylaitteilla verkossa käydessäsi kuin tavallisella tietokoneellakin.

### Hankkiessasi älypuhelimien tai tabletin

- Mieti mihin ja miten laitetta käytät, satunnaiseen surffailuun ja Facebook-käyntiin ei tarvitse huippuominaisuuksin varustettua laitetta. Onko työ- vai huvikäyttöä? Tarvitsetko Office-pakettia? Pelaatko mobiilipelejä?
- Mieti, missä laitetta käytät.
- Mieti budjettisi ja pysy siinä.
- Tutustu laitteisiin ja eri vaihtoehtoihin netissä ja kysy asiantuntijalta apua, jos tunnet tarvitsevasi.

**Vinkkejä:** Mobiiliasiantuntijat, Viestintävirasto, Kuluttajavirasto, Mobile Security for Dummies, F-Secure, Trend Micro, ENISA, Hacker Exposed Mobile Security

## Liite 2

Kooste tietoturvyhtiöiden tulevaisuuden uhkaennusteista

TIETOTURVAYHTIÖ	MOBIILILAITTEIDENKÄRKIUHAT
Acronis	Salaamattoman tiedon siirto, varastetut kadonneet laitteet, avoimet Wi-Fi ja julkiset Hotspotit, haittaohjelmat, epäselvät käytännöt yrityksissä
	Trojialaiset ja madot (etenkin man-in-the-mobile hyökkäysten esiintyminen), varkaus-katoaminen-vahingoittuminen, drive-by lataukset, exploit kits, koodin injektointi, phishing, identiteetivarkaudet, tietovuodot, botnetit, tietoturvaloukkaukset
Fortinet	Android-haittaohjelmien määrän kasvu, Android-käyttöjärjestelmän kasvu kun suuri osa käyttäjistä on verkon ensikertalaisia, järjestelmästä toiseen siirtyvät haittaohjelmat
F-Secure (Mikko Hyppönen)	Kännykän hukkaaminen, varastaminen tai kastuminen, lapsi kuluttaa tuhansia in-app ostoksia, liikenteen salakuuntelu WLANin kautta, sovellusten tekemä seuranta (yksityisyyden murtuminen), tietojen (puhelinnumeron) kalastelu webin kautta, Androidin haittaohjelmat
Kaspersky	Pankkitrojialaiset, haittaohjelmien parempi piiloutuminen, root access, haittaohjelmien määrän kasvu, Wi-Fi, järjestelmäriippumattomat haittaohjelmat
Marble Labs	Kalastelusovellukset, yritystietojen urkintaan erikoistuneet haittaohjelmat, jailbreaking ja rooting, SSL haavoittuvuudet, vihamieliset konfiguraatioprofiilit, salaamattomat sähköpostiliitteet, ransomware, varmuuskopiointikaappaukset, käyttöjärjestelmien hajanaisuus, oheislatautuvat sovellukset
McAfee	Haittaohjelmien määrän kasvu, ransomware, uudet murtautumistaktiikat, nfc-uhat, yritysinfraan kohdistuvat hyökkäykset ja byod, ytimeen tunkeutuminen, rootkit
Norton/Symantec	Alustojen sirpaloituminen/versioituminen, sovellusmarkettien määrän kasvu, varkaus ja katoaminen, tietovuoto, haittaohjelmien määrä, jaetut laitteet ja salasanat, jailbreak ja rooting, Wi-Fi ja langaton nuuskinta
Sophos	Hyökkäykset pilvessä olevaan yritys- ja hlökohtaiseen dataan, APT ja Android-haittojen kehittyminen sekä uudet kohteet, haittaohjelmien erikoistuminen ja monimuotoistuminen, yksityisyyden vaarantuminen sovellusten ja somen parissa, suojaohjelmien läpäisy uusilla menetelmillä, 64-bittiset haittaohjelmat, exploit kitit, underminig, ”kaiken” hakkerointi
Trend Micro / TrendLabs	Järjestelmäriippumattomat haittaohjelmat, uudelleen pakatut sovellukset, käyttöjärjestelmän haavoittuvuudet, päivitysten puute, Android-haittaohjelmien määrän kasvu ja datan määrä laitteessa, liian yksityiskohtaisen tiedon jako somessa, PUA, Wi-Fi ja Hotspotit, heikot salasanat, epäluotettavat pilvipalvelut