Tomi Koivisto

MOBIILILAITTEIDEN TIETOTURVALLINEN KÄYTTÖ

Tietojenkäsittelyn koulutusohjelma

2014

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

MOBIILILAITTEIDEN TIETOTURVALLINEN KÄYTTÖ

Koivisto, Tomi
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Marraskuu 2014
Ohjaaja: Grönholm, Jukka
Sivumäärä: 48
Liitteitä: 1

Asiasanat: mobiililaite, tietoturva, tietoturvauhat

Tässä opinnäytetyössä tutkittiin kuinka tietoturvallisesti tavalliset kuluttajat käyttävät mobiililaitteitaan. Tutkimuksessa käsiteltiin erilaisia tietoturvallisia mobiililaitteen käyttökeinoja. Asiakokonaisuuden hahmottamisen helpottamiseksi käyttökeinot jaettiin osa-alueisiin. Lisäksi tutkimuksessa selvitettiin löytyykö laitteen tietoturvaan liittyvien keinojen välillä riippuvuuksia ja vaikuttaako käyttäjien sukupuoli, mobiililaitteiden määrä tai käytettävä käyttöjärjestelmä tietoturvan tasoon.

Tutkimus toteutettiin, koska tiedossa ei ollut aiempaa, tavallisten käyttäjien osalta tehtyä mobiililaitteiden tietoturvaselvitystä. Nopeasti kasvavan mobiililaitteiden määrän myötä tietoturvallisuus on tullut ajankohtaiseksi ja entistä tärkeämmäksi. Mobiililaitteen tietoturvallisuutta voidaan parantaa pienin yksinkertaisin toimenpitein, käyttäjien on vain ensin tiedostettavat ne.

Tutkimuksen aineisto kerättiin e-lomake kyselyllä. Saatu raaka-aineisto käsiteltiin SPSS-ohjelmistolla, jonka avulla saatiin selville prosentuaalisia arvoja ja riippuvuuksia. Tutkimustulokset esitellään osa-alueittain, käyttäen kuvioita visuaalisuuden parantamiseksi.

INFORMATION SECURE USAGE OF MOBILE DEVICES

Koivisto, Tomi
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in information technology
November 2014
Supervisor: Grönholm, Jukka
Number of pages: 48
Appendices: 1

Keywords: mobile device, information security, data security threats

---

The purpose of this thesis was to investigate how securely ordinary consumers use their mobile devices. In the study safe use of mobile was examined. To make understanding easier the methods were divided into different sub-areas. Additionally, the study work tried to resolve if there are dependencies between different safe use methods of mobile devices and if the gender of users, number of mobile devices in use or operating system in use affect to the level of security.

The main reason to perform this research was the lack of earlier research results on mobile security based on ordinary mobile users. Rapidly growing number of mobile devices make information and data security actual and more important issue. Mobile device security can be improved with the small counteractions, assuming the users are aware of these.

The data was collected using e-form questionnaire. The raw data was analyzed with SPSS software, in order to evaluate the percentage values and dependences. The results are divided and presented in sub-sectors, using diagrams for better visualization.

SISÄLLYS

1 JOHDANTO

Tämä opinnäytetyö käsittelee mobiililaitteiden tietoturvaa. Tietoturvallisuus on nykyään tuttua käsite lähinnä puhuttaessa tietokoneista. Mobiililaite on monelle jo niin arkinen esine, ettei tietoturvaa välttämättä edes ajatella laitetta käytettäessä. Osa esiin nousevista tietoturvaa uhkaavista asioista on arkisia, mutta niiden varalta voi suojautua pienillä asioilla.

Aiheena mobiililaitteiden tietoturva alkoi kiinnostaa vuoden 2014 keväällä. Kirjoitin aiheesta teoriapohjaisen seminaarityön, joka jalostuu nyt opinnäytetyöksi lisääntyvän teorian ja tutkimuksen myötä. Aiheena mobiililaitteiden tietoturva on mielenkiintoinen sen ajankohtaisuuden takia. Mobiililaitteet, kuten älypuhelimet ja tabletit, ovat yleistyneet lyhyessä ajassa räjähdysmäisesti. Nopea laitteiden määrän kasvu ja edelleen kehittyvä teknologia voivat johtaa siihen, että käyttäjät eivät enää tiedä ja tunnista tilanteita joissa tietoturvallisuus voi joutua uhatuksi. Tietoturvan tärkeys korostuu laitteiden kasvun ohessa, sillä yhä useampi henkilö omistaa mobiililaitteen. Tutkimus painottuu juuri tavallisten käyttäjien, eli kuluttajien mobiililaitteiden tietoturvallisuuden nykyisen tason tutkimiseen.

Opinnäytetyön teoriaosassa käydään läpi tietoturvauhkia, joita mobiililaitteen omistaja voi kohdata. Havaittuihin uhkiin sekä mobiililaitteen käyttöön yleisesti esitetään keinoja, joiden noudattaminen parantaa mobiililaitteen tietoturvallisuuden tasoa. Työssä suoritetaan tutkimus, jonka pohjalta esitetään millä tasolla kohderyhmän kuluttajien mobiililaitteiden tietoturvallisuus on. Tutkimuksen tavoitteena on selvittää prosentuaalisia osuuksia teoriaosassa esitettyjen tietoturvallisuutta edistävien asioiden käytöstä, selvittää riippuvuuksia eri vastausten välillä ja saada käsitys kuinka mobiililaitteiden tietoturvallisuuteen suhtaudutaan. Tutkimuksen kohderyhmä valitaan siten, että vastauksia on mahdollista peilata koskemaan suurempaa joukkoa.

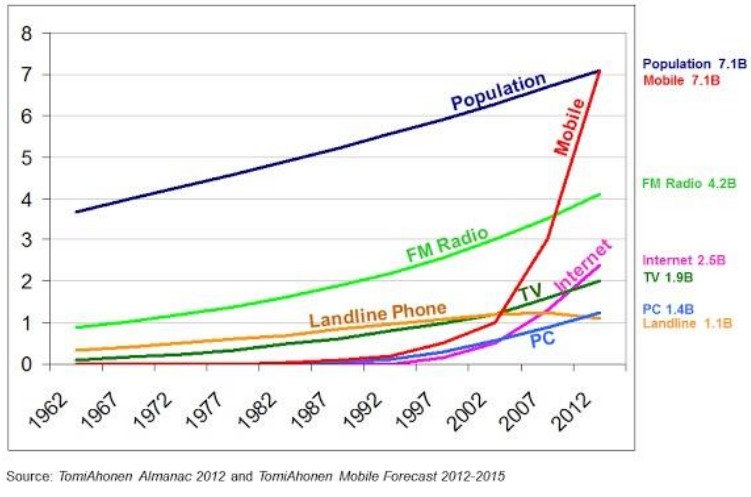
2 MOBIILILAITE

2.1 Mobiililaitteen määritelmä

On tärkeää, että tiedetään, mitkä laitteet ovat mobiililaitteita, jotta tiedetään, mistä puhutaan. Esimerkiksi älypuhelin on mobiililaite, mutta sana mobiililaite ei ole synonyymi älypuhelimelle, sillä määritelmä mobiililaite on hieman laajempi. ”Mobiililaitteita ovat periaatteessa kaikki mukana kulkevat tieto- ja viestintätekniikan laitteet, kuten matkapuhelimet, tablettitietokoneet, paikantimet, kannettavat tietokoneet (esim. miniläppärit) jne. Usein mobiililaitteista käytetään rajatumpaa englanninkielistä määritelmää "hand-held-devices", eli kädessä kulkevat laitteet” (Mobiiliopas 2 www-sivut).

2.2 Mobiililaitteiden yleistyminen

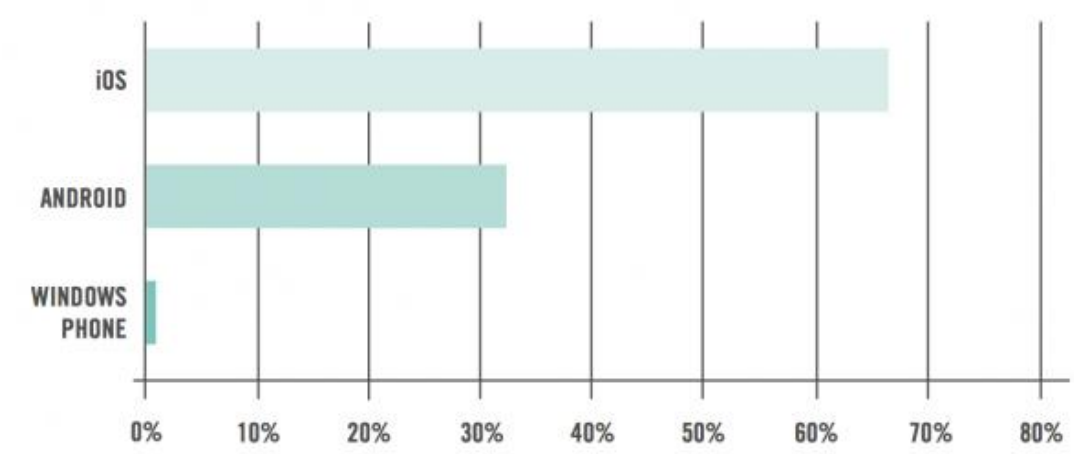
Mobiililaitteet yleistyvät kovaa vauhtia. Arvioiden mukaan vuoteen 2016 mennessä mobiililaitteiden määrä kohoaa 1,4 laitteeseen yhtä ihmistä kohden. Maapallon väkiluku on myös kasvussa, ja vuoden 2016 väkiluvun arvioidaankin olevan 7,3 miljardia ihmistä. 1,4 mobiililaitetta/ihminen kaavalla saadaan siis mobiililaitteiden määräksi vuonna 2016 jo yli 10 miljardia mobiililaitetta. (Luotola 2012 www-sivut.) Alla olevassa kuviossa on esitetty mobiililaitteiden määrän kasvu. Kuviosta käy ilmi, että kesäkuussa 2013 mobiililaitteiden määrä ylsi jo maailman väkiluvun tasolle (Ahonen 2013 www-sivut).



Kuvio 1. Mobiililaitteiden kasvu (Ahonen 2013 www-sivut.)

Mobiililaitteet yleistyvät myös yrityskäytössä, vaikka siihen tiedostetaankin liittyvän omat riskinsä. State of Mobility- tutkimuksessa haastateltiin yli 6000 organisaation edustajaa. 71 % organisaatioiden edustajista ilmoitti, että yritys käyttää, tai vähintään suunnittelee mobiililaitteiden käyttöä. (Symantec www-sivut 2014.)

Yrityskäyttöön tarkoitetuista mobiililaitteista Applen laitteet pitävät selvää johtopaikkaa. Tämä käy ilmi tietoturvaratkaisuja tarjoavan Good Technologyn teettämästä tutkimuksesta. Tutkimus perustuu mobiililaitteiden sekä yrityskäyttöön tarkoitettujen sovellusten aktivointeihin. Alla olevavasta kaaviosta käy ilmi että vuoden 2014 toisella vuosineljänneksellä 67 % käyttöönotetuista laitteista käytti Applen iOS käyttöjärjestelmää, Androidin jäädessä vain 32 prosenttiin. (Laakso 2014 www-sivut.)



Kuvio 2. Mobiililaitteiden käyttöjärjestelmät yrityskäytössä. (Mobiili www-sivut 2014.)

2.3 Mobiililaitteiden käyttö

Mobiililaitteita käytetään nykyään monenlaisiin tarkoituksiin. Perinteiset käyttötarkoitukset, kuten puhelut, viestit ja valokuvaus eivät ole poistuneet mihinkään. Mobiililaitteiden kasvava määrä lisää kuitenkin laitteille jatkuvasti myös uusia palveluja. Palvelut ovat pääasiassa internetpalveluja ja niitä hyödynnetään erillisten ladattavien sovellusten kautta tai internetselaimen välityksellä. (Viestintävirasto www-sivut 2014.) Sovellukset tarjoavat monipuolisen valikoiman käytettäviä palveluita. Esimerkkinä voidaan mainita muun muassa sähköposti, sosiaalisen median sovellukset,

pankkipalvelut, pilvipalvelut, televisio, radio sekä kartta- ja navigointisovellukset. (Hel www-sivut 2014.)

Mobiililaitteiden monipuoliset käyttömahdollisuudet ovat lisänneet saman laitteen käyttöä niin yksityis- kuin yrityskäytössäkin. Vuonna 2014 Recoden teettämän tutkimuksen mukaan 174 miljoonaa ihmistä käytti samaa mobiililaitetta töissä ja kotona. Määrän odotetaan kasvavan reilusti, sillä arvioiden mukaan vuonna 2017 328 miljoonaa ihmistä käyttäisi henkilökohtaista mobiililaitettaan myös työasioiden hoitoon. (Fried 2014 www-sivut.) Saman mobiililaitteen käyttäminen työpaikalla ja kotona helpottuu profiilien avulla, joilla laitteeseen saadaan luotua työ- ja kotikäyttöön sopivat alueet (ks. 4.9).

Perinteisesti yritysten mobiilinkäytön ensimmäinen vaihe on sähköpostipalveluiden käyttö. Mobiilikäytön laajentuessa huomataan kuitenkin, että tietokoneiden parista tuttu, keskitetty laitehallinta voisi olla toimiva ratkaisu myös mobiililaitteiden osalta. Keskitetyn laitehallinnan avulla kaikki yrityksen mobiililaitteet saadaan yhteneväisiksi. Laitehallinnan kautta voidaan asentaa kaikki tarvittavat päivitykset, sovellukset ja virustorjunta, eikä käyttäjän tarvitse vaivata päätään niillä. Ongelmatilanteissa laitehallinta kykenee käyttämään mobiililaitetta etäältä, lukitsemaan laitteen ja tyhjentämään laitteen muistin. (Tieto www-sivut 2014.) Yrityksen näkökulmasta myös sovellusten käyttöönotto ja opastus helpottuu. Laitehallinnan avulla voidaan kaikkiin laitteisiin asentaa uusi sovellus samanaikaisesti, ja järjestää yhteinen koulutustilaisuus käyttöä varten.

3 TIETOTURVAUHAT

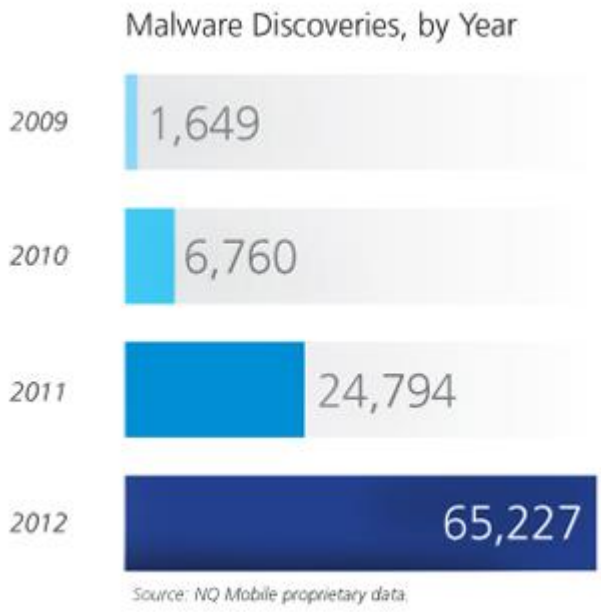
Mobiililaitteet ovat alttiita monenlaisille tietoturvauhille. Toisin kuin tietokoneet, mobiililaitteet on suunniteltu mukana kuljetettaviksi. Mukana kuljetettava pienikokoinen arvokas laite on jo itsestään kokonaisuus, joka altistaa laitteen tietoturvauhille. Mobiililaitteet sisältävä yhä useammin arkaluontoista yksityistä dataa, tai vähintään pääsyn yksityisen datan sisältöön. Myös monipuolistuva yrityskäyttö lisää ar-

vokkaan datan määrää mobiililaitteella. Seuraavaksi käydään läpi yleisimpiä mobiililaitteiden tietoturvauhkia.

3.1 Haittaohjelmat

Jotkut käyttäjät voivat ajatella, että virukset ovat ainoastaan tietokoneisiin kohdistuva uhka. Nykyaikaiset mobiililaitteet altistuvat kuitenkin tietokoneiden tavoin viruksille, vakoiluohjelmille, troijalaisille sekä rootkit- ohjelmistoille. Edellä mainitut haittaohjelmat voivat muun muassa edelleen lähettää tai hävittää laitteen tärkeitä tietoja, muodostaa liittymään puhelinlaskua sekä vakoilla laitetta ja samalla laitteen käyttäjää. (Mobiiliasiantuntijat www-sivut 2014.)

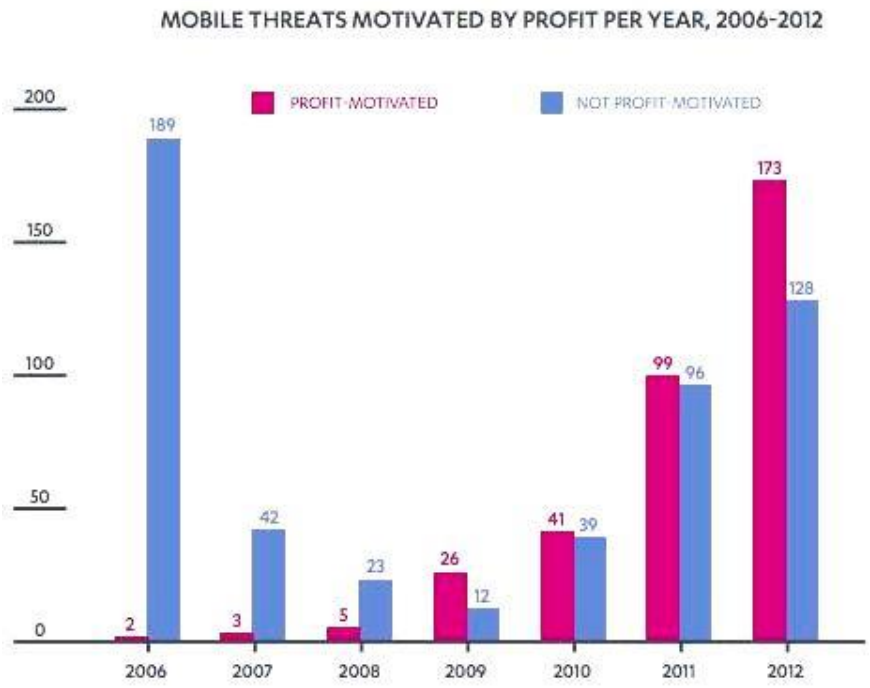
NQ Mobilen julkaiseman raportin mukaan mobiililaitteille suunnatut haittaohjelmat lisääntyvät 163 % vuodessa. Alla olevasta kuviosta käy hyvin ilmi haittaohjelmien räjähdysmäinen kasvu. Vertaamalla vuoden 2009 lukemaa vuoden 2012 lukemaan voidaan todeta, että haittojen määrä on tällä aikavälillä liki 40-kertaistunut. (NQ Mobile www-sivu 2012.) Tietoturvayhtiö Kasperskyn mukaan vuonna 2013 mobiililaitteiden haittaohjelmia oli havaittu jo miltei 150 000 kappaletta (Securelist www-sivut 2013).



Kuvio 3. Haittaohjelmien lisääntyminen (NQ Mobile www-sivut 2012)

NQ Mobilen teettämän tutkimuksen mukaan nuoret mobiililaitteiden käyttäjät ovat alttiimpia tietoturvaohjelmistojen hyökkäyksille. Syy tähän löytyy NQ Mobilen mukaan siitä, että nuoret käyttäjät ovat ahkeria lataamaan mobiililaitteilleen uusia sovelluksia, mutta sovellusten luotettavuuden ja alkuperäisyyden varmistus unohtuu. (Haltia 2013 www-sivut.)

Mobiililaitteille suunnattujen haittaohjelmien tarkoitusperä on muuttunut vuosien kuluessa. Alla olevasta kuviosta käy ilmi, että haittaohjelmien motiivina on yhä useammin raha eikä kiusanteko.



Kuvio 4. Haittaohjelmien motiivit (Dazeinfon www-sivut 2013)

Haittaohjelmien avulla rahaa voidaan tavoitella monin eri keinoin. Yleisimpiä ovat kuitenkin esimerkiksi ponnahdusikkunamainokset, jotka mainostavat käyttäjälle luvallisen näköistä ohjelmaa. Ohjelma saattaa kuitenkin olla haittaohjelma, joka on naamioitu näyttämään oikealta ohjelmalta. Mainoksen avulla pyritään siis saamaan käyttäjä asentamaan haittaohjelma omalle laitteelleen ja pahimmassa tapauksessa vieläpä maksamaan siitä haittaohjelman tekijälle. (Strom 2013 www-sivut.)

Seuraavaksi käydään läpi kolme yleistä mobiililaitteiden käyttöjärjestelmää. Käyttöjärjestelmät ovat erilaisia, joten haittaohjelmatkaan eivät pääse leviämään samoja

kanavia pitkin. Käydään läpi kuinka alttiita käyttöjärjestelmät ovat haittaohjelmille ja kuinka mahdolliset haittaohjelmat pääsevät tunkeutumaan käyttöjärjestelmään.

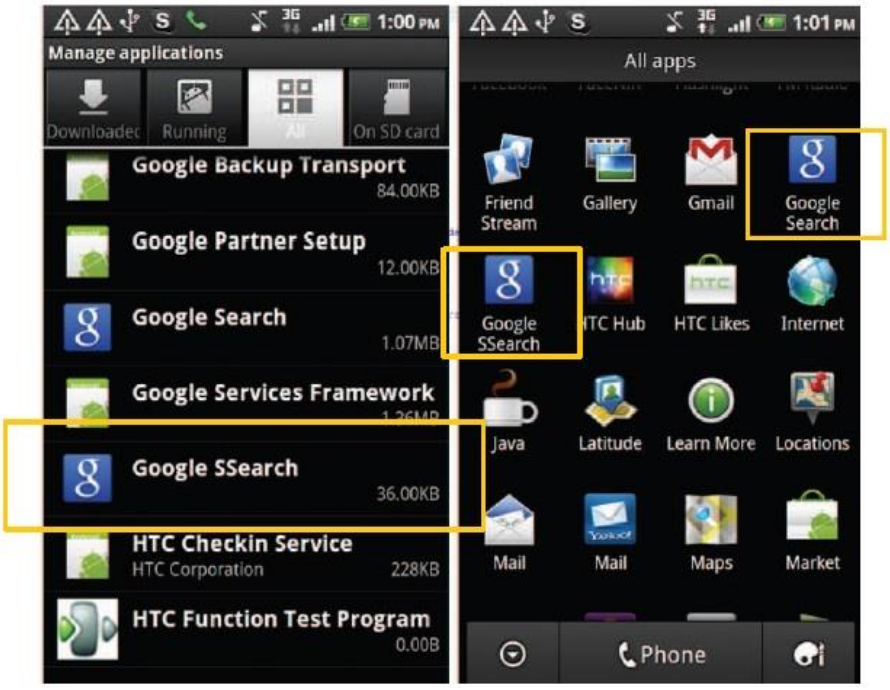
3.1.1 Android

Suomalaisen tietoturvatalo F-Securen mukaan Android-käyttöjärjestelmällä varustetut mobiililaitteet ovat ylivoimaisesti suosituin kohde viruksille ja haittaohjelmille. Vuoden 2013 alussa havaituista viruksista jopa 96 % löydettiin Androidia käyttävästä laitteesta. Vuoden 2013 kesäkuuhun mennessä Android oli kuitenkin kasvattanut johtoaan epämieluisassa tilastossa, sillä jopa 99 % havaituista viruksista oli Android käyttöjärjestelmälle suunnattuja. (F-Secure 2013.)

Androidin ongelmana on ollut Googlen oma Play-sovelluskauppa, jonka kautta käyttäjä on voinut itse asentaa tietämättään haittaohjelmia mobiililaitteelleen. F-Securen mukaan Google on kuitenkin parantanut Play-kaupan sovellusten ennakkotarkastusten tasoa, joten suoranaisten haittaohjelmien määrä kaupassa on romahtanut. Kaupan kautta on silti edelleen mahdollista ladata häiritsevää mainontaa sisältäviä sovelluksia, jotka voivat johdattaa käyttäjää epäluotettaville sivustoille. (F-Secure 2013.)

Sovelluskauppojen parannettua tietoturvaansa ovat haittaohjelmien tekijät pyrkineet etsimään uusia kanavia haittaohjelmiensa levittämiseen. Yhtenä keinona on käyttää hyvämaineisia sovelluksia houkuttimena. Käyttäjälle näytetään mainos, jonka kautta on mahdollista siirtyä suoraan esimerkiksi ”Play-kauppaan” lataamaan mainostettu sovellus. ”Play-kaupan” ulkoasu näyttää samalta kuin oikea Play-kauppa, mutta sitä kautta ladattavat sovellukset sisältävät haittaohjelmia. (F-Secure 2013.)

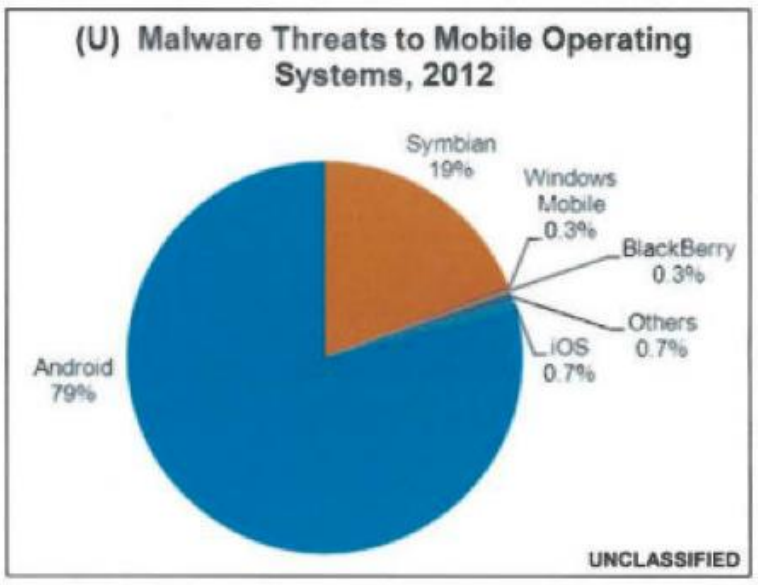
Alla olevassa kuvassa näkyy esimerkki, jossa käytetään valmistajan omaa sovellusta houkuttimena. Mobiililaitteelle on jotain kanavaa pitkin päässyt haittaohjelma, jonka nimi on ”Google SSearch”. Käyttäjä ei välttämättä huomaa sovellusta, sillä ero alkuperäiseen sovellukseen on vain yksi kirjain (Google Search).



Kuva 1. Esimerkki Androidin haittaohjelmasta (F-Secure www-sivut 2012)

3.1.2 iOS

Applen iOS on haittaohjelmien osalta varsin tietoturvallinen käyttöjärjestelmä. Alla olevasta kuviosta käy ilmi, että mobiilijärjestelmissä havaituista haittaohjelmista ainoastaan 0.7 % on suunnattu iOS-käyttöjärjestelmälle.



Kuvio 5. Haittaohjelmat käyttöjärjestelmittäin. (Tuaw www-sivut 2013)

Lähes ainoa tapa tartuttaa iOS-laite on ujuttaa haittaohjelma laillisen sovelluksen koodiin ja sitä kautta tartuttaa mobiililaite. Applen omalla sovelluskaupalla AppStorella on kuitenkin tiukka hyväksymisprosessi uusille sovelluksille. Uusien sovellusten sekä sovellusten kehittäjien on läpäistävä prosessi, ennen kuin sovellus pääsee AppStoreen käyttäjien ladattavaksi. (Digitoday www-sivut 2012.)

Mobiililaitteet joiden tietoturvatoiminnot on kytketty pois päältä, houkuttelevat kuitenkin verkkohyökkäyksiä. iOS-käyttöjärjestelmässä tämä korostuu, mikäli valistuneempi käyttäjä haluaa käyttää laitteellaan itse tehtyjä tai ei hyväksyttyjen ohjelmistokehittäjien tekemiä ohjelmistoja. Tämä johtaa niin sanottuun ”jailbreikkaukseen” eli toimintoon jossa kierretään laitteen turvallisuusohjelmisto. ”Jailbreakkauksen” avulla saadaan siis kierrettyä Applen tiukka sovellusverifiointi ja näin mahdollistetaan kolmansien osapuolten ohjelmien käyttö laitteessa. (Ijailbreak www-sivut 2014.)

3.1.3 Windows Phone

Tietoturvatalo F-Securen tutkimusjohtaja Mikko Hyppönen pitää Windows Phone -käyttöjärjestelmää tällä hetkellä kaikkein turvallisimpana käyttöjärjestelmänä. Hyppönen ennakoikin, että Windows Phone tulee pysymään turvallisena käyttöjärjestelmänä, sillä suojauksen ansiosta verkkorikollisten on vaikea päästä järjestelmään käsiksi. (Vaalisto 2012 www-sivut.) Windows Phone -käyttöjärjestelmän suunnittelun yksi päätavoitteista on ollut, että laitteisiin ei tarvitsisi erillistä haittaohjelmien torjuntaohjelmistoa, mutta laite olisi silti turvallinen käyttää. Tavoite saavutetaan neljällä erillisellä keinolla, jotka esitellään seuraavaksi. (Wordpress www-sivut 2012.)

Windows Phonella voidaan suorittaa vain kahdenlaisia ohjelmatyyppejä. Tyypit ovat Microsoftin omassa selaimessa, Internet Explorerissa, suoritettavat HTML5 webpohjaiset sovellukset sekä .NET-pohjaiset sovellukset. Kaikki mobiililaitteelle asennettavat sovellukset ovat .NET-tyyppiä, minkä ansiosta sovellusten valvontaa pystytään suorittamaan tarkasti. (Wordpress 2012.)

Windows Phone -käyttöjärjestelmälle asennettavat sovellukset on aina asennettava Microsoftin oman verkkokaupan, Marketplacen kautta. Tämä mahdollistaa sen, että kaikki sovelluskauppaan päätyvät sovellukset ovat läpäisseet Microsoftin sertifioinnin, eivätkä siis sisällä mitään haitallista. Jokainen sovellus vaatii siis toimiakseen vahvistetun, voimassa olevan sertifikaatin. Microsoftille on oman maineensakin takia tärkeää, että haitallista koodia sisältävät ohjelmat eivät läpäise sertifiointia. Äärimmäisissä tilanteissa Marketplacen kautta on mahdollista estää jo puhelimeen asennettu sovellus, mikäli huomataan sovelluksen olevan haitallinen. (Wordpress 2012.)

Suoritettavat sovellukset suoritetaan aina omassa, yhtä sovellusta varten rajatussa ympäristössä, jossa toimii siis ainoastaan yksi sovellus. Rajatulla alueella sijaitsee sovelluksen henkilökohtainen tallennusalue, johon tallentuvat sovelluksen käyttöön tarvitsemat tiedot. Muilla sovelluksilla ei siis ole asiaa toisen sovelluksen rajatuille alueille, eikä näin ollen pääsyä sovelluskohtaisiin tallennettuihin tiedostoihin. Tämän lisäksi käyttöjärjestelmä pitää silmällä sovellusten suoritusta sekä tarkkailee sovellusten toimintaa niiden käyttäessä käyttöjärjestelmän palveluita. Rajattu ympäristö tarkoittaa siis sitä, että mikäli alustalle asennettaisiin virustorjuntaohjelmisto, rajattaisiin sekin ohjelmisto omalle alueelleen, ja näin ohjelmisto kykenisi tarkkailemaan ainoastaan omaa toimintaansa. (Wordpress 2012.)

Neljänneksi, alustan muistin käyttö on rajattua. Tämä tarkoittaa sitä, että laitteeseen pystyy siirtämään dataa ainoastaan käyttäen sovellusten omia toimintoja. Tällöin data tallentuu sovelluksen henkilökohtaiseen, rajattuun tallennusalueeseen. Esimerkiksi USB-yhteydellä ei ole mahdollista käyttää suoraan laitteen muistia, vaan käyttö tapahtuu aina jonkun sovelluksen kautta. Edellä lueteltujen keinojen avulla pyritään saavuttamaan tilanne, että Windows-mobiilikäyttöjärjestelmään ei pääse lainkaan haitallisia ohjelmia, vaikka käytössä ei olekaan erillistä haittaohjelmien torjuntaohjelmistoa. (Wordpress 2012.)

3.2 PIN-koodi ja salasanat

Nortonin teettämän tutkimuksen mukaan 69 % mobiililaitteiden käyttäjistä pystyy käsittelemään luottamukselliseksi luokiteltavaa tietoa laitteellaan. On kuitenkin huo-

lestuttavaa huomata, että saman tutkimuksen mukaan 35 % käyttäjistä ei ole suojannut tietosisältöään salasanalla. Mikäli mobiililaitteelle ei ole asetettu näytönlukituksen yhteydessä kysyttävää salasanaa, esimerkiksi lukituskuviota olisi ulkopuolisella henkilöllä suora pääsy omistajan tärkeään dataan, kuten kuviin ja mahdollisesti muihin tallennettuihin salasanoihin. Mikäli mobiililaite varastettaisiin tai laite hukkuisi, olisi todennäköisyys laitteen väärinkäyttöön suuri salasanan puuttuessa. (Kotimikro www-sivut 2013.)

Mobiililaitteella on käytössä yleensä paljon muitakin salasanoja kuin näytönlukituksen avaamiseen tarkoitettu salasana. Mikäli sovellusten ja palvelujen salasanat ovat heikkoja, tai etenkin jos laite muistaa ne automaattisesti, on mobiililaitteen data ulkopuoliselle henkilölle helposti saatavissa mobiililaitteen katoamistilanteissa. Mikäli ulkopuolinen henkilö saa käsiinsä mobiililaitteen, ja salasanat ovat valmiiksi tallennettu laitteeseen, on henkilöllä suora pääsy esimerkiksi omistajan sähköpostiin ja pilvipalveluun. (Kotimikro www-sivut 2013.)

Mobiililaitteisiin asetettava SIM-kortti vaatii PIN-koodin toimiakseen. Kun sammutettu SIM-kortin sisältävä mobiililaite käynnistetään, kysyy laite PIN-koodia, jonka kautta esimerkiksi laitteen mobiilidata tulee käyttöön. Mikäli PIN-koodiksi on jätetty operaattoreiden oletus koodi, (0000 tai 1234) mahdollistaa se SIM-kortin väärinkäytön laitteen joutuessa vääriin käsiin. Joissain laitteissa PIN-koodin kysely on mahdollista ohittaa, mutta se vain lisää tietoturvariskiä. (Mobiiliasiantuntijat 2014.)

3.3 Laitteen katoaminen

Koska kyse on mukana kuljetettavasta mobiililaitteesta, on laitteen katoaminen vakava tietoturvariski. Nortonin teettämän tutkimuksen mukaan 34 % eurooppalaisista mobiililaitteen käyttäjistä ei voisi koskaan luopua laitteestaan, eli laite kulkee aina käyttäjän mukana. Mikäli tulipalon sattuessa olisi mahdollista pelastaa vain kaksi esinettä, olisi miltei neljänneksellä käyttäjistä toinen valinta oma mobiililaite. (Norton www-sivu 2013.) Koska mobiililaite kulkee usein käyttäjän mukana, ei sen kadottaminen ole tavatonta. Suomessa arvioidaan noin 1000 puhelimen hukkuneen vuonna 2005 (Mobiiliasiantuntijat 2014). Mobiililaitteiden räjähdysmäisen kasvun

myötä (ks. 2.2) laitteita omistetaan enemmän, jolloin todennäköisesti hukkuneiden laitteidenkin määrä kasvaa.

Tablettitietokoneiden ja älypuhelimien kallis hinta altistaa laitteita myös varkauksille. Tietoturvayhtiö McAfeen tutkimuksen mukaan mobiililaitteita varastetaankin noin viisitoista kertaa enemmän kuin tavallisia kannettavia tietokoneita. Varkauksia ja katoamisia sattuu erityisesti tapahtumissa, joihin kerääntyy paljon ihmisiä. Tätä todistaa muun muassa se, että Lontoon olympialaisissa arvioitiin noin 67 000 matkapuhelimen kadonneen. (Mobiiliasiantuntijat 2014.)

Mikäli mobiililaite katoaa, eikä laitetta ole suojattu asianmukaisella tavalla, on riski laitteen väärinkäytölle suuri. Ponemon Instituten teettämän tutkimuksen mukaan 35 % yhdysvaltalaisista yrityksistä ilmoitti, että kadonnut yrityspuhelin oli aiheuttanut tietoturvaloukkauksen yritystä kohtaan. Pelkän mobiililaitteen löytäminen ei välttämättä tarkoita vielä tietoturvaloukkausta, mutta mobiililaitteen sisältämä data mahdollistaa sen. Jos data on suojaamatonta ja salasanat on tallennettu valmiiksi laitteeseen, on tietoturvaloukkaus mahdollinen. (Mobiiliasiantuntijat 2014.)

3.4 Vanhentunut laite

Vanhentuneiden mobiililaitteiden käyttöön liittyy ongelmia, sillä käytössä on tällöin myös vanhentunut käyttöjärjestelmä. Vanhentuneeseen käyttöjärjestelmään ei enää julkaista korjauspäivityksiä. Tämä johtaa siihen, että mikäli mobiililaitteen käyttöjärjestelmästä löytyy tietoturva-aukko, on tätä haavoittuvuutta mahdollista käyttää hyväksi loputtomiin, sillä korjaavaa päivitystä ei ole enää saatavilla. (Viestintävirasto www-sivut 2014.)

Esimerkkinä tällaisesta tilanteesta mainitaan Applen iOS 7 käyttöjärjestelmä, johon ei enää julkaista päivityksiä. iOS 7 on käytössä vanhentuneilla Applen mobiililaitteilla, esimerkiksi vuonna 2010 ilmestynyt iPhone 4 käyttää sitä. iOS 7:n sisältämästä Safari-mobiiliselaimesta on löytynyt tietoturva-aukko, joka mahdollistaa haitallisen ohjelmakoodin suorittamisen laitteella, mikäli Safaria käytetään internetselailuun. Koska tätä hyväksikäyttömenetelmän ohjetta jaetaan internetissä avoimesti, on haa-

voittuvuuden hyödyntäminen viestintäviraston mukaan jopa todennäköistä. (Viestintävirasto www-sivut 2014.)

4 TIETOTURVAN PARANTAMINEN

4.1 Päivitykset ja virustorjunta

Mobiililaitteen ohjelmisto on syytä pitää ajan tasalla. Päivitykset voivat parantaa ohjelmiston käyttöä ja lisätä sujuvuutta, mutta ne voivat myös paikata ohjelmistossa havaittuja tietoturva-aukkoja. (Mobiiliasiantuntijat 2014.) Säännöllisillä päivityksillä saadaan siis ylläpidettyä mobiililaitteen tietoturvaa, sillä myös haittaohjelmat kehittyvät, joten ohjelmiston täytyy kehittyä myös. Esimerkiksi Applen iOS 8 käyttöjärjestelmä korjaa 56 tietoturva-aukkoa, jotka on havaittu aiemmissa iOS-versioissa. Mistään pienistä haavoittuvuuksista ei ole kyse, sillä osa niistä mahdollistaa jopa mielivaltaisen koodin suorittamisen, eli hyökkääjä pystyy käyttämään laitetta kuin käyttäjä itse. (Viestintävirasto www-sivut 2014.)

Mobiililaitteisiin on suositeltavaa myös asentaa haittaohjelmien torjuntaohjelma, eli virustorjuntaohjelma, varsinkin jos mobiililaitteessa on käytössä Googlen Android -alusta (ks. 3.1.1). Mobiililaitteisiin on mahdollista asentaa sekä maksullisia että maksuttomia virustorjuntaohjelmia. Virustorjuntaohjelma suojelee mobiililaitetta monella eri tavoin. Yleisin ja ehkä tunnetuin virustorjuntaohjelman muoto on laitteen skannaus. Skannauksessa ohjelma analysoi laitteen tiedostot, tai halutessa vain tietyn osan tiedostoista. Skannauksen aikana ohjelma vertaa laitteella olevien tiedostojen koodia virusten tunnistetietokantaan. Mikäli mobiililaitteesta ja tunnistetietokannasta löytyy samaa ohjelmistokoodia, merkkaa virustorjuntaohjelma kyseisen tiedoston haitalliseksi, ja ehdottaa jatkotoimenpiteitä. Skannaus on mahdollista suorittaa manuaalisesti, tai ajoitetusti. (Symantec www-sivut.)

Toinen virustorjunnan tärkeä osa on reaaliaikainen valvonta. Ohjelma suorittaa reaaliaikaista valvontaa mobiililaitteen taustalla, eikä se vaadi käyttäjältä toimenpiteitä toimiakseen. Tämä toiminto analysoi automaattisesti mobiililaitteen uudet tiedostot

ja sovellukset, ja vertaa tiedostojen koodia skannauksen tapaan virustunnistetietokantaan. (Symantec.) Edellä mainitut toiminnot ovat virustorjunnan perustoimintoja, ja ne löytyvät jokaisesta toimivasta virustorjuntaohjelmasta. Eroa eri ohjelmien välillä kuitenkin löytyy. Ilmainen ohjelma saattaa sisältää ainoastaan perustoiminnot, kun taas maksullinen versio saattaa sisältää laajemman tunnistetietokannan, sekä enemmän ominaisuuksia, esimerkiksi QR-koodien skannauksen (ks. 4.7).

Virustorjuntaohjelman sekä tunnistetietokannan päivittäminen nousee erittäin tärkeään rooliin haittaohjelman havaitsemisessa. Uusia haittaohjelmia tehdään nimittäin jatkuvasti lisää. Pahimmassa tapauksessa haittaohjelma jää tunnistamatta, koska virustorjuntaohjelma on vanhentunut tai sillä on käytössä vanhentuneet virustunnisteet. Virustorjuntaohjelman asentamisen lisäksi on siis huolehdittava siitä, että ohjelman päivitykset ovat ajan tasalla. (Symantec.)

4.2 PIN-koodi

PIN-koodi on nelinumeroinen tunnusluku, joka tarvitaan puhelinliittymän käyttöön. Mikäli mobiililaite on sammutettu, ja SIM-kortti on laitteen sisällä, kysyy laite PIN-koodia käynnistyksen yhteydessä. Operaattoreiden yleisimpiä alkuperäisiä PIN-koodeja ovat 0000 ja 1234. Näitä alkuperäisiä koodeja ei ikinä tulisi käyttää, sillä niiden arvaaminen on helppoa. PIN-koodin tulisi olla sellainen, jonka käyttäjä pystyy helposti muistamaan, mutta samalla sellainen, joka ei ole helposti pääteltävissä. Syntymäaika ja vuosi ovat mahdollisia PIN-koodeja, joita ulkopuolinen henkilö pystyy päättelemään, mikäli tuntee mobiililaitteen omistajan. PIN-koodi ei kuitenkaan suojaa mobiililaitteen dataa, sillä esimerkiksi laitteen muistikorttiin on pääsy, vaikka laitteen PIN-koodi ei olisikaan tiedossa. (Mobiiliasiantuntijat 2014.)

4.3 Vahvan salasanan käyttö

Jotta salasana tarjoaa parhaan mahdollisen suojan, tulisi aina käyttää vahvoja salasanoja. Vahva salasana on 7-16 merkkiä pitkä, ja sen tulisi sisältää vähintään kolmea erilaista merkkityyppiä. Merkkityypit ovat isot kirjaimet, pienet kirjaimet, numerot sekä erikoismerkit. Koska vahvan salasanan tarkoitus on olla mahdollisimman vaike-

asti murrettavissa, on suositeltavaa, että salasana ei ole sana tai sanan muunnelma. Vahvimmatkin salasanat ovat kuitenkin murrettavissa. Tämän johdosta suositellaankin, että salasana vaihdettaisiin uuteen aina tietyin väliajoin, esimerkiksi 3 kuukauden välein. Salasanan vaihdossa tulisi välttää vanhojen salasanojen kierrätystä. (Helsingin tietotekniikkapalvelut www-sivut.)

Usein mobiililaitteisiin on mahdollista asettaa salasana tai suojakoodi, joka estää laitteen luvattoman käytön. Mobiililaite kysyy käyttäjältä salasanaa esimerkiksi, kun laite on ollut minuutin käyttämättä. Ilman oikeata salasanaa mobiililaitetta ei ole mahdollista käyttää. Kun käyttäjä on asettanut vielä mobiililaitteella käytettäviin palveluihin vahvat salasanat, jotka kaikki poikkeavat toisistaan, suojaus moninkertaistuu. Salasanojen ei kuitenkaan tulisi unohtua, sillä mobiililaitteissa ei yleensä ole takaporttia salasanojen ohittamiselle. (Mobiiliasiantuntijat 2014.)

Vahvan salasanan keksiminen voi olla joskus haastavaa, mutta esimerkiksi Mozilla tarjoaa apua oman salasanan kehitykselle. Mozillan ohjeessa vahvan salasanan luominen sisältää kolme eri vaihetta:

1) fraasi
2) erikoismerkit
3) liittäminen tiettyyn sivustoon.

Ensimmäisessä vaiheessa keksitään fraasi esimerkiksi "Ja niin olen kertonut seitsemästä veljeksestä Suomen saloissa." (Mozilla www-sivut). Fraasi lyhennetään siten, että käytetään jokaisen sanan ensimmäistä kirjainta, ja sana ”seitsemän” korvataan numerolla ”7”. Näin saadaan merkkijono Jnok7vSs. Toisessa vaiheessa saatuun merkkijonoon lisätään erikoismerkki tai erikoismerkkejä. Esimerkiksi lisätään merkkijonon alkuun huutomerkki (!) sekä loppuun kysymysmerkki (?). Näin saadaan merkkijono !Jnok7vSs?. Kolmannessa vaiheessa lisätään saatuun merkkijonoon etu- tai takaliite, joka linkittää salasanan sivustoon tai palveluun, jossa salasanaa käytetään. Salasanaa käytetään esimerkiksi verkkosivustolla www.huuto.net. Lisätään merkkijonon !Jnok7vSs? alkuun ”Huu”, ja vahva salasana Huu!Jnok7vSs?, on syntynyt. (Mozilla.)

4.4 Salasanojen hallintaohjelma

Vaikka käytössä olisikin vahva salasana, voi tietoturvariskiksi muodostua saman salasanan käyttäminen useammassa paikassa. Salasanojen hallintaohjelma tarjoaa käyttäjille vahvaa salasanasuojausta siten, että käyttäjän tarvitsee muistaa vain yksi salasana. Salasanaohjelma nimittäin tarvittaessa luo, muistaa sekä automaattisesti täyttää sisäänkirjautumistiedot käyttäjän käyttämiin palveluihin. Käyttäjän täytyy ainoastaan määrittää, sekä muistaa ohjelman pääsalasana. (Taipale 2013 www-sivut.)

Salasanaohjelma tallentaa salasanat kryptattuun, eli salattuun tiedostoon. Tiedosto on suojattu ohjelmaan määritetyllä pääsalasanalla, joten ulkopuolisilla tahoilla ei ole pääsyä tiedostoon. Luotettava salasanaohjelma käyttää tunnettuja, sekä vahvoja salasana-algoritmeja, ja tällaisia ovat esimerkiksi Serpent, AES ja Blowfish. (Mobiiliasiantuntijat 2014.)

Hyvä salasanojen hallintaohjelma toimii ja synkronoituu useamman alustan välillä. Tällainen on esimerkiksi F-securen tarjoama KEY-salasanaohjelma. KEY toimii mobiililaitteissa, joissa on vähintään Android 4.0- tai iOS 5-käyttöjärjestelmä. KEY tallentaa salasanat salattuna mobiililaitteen muistin lisäksi myös F-securen palvelimelle. Tallennus tapahtuu nimettömästi, joten palvelimella olevaa salattua tiedostoa ei voida mitenkään yhdistää tiettyyn käyttäjään. Palvelimen kautta KEY pystyy synkronoimaan salasanat useammalle laitteelle, mikäli käyttäjällä on käytössä useampi mobiililaite, jossa KEY on asennettuna. (F-secure.)

4.5 Varmuuskopiointi

Mikäli mobiililaite hukkuu tai hajoaa, katoaa sen mukana kaikki sen sisältämä data. Data on kuitenkin mahdollista pelastaa säännöllisellä varmuuskopioinnilla. Tarvittaessa kadonnut data voidaan palauttaa korjattuun tai kokonaan uusittuun laitteeseen. Esimerkiksi älypuhelimissa valmistajat tarjoavat sovelluksia varmuuskopiointiin, mutta erikseen asennettavia sovelluksia löytyy myös. (Mobiiliasiantuntijat 2014.)

Varmuuskopioitu data on mahdollista tallentaa moniin eri paikkoihin. Tallennusaluetta miettiessä kannattaa kuitenkin huomioida se, että mikäli mobiililaite katoaa, ei varmuuskopio katoaisi laitteen mukana. Tästä syystä esimerkiksi mobiililaitteessa käytettävät muistikortit ovat huono sijainti varmuuskopioille. Hyviä tallennuspaikkoja sen sijaan ovat alueet, jotka ovat kokonaan erillisiä mobiililaitteista. Tietokoneen kovalevy, ulkoiset kovalevyt sekä pilvipalvelut ovat esimerkkejä hyvistä tallennuspaikoista. (Mobiiliasiantuntijat 2014.) Varmuuskopiointi on syytä muistaa tehdä säännöllisesti, sillä hyöty varmuuskopioinnista katoaa, mikäli varmuuskopioidut tiedostot ovat vanhentuneita.

Myös pilvipalveluita on mahdollista käyttää varmuuskopioinnissa. Mobiililaitteilla on mahdollista ottaa automaattinen synkronointi käyttöön, jolloin tärkeä data, esimerkiksi valokuvat, tallentuvat mobiililaitteen muistin lisäksi myös etäpalvelimelle. Mikäli tärkeä data katoaa mobiililaitteesta, automaattisen synkronoinnin ansioista ne löytyvät kuitenkin pilvestä. Jotta pilvestä löytyisi aina päivitetty materiaali, tulee datan ehtiä synkronoitua etäpalvelimelle ennen datan mahdollista katoamista. Pilvipalveluun synkronoituja tiedostoja on mahdollista tarkastella esimerkiksi tietokoneen kautta. (Mobiiliasiantuntijat 2014.)

Pilvipalveluja käytettäessä on kuitenkin syytä muistaa, että pilvipalvelun käyttöön liittyy myös riskinsä, joista suurimmat liittyvät käyttäjän tietosuojaan. Pilvipalveluissa käyttäjien tiedostot säilötään suurille palvelimille, joissa ne voivat altistua hakkeroinneille sekä väärinkäytölle. (Helsingin Sanomat www-sivut.) Pilvipalvelun käytössä on suuret mahdollisuudet, mutta se sisältää myös riskinsä. Kannattaa siis harkita, käyttääkö pilvipalveluita korvaamattoman arvokkaan datan käsittelyssä.

4.6 Varkaudenhallintajärjestelmä

Eri varkaudenhallintajärjestelmillä on erilaisia ominaisuuksia, ja ominaisuuksien määrä riippuu pitkälti siitä, onko sovellus maksuton vai maksullinen. Hyvän ja monipuolisen varkaudenhallintajärjestelmän avulla pystyy estämään mobiililaitteen luvattoman käytön ja jopa paikantamaan varkaan. Varkaudenhallintajärjestelmä mahdollistaa esimerkiksi mobiililaitteen käytön eston etäältä. Mobiililaite lukkiutuu au-

tomaattisesti, jos siihen vaihdetaan SIM-kortti. Laitteen lukitseminen onnistuu myös lähettämällä siihen tekstiviestillä lukituskoodi. Kadonnut tai varastettu mobiililaite pystytään paikantamaan GPS-signaalin avulla lähettämällä laitteeseen tekstiviesti-koodi, jolloin paluuviestinä saadaan mobiililaitteen sijaintitiedot. Erityisesti yritys-käyttöön hyödyllinen ominaisuus on laitteen tyhjennys etäältä. Mobiililaitteen hukkuessa yritykselle tärkeä data ei joudu vääriin käsiin, vaan kadonnut data voidaan tuhota. (Mobiiliasiantuntijat 2014.)

Varkaudenhallintajärjestelmän voi asentaa mobiililaitteeseen omana erillisenä ohjelmana, mutta esimerkiksi suomalainen F-Secure tarjoaa kyseisen palvelun virustorjuntaohjelmistonsa yhteydessä. F-Securen Mobile Security on maksullinen ohjelmisto, mutta se tarjoaa laajan ja luotettavan suojan mobiililaitteelle. Ohjelmisto sisältää kaikki edellä mainitut ominaisuudet sekä lisäksi muutaman lisäominaisuuden, joita ovat hälytystoiminto sekä varkaan puhelinnumeron ilmoittaminen. Hälytystoiminto on hyödyllinen, jos mobiililaite on hukkunut. Tekstiviestin avulla mobiililaite saadaan pitämään kovaa hälytysääntä, jolloin laitteen löytäminen on helpompaa. Theft control -järjestelmä puolestaan ei ainoastaan lukitse mobiililaitetta, mikäli siihen asennetaan toinen SIM-kortti, vaan se myös lähettää uuden SIM-kortin numeron ennalta määriteltyyn numeroon. Näin varkaan henkilöllisyyden selvittäminen helpottuu huomattavasti. (F-Secure www-sivut.)

4.7 Luotettavat lähteet

Haittaohjelmilta suojautumiseen on olemassa omia ohjelmistoja (ks. 4.1), mutta niitä pystyy välttämään myös viisaalla mobiililaitteen käytöllä. Tiedostoja ja ohjelmistoja ei ikinä tulisi ladata tuntemattomasta lähteestä (Webopas). Mobiililaitteen omat sovelluskaupatkin saattavat sisältää haitallisia ohjelmistoja (ks. 3.1), joten ennen latausta on syytä tarkistaa ladattavan ohjelmiston lähde ja esimerkiksi muiden käyttäjien arvioinnit ja kommentit.

Samanlaiset suositukset turvalliseen mobiililaitteen käyttöön pätevät myös internet-selailuun sekä sähköpostin käyttöön. Selaimella suositellaan käytettäväksi vain luotettavia, paljon käytettäviä sivustoja. Osoiteriville kirjoittaessa on syytä olla tarkka-

na, sillä kirjaimenkin heitto osoitteessa voi ohjata käyttäjän väärälle sivulle. Haittaohjelmien kehittäjät pyrkivät käyttämään juuri tällaisia inhimillisiä erehdyksiä hyväkseen. Esimerkiksi käyttäjän on tarkoitus kirjoittaa osoiteriville www.google.fi, mutta hän kirjoittaakin epähuomiossa www.gooogle.fi. Tällaisella inhimillisellä erehdyksellä käyttäjä voi navigoitua täysin väärälle sivustolle. (Webopas.)

Myös sähköpostia käytettäessä epämääräisiltä lähettäjiltä tulleita posteja ei kannata edes avata. Itse sähköpostin avaaminen ei vielä välttämättä altista mobiililaitetta haittaohjelmalle, mutta epäluotettavien sähköpostien sisältämät liitetiedostot voivat olla haitallisia, joten niitä ei tulisi avata. Sähköposteissa on käytössä roskapostisuodattimia, joiden avulla mainospostiksi luokiteltavat viestit siirretään suoraan roskapostikansioon (Webopas.)

Bluetooth on kätevä tapa siirtää dataa laitteesta toiseen. Bluetoothin välitykselläkin pystyy kuitenkin lähettämään haitallisia tiedostoja laitteelta toiseen. Tästä syystä Bluetooth-asetukset kannattaa määritellä niin, että tiedostoja vastaanotetaan ainoastaan varmennetusta ja luotetusta lähteestä. Infrapunatoiminnossa tilanne on sama kuin Bluetoothissa. Signaalia kannattaa vastaanottaa vain silloin, kun se on tunnettu. (Webopas.)

Mobiililaitteiden räjähdysmäisen kasvun myötä, myös QR-koodit ovat yleistyneet. QR-koodit ovat kaksiulotteisia ruutukoodeja, joita luetaan mobiililaitteeseen ladatulla lukuohjelmalla. Tällaisia ruutukoodien lukuohjelmia pystyy lataamaan sovelluskaupoista täysin ilmaiseksi. QR-koodit eivät kuitenkaan aina ole niin vilpittömiä kuin voisi kuvitella, sillä myös QR-koodin kautta levitetään haittaohjelmia. Haittojen levittäjien näkökulmasta ruutukoodit on houkutteleva levityskanava, sillä pelkän silmän perusteella ei pysty toteamaan, onko ruutukoodi haitallinen vai ei. (Tivi www-sivut 2013.)

Yleinen QR-koodin kautta leviävä haitta on javascript-troijalainen. Käyttäjä lukee laitteellaan QR-koodin, laite lukee koodin linkkinä ja avaa linkin mukaisen verkkosivun. Avattu verkkosivu saattaa näyttää täysin turvalliselta, mutta verkkosivulle on piilotettu haitallista koodia. Sivun avaamisen yhteydessä myös haittakoodi aktivoituu, ja pyrkii siirtämään haittaohjelman mobiililaitteeseen. (Tivi 2013.)

QR-koodien käyttöön on olemassa myös turvallisia lukuohjelmia. Tällainen on esimerkiksi Symantecin valmistama Norton Snap. Snap lukee ruutukoodin, mutta ennen kohteen avaamista se tarkistaa Symantecin palvelimelta, onko avattava kohde turvallinen. Mikäli kohde osoittautuu haitalliseksi, Snap estää linkin aukeamisen eikä päästä käyttäjää tietoturvattomalle sivustolle. (Norton www-sivut 2013.)

Luotettavan lähteen käyttöä kannattaa ajatella myös etsiessään mobiililaitteella latauspaikkaa. Harva nimittäin tulee ajatelleeksi, että ladattaessa laitetta esimerkiksi tuntemattoman PC:n, tai vaikkapa auton USB-portin kautta, saattaa puhelimen data olla vaarassa. Yleensä mobiililaitteella USB-yhteyttä muodostettaessa, yhteystyyppi on automaattisesti joko MTP tai PTP. MTP-tyyppi on suunniteltu kaikkien mediatiedostojen siirtämiseen USB-liitännän avulla. PTP puolestaan on tarkoitettu valokuvien ja kaikkien MTP:tä tukemattomien tiedostotyyppien siirtoon. Mikäli jompikumpi edellämainituista yhteystyypeistä on valittuna, on mahdollista että USB-portin kautta mobiililaitteen dataa kopioituu esimerkiksi PC:n kiintolevylle. Mikäli kuitenkin tuntematonta porttia on käytettävä lataukseen, on laite hyvä sammuttaa latauksen ajaksi. (Malenkovich 2013 www-sivut.)

Androidin käyttöjärjestelmällä toimiva mobiililaite voi joutua myös haittaohjelman uhriksi kun mobiililaite liitetään tietokoneen USB-porttiin. Suurin osa käyttäjistä on kuitenkin suojassa tältä uhalta. Mobiililaitteessa tulisi olla debug mode, eli kehittäjätila päällä sekä sovelluskehittäjän asetuksista USB-virheenkorjaus sallittuna, jotta haittaohjelma pystyisi asentumaan automaattisesti USB-portin kautta laitteeseen. Edellä mainitut asetukset ovat kuitenkin oletuksena poissa käytöstä. (Digitoday www-sivut 2014.)

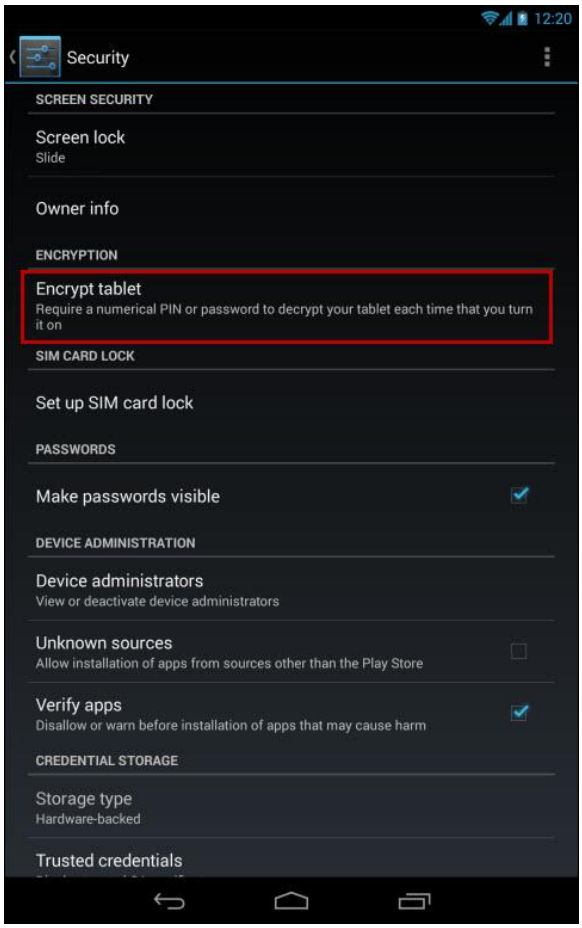
4.8 Datan salaus

Mobiililaitteen sisältämä data voi joutua vääriin käsiin, vaikka käyttäjä olisi suojannut laitteensa kaikilla edellä mainituilla keinoilla. Esimerkkinä voidaan ajatella tilannetta, jossa mobiililaite hukkuu. Laitteen löytää vieras henkilö, joka ei kuitenkaan pääse näyttölukituksen ohi käsiksi laitteen tietoihin. Löytäjä pystyy kuitenkin siirtä-

mään mobiililaitteen muistikortin omaan laitteeseensa ja kaikki SD -eli muistikortille tallennetut tiedostot ovat hänen käytettävissään. Tällaisia tilanteita varten on suunniteltu kryptaus, eli tietojensalausohjelmia.

Tietojensalausohjelman avulla on mobiililaitteen data mahdollista salata siten, että ulkopuolinen taho ei pääse käsiksi dataan, vaikka saisikin laitteen haltuunsa. Datansalaukseen on tarjolla ulkopuolisia ohjelmia, mutta useimpiin nykyaikaisiin mobiililaitteiden käyttöjärjestelmiin on sisäänrakennettu tietojensalausohjelma, jolla datan salaaminen onnistuu. (Mobiiliasiantuntijat 2014.) Tietojensalausohjelman avulla voidaan salata mobiililaitteen omassa muistissa oleva data, sekä ulkoisella SD-kortilla oleva data.

Alla olevassa kuvassa näkyy tilanne, jossa tabletin oma muisti ollaan salaamassa. Tabletissa on Androidin käyttöjärjestelmä, ja käytettävä tietojensalausohjelma on Androidin oma ohjelma. Ohjelma pyytää käyttäjää asettamaan laitteen näytönlukitukseksi joko PIN-koodin tai salasanan ennen datan salaamista. Asetettua koodia tullaan kysymään käyttäjältä aina ennen mobiililaitteen avaamista, ja salattu data purkaantuu oikealla koodilla. (Helsinki www-sivut 2012)



Kuva 2. Androidin sisäänrakennettu tietojensalausohjelma (Helsinki www-sivut 2012)

Datan salauksen yhteydessä asetettu salasana kannattaa pitää mielessä, sillä salausohjelmat ovat yleensä ohjelmoitu ilman takaportteja. Tämä tarkoittaa sitä, että mikäli salasana unohtuu, pääsyä salattuun dataan ei enää ole. Tietojensalausohjelma tai mobiililaitteen käyttöjärjestelmä on toki mahdollista asentaa uudelleen, mutta tällöin katoaa myös kaikki salattu data. (Mobiiliasiantuntijat 2014.)

4.9 Turvalliset käyttöympäristöt

Etenkin yrityskäytössä nousee esiin ohjelmistoja, jotka tarjoavat käyttäjille turvallisemman ympäristön käyttää mobiililaitetta. Esimerkkinä tällaisesta ohjelmistosta voidaan mainita Samsung Knox. Knox on Androidille asennettava ohjelmisto ja se on suunniteltu erityisesti henkilöille, jotka käyttävät samaa mobiililaitetta työssä ja vapaa-ajalla. Knox mahdollistaa profiilien luomisen käyttöjärjestelmään, joten yrityksen sovellukset ja data saadaan eristettyä omalle suojatulle alueelle. Tämä mah-

dollistaa sen, että yrityksen tärkeä data on aina suojattuna oman profiilin takana, ja henkilökohtainen käyttö voidaan suorittaa siihen tarkoitetussa erillisessä profiilissa. Profiilien ansiosta henkilökohtainen käyttö pysyy yksityisenä, ja mobiililaitetta onkin tarpeen tullen mahdollista kierrättää työyhteisössä. (Samsung www-sivut 2014.)

Knox ohjelmiston datan suojaus toteutetaan kolmiosaisella strategialla. Normaalin Androidin käyttöjärjestelmän lataaja, eli boot loader on korvattu suojatummalla customizable secure bootilla. Ohjelmistoon on sisäänrakennettu Security Enhancement datan salausmenetelmä ja TrustZone teknologia. TrustZone jakaa laitteen prosessorin kahteen virtuaaliseen osaan ja suorittaa arkaluontoiset tehtävät suojatummassa prosessorissa ja muut tehtävät normaalin suojauksen omaavassa prosessorissa. (Samsung 2014.; Suvanto www-sivut 2012.)

5 TUTKIMUS

5.1 Tutkimusmenetelmät

5.1.1 Kvantitatiivinen tutkimus

Kvantitatiivinen eli määrällinen tutkimus perustuu lukumääriin ja prosenttiosuuksiin, ja siitä voidaan käyttää myös nimitystä tilastollinen tutkimus. Onnistunut ja luotettava määrällinen tutkimus edellyttää tarpeeksi laajaa aineistoa tutkittavasta aiheesta. Aineiston keruu tapahtuu yleensä tutkimuslomakkeen avulla. Lomake sisältää pääsääntöisesti valmiita vastausvaihtoehtoja, jotta prosentuaaliset osuudet vastauksista olisi helppo muodostaa. Kerättyä aineistoa käsitellään numeeristen arvojen kautta, ja näitä arvoja esitetään usein erilaisten kuvioiden sekä taulukoiden avulla. (Heikkilä 2008, 16.)

Syventyneemmässä määrällisessä tutkimuksessa ei ainoastaan esitetä jokaista kysymyksen vastausta taulukon avulla, vaan siinä selvitetään myös eri vastausten riippuvuuksia toisistaan. Kerättyjä tuloksia pyritään myös yleistämään koskemaan alkupe-

räistä otantaosuutta suurempaa joukkoa käyttäen tilastollista päättelyä. Määrällisellä tutkimuksella saavutetaan yleensä parhaiten olemassa oleva tilanne tutkitusta aiheesta. (Heikkilä 2008, 16.)

5.1.2 Kvalitatiivinen tutkimus

Kvalitatiivisella eli laadullisella tutkimuksella ymmärretään tutkimuskohteen päätösten ja käyttäytymisen syitä. Tutkimuksen kohderyhmän tarpeiden ja odotusten selvittämisellä saadaan tärkeää informaatiota, joiden avulla saadaan vastauksia myös olemassa olevan toiminnan kehittämiseen, ongelmien tutkimiseen ja vaihtoehtoisten ratkaisujen etsimiseen. (Heikkilä 2008, 16.)

Tutkittava kohderyhmä on yleensä harkinnanvaraisesti valittu pieni ryhmä, joilta kerätty aineisto analysoidaan tarkasti. Aineistoksi ei yleensä haluta tilastollisesti yleistettyjä vastauksia, ja määrällisestä tutkimuksesta poiketen, aineistot ovatkin yleensä tekstimuodossa. Aineiston kerääminen voi tapahtua määrällisen tutkimuksen tavoin lomakkeen avulla, mutta muita keinoja ovat myös esimerkiksi haastatteleminen, ryhmäkeskustelut ja valmiiden aineistojen kuten päiväkirjojen käyttö. (Heikkilä 2008, 16.)

5.2 Valittu menetelmä

Valitsin tutkimusmenetelmäkseni kvantitatiivisen eli määrällisen tutkimuksen. Tutkimuksella selvitetään mobiililaitteiden tietoturvan nykyistä tasoa. Tason kuvaamisen ja hahmottamisen pohjaksi on hyvä esittää tilastoja tutkitusta aiheesta. Tilastojen ja kuvaajien kautta kokonaisuuden hahmottaminen on helpompaa ja riippuvuuksien hahmottaminen helpottuu. Luotettavien tilastojen, sekä informatiivisten vastausten saaminen vaatii mielestäni laajaa otantaa. Laajan otannan saaminen onnistuu helpoiten tutkimuslomakkeen avulla. Kohderyhmäksi valikoitui Satakunnan ammattikorkeakoulun tiedepuisto A:n opiskelijat. Kohderyhmä koostuu pääasiassa 20-30 vuotiaista henkilöistä, joten tilastollista päättelyä käyttäen tuloksia on mahdollista soveltaa koskemaan suurempaa joukkoa.

5.3 Onnistunut tutkimus

Luotettavat vastaukset ovat avainedellytys onnistuneelle tutkimukselle. Vastausten avulla tutkimus tulee suorittaa täysin puolueettomasti, rehellisesti ja vastaajia kunnioittaen. (Heikkilä 2008, 29.) Seuraavaksi esitellään hyvän ja onnistuneen määrällisen tutkimuksen vaatimuksia.

5.3.1 Pätevyys ja luotettavuus

Validi eli pätevä tutkimus perustuu siihen, että tutkimus kohdistuu juuri siihen asiaan mitä on tarkoituskin tutkia. Tämä edellyttää sitä, että tutkija määrittää tarkat tavoitteet tutkimukselle, eikä näin lähde tutkimaan vääriä asioita. Karkeasti sanottuna pätevyys tarkoittaa tutkimuksessa systemaattisen virheen eli mittausvirheen poissaoloa. Systemaattinen virhe voi syntyä jos esimerkiksi tutkitaan suomalaisten alkoholikulutusta, mutta tutkimus mittaa vain kotimaasta ostettuja tuotteita, jättäen ulkomailta ostetut tuotteet pois laskuista. Systemaattisen virheen ollessa läsnä, tutkimustulos vääristyy aina, vaikka tutkimus toistettaisiin useita kertoja. (Heikkilä 2008, 29-30.)

Tutkittavat muuttujat, asiat ja käsitteet tulee määrittää tarkoin ennen tutkimusta, jotta saadut tulokset olisivat valideja. Tutkimuslomakkeen suunnitteluun kannattaa varata riittävästi aikaa, jotta tiedonkeruu olisi harkittua ja kerätty tieto halutun kaltaista. Kysyttävät kysymykset tulee muotoilla yksiselitteisiksi, että väärinymmärtämisen mahdollisuutta ei muodostuisi. Kyselyyn vastaavan joukon määrittely on myös tärkeää, jotta saadaan kerättyä edustava otos vastauksia ja mahdollistettua tilastollinen päättely. Kyselyn korkea vastausprosentti vähentää virheiden mahdollisuutta ja edesauttaa tutkimusta validimpaan suuntaan. Tutkimuksen pätevyyttä on vaikea tutkia jälkeenpäin, ellei näitä seikkoja ota huomioon. (Heikkilä 2008, 30.)

Reliabiliteettilla tarkoitetaan tutkimustulosten tarkkuutta ja luotettavuutta. Luotettavat tutkimustulokset eivät ole sattumanvaraisia, vaan mikäli tutkimus toteutetaan uudelleen, tulee saatujen tulosten olla samankaltaisia. Tutkimusta toistettaessa on kuitenkin huomioitava se, että saadut tulokset saattavat vaihdella eri ajanjaksojen ja yh-

teiskuntien välillä, tarkoittamatta sitä että tutkimus olisi epäluotettava. (Heikkilä 2008, 30.)

Tutkijan tulee olla tarkkana tuloksia käsitellessään. Virheitä voi tapahtua monessa eri tulosten analysointivaiheissa ja saatujen tulosten väärintulkitseminenkin on mahdollista. Tuloksia kohtaan kannattaa olla siis kriittinen, jotta mahdolliset virheet huomataan. Luotettavuuden kannalta ehdottoman tärkeää on se, että tutkija tulkitsee tulokset oikein ja tätä edesauttaa hallitun analysointimenetelmän käyttö. (Heikkilä 2008, 30.)

Tutkimukseen osallistuvien otantakoko vaikuttaa myös oleellisesti tutkimuksen luotettavuuteen. Suppea otanta jättää suuren mahdollisuuden vääristymiin, ja saadut tulokset ovat sattumanvaraisia. Vastaajia valittaessa on myös huomioitava se, että kohderyhmä ei ole vino. (Heikkilä 2008, 30-31.) Vinolla kohderyhmällä tarkoitetaan esimerkiksi tilannetta, jossa tutkitaan suomalaisten ravintolamieltymyksiä, mutta kysely toteutetaan alueella, jossa on vain yksi ravintola.

5.3.2 Puolueettomuus ja avoimuus

Objektiivisuus eli puolueettomuus nousee esiin valintoja tehdessä. Tutkimusta tehdessä tulee tutkijan tehdä valintoja liittyen tutkimusmenetelmään, kysymysten muotoiluun, analysointiin ja raportointiin. Valintoja tehdessä on kiinnitettävä huomiota, että tutkijan vakaumus, poliittinen suuntaus tai mielipiteet eivät aiheuta puolueellisuutta. Puolueellisuudella tarkoitetaan esimerkiksi kysymysten johdattelevaa asettelua, jolla yritetään saada tietynlaista vastausta. Kerättyjen tutkimustulosten tahallinen vääristely tekee tutkimuksesta täysin arvottoman ja koko tutkimuksen toteuttamisesta ajanhukkaa. Tutkimuksessa saadut tulokset eivät saa johtua tutkijasta vaan, vaikka tutkijaa vaihdettaisiin, tulisi tutkimuksen tulos olla sama. (Heikkilä 2008, 31.)

Tutkimusta suoritettaessa tulee tutkimukseen osallistuville kertoa avoimesti mitä tutkitaan ja mikä on tutkimuksen käyttötarkoitus. Tutkimustuloksia raportoidessa esitetään kaikki saadut tulokset, eikä vääristellä kokonaisuutta esittämällä ainoastaan

edullisia ja toivottuja tuloksia. Käytetyt tutkimusmenetelmät kerrotaan ja mahdolliset epätarkkuustekijät tuodaan myös julki. (Heikkilä 2008, 31-32.)

5.3.3 Hyödyllisyys ja käyttökelpoisuus

Tutkimuksen tulee tuoda esiin jotain uutta, jotta se olisi mahdollisimman hyödyllinen. Mikäli tutkitaan aihetta, josta on suoritettu jo useita tutkimuksia aiemmin, on vaarana, että oman tutkimuksen käyttö ja hyöty jäävät varsin vähäisiksi. Tutkimuksen aiheen ollessa ajankohtainen ja kiinnostava, on hyödyllisen tutkimuksen toteuttaminen huomattavasti helpompaa, kuin käsiteltäessä jotakin epäoleellista aihetta. Tutkimuksen kyselylomakkeen käyttötarkoitus kannattaa miettiä etukäteen tarkoin. Näin säästytään esittämästä täytekysymyksiä, joiden tuoma informaatio jää yleensä vähäiseksi. (Heikkilä 2008, 32.)

5.3.4 Tietosuoja

Tutkimuksen tuloksia käsiteltäessä ja raportoitaessa on kiinnitettävä huomiota siihen, että kenenkään yksityisyyttä ei loukata, eikä ammattisalaisuutta tuoda julki. Mikäli tutkimukseen vastataan luottamuksellisesti, tulee tutkimusraportin olla sellainen, että yksittäisen henkilön vastauksia ei pystytä tunnistamaan. Lähtökohta on, että tutkimuksen tuloksia käytettäessä noudatetaan aina tietosuojaa niin yksilön kuin yrityksenkin kohdalla. Periaatteena pidetään, että tutkimuksen tuloksia ei ikinä luovuteta tutkimuksen käyttäjille sellaisessa muodossa, jossa tunnistaminen olisi mahdollista. (Heikkilä 2008, 32.)

5.4 Tilastolliset määritelmät ja lyhenteet

Tutkimuksen tilastollisia riippuvuuksia tutkiessa ilmoitetaan riippuvuuden merkitsevyys- eli riskitaso p-arvolla (probability). P-arvo kertoo kuinka suurella todennäköisyydellä löydetty riippuvuus tai ero johtuu sattumasta eli oikeastaan se kertoo kuinka todennäköisesti tehty johtopäätös on virheellinen. Ennen tutkimustulosten analysointia tutkijan on päätettävä käytettävä merkitsevyystaso. Yleisesti käytössä ovat seu-

raavat rajat: p=0,05 (5 % todennäköisyys, että riippuvuus johtuu sattumasta), p=0,01 (1 %) ja p=0,001 (0,1 %). Paljolti käytetty raja p ≤ 0,05 on yleensä riittävä opinnäytetöissä. Riippuvuus tai ero testattavien kohteiden välillä on erittäin merkitsevä, jos p ≤ 0,001, merkitsevä jos p ≤ 0,01 ja melkein merkitsevä jos p ≤ 0,05. (Heikkilä 2008, 194-195.)

Tutkimuksessa käytetään myös frekvenssiarvoja ja prosentteja (%). Frekvenssiarvolla ilmaistaan kuinka monta kertaa jokin tietty havaintoarvo esiintyy. Esimerkiksi kysymys johon vastataan kyllä tai ei, kyllä-vastauksia esiintyy yhteensä 35 kappaletta, on 35 kyllä-vastauksen frekvenssi. Frekvenssiksi saadut arvot on mahdollista ilmoittaa prosentteina eli prosentuaalisena frekvenssijakaumana. (Edu www-sivut.) Prosentti (%) on suhteellinen yksikkö, joka tarkoittaa sadasosaa jostakin joka voidaan laskea. Prosenttia ei kuitenkaan pidä sekoittaa prosenttiyksikköön, jota käytetään vertailuun prosenttilukujen välillä. Prosentti voidaan ilmaista joko kirjoittamalla tai merkillä %, mutta prosenttiyksikkö on aina hyvä kirjoittaa selvyyden merkiksi. (Kotimaisten kielten keskus www-sivut 2006.)

5.5 Tavoitteet

Tutkimuksen aihe valikoitui, koska mobiililaitteiden kasvavan määrän ja käytön johdosta aihe on erittäin ajankohtainen. Laitteiden kasvavan määrän takia herää kysymys, pysyykö tietoturvallisuus kiihtyvän käytön mukana? Tähän halutaan saada selvyys tutkimuksella. Samanlaisia tutkimuksia ei myöskään löytynyt, joten koin tutkimuksen tekemisen hyödylliseksi.

Tutkimuksen päätavoitteena on selvittää kuinka tietoturvallisesti mobiililaitteita käytetään, ja samalla saada selvyys käyttäjien mobiililaitteiden tietoturvan nykyisestä tasosta. Nykyisen tason selvityksen helpottamiseksi kysymykset on jaettu eri kokonaisuuksiin. Kokonaisuuksia vertailemalla saadaan kokonaiskuva koko mobiililaitteiden tietoturvan tasosta.

Tutkimuksen kyselylomakkeen (Liite 1) jaotellut kokonaisuudet ovat tietoturvauhkien tietoisuus, salasanat, luotettavat lähteet, päivitykset sekä varautuminen tietotur-

vauhkiin. Tavoitteena on saada aikaan selkeät kuvaajat kunkin kokonaisuuden eri osa-alueiden kohdista, sekä tutkia myös riippuvuuksia eri asioiden ja kokonaisuuksien välillä. Tutkimuksessa pyritään myös selvittämään vaikuttaako sukupuoli, mobiililaitteiden määrä tai käytettävä käyttöjärjestelmä tietoturvallisuuteen.

Kyselylomakkeeseen on tarkoitus saada vähintään 50 vastausta, jotta tutkimustulosta voidaan pitää luotettavana. Tutkimuksen kohderyhmä on valittu siten, että tutkimukseen osallistuvat edustaisivat mahdollisimman tasaista, ja yleistä joukkoa. Tavoitteena on, että tutkimuksen tuloksia voidaan näin tilastollisen päättelyn avulla soveltaa koskemaan suurempaa joukkoa. Tutkimuksen tulosten peilaaminen tulee kasvattamaan tutkimuksen hyödyllisyyttä merkittävästi.

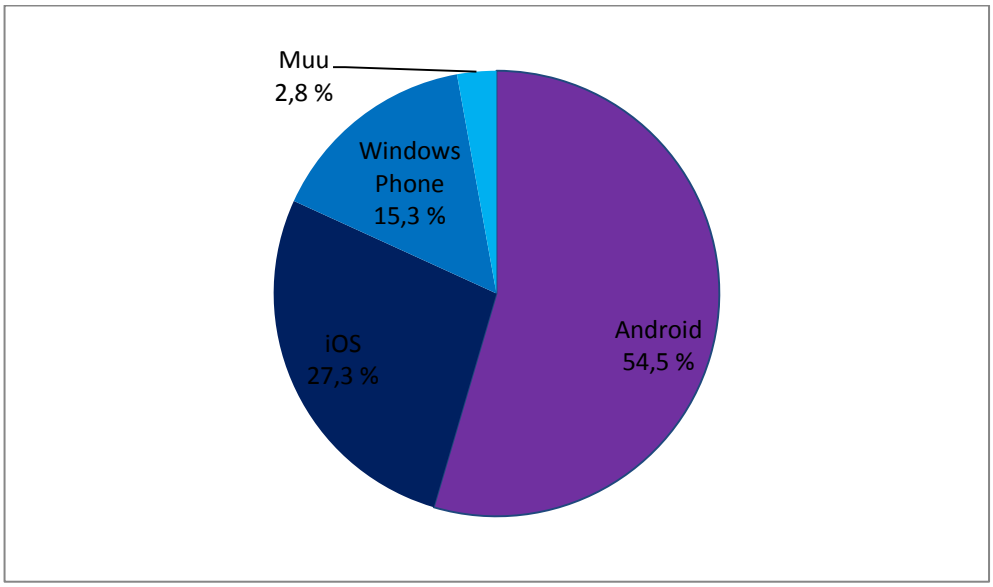
5.6 Toteutus

Oman tutkimuksen pätevyydestä ja luotettavuudesta on huolehdittu monin eri tavoin. Ennen tutkimuksen aloittamista asetettiin selkeät tavoitteet, mitä tutkimuksella on tarkoitus tutkia. Kyselylomakkeen suunnittelussa keskityttiin siihen, että kysymykset olisivat helposti ymmärrettäviä ja vastattavia sekä siihen, että vastaukset olisivat yksinkertaisia tilastoida. Kysely lähetettiin tarkoituksella suurelle joukolle, jotta palautuksia saataisiin riittävästi luotettavan otantakoon muodostumiselle. Kohderyhmän kokoa suunnitellessa otettiin huomioon myös katoprosentti, eli vastaamatta jättäneiden määrä.

Tutkimuksen tiedonhankinta toteutettiin kyselylomakkeen avulla. Kyselylomakkeena käytettiin Satakunnan ammattikorkeakoulun sähköistä e-lomaketta. E-lomakekysely lähetettiin sähköpostilla kohderyhmälle, joka koostuu Satakunnan ammattikorkeakoulun Tiedepuisto A:n opiskelijoista. Kohderyhmään kuului 974 opiskelijaa. Kysely pidettiin avoimena 8 päivää, ja vastauksia saatiin 176 kappaletta. Kerätty materiaali käsiteltiin SPSS-ohjelmistolla, joka on juuri tilastotieteellistä analyysiä varten suunniteltu ohjelmisto. SPSS-ohjelmiston avulla saatiin laskettua vastausten riippuvuudet (p-arvo), frekvenssijakaumat ja prosentuaaliset osuudet (ks. 5.4). Tutkimuksessa käytetty riippuvuuden merkitsevyysraja on 0,05. Tämä tarkoittaa sitä, että aina kun $p \leq 0{,}05$ todetaan asioiden välillä olevan riippuvuutta.

6 TUTKIMUKSEN TULOKSET JA ANALYSOINTI

Tutkimukseen osallistui 176 opiskelijaa, ja näin ollen kyselyn vastausprosentiksi muodostui 18. Puolet vastaajista ilmoitti koulutusohjelmakseen liiketalouden, 26,7 % matkailun, 17,6 % tietojenkäsittelyn ja 5,7 % vastaajista oli viestinnän opiskelijoita. Miesten osuus vastaajista oli 28,4 prosenttia, ja loput, eli 71,6 prosenttia vastaajista oli naisia. Tutkimuksessa selvisi, että vastaajat omistavat keskimäärin 1,53 mobiililaitetta henkilöä kohden. Yleisin käyttöjärjestelmä oli Android, jättäen taakseen Applen iOS:n sekä Windows Phonen. Kuten alla olevasta kuviosta käy ilmi, kolmen kärki erottui kyselyssä selvästi. Lisäksi muutamat vastaajat ilmoittivat käyttävänsä Sailfish-, Nucleus- sekä Symbian-käyttöjärjestelmiä.



Kuvio 6. Kohderyhmän käyttöjärjestelmät.

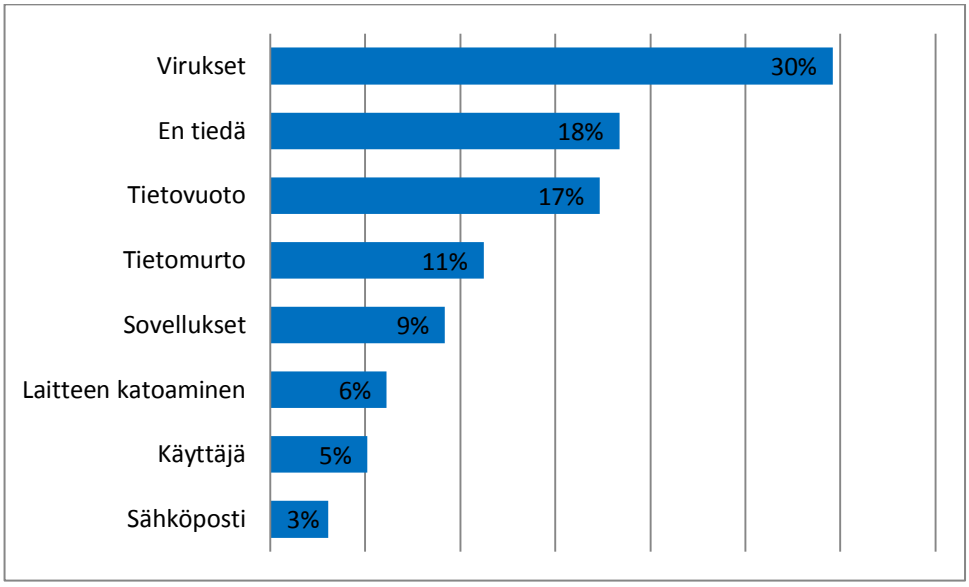
6.1 Tietoisuus

Kyselyn avulla selvitettiin, ovatko käyttäjät tietoisia siitä, että myös mobiililaitteisiin kohdistuu haittaohjelmia. Lisäksi avoimella kysymyksellä kysyttiin, mikä on käyttäjien mielestä yleisin mobiililaitteiden tietoturvauhka. Vastausten yhtäläisyyksiä tutkittaessa voidaan huomata selkeä riippuvuus uhkien tietoisuuden ja niihin varautumisen välillä.

85,2 % vastaajista tiedosti, että myös mobiililaite on altis haittaohjelmille. Jäljelle jäävät 14,8 % ajattelivat, että mobiililaitteeseen ei ole mahdollista saada haittaohjelmatartuntaa. Tietämättömyys haittaohjelmista vaikutti suoraan myös laitteen tietoturvalliseen käyttöön. Riippuvuus haittaohjelmien tietämättömyyden ja virustorjunnan käytön (p=0,001), sovellusten säännöllisen päivittämisen (p=0,017) ja tuntemattomien langattomien verkkojen käytön (p=0,012) välillä on selkeä. Kaikki edellä mainitut asiat voivat vaikuttaa haittaohjelman pääsyyn mobiililaitteelle. Koska mobiililaitteiden haittaohjelmien olemassaoloa ei tiedetä, ei myöskään ajatella että vanhentuneet sovellukset ja tuntemattomat langattomat verkot voivat olla kanavia, joita haittaohjelmat hyödyntävät.

Lähes kaikki (96 %) niistä vastaajista, jotka eivät tienneet mobiilihaittojen olemassaolosta, eivät myöskään käyttäneet virustorjuntaohjelmistoa laitteillaan. Tietämättömyys näkyi myös mobiililaitteen sovellusten säännöllisessä päivittämisessä. Päivittämisestä huolehti 58 % käyttäjistä, kun mobiilihaitat tiedostavan ryhmän vastaava prosenttiosuus oli 79. Tuntemattomia langattomia verkkoja käytti puolestaan 46 % tietämättömistä vastaajista, kun tietoisten osalta käyttöprosentti on 23.

Kysyttäessä käyttäjien mielestä yleisintä mobiililaitteiden tietoturvauhkaa, miltei joka kolmas käyttäjä mainitsi virukset. Alla olevasta kuviosta käy kuitenkin ilmi, että epätietoisuus tietoturvauhkia kohtaan nousi esiin, sillä toiseksi yleisin vastaus oli ”En tiedä”. Kysymys osoittautui muutenkin haastavaksi, sillä 76 vastaajaa jätti vastauksen kokonaan tyhjäksi. Käyttäjät olivat myös erityisen huolestuneita tietovuodoista, jolloin esimerkiksi kuvat ja salasanat päätyisivät vääriin käsiin. Tietovuodon syiksi mainittiin muun muassa epäluotettavat pilvipalvelut ja tietojen kalastelu. Tietomurto eli hakkerointi nousi esiin etenkin pankkisovellusten käytön yhteydessä. Vanhentuneet sovellukset mainittiin perusteluina niiden sisältämät tietoturva-aukot. Myös kolmansien osapuolten sovelluksia pidettiin epäluotettavina. Yllättävän pieni määrä vastaajista (6 %) mainitsi laitteen katoamisen/varastamisen yleisimmäksi tietoturvauhaksi. Laitteen katoaminen on kuitenkin erittäin merkittävä tietoturvauhka, koska tietoturvaloukkausten riski on tällöin suuri. Käyttäjä itse on kekseliäs vastaus, sillä tietoturvauhat eivät synny itsestään, vaan usein käyttäjän omat toiminnot aiheuttavat ne. Osa vastaajista mainitsi sähköpostin ja sähköpostin liitteet yleisimmäksi uhaksi.

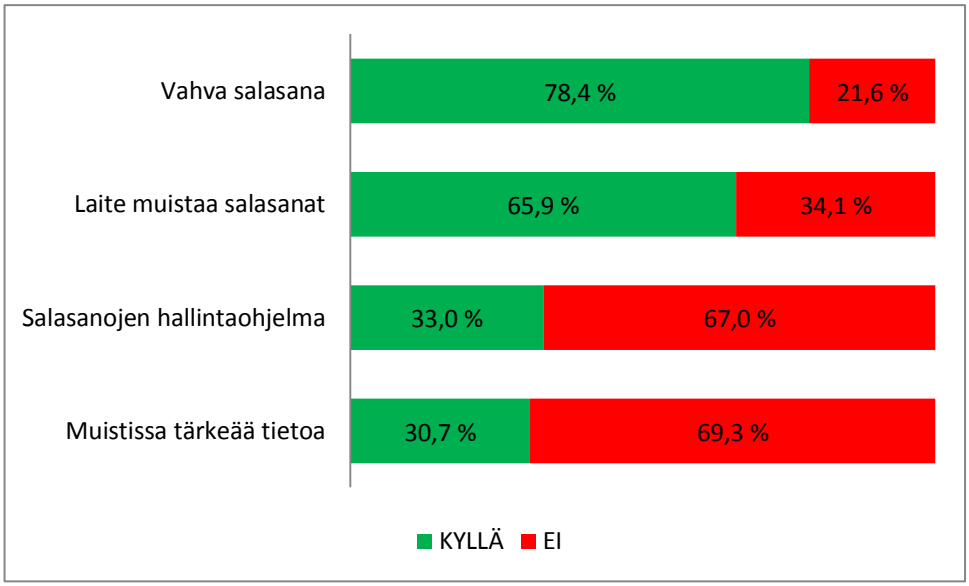


Kuvio 7. Käyttäjien mainitsemat yleisimmät tietoturvauhat.

Mobiililaitteen katoaminen on kuitenkin yleisempi uhka, kuin yllä (kuvio 7) käy ilmi. Tutkimukseen vastanneista 13,6 % oli nimittäin kadottanut mobiililaitteensa. Laitteen katoaminen on tapahtunut yleensä kahdella tapaa, joko hukkaamalla laitteen itse, tai laite on tullut varastetuksi. Mobiililaitteensa hukanneista henkilöistä vain 20,8 % käyttää varkaudenhallintajärjestelmää.

6.2 Salasanat

Kyselyssä tiedusteltiin vastaajien salasanojen käyttöä. Valtaosa vastaajista ilmoitti käyttävänsä vahvoja salasanoja. Yli puolet käyttäjistä kertoi myös tallentaneensa salasanansa mobiililaitteen muistiin niin, ettei sitä tarvitsisi kirjoittaa kirjautumisen yhteydessä lainkaan. Kolmasosa vastaajista ilmoitti käyttävänsä salasanojen hallintaohjelmaa mobiililaitteilla. Vajaa kolmannes vastaajista ilmoitti tallentaneensa mobiililaitteen muistiin tärkeää tietoa, kuten osoitteita ja salasanoja, jotta ne eivät unohtuisi. Vastausten prosentuaaliset osuudet esitetään alla olevassa kuviossa.



Kuvio 8. Salasanojen käyttö.

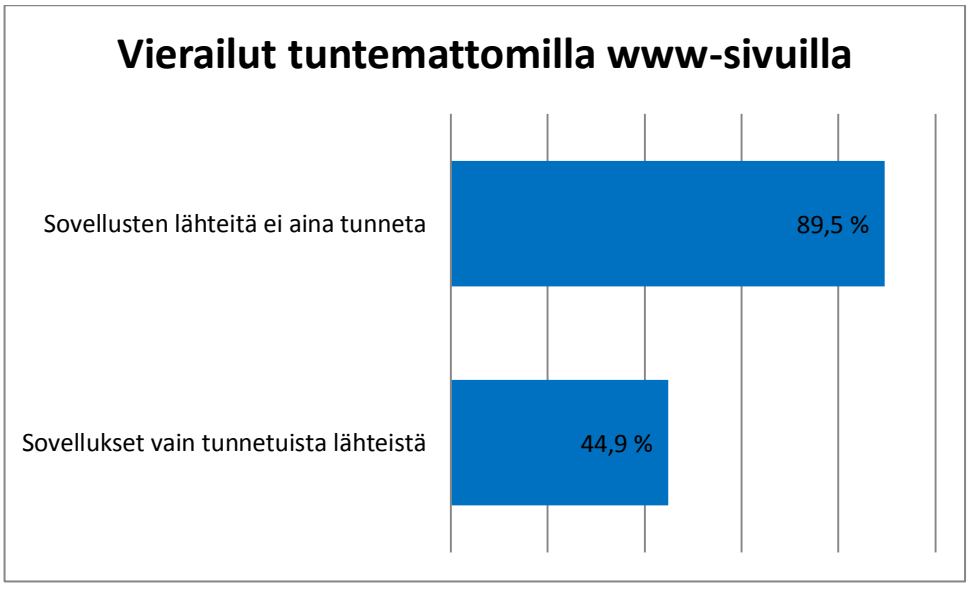
Miehet käyttävät vahvoja salasanoja naisia useammin (p=0,019). Tutkimustuloksista käy ilmi että 90 % miehistä on panostanut salasanojensa laatuun, kun samalla 74 % naisista käyttää vahvoja salasanoja. Vahvan salasanan avulla pystytään ehkäisemään tietomurtojen määrää, jonka käyttäjät nimesivät (kuvio 7) yhdeksi yleisimmäksi tietoturvauhaksi.

Salasanojen hallintaohjelman käytön yhteydessä voidaan todeta, varsin looginen, yhteys salasanojen automaattiseen muistamiseen (p=0,022), sekä tärkeän tiedon tallentamiseen laitteelle (p=0,00). Salasanojen automaattinen muistaminen mobiililaitteelle kasvoi 17,4 prosenttiyksikköä, kun henkilöllä oli käytössä salasanojen hallintaohjelma. Samanlaisessa vertailussa tärkeän tiedon tallentaminen kasvoi peräti 26,2 prosenttiyksikköä.

Salasanojen hallintaohjelman kautta salasanojen muistaminen tapahtuu tietoturvallisesti, sillä käyttäjän täytyy kuitenkin syöttää ohjelman pääsalasana, ennen muiden salasanojen automaattista käyttöä. On kuitenkin huolestuttavaa huomata, että 60 % henkilöistä, jotka eivät käytä salasanojen hallintaohjelmaa, tallentavat kuitenkin salasanansa laitteen muistettavaksi. Tietoturvallisuuden kannalta tämä lisää tietoturvaloukkausten riskiä huomattavasti, mikäli laite joutuu vääriin käsiin.

6.3 Luotettavat lähteet

78,4 prosenttia vastaajista lataa sovellukset ja tiedostot mobiililaitteelleen käyttäen ainoastaan tunnettuja ja luotettavia lähteitä. Mobiililaitteella tapahtuvan internetselailun kanssa ei olla yhtä huolellisia, sillä vain vajaa puolet (45,5 %) käyttäjistä vierailee ainoastaan tunnetuilla www-sivustoilla. Luotettavien sovellus- ja tiedostolähteiden käyttö heijastuu suoraan mobiililaitteella tapahtuvaan internet-selailuun (p=0,00). Mikäli käyttäjä lataa tiedostoja ja sovelluksia tuntemattomista lähteistä, on myös hyvin todennäköistä, että luotettavuutta ei selvitetä www-sivustojenkaan suhteen. Alla olevassa kuviossa on esitetty prosentuaaliset arvot vierailuista tuntemattomiin www-sivustoihin. Kuviossa ylempi palkki kuvaa ryhmää, jonka käyttäjät eivät tarkista sovellusten lähdettä, kun taas alempi palkki kuvaa joukkoa, jonka käyttäjät lataavat sovellukset ainoastaan tunnetuista lähteistä. Kuviosta käy ilmi, että tuntemattomia sovelluksia lataavien ryhmä (89,5 %) vierailee huomattavasti useammin tuntemattomilla www-sivuilla, kun vertailukohteena oleva toinen ryhmä (44,9 %).



Kuvio 9. Vierailut tuntemattomilla www-sivustoilla.

Ennen sovelluksen asennusta, sovelluksen käyttöönsä vaatimat valtuudet tarkistaa 57,4 % käyttäjistä. Miehet kiinnittävät naisia enemmän huomiota sovellusten vaatimiin valtuuksiin (p=0,033). Naisista hieman yli puolet lukevat sovellusten valtuusvaatimukset, kun miehien osalta osuus on 70 prosenttia.

Tuntemattomien langattomien verkkojen käyttö ei ole yleistä mobiililaitteilla. Tutkimuksen perusteella vain 26,1 prosenttia vastaajista ilmoitti käyttävänsä tuntemattomia verkkoja. Tietoturvallisuuden näkökulmasta voidaan löytää yhteys tuntemattomien verkkojen ja tuntemattomien www-sivujen käytön välillä (p=0,017). Mikäli käyttäjä käyttää mobiililaitteella tuntemattomia langattomia verkkoja, vierailee hän myös 69,5 prosentin todennäköisyydellä tuntemattomilla www-sivuilla. Tästä voidaan todeta, että mikäli käyttäjä ei koe luotettavien lähteiden käyttöä tärkeäksi esimerkiksi sovellusten suhteen, heijastuu se myös muiden lähteiden käyttöön.

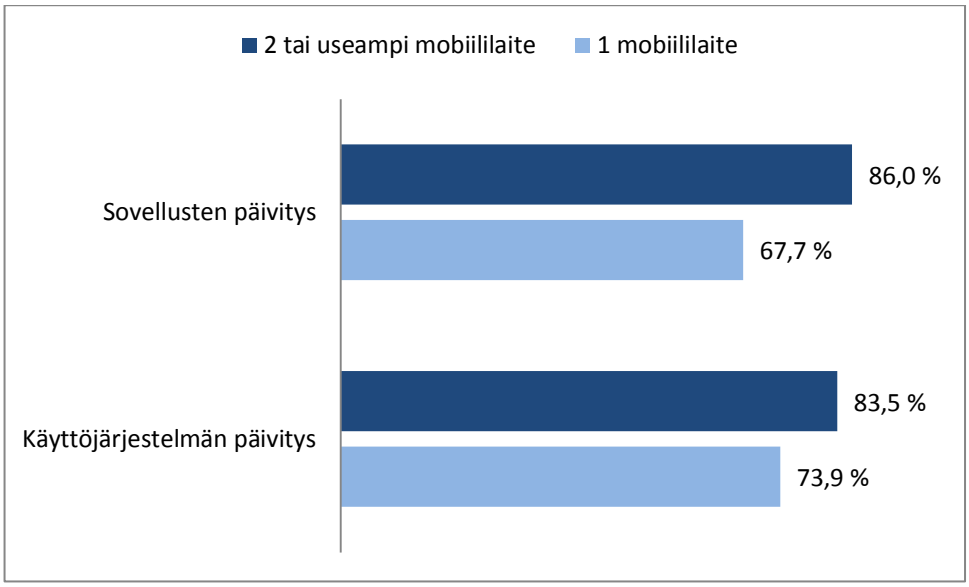
Pilvipalveluja mobiililaitteella käytti 46,6 % vastaajista. Pilven käyttö näkyi erityisesti varmuuskopioinnin yhteydessä (p=0,00), mikä kertoo pilvipalvelun olevan varsin suosittu varmuuskopioinnin kohde. Käyttäjistä, jotka varmuuskopioivat tiedostonsa, 63 % käytti pilvipalveluja kun henkilöistä, jotka eivät teetä varmuuskopioita tärkeistä tiedostoista, vain 32,6 % käytti pilvipalveluja.

6.4 Päivitykset

Sekä mobiililaitteen käyttöjärjestelmän että sovellusten päivittämisestä huolehditaan melko hyvin. Tulosten perusteella 78,4 prosenttia mobiililaitteiden käyttäjistä päivittää käyttöjärjestelmänsä aina uusimpaan versioon, kun päivitys on saatavilla. Säännöllinen sovellusten päivittäminen ei ole aivan yhtä yleistä, mutta siitäkin huolehtii 76,1 prosenttia vastaajista. Tutkimuksen perusteella voidaan todeta, että edellä mainitut päivitykset kulkevat käsi kädessä (p=0,00). Mikäli käyttäjä huolehtii käyttöjärjestelmän päivityksestä, päivittää hän myös sovellukset ja päinvastoin.

Käyttöjärjestelmän päivittämisessä ei näy eroja sukupuolten välillä, mutta sovellusten päivittämisessä eroja löytyy (p=0,020). Miehet nimittäin päivittävät mobiililaitteidensa sovellukset 88 % todennäköisyydellä, kun samalla 71,4 % naisista tekee saman. Mobiililaitteiden määrä vaikuttaa myös sovellusten päivittämisen aktiivisuuteen. Vaikutus esitetään alla olevassa kuviossa. Kuviossa vertaillaan päivitysaktiivisuutta käyttäjän omistaessa yhden mobiililaitteen ja kaksi tai useamman mobiililaitteen. Vertailukohteeksi on otettu mobiililaitteiden määrän vaikutus käyttöjärjestelmän päivittämiseen. Mobiililaitteiden kasvava määrä näyttää lisäävän kummankin

päivitystoimen prosentuaalista osuutta. Käyttöjärjestelmän kohdalla kasvu on kuitenkin vain noin 10 prosenttiyksikön luokkaa, joten riippuvuutta kasvun ja laitteiden määrän välillä ei voida osoittaa (p=0,221). Sovellusten kohdalla kasvu on jo miltei 20 prosenttiyksikköä, joten riippuvuus asioiden välillä voidaan osoittaa (p=0,046).



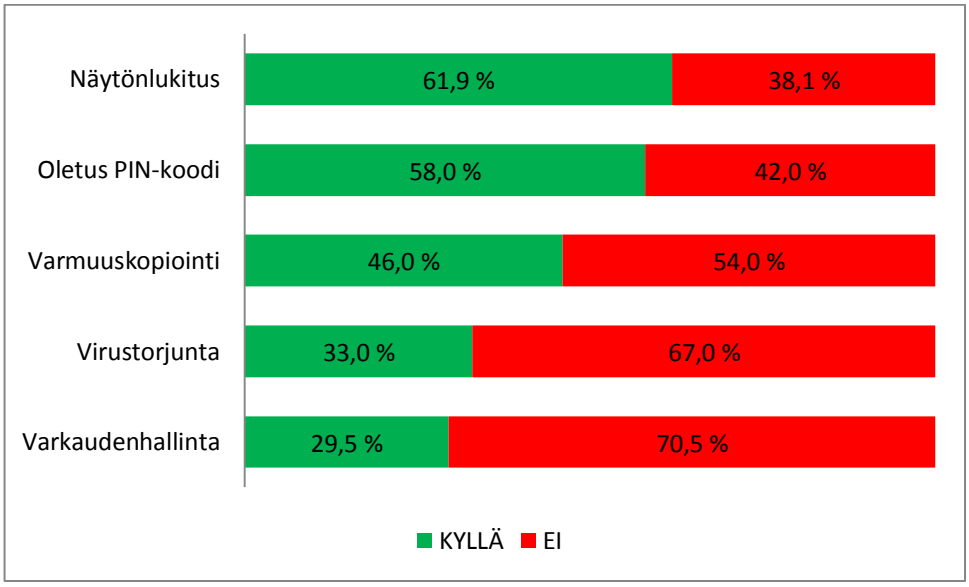
Kuvio 10. Mobiililaitteiden määrän vaikutus päivitysaktiivisuuteen.

6.5 Varautuminen

Teoriaosuudessa kerrottiin mobiililaitteiden sisältävän yhä useammin arkaluontoista ja henkilökohtaista dataa tai vähintään pääsyn tällaiseen dataan. Tätä teoriaa tukee se, että tutkimukseen osallistuneista henkilöistä 61,4 % käytti verkkopankkisovelluksia mobiililaitteellaan. Verkkopankkisovelluksen kautta saatavaa dataa voi pitää hyvin henkilökohtaisena, joten varautuneisuus tietoturvauhkia kohtaan tulee ottaa huomioon myös mobiililaitteilla.

Alla olevassa kuviossa esitetään tietoturvan kannalta keskeisten toimien käyttöä. Näytönlukituksen, esimerkiksi kuviolukituksen, käyttö on yleisin tapa estää ulkopuolisen pääsy mobiililaitteelle. Oletus PIN-koodin (0000 tai 1234) on vaihtanut yli puolet kohderyhmän mobiililaitteen käyttäjistä. Varmuuskopioinnin osalta määrä putoaa jo alle puoleen, ja virustorjuntaa käyttää enää kolmasosa vastaajista. Varkaudenhal-

lintajärjestelmän käyttö on kaikista harvinaisinta, määrän tipahtaessa alle kolmannekseen käyttäjistä.



Kuvio 11. Tietoturvallisuudesta huolehtiminen.

Tutkimuksen perusteella voidaan todeta, että tietoturvallisuudesta huolehtivat henkilöt käyttävät yleensä useampaa kuin yhtä yllä (kuvio 11.) mainittua keinoa. Esimerkiksi näytönlukituksen käytöllä on yhteys varkaudenhallinnan ($p=0,008$) ja oletus PIN-koodin vaihdon kanssa ($p=0,032$). Mikäli mobiililaitteessa on käytössä varkaudenhallintajärjestelmä, kasvattaa se näytönlukituskuvion todennäköistä käyttöastetta 21,4 prosenttiyksikköä. Vastaavasti oletus PIN-koodin vaihtaminen kasvattaa näytönlukituksen käytön todennäköisyyttä 15,9 prosenttiyksikköä.

Virustorjuntaohjelmiston käyttö on painottunut vahvasti Android käyttöjärjestelmälle ($p=0,00$), mikä on loogista, sillä valtaosa mobiiliviruksista on tehty juuri Androidille. Androidin käyttäjistä 50 % käyttää virustorjuntaa, kun Windows Phonen käyttäjistä 17,4 %, ja iOS:n käyttäjistä vain 10,4 % tekee samoin.

Suosituin varmuuskopiointimenetelmä on pilvipalvelujen käyttö. Suurin osa vastaajista sanoo siirtävänsä varmuuskopioitavat tiedostot itse pilveen, vain harvat suorittivat varmuuskopioinnin ajastettuna ja automaattisesti. Tietokoneen kovalevy, ulkoiset kovalevyt ja muistitikut mainittiin myös pilvipalvelun ohella varmuuskopioiden si-

jainniksi. Tulosten perusteella mobiililaitteella olevat kuvat ovat yleisin varmuuskopioinnin kohde.

6.6 Vastaajien kokemuksia

Kyselylomakkeen lopussa esitettiin kaksi avointa kysymystä liittyen tietoturvallisuuteen. Avointen kysymysten avulla saadaan hyviä vastauksia käyttäjien omakohtaisista kokemuksista tietoturvallisuudesta. Alla esitetään muutamia suoria lainauksia, jotka saatiin kyselyn vastauksiksi.

Oletko kokenut tilanteita, joissa mobiililaitteesi tietoturvallisuus on ollut uhattuna, millaisia?

- ”En ole. Siksi varmaan ajattelen naiivisti ettei puhelimeeni (mobiililaitteeseeni) voi tulla viruksia tms haittaohjelmia.”
- ”Tuntuu, että se on uhattuna jatkuvasti: lähes kaikki sovellukset tuntuvat tarvitsevan luvan päästä käsiksi kaikkiin puhelimen käyttäjätietoihin, tiedostoihin yms.”
- ”Kun hukkasin puhelimeni.”
- ”En, ainoastaan tämä verkkopankkiasia mietityttää. Käyn silti puhelimellani verkkopankissa!”
- ”Asentanut appseja jotka ovat sisältäneet haitallista sisältöä.”

Pyritkö käyttämään mobiililaitettasi tietoturvallisesti, miten?

- ”En mene epämääräisille sivustoille ja lataan kaikki sovellukse Google Play kaupasta tunnetuilta kehittäjiltä.”
- ”Jos lataan uuden sovelluksen, viruksentorjuntaohjlema käy sen läpi, jos ohjelma sanoo että sovellus ei ole luotettava en lataa sitä tai poistan sen.”
- ”Kyllä. En käytä tuntemattomia langattomia verkkoja. En käytä verkkopankkia. Luen mitä sovellukset vaatii käyttöönsä. Jos joku epäilyttää niin en käytä sitä.”
- ”Kyllä. Pyrin käyttämään laitteen suojausta kuten näytön lukituskuvaa, keksimään mielenkiintoisia salasanoja ja nyt seuraavaksi muutan PIN-koodini oletuksesta pois (vihdoin, hups)”

- ”Pyrin päivittämällä ohjelmat ajantasalle ja manuaalisesti estän osan ohjelmien käyttämät oikeudet custom ROM:illa”
- ”Päivittämällä ohjelmiston ja sovellukset heti, f-securen mobiiliversio ja freedomo on myös käytössä. Salasanojen hallintaohjelma on käytössä.”

7 YHTEENVETO

Kun ajatellaan koko opinnäytetyötä oppimisprosessina, voidaan sanoa että on onnistuttu. Teoriaosuuden kirjoittaminen on havainnollistanut hyvin, kuinka monet eri asiat voivat vaikuttaa mobiililaitteiden tietoturvaan. Kyselylomakkeen suunnitteleminen, laatiminen ja kyselyn toteuttaminen edesauttavat varmasti tulevaisuudessa mahdollisten vastaavien tehtävien suorittamista. Tulosten analysointi ja kokemus SPSS ohjelmiston käytöstä on varmasti hyödyksi tulevaisuudessa.

Kyselomakkeesta saatiin selkeä, eikä vastauksista ilmennyt kysymysten väärinymmärryksiä. Kysymykset oli suunniteltu siten, että niillä saataisiin vastauksia eri tietoturvaan liittyviin alueisiin. Vastaukset olivat odotetunlaisia ja jokaisen kysymyksen vastaukset toivat jotain lisäarvoa tutkimukseen, eikä niin sanottuja täytekysymyksiä ollut mukana. Vastauksia analysoidessani huomasin, että kyselyyn olisi voinut vielä lisätä tarkentavia kysymyksiä esimerkiksi haittaohjelmien leviämiskanavista ja omakohtaisista hyvistä/huonoista kokemuksista luotettavien lähteiden käytöstä. Tämä olisi kuitenkin lisännyt työn laajuutta, sillä päämääränä oli selvittää kuinka hyvin uhilta suojaudutaan.

Tutkimus onnistui tavoitteisiin nähden hyvin. Tuloksista voidaan havaita yksittäisten tietoturvallisten/tietoturvattomien toimien käyttöaste. Toimet on jaoteltu kokonaisuuksiin, joten kokonaisuuksia tarkastelemalla saadaan kokonaiskuva, jossa selviää mistä osa-alueesta huolehditaan parhaiten ja missä olisi parantamisen varaa. Kokonaisuuksista päivitykset oli parhaiten huolehdittu osa-alue. Henkilöiden omistaessa useamman kuin yhden mobiililaitteen, kasvaa samalla valveutuneisuus päivityksiä kohtaan. Mielenkiintoista oli huomata, että teoria-osassa arvioitiin mobiililaitteita

olevan vuonna 2016 1,4 laitetta käyttäjää kohden. Tämän tutkimuksen kohderyhmä omisti jo nyt 1,53 mobiililaitetta/henkilö. Mobiililaitteiden suuri määrä selittyy varmasti sillä, että kohderyhmä koostui lähinnä 20-30 vuotiaista henkilöistä, joille mobiililaitteet ovat jo osa arkea. Tutkimustuloksissa erityisen yllättävää oli huomata, että enemmän kuin joka kymmenes käyttäjä oli hukannut mobiililaitteensa. Mobiililaitteen hukkuminen voi johtaa helposti tietovuotoihin, mikäli turvatoimet on laiminlyöty. Varautuneisuus oli kokonaisuutena prosentuaalisesti heikoin. Tilastoista täytyy kuitenkin sanoa, että esimerkiksi virustorjunnan käyttöprosentti olisi ollut huomattavasti korkeampi jos tutkimuksessa olisi ollut mukana vain Android laitteet. Tutkimuksen perusteella voidaan myös päätellä, että varkaudenhallinnan ja salasanojen hallintaohjelmien käytön varsin pienet prosenttiosuudet selittyvät, ainakin osittain, sillä että normaalit käyttäjät eivät tiedä kyseisistä ohjelmista.

Tutkimus toteutettiin melko tiiviillä aikataululla. Vastausten käsittelyyn kului aikaa noin kaksi viikkoa. Koen kuitenkin, että tiivis aikataulu ei heikentänyt tutkimustulosten laatua, vaan tutkimukseen vaikutti positiivisesti se, että siihen piti paneutua intensiivisesti. Laajemmalla aikataululla toteutettu tutkimus olisi kuitenkin varmasti mahdollistanut asioiden pohtimisen vielä laajemmalta kantilta. Kyselylomakkeeseen saadut 176 vastausta yllättivät erittäin positiivisesti, koska tavoite oli saada kasaan vähintään 50 vastausta. Vastausten laaja määrä auttoi tutkimusta luotettavampaan suuntaan.

En löytänyt aiheesta aiempia tutkimuksia, joten katsoin että erityisesti kuluttajanäkökulmaiselle tutkimukselle olisi kysyntää. Tuloksista hyötyy oikeastaan jokainen yksityinen mobiililaitteiden käyttäjä, mutta tutkimusta voi hyödyntää esimerkiksi isompien ryhmien, vaikkapa koulujen tai yritysten yhteisen mobiililaitteiden tietoturvastrategian suunnittelussa. Avointen kysymysten vastauksista kävi ilmi, että osa vastaajista ryhtyi suojautumaan tietoturvauhilta laajemmin, koska kyselyyn vastaaminen laittoi vastaajat ajattelemaan tietoturvallisuutta laajempana käsitteenä. Toivon että moni vastaaja koki samoin. Syventävälle jatkotutkimukselle olisi käyttöä, koska tässä tutkimuksessa keskityttiin yleisellä tasolla eri osa-alueisiin. Syventävä tutkimus voisi keskittyä yhteen osa-alueeseen, ja selvittää esimerkiksi varkaudenhallintajärjestelmän käytön perusteluja, hyötyjä ja kokemuksia tarkemmin.

LÄHTEET

Ahonen, T. 2013. www-sivut. Viitattu 24.2.2014.
http://blog.3g4g.co.uk/2013/05/around-world-with-mobile-global.html

Dazeinfon www-sivut. Viitattu 21.2.2014.
http://www.dazeinfo.com/2013/03/08/google-android-devices-accounts-malware

Digitoday www-sivut 2014. Viitattu 29.10.2014.
http://www.digitoday.fi/tietoturva/2014/01/24/kytketko-android-puhelimesi-tietokoneeseen-ole-tarkkana/20141219/66

Digitoday www-sivut. Viitattu 24.2.2014.
http://www.digitoday.fi/tietoturva/2012/05/22/apple-ei-anna-kehittaa-virustorjuntaa-iphoneen/201229894/66

Edu www-sivut. Viitattu 19.11.2014.
http://www03.edu.fi/oppimateriaalit/tilastomatikka/sanasto.html#Frekvenssi

F – Secure www-sivut. Viitattu 20.2.2014. http://www.f-secure.com/fi/web/home_fi/mobile-security#features

F – Secure www-sivut. Viitattu 22.2.2014. http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf

Fried, I. 2014. www-sivut. Viitattu 30.10.2014.
http://recode.net/2014/02/12/business-use-of-mobile-apps-continues-to-rise-while-iphone-gains-ground-in-q4/

F-secure www-sivut. Viitattu 28.10.2014. https://www.f-secure.com/fi_FI/web/home_fi/key

Haltia, E. 2013. www-sivut. Viitattu 21.2.2014.
http://mobiili.fi/2013/04/15/haittaohjelmien-maara-mobiililaitteissa-lisaantynyt-163-vuodessa-vaittaa-tietoturvayhtio/

Heikkilä, T. 2008. Tilastollinen tutkimus. Helsinki: Edita.

Hel www-sivut 2014. Viitattu 30.10.2014. http://blogs.hel.fi/it-opastajat/2014/01/7-asiaa-jota-voi-tehd%C3%A4-tabletilla-ja-kolme-mit%C3%A4-ei-voi.html

Helsingin Sanomat www-sivut 2012. Viitattu 25.2.2014.
http://www.hs.fi/paakirjoitukset/a1348973187274

Helsingin tietotekniikkapalvelut www-sivut. Viitattu 19.2.2014.
http://www.httpoy.fi/main.php?sivu_id=28

Helsinki www-sivut 2012. Viitattu 27.10.2014
http://www.helsinki.fi/helpdesk/ohjeet/mobiililaitteet/android/android_salaus.html

ijailbreak www-sivut 2014. Viitattu 24.2.2014.
http://www.ijailbreak.com/news/ijailbreak-top-10-news/

Kotimaisten kielten keskus www-sivut 2006. Viitattu 19.11.2014.
http://www.kotus.fi/index.phtml?s=1274

Kotimikro www-sivut. 2013. Viitattu 16.2.2014. http://kotimikro.fi/tietoturva/onko-mobiililaitteesi-suojattu

Laakso, J. 2014. www-sivut. Viitattu 30.10.2014. http://mobiili.fi/2014/08/13/good-technology-apple-jatkaa-yritysmaailman-mobiililaitteiden-valtiaana-android-kirinyt-eroa-umpeen/

Luotola, J. 2012. www-sivut. Viitattu 24.2.2014.
http://www.tekniikkatalous.fi/ict/nettia+kayttavien+mobiililaitteiden+maara+ylittaa+tana+vuonna+maapallon+vakiluvun/a778229

Malenkovich, S. 2013. www-sivut. Viitattu 29.10.2014.
http://blog.kaspersky.com/charging-your-smartphone/

Mobiiliasiantuntijat www-sivut. 2014. Viitattu 29.10.2014.
http://www.mobiiliasiantuntijat.fi/mobiilitietoturvavinkit.html

Mobiiliopas www-sivut. 2011. Viitattu 15.2.2014.
https://sites.google.com/site/mobiililillaluonnollisesti/kaesitteet

Mozilla www-sivut. Viitattu 19.2.2014. https://support.mozilla.org/fi/kb/paranna-tietoturvaasi-vahvoilla-salasanoilla

Norton www-sivut 2013. Viitattu 29.10.2014.
https://support.norton.com/sp/fi/fi/home/current/solutions/v64690996_EndUserProfile_fi_fi

Norton www-sivut. 2013. Viitattu 18.2.2014. http://now-static.norton.com/now/en/pu/images/Promotions/2013/PDFs/NCR%20-%20%20Mobile%20-%20Europe%20FINAL%20FINAL.pdf

NQ Mobile www-sivut. 2012. Viitattu 16.2.2014.
http://en.nq.com/2012_NQ_Mobile_Security_Report.pdf

Samsung www-sivut 2014. Viitattu.6.11.2014.
http://www.samsung.com/fi/business/solutions-services/mobile-solutions/security/knox

Securelist www-sivut 2013. Viitattu 24.2.2014.
https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013#02

Strom, D. 2013. www-sivut. Viitattu 24.2.2014. http://mozy.com/blog/small-business-tips/how-to-make-money-with-malware/

Suvanto, V. 2012. www-sivut. Viitattu 23.11.2014. http://muropaketti.com/armn-tietoturvateknologia-integroidaan-amdn-apu-piireihin

Symantec www-sivut 2014. Viitattu 30.10.2014. http://www.symantec.com/fi/fi/about/news/release/article.jsp?prid=20120222_01

Symantec www-sivut. Viitattu 29.10.2014. http://www.symantec.com/region/fi/resources/antivirus.html

Taipale, K. 2013. www-sivut. Viitattu 28.10.2014. http://www.mbnet.fi/artikkelit/nain_saat_turvalliset_salasanat

Tieto www-sivut 2014. Viitattu 31.10.2014. http://www.tieto.fi/palvelut/infrastruktuuriratkaisut/sahkoinen-tyopiste/mobiililaitteiden-hallinta

Tietoturvapaiva www-sivut. Viitattu 22.2.2014. http://www.tietoturvapaiva.fi/uploads/Tietoturva%202012/fsecure.pdf

Tivi www-sivut 2013. Viitattu 29.10.2014. http://www.tivi.fi/kaikki_uutiset/huijarille+taysi+hallinta+puhelimeen++qrkoodien+skannauksesta+varoitetaan/a922984

tuaw www-sivut 2013. Viitattu 24.2.2014. http://www.tuaw.com/2013/08/26/u-s-government-finds-0-7-of-all-mobile-malware-affects-ios-wh/

Vaalisto, H. 2012. www-sivut. Viitattu 24.2.2014. http://www.digitoday.fi/tietoturva/2012/11/19/hypponen-windows-phone-turvallisempi-kuin-android/201242281/66

Webopas www-sivut. Viitattu 21.2.2014. http://www.webopas.net/mobiilivirus.html

Viestintävirasto www-sivut 2014. Viitattu 19.11.2014. https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/09/ttn201409241655.html

Viestintävirasto www-sivut 2014. Viitattu 19.11.2014. https://www.viestintavirasto.fi/tietoturva/haavoittuvuudet/2014/haavoittuvuus-2014-105.html

Viestintävirasto www-sivut 2014. Viitattu 30.10.2014. https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2014/ohjeitaalypuhelintenkayttoonjatietojensuojaamiseen.html

Wordpress www-sivut 2012. Viitattu 24.2.2014. http://mrwpf.wordpress.com/2012/04/27/windows-phone-haitaohjelmat-virustorjunta-ja-palomuuri/

Mobiililaitteen tietoturva

Olen tietojenkäsittelyn opiskelija, ja teen opinnäytetyötä aiheesta mobiililaitteiden tietoturva. Tähän kyselyyn vastataan täysin nimettömästi. Kyselyn vastausten perusteella tehdään tutkimus, jolla selvitetään käyttäjien tietoisuutta, sekä varautuneisuutta mobiililaitteisiin kohdistuviin uhkiin. Tutkimus on osa opinnäytetyötäni.

Terveisin,

Tomi Koivisto

Perustiedot

Sukupuoli
- Mies
- Nainen

Koulutusohjelma
- Liiketalous
- Matkailu
- Tietojenkäsittely
- Viestintä

Mobiililaitteista käytetään määritelmää kädessä kulkevat laitteet.

Tässä tutkimusessa mobiililaitteiksi laskentaan älypuhelimet, sekä tabletit.

Kuinka monta mobiililaitetta omistat?

--Valitse tästä--

Mikäli omistat useamman kuin yhden mobiililaitteen, vastaa kyselyyn eniten käyttämäsi laitteen tietoihin perustuen.

Mobiililaitteen käyttöjärjestelmä?
- Android
- iOS
- Windows Phone
- Blackberry OS
- Symbian
- Muu, mikä?

Tietoisuus

Onko mobiililaitteille mielestäsi olemassa haittaohjelmia?
- Kyllä
- Ei

Mikä on mielestäsi yleisin mobiililaitteisiin kohdistuva tietoturvauhka?

Salasanat

Vahva salasana on 7-16 merkkiä pitkä, ja sisältää kolmea seuraavista merkkityypeistä: isot kirjaimet, pienet kirjaimet, numerot ja erikoismerkit.

Käytätkö vahvoja salasanoja
- Kyllä
- Ei

Kirjautuessasi mobiililaitteella esimerkiksi sähköpostiin tai facebookkiin, on mahdollista tallentaa salasana laitteen muistiin.

Muistaako mobiililaitteesi salasanasi?
- Kyllä
- Ei

Oletko tallentanut mobiililaitteen muistiin tärkeää tietoa, jotta et unohtaisi niitä? (Esimerkiksi salasanat, osoitteet)
- Kyllä
- Ei

Salasanojen hallintaohjelma täyttää käyttäjän puolesta sisäänkirjautumiseen tarvittavat tiedot. Käyttäjän täytyy muistaa vain ohjelman pääsalasana.

Käytätkö salasanojen hallintaohjelmia?
- Kyllä
- Ei

Luotettavat lähteet

Lataatko tiedostoja/sovelluksia ainoastaan tunnetuista ja luotettavista lähteistä? ◯ Kyllä ◯ Ei

Vierailetko internet-selailun aikana sivustoilla, joiden luotettavuudesta sinulla ei ole tietoja? ◯ Kyllä ◯ Ei

Luetko/tarkistatko ikinä mitä valtuuksia sovellus vaatii käyttöönsä, ennen sovelluksen asennusta? ◯ Kyllä ◯ Ei

Käytätkö tuntemattomia langattomia verkkoja? ◯ Kyllä ◯ Ei

Käytätkö mobiililaitteella pilvipalveluja? ◯ Kyllä ◯ Ei

Päivitykset

Päivitätkö käyttöjärjestelmäsi aina uusimpaan versioon? ◯ Kyllä ◯ Ei

Päivitätkö säännöllisesti laitteesi sovellukset? ◯ Kyllä ◯ Ei

Varautuminen

Varkaudenhallintajärjestelmä mahdollistaa esimerkiksi mobiililaitteen lukitsemisen etäältä, tietojen tyhjentämisen etäältä ja kadonneen laitteen jäljittämisen.

Käytätkö mobiililaitteella varkaudenhallintajärjestelmää? ◯ Kyllä ◯ Ei

Mobiililaitteisiin asetettava SIM-kortti vaatii PIN-koodin toimiakseen.

Oletko vaihtanut SIM-kortin oletus PIN -koodin? (esimerkiksi 0000 tai 1234) ◯ Kyllä ◯ Ei

Käytätkö mobiililaitteellasi virustorjuntaohjelmistoa? ◯ Kyllä ◯ Ei

Varmuuskopioitko tärkeitä tiedostoja? ◯ Kyllä ◯ Ei Jos kyllä, minne/miten?

Käytätkö mobiililaitteellasi jotain näytönlukitusta? (Esimerkiksi näytön lukituskuvio) ◯ Kyllä ◯ Ei

Lopuksi

Käytätkö verkkopankkisovelluksia mobiililaitteella? ◯ Kyllä ◯ Ei

Oletko joskus kadottanut mobiililaitteesi? ◯ Kyllä ◯ Ei

Oletko kokenut tilanteita, joissa mobiililaitteesi tietoturvallisuus on ollut uhattuna? Millaisia?

Pyritkö käyttämään mobiililaitetta tietoturvallisesti? Miten?