Haaga-Helia
ammattikorkeakoulu Oy

Älypuhelimen tietoturva yksityiskäyttäjän näkökulmasta

Anna Iivarinen

11.05.2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Anna Iivarinen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön nimi
Älypuhelinten tietoturva yksityiskäyttäjän näkökulmasta

Sivu- ja liitesivumäärä
27 + 6

Tämä opinnäytetyö tarkastelee älypuhelimen tietoturvaa yksityiskäyttäjän näkökulmasta. Opinnäytetyön tarkoitus on esitellä älypuhelimeen kohdistuvia tietoturvariskejä sekä keinoja, joilla näitä riskejä on helppo välttää tai ehkäistä. Tietoturvaa käsitellään yleisellä tasolla kaikkien älypuhelinten näkökulmasta, eikä työ erittele eri käyttöjärjestelmiä. Opinnäytetyössä ei myöskään perehdytä tietoturvaohjelmistoihin, jotka voivat sisältää esimerkiksi viruksentorjunta- tai salasananhallintasovelluksia. Opinnäytetyö jakautuu kahteen eri osa-alueeseen: teoriaosuuteen tietoturvariskeistä ja niiden ehkäisystä sekä kyselytutkimukseen, jossa kartoitettiin käyttäjien tietämystä tietoturvariskeistä ja niiden ehkäisemisestä.

Opinnäytetyön teoriaosuus jakautuu kolmeen eri osa-alueeseen: fyysisiin riskeihin, langattomiin yhteyksiin sekä haittaohjelmiin, jotka myös edustavat yleisimpiä älypuhelimen tietoturvaan kohdistuvia riskejä. Älypuhelinten yleistyessä ja teknologian kehittyessä myös niihin tallennetun tiedon määrä on kasvanut merkittävästi, ja sen katoaminen tai vääriin käsiin joutuminen voi aiheuttaa käyttäjälle haittaa pienestä ongelmasta aina suuriin taloudellisiin seurauksiin. Tietoturvan tulisi siis olla yhä tärkeämpi osa älypuhelimen käyttöä.

Ensimmäinen teoriaosuuden osio kattaa älypuhelimeen kohdistuvia fyysisiä riskejä, esimerkiksi rikkoutumisen tai katoamisen. Nämä aiheutuvat usein käyttäjän oman toiminnan johdosta, mutta fyysisille riskeille altistavat myös laitteen pienehkö koko, suuri, usein helposti rikkoutuva näyttö. Toisessa teoriaosassa käsitellään langattomien yhteyksien riskejä. Langattomat yhteydet ovat pääsääntöinen älypuhelimen kommunikointikeino, ja langattomiin yhteyksiin sisältyvät esimerkiksi GSM, mobiilidata, langattomat lähiverkot, Bluetooth sekä NFC eli Near Field Communication. Niitä voidaan käyttää tiedonsiirtoon laitteiden välillä, mutta langattomat yhteydet voivat altistaa älypuhelimen palvelunesto- tai mies välissä -hyökkäykselle. Teoriaosuuden kolmas osa käsittelee haittaohjelmia, jotka voidaan jakaa karkeasti kahteen eri osa-alueeseen: haittaohjelmiin (esimerkiksi troijalaiset ja madot) ja ei-toivottuihin sovelluksiin (PUA eli Potentially Unwanted Applications), jotka voivat sisältää häiritsevää mainontaa tai käyttäjän vakoilua. Ne saattavat myös aiheuttaa haittaa älypuhelimen käytössä laskien sen suorituskykyä tai akunkestoa.

Lisäksi opinnäytetyössä toteutettiin yksityiskäyttäjille suunnattu teoriaosan pohjalta laadittu kyselytutkimus, jonka tarkoituksena oli kartoittaa käyttäjien tietämystä älypuhelimeen kohdistuvista tietoturvariskeistä ja selvittää, huomioivatko käyttäjät nämä riskit päivittäisessä käytössään. Kysely toteutettiin verkossa olevalla lomakkeella, jota jaettiin kahden viikon ajan aktiivisesti eri sosiaalisen median alustoilla. Vastauksia kyselyyn kertyi yhteensä 64. Vastauksista on nähtävissä, että käyttäjät ovat tietoisia joistain älypuhelimeen kohdistuvista riskeistä, mutta he eivät aina osaa nimetä niitä.

Asiasanat
Älypuhelin, tietoturva, käyttäjä

Sisällys

1 Johdanto

Yhä yleistyvä teknologia on tuonut mukanaan uusia innovaatioita ja uusia laitteita, joilla voidaan pitää yhteyttä yhä pienenevään maailmaan. Yksi näistä laitetyypeistä ovat älypuhelimet, joiden määrä on kasvanut nopeaa tahtia teknologian kehittyessä. Tilastokeskuksen mukaan vuonna 2016 suomalaisista 72%:lla oli älypuhelin omassa käytössään, ja 82%:ssa kotitalouksista verkkoyhteyttä käytti älypuhelimeksi luokiteltava laite.

Älypuhelimista on monia erilaisia määritelmiä sekä laitteita on lukuisia erilaisia eri valmistajilta, mutta yhteistä näille kaikille on älypuhelinten tietokoneisiin verrattava laskenta- ja prosessointivoima, joka mahdollistaa usein erilaisten palveluiden käyttämisen laitteella (Schmidt. A., 2011). Tärkeimpänä älypuhelimien ominaisuutena usein mainitaan mahdollisuus ladata kolmannen osapuolen luomia sovelluksia, sekä mahdollisuus käyttää internetiä laitteella. Älypuhelinten yleisiin ominaisuuksiin kuuluvat lisäksi erilaiset käyttöjärjestelmät, laitteen sisäinen muisti, GPS-navigointimahdollisuus sekä kamera. (Javaid, Q., Kamran, M., Shah, M., Zaidi, S., Zhang, S. 2016, 1). Yleisin käyttöjärjestelmä älypuhelimissa oli vuonna 2017 Android-pohjaiset käyttöjärjestelmät noin 88%:n markkinaosuudellaan sekä toiseksi yleisimpänä olivat iOS-käyttöjärjestelmät noin 12% markkinaosuudellaan (Statista.com 2018).

Älypuhelimet voivat tallentaa paljon erityyppistä tietoa aina henkilökohtaisista, henkilön identifioivista tiedoista eri palveluiden autentikoinnissa käytettäviin tietoihin. Henkilökohtainen tieto voi sisältää esimerkiksi viestejä, kuvia ja videoita, joita käyttäjä on tallentanut älypuhelimeensa. Tämä voi johtaa suuriinkiin ongelmiin, mikäli tietoa katoaa syystä tai toisesta. Henkilökohtaista tietoa suurempaa vahinkoa tiedon varastamisesta voi henkilölle olla, mikäli se sisältää autentikointiin käytettävää tietoa. Tämä voi sisältää esimerkiksi käyttäjätunnuksia, salasanoja ja PIN-koodeja, jotka voivat päästää hyökkääjän käsiinsä saamista käyttäjätunnuksista ja salasanoista esimerkiksi sosiaaliseen mediaan aina jopa pankkitietoihin saakka. (Gritzalis, D., Mylonas, A. Theoharidou, M.)

Älypuhelinten määrän kasvaessa erilaisissa verkoissa liikkuvan tiedon määrä on myös kasvanut tehden siitä houkuttelevampaa myös rikollisille. Tämä tuo usein ihmisten mieliin riskin laitteeseen tallennetun tiedon menettämisestä tai sen joutumisesta vääriin käsiin. Tietoturva onkin moniulotteinen ja -syinen osa-alue, joka on kuitenkin helppo sivuuttaa päivittäisissä toimissa, sillä usein tietoturvan edistäminen ja ylläpitäminen vaativat tietoisia toimia ja saattavat hidastaa älypuhelimen käyttöä lisäämällä esimerkiksi lukituskoodin, joka tulee avata ennen laitteen käyttöä. Yksinkertaisimmillaan tietoturvan voi määritellä

”järjestelyiksi, joilla pyritään varmistamaan käytettävyys, tiedon eheys ja luottamuksellisuus” (Vahti 2008). Tiedon tulee siis olla muuttumattomana vain oikeutettujen henkilöiden ja laitteiden käytössä, kun nämä sitä tarvitsevat, luottamuksellisesti. Tietoturvan menettäminen voi johtaa pienestä harmista aina suuriin taloudellisiin menetyksiin, mikäli esimerkiksi luottokorttitiedot joutuvat vääriin käsiin. Näin ollen myös yksityishenkilöiden tulisi olla kiinnostunut tietoturvastaan ongelmien välttämiseksi.

Tämä opinnäytetyö käsittelee yksityiskäyttäjän tietoturvaa päivittäisissä toimissa, ja kertoo, miten sitä on mahdollista parantaa omilla valinnoillaan. Opinnäytetyö esittelee helppoja keinoja, joilla tietoturvallisuutta voidaan parantaa puhelimen käyttökokemusta vähentämättä. Työn teoriaosuuden lisäksi yksityiskäyttäjille suunnattu kysely kartoittaa yksityiskäyttäjien älypuhelimen käyttökokemuksia tietoturvan näkökulmasta. Opinnäytetyön ulkopuolelle rajataan eri mobiilikäyttöjärjestelmät ja niiden erittely, ja opinnäytetyö keskittyy tarkastelemaan kaikille käyttöjärjestelmille yleisiä uhkia ja niiltä suojautumista. Lisäksi opinnäytetyön ulkopuolelle rajataan erilaiset kolmannen osapuolen sovellukset, joita mainostetaan niin kutsuttuina tietoturvasovelluksina, joiden tavoite on edistää käyttäjänsä tietoturvaa.

2 Fyysiset riskit

Älypuhelin on pienikokoinen ja helppo laite mukanakuljetettavaksi, mikä lisää sen riskiä tippua ja kadota mitä erikoisimpiin paikkoihin ja sen myötä rikkoutua. Älypuhelinten suuret, usein lasiset näytöt ja kasvava koko tekevät ne alttiimmiksi kolhuille, jotka voivat vahingoittaa laitetta tehden siitä jopa käyttökelvottoman. Pienikokoinen laite on myös altis varkauksille joko huolimattoman käsittelyn tai näpistelyn johdosta. Esimerkiksi avoimessa taskussa tai laukussa laitteen säilyttäminen ruuhkassa kulkiessa altistaa sen katoamiselle joko putoamisen tai varkauden myötä. Varkaudesta ja laitteen kadottamisesta voi seurata laitteen menetyksen lisäksi tärkeiden tietojen menetys aina vuosia kerätystä kontaktiluettelosta muistoina toimiviin kuviin. Laitteiden ominaisuuksien lisääntyessä ja niiden yleistyessä myös hinnat ovat nousseet useisiin satoihin euroihin, mikä itsessään jo johtaa taloudelliseen menetykseen puhumattakaan siitä mitä mahdollinen tiedonmenetys voi pahimmillaan aiheuttaa. (Mooney, P. 2013)

Riskejä laitteen kadottamisesta tai rikkoutumisesta on siis aina taloudellisista menetyksistä pieneen mielipahaan. Fyysisiltä uhkilta suojaaminen kiteytyy lyhyesti sanottuna laitteen huolelliseen käsittelyyn ja säilytykseen, sekä laitteen suojaamiseen väärinkäytöksiä vastaan käyttämällä laitteen lukitukseen vähintään pääsykoodia tai sormenjälkitunnistetta. Lukituksen tulisi mielellään olla helposti muistettava, mutta uniikki, jolloin ulkopuolisen ei ole sitä helppo arvata. (Mooney, P. 2013) Tämä hidastaa merkittävästi tai kokonaan ehkäisee laitteen luvatonta käyttöä yhdessä mahdollisen etähallinnan kanssa. Etähallinnalla voidaan paikallistaa älypuhelin tai tarvittaessa jopa pyyhkiä laiteeseen tallennetut tiedot toiselta laitteelta käsin. Huolellisella käsittelyllä voidaan myös ehkäistä haittaohjelmien asentamista laitteelle. (F-Secure 2013) Lisäksi älypuhelimille on lukuisia erityyppisiä suojalaseja ja -koteloita, joilla laitteen voi suojata kolhuilta. Näitä saa lukuisissa eri väreissä ja merkeissä. Esimerkiksi Verkkokauppa.comin ”Kotelot ja suojakuoret” älypuhelimille kateogoriassa on yli 2000 tuotetta (Verkkokauppa.com. 2018).

Käyttäjän oma toiminta ja laitteen huolellinen käsittely on siis suuressa osassa varkauksien ja rikkoutumisen ehkäisyssä, mutta älypuhelimissa on myös joitain sisäänrakennettuja ominaisuuksia varkauksien ja väärinkäytöksien ehkäisyyn. On mahdollista esimerkiksi paikallistaa laite tai soittaa hälytysääni, kun laitetta yritetään paikantaa. Lisäksi eri älypuhelinvalmistajien sovelluskaupoista on mahdollista ladata erityyppisiä sovelluksia laitteen suojaamiseen (F-Secure 2013).

Mikäli puhelin varastetaan tai se katoaa, voi laitteen IMEI-numeron ilmoittaa operaattorille varastettuna laitteena, kun rikosilmoitus on tehty poliisille (Telia.fi 2018). Lisäksi liittymä on hyvä sulkea, jotta estetään SIM-kortin käyttö. IMEI- eli International Mobile Equipment Identity -numerolla tarkoitetaan 15-merkkistä numerosarjaa, joka identifioi useimpia älypuhelimia (imei.info 2018).

IMEI-numero ilmoitetaan operaattorin toimesta kansainväliselle mustalle listalle (CEIR-rekisteri), joka tekee puhelimen käytöstä soittamiseen mahdotonta estämällä soittamisen ja puheluiden vastaanottamisen. Laitteen omistaja voi laitteen löytyessä poistaa sen mustalta listalta päivitetyn rikosilmoituksen avulla operaattorille ilmoittamalla ja palauttaa sen jälleen käyttöön (Telia.fi 2018). IMEI-numeron voi tarkastaa omasta älypuhelimestaan soittamalla *#06#, jolloin laite näyttää näytöllä IMEI-numerot (imei.info 2018). IMEI-numeron voi myös löytää laitteen omaan laatikkoon liimatusta tarrasta, puhelimesta itsestään akun kanssa samalta alueelta sekä joillain laitteilla asetuksien kautta puhelimen tiedoista (imei.info 2018).

3 Langattomat yhteydet

Langattomiin yhteyksiin lasketaan puheluita ja tekstiviestejä välittävän GSM- eli matkapuhelinverkon lisäksi mobiilidatana tunnetut 3G ja 4G-verkot, jotka mahdollistavat nopean internetin käytön. Pienemmän kantaman langattomia lähiverkkoja on kotien lisäksi useissa julkisissa paikoissa aina kahviloista hotelleihin (Viestintävirasto. 2015). Päivittäisessä käytössä lähes kaikki älypuhelimen kommunikaatiosta on langatonta yhteyksien helppouden ja nopeuden vuoksi. Enää ei ole tarvetta kytkeä laitetta kiinni langalliseen verkkoon, kun mobiiliverkkojen kehittyessä ja langattomien verkkojen yleistyessä älylaitteet ovat yhdistettynä verkkoon lähes koko ajan joko mobiilidatan tai langattomien verkkojen kautta. Myös laitteen synkronointi sekä varmuuskopioiden tekemisen ja palauttamisen voi jo tehdä langattomasti esimerkiksi Bluetooth-yhteyttä käyttäen (Haataja, K. 2009). Langattomien yhteyksien suosiota ja kasvua selittää niiden vaivattomuus ja saatavuus: älypuhelin on käytännössä lähes koko ajan yhdistetty mobiiliverkkoon, ja verkko on saatavilla lähes kaikkialla.

3.1 Suojaamattomat langattomat lähiverkot

Suojaamattomalla langattomalla verkolla tarkoitetaan verkkoa, jota ei ole suojattu millään salauksella, esimerkiksi salasanalla vaan siihen liittyminen on vaivatonta ja nopeaa, eikä ylimääräisiä kysymyksiä kysytä. Suojaamaton verkko on siis avoin kaikille sen kantaman sisällä oleville laitteille ja käyttäjille (Viestintävirasto 2014). Vapaasti käytettäviä langattomia verkkoja on tullut kuluttajien ulottuville erilaisissa julkisissa paikoissa aina kauppakeskuksista ravintoloihin ja kahviloihin. Ne ovat suosittuja, sillä säästävät tarvittaessa mobiilidataa verkon käytössä, ja tarjoavat jopa suurempia nopeuksia verkonkäytölle, mitä mobiilidata. Usein vapaasti käytettävät verkot ovat suojaamattomia yhdistämisen ja nopean käytön takaamiseksi. Ne tarjoavat kuitenkin mahdollisuuden seurata ja kuunnella verkkoliikennettä käyttäjän sitä huomaamatta.

Automaattinen, tunnettuihin tai suojaamattomiin langattomiin verkkoihin liittyminen nopeuttaa älypuhelimen käyttöä, kun käyttäjän ei tarvitse erikseen valita verkkoa laitteen asetuksista. Kun laite jo on esimerkiksi yhdistynyt aiemmin kahvilan suojaamattomaan verkkoon, yhdistää se usein asetuksiensa perusteella suoraan uudelleen siihen ollessaan tukiaseman lähettyvillä. Tällöin hyökkääjä voi tarjota esimerkiksi hieman vahvemman, samannimisen suojaamattoman yhteyden jolloin älypuhelin itse tai käyttäjä voi yhdistää laitteen kyseiseen verkkoon sen ollessa houkuttelevampi paremman signaalin toivossa.

Tämä kuitenkin tuo myös riskin man-in-the-middle -hyökkäykselle eli välimies- tai valetukiasemahyökkäykselle, jossa hyökkääjä naamioi oman tukiasemansa SSID:n, eli verkon nimen samaksi, jonka siihen yhteyttä ottava laite jo tuntee. Älypuhelin tunnistaa verkon samaksi, johon se on jo aiemmin yhdistynyt, tai käyttäjä valitsee hyökkääjän verkon paremman signaalin vuoksi. Kun laite yhdistetään langattomaan verkkoon, kulkee liikenne hyökkääjän tukiaseman kautta. Näin ollen hyökkääjä pääsee kuuntelemaan ja tarkkailemaan kaikkea tukiasemansa lävitse kulkevaa verkkoliikennettä, ja voi saada tietoonsa sen avulla salasanoja ja henkilökohtaisia tietoja. (Anderson, J., Nampalli, J., Nykamp, D., Speed, T. 2013)

Langattomien verkkojen sijaan Suomessa on varteenotettava vaihtoehto käyttää mobiilidataa, eli 3G ja 4G yhteyksiä. Useat operaattorit tarjoavat rajattoman mobiilidatan liittymiä kohtuulliseen hintaan. Lisäksi verkkoliikenteen salaamiseen vaihtoehto on käyttää VPN:ää eli Virtual Private Networkia, jonka tarkoitus on lähettää liikenne salattuna luotetulle palvelimelle, joka edelleen lähettää tiedon internetiin. Tämä muodostaa salatun liikenteen niin kutsutun tunnelin, joka on turvallisempi käyttää, mitä julkiset langattomat verkot usein ovat. Usein VPN-palvelut ovat maksullisia, mutta osa yrityksistä tarjoaa työntekijöidensä käyttöön palvelun parantaakseen tietoturvaa. (Athow, D. 2017)

3.2 Bluetooth -yhteys

Bluetooth on lyhyen välimatkan radioaaltoyhteys, jonka avulla voidaan siirtää tietoa laitteesta toiseen, ja yhdistää eri laitteita toisiinsa. Se kehitettiin, jotta olisi mahdollista siirtää laiteelta laitteelle tietoa ilman kaapeleita ja helpottaa näin myös laitteiden välistä synkronointia. Lisäksi Bluetooth-yhteyden kautta voidaan tarvittaessa jakaa myös internetyhteyttä. Yhteys toimii esimerkiksi älypuhelinten, tietokoneiden, tulostimien, hiirten ja näppäimistöjen välillä, ja on yleinen jokapäiväisessä käytössä. Bluetoothilla voidaan myös tarvittaessa muodostaa useiden laitteiden verkkoja, joissa jokainen laite jatkaa verkon kantamaa, tai niitä voidaan käyttää kahden laitteen välillä. Molemmissa tapauksissa Bluetoothin käyttö perustuu laitteiden parien muodostamiseen, ja näitä pareja voidaan muodostaa lukemattomia. Kuten muutkin langattomat yhteydet, eivät Bluetooth-yhteydetkään ole riskittömiä. (Haataja, K. 2009)

Bluetooth-yhteyksiä voidaan muiden langattomien verkkojen tapaan salakuunnella aiemminkin kuvatun man-in-the-middle- tai välimieshyökkäyksen avulla, jolloin hyökkääjän laite on naamioitu samannimiseksi kuin mitä hyökkäyksen kohteena olevan parin toinen laite on. Tämä mahdollistaa salakuuntelun lisäksi tiedonsiirron molempiin suuntiin. Bluetooth-yhteydet altistavat laitteita myös DoS- eli Denial of Service-hyökkäyksille, jotka

ovat usein paremmin tunnettuja palvelimiin ja tietokoneisiin kohdistuvissa hyökkäyksissä. Bluetooth kuitenkin altistaa myös älypuhelimet tälle hyökkäykselle laitteiden muistuttaessa yhä enemmän ja enemmän pieniä tietokoneita. Denial of Service eli palvelunestohyökkäyksen tarkoitus on saada lähettää laitteelle niin paljon turhaa tietoa, että laitteen toiminta häiriintyy, hidastuu tai muuttuu kokonaan mahdottomaksi. Se voi nopeuttaa laitteen akun tyhjenemistä, tai jopa saada laitteen käyttöjärjestelmän kaatumaan, kun käyttöjärjestelmä ei kykene käsittelemään kaikkea sille lähetettävää tietoa. (Chen, L., Padgette, J., Scarfone, K. 2012)

Lisäksi Bluetooth-yhteyksillä on vain niille ominaisia riskejä sen toimintamallista, laitteiden parina toimimisesta ja pareiksi yhdistämisestä johtuen. Bluetooth-yhteyttä käyttävään laitteeseen on mahdollista yhdistää toinen laite käyttäjän sitä huomaamatta ja varastaa näin tietoja, esimerkiksi älypuhelimen kontaktiluettelon, kalenteritietoja tai kuvia hyökkäyksen kohteen sitä huomaamatta. Tämä voi tapahtua, kun luotetut laitteet, esimerkiksi älypuhelin ja kuulokkeet, ovat jo muodostaneet parin, jonka jälkeen hyökkäys voidaan suorittaa käyttäjän sitä tietämättä yhteyttä salakuuntelemalla ja yhteyteen liittymällä käyttämällä esimerkiksi kuulokkeiden nimeä tunnistautumisessa. Sen lisäksi onnistuneen yhdistämisen jälkeen hyökkääjä voi hallita laitetta etänä, jolloin tämä voi esimerkiksi lähettää saapuneita viestejä eteenpäin, muuttaa laitteen asetuksia tai tarkkailla, mitä laitteella kirjoitetaan mahdollistaen esimerkiksi salasanojen selvittämisen (Chen, L., Padgette, J., Scarfone, K. 2012).

Bluetooth-yhteyksillä on erilaisia tietoturvamekanismeja, jotka jaetaan neljään eri tasoon. Ensimmäinen näistä tasoista ei tarjoa mitään suojausta esimerkiksi autentikoinnin tai tiedonsiirron salauksen suhteen, vaan mitään kyselemättä yhdistää Bluetooth-yhteyttä käyttävät laitteet pariksi. Toisella tasolla laite kysyy autentikointia ja yhdistämisen huomioimista, mutta ongelmana on se, että laitteet yhdistyvät jo ennen autentikointia, jolloin se jättää hyökkääjälle mahdollisuuden salakuunnella liikennettä. Laitteet autentikoivat toisensa ennen yhdistämistä kolmannella tasolla, mikä vie toisella tasolla esiintyvän ongelman autentikoimattomasta yhdistämisestä pois. Neljännellä tasolla käytetään kolmannen tason tapaan autentikointia, mutta autentikointimenetelmä käyttää vahvempaa tunnistautumista. (Haataja, K. 2009) On hyvä tietää, mitä suojaustasoa mikäkin laite käyttää.

Helpoin tapa turvautua Bluetooth-hyökkäyksiä vastaan on ottaa Bluetooth-yhteys pois käytöstä, kun sitä ei tarvita laitteiden parin muodostamiseen. Tämä ehkäisee helposti ei-toivotut yhteydenotot, eikä yhteyden luvattomasta käytöstä tarvitse huolehtia. Lisäksi silloin, kun Bluetooth on käytössä, on hyvä pitää laite tilassa, jossa se ei näy julkisesti

kaikille muille laitteille. Se ei kokonaan estä hyökkäyksen mahdollisuutta, mutta vähentää sitä. Mikäli laite, jota olet aiemmin käyttänyt toisen laitteesi kanssa katoaa, et käytä sitä enää lainkaan tai se rikkoutuu, on suositeltavaa poistaa se toisen laitteesi listalta hyväksytyistä yhteyksistä. Kuten monet muutekin laitteet, myös Bluetooth-laitteet, sekä tietenkin älypuhelimet saavat päivityksiä käyttöjärjestelmiinsä, ja on tärkeää pitää ne ajantasalla. (Viestintävirasto. 2017)

3.3 Near Field Communication

NFC eli ”Near Field Communication” on langaton yhteystyyppi, joka toimii laitteessa olevan NFC-sirun avulla (Triggs, R. 2018). Nimensä mukaisesti yhteys toimii lyhyellä välimatkalla, vähintään kahden laitteen välillä. Tällöin toinen laite on tietoa lähettävässä roolissa, ja toinen tietoa vastaanottavana osapuolena. NFC-yhteyden etuna voidaan nähdä se, että kahden laitteen yhteyden välillä vain toisen tarvitsee olla aktiivinen yhteyden muodostamista varten. Vain aktiivinen laite voi sekä lähettää että vastaanottaa tietoa. Teknologiaa käytetään esimerkiksi julkisen liikenteen matkakorteissa, jolloin lukijalaite on aktiivinen, ja kortti passiivinen ilman omaa virtalähdettä. Älypuhelimissa NFC -yhteyttä käytetään yleisimmin mobiililaitteella maksamisessa (Paganini, P. 2012).

NFC-yhteys hyödyntää elektromagneettista kenttää sekä radioaaltoja kommunikointiin ja sillä on useita käytännön sovelluksia. Yhteyttä voidaan käyttää vertaisverkon osana yhdessä muiden eri kommunikaatioprotokollaa käyttävien langattomien yhteyksien, kuten esimerkiksi Bluetoothin tai Wi-Fi:n kanssa. NFC-yhteyttä voidaan käyttää myös kortin ja laitteen välillä esimerkiksi matkakortissa, joka voi vastaanottaa tietoa kortin lukijalta päivittäen kortin tiedot tapahtumaa vastaaviksi. Älypuhelimille yleisin yhteystyyppi NFC-yhteydelle on toimia virtuaalisten korttien emuloinnissa, jolloin kortin tieto tallennetaan NFC-sirulle. Kortteja voidaan tallentaa tarvittaessa useita yhdelle NFC-sirulle. Käytännössä tämä tarkoittaa usein virtuaalista luottokorttia, joka toimii maksuvälineenä mobiilimaksamisessa. (Paganini, P. 2013)

Vaikka nopea yhteydenmuodostus ja yhteyden käytön helppous houkuttavat, sisältyy muiden langattomien yhteyksien tapaan myös NFC-yhteyteen tietoturvariskejä mukaan lukuen salakuuntelun, tiedon korruptoimisen tai muokkaamisen. Salakuuntelu ja riski aiemmin kuvatulle man-in-the-middle -hyökkäykselle muodostuu, mikäli hyökkääjä saa tarpeeksi vahvan antennin NFC-yhteyden käyttötilanteen lähelle. Vaikka signaali onkin heikko ja toimii vain lyhyellä etäisyydellä, voi signaalin osia poimia vahvoilla antenneilla otollisissa olosuhteissa. Tällöinkin välimatkan on oltava korkeintaan kymmenen metriä, ja tämä voi tuoda ongelmia esimerkiksi tarpeeksi suuren antennin signaalin lähelle

saattamisessa. Antennin avulla voidaan myös altistaa NFC-yhteyttä käyttävät laitteet Denial of Service (DoS) -hyökkäykselle lähettämällä laitteelle enemmän dataa, mitä se kykenee käsittelemään. Hyökkääjän on myös mahdollista syöttää tietoja laitteelle, mikäli yhteydenmuodostus onnistuu. (Radio-Electronics.com)

Turvallisen kanavan/protokollan (secure channel) käyttäminen suojaa salakuuntelulta ja tiedon muuntamiselta tai korruptoimiselta. Turvallinen kanava hyödyntää autentikointia salausavaimia vaihtamalla ja näin autentikoidaan jokainen NFC-yhteyksien muodostamaan verkkoon liittyvät laitteet. Yhteystyyppi myös salaa liikenteen, mutta jokaisen verkossa olevan laitteen on käytettävä turvallista kanavaa. (Radio-Electronics.com) Lisäksi esimerkiksi virtuaalista luottokorttia käyttäessä voidaan hyödyntää maksurajoja, jotka estävät rahan käytön asetetun rajan täytyttyä. Lisäksi yhteyttä käyttävän sovelluksen voi sulkea, kun sitä ei käytä, jolloin laite ei lähetä signaalia turhaan ympäristöön etsiessään vastaparia.

4 Haittaohjelmat

Haittaohjelma (malware) on nimensä mukaisestikin laitteelle ja laitteen käyttäjälle haittaa aiheuttava sovellus, jonka tarkoitus on tuottaa hyötyä tekijälleen. Haittaohjelmia on erityyppisiä eri tarkoituksiin, ja älypuhelimissa yleisimpiä haittaohjelmia ovat troijalaiset, takaovisovellukset sekä madot. Lisäksi haittaa voivat aiheuttaa mahdollisesti ei-toivotut sovellukset eli PUA-sovellukset (Potentially Unwanted Appications), joihin kuuluvat vakoiluohjelmat, käyttäjän toimia jäljittävät ohjelmat sekä haitallisia mainoksia käyttäjälle näyttävät ohjelmat (F-Secure 2013).

Käyttäjälle suurinta näkyvää vahinkoa haittaohjelmista syntyy, kun hyökkäyksen uhrin luottokortti- ja salasanatietoja vuotaa haittaohjelman kautta hyökkääjälle. Haittaohjelmat voivat myös rikkoa tietoturvaa vakoillemalla käyttäjän tapoja ja keräten tietoa, jotta sitä voidaan myydä eteenpäin kaupallisiin tarkoituksiin. Nämä eivät aiheuta näkyvää haittaa, mutta voivat aiheuttaa älypuhelimen hidastumista, käyttää laitteen muistia ja resursseja vähentäen näin esimerkiksi akunkestoa (F-Secure 2013). On myös mahdollista, että yhden haittaohjelman avulla voidaan asentaa laitteeseen lisää haittaohjelmia ja altistaa laitteen uusille hyökkäyksille. (Schmidt, A. 2011)

Ensimmäinen varsinaisesti älypuhelimille suunnattu haittaohjelma tehtiin vuonna 2004 Symbian-käyttöjärjestelmää käyttäville älypuhelimille (Srikanth, R. 2012). Haittaohjelma levisi suojaamattomien Bluetooth-yhteyksien välityksellä. Seuraavina vuosina älypuhelinten yleistyessä myös niille suunnattujen haittaohjelmien määrä kasvoi, kun älypuhelimista kasvoi perinteisten tietokoneiden haastaja internetin selaamiseen. Vuoden 2016 Kaspersky Labin raportissa haitallisia ohjelmien asennuspaketteja on 8,5 miljoonaa, sekä troijalaisia yhteensä noin 300 000 (Kasperky Lab. 2016). Tämä on lähes kolminkertainen määrä vuoteen 2015 nähden. Haittaohjelmat voidaan jakaa kolmeen eri tyyppiin: takaovisovelluksiin, troijalaisiin sekä matoihin. Kaikkien tarkoitus on aiheuttaa käyttäjälleen haittaa esimerkiksi varastamalla tai väärentämällä tietoa (F-Secure. 2013).

Ensimmäisenä haittaohjelmien niin kutsuttuna kateokogriana tässä ovat takaovisovellukset (backdoor), jotka antavat mahdollisuuden hallita laitetta etäältä ilman käyttäjän lupaa tai jopa tämän tietämättä avaamalla laitteeseen reitin muille haittaohjelmille. Nämä voivat tulla esimerkiksi toisen sovelluksen mukana. (F-Secure. 2013)

Yleisimpänä haittaohjelmatyyppinä pidetään troijalaisia (trojan), joiden tarkoitus on suorittaa haitallisia toimia laitteessa. Nämä varastavat tietoa, vievät laitteen resursseja, ja

troijalaisia voidaan luokitella niiden käyttötarkoituksen mukaan. Yhä kehittyvät troijalaiset voivat älypuhelimeen asennuttuaan varastaa esimerkiksi kirjautumistietoja, tai jopa asentaa uusia sovelluksia ilman käyttäjän lupaa (Kaspersky Lab. 2016). Troijalaiset asentuvat laitteelle yleensä käyttäjän omien toimien kautta tämän ladatessa uusia sovelluksia älypuhelimeensa. Troijalainen voi myös tulla ladattavan sovelluksen mukana. (Shrikanth, R. 2012)

Madot (worm) toimivat kopioimalla itsestään toimivia kopioita, ja lähettämällä niitä eteenpäin esimerkiksi Bluetooth-yhteyksien tai muiden laiteeseen yhdistettävien laitteiden kautta (F-Secure. 2013). Madon saaneesta tietokoneesta voi älypuhelimen kanssa synkronoidessa tarttua mato myös älypuhelimeen ja niiden pyrkimys on levitä mahdollisimman moneen laitteeseen.

4.1 Ei-toivotut sovellukset

PUA-sovelluksiin (Potentially Unwanted Applications) eli ei-toivottuihin sovelluksiin kuuluvat vakoiluohjelmat, käyttäjän toimia jäljittävät sovellukset sekä haitallisia mainoksia käyttäjälle näyttävät sovellukset. (F-Secure. 2013)

Vakoiluohjelmien (spyware) tarkoitus on kerätä tietoa käyttäjän laitteen käyttötavoista, kuten esimerkiksi internetin tai sovelluksien käytöstä. Vakoiluohjelmat voivat lähettää tiedon eteenpäin, tai varastoida sen laitteeseen. Vakoiluohjelmien kanssa melko samankaltaisia ovat jäljittämiseen tarkoitetut ei-toivotut sovellukset (trackware), joiden tarkoitus on tunnistaa käyttäjä tai laite kolmannelle osapuolelle tarjoten mahdollisuuden kerätä esimerkiksi tietoa sijainnista (F-Secure. 2013). Näitä jäljittämiseen tarkoitettuja sovelluksia voidaan käyttää myös varkauden ehkäisyyn tai kadonneen laitteen etsimiseen, mutta käyttäjän tietämättä asennetut jäljityssovellukset voivat lähettää tiedon hyökkääjille tiedon jatkokäyttöä varten. (Shrikanth, R. 2012).

Ei-toivottuihin sovelluksiin kuuluvat myös sovellukset, joiden pääasiallinen tarkoitus on näyttää käyttäjälle mainoksia, jotka potentiaalisesti voivat altistaa käyttäjän yksityisyyden riskiin, ja esittää häiritsevää tai jopa aggressiivista mainontaa. Yksityisyyden suojaa nämä sovellukset voivat rikkoa keräämällä tietoa laitteesta aina sen mallista IMEI-numeroon saakka. Lisäksi sovellukset voivat muuttaa laitteen asetuksia aina kotinäytön pikavalikoista internetselaimen kirjanmerkkeihin ja aloitussivuun. Tietoturvariskin tästä tekee mahdollisuus altistua tahtomattaan kyseenalaisille sivustoille, sovelluksille tai mainonnalle. (Shrikanth, R. 2012).

4.2 Haittaohjelmilta suojautuminen

Osa älypuhelimista sallii myös käyttöjärjestelmän omien sovelluskauppojen lisäksi sovellusten lataamisen myös niiden ulkopuolelta. Tällöin on vaikea varmistua siitä, että sovellus on turvallinen, eikä sen mukana tule mitään ei-toivottuja ohjelmia. Onkin turvallisinta käyttää sovellusten lataamiseen vain käyttöjärjestelmien omista sovelluskaupoista. Esimerkiksi Android-puhelimissa asetuksissa voi kieltää muut kuin Google Play -sovelluskauppa latauksien lähteenä. Lisäksi ladattavia sovelluksia valitessa useista vaihtoehdoista on kannattavaa valita se, jolla on paremmat arviot sovelluskaupassa ja enemmän latauskertoja. (Shrikanth, R. 2012)

Sovellusten pyytämien lupien tarkastaminen on hyvä tehdä sovelluksen kysyessä lupaa käyttää älypuhelimen tietoja (Shrikanth, R. 2012). Mikäli sovellus tuntuu kysyvän lupia omituisiin asioihin sovleluksen käyttötarkoitukseen nähden, voi sovelluksella olla haitallisia motiiveja tiedon eteenpäin levittämisestä tai vakoilusta. Lisäksi laitteen muuttuneet ominaisuudet käytön aikana voivat olla merkki haittaohjelmasta. Esimerkiksi nopeasti kasvanut akun tai verkon ylitse siirretyn datan kulutus voi olla merkki haittaohjelmista. Lisäksi erilaiset tietoturvasovellukset ja viruksentorjuntaohjelmat tarjoavat mahdollisuuden etsiä ja poistaa haitallisia sovelluksia ja tiedostoja laitteesta. (F-Secure. 2013)

5 Kyselytutkimus

Tutkimuksessa tutkitaan käyttäjän tietoisuutta älypuhelimen tietoturvasta, ja tätä tarkennetaan tutkimuskysymysten muodossa myöhemmin. Tutkimuksen tarkoitus on kartoittaa käyttäjien kokemuksia ja tapoja, mikä tekee tutkimuksesta käyttäjälähtöisen. Tämä itsessään jo luo tutkimukselle näkökulman siitä, että käyttäjäkokemukset ja erityisesti yksityishenkilöiden kokemukset ovat tärkeä osa tutkimuksen tarkoitusperien saavuttamisessa. Tämän johdosta tutkimusmenetelmäksi valittiin kyselytutkimus, jolla oli tarkoitus tavoittaa mahdollisimman suuri yleisö laajan tutkimusaineiston saavuttamiseksi. Lisäksi tutkimustyypin etuna on toteutuksen helppous ja nopeus olivat tärkeä osa-alue tutkimusta suunnitellessa. Kyselytutkimuksessa voi lisäksi esittää runsaasti kysymyksiä, kun ne on muotoiltu tarkasti. Ongelmakohtia tutkimusmenetelmässä voivat olla esimerkiksi vastaajien suhtautuminen kyselyn aiheeseen, vastaavatko he rehellisesti ja huolellisesti, mutta myös kysymys siitä, ymmärtävätkö vastaajat kysymykset ja niiden aiheyhteydet. (Taanila, A. 2014)

Tutkimus toteutettiin kyselytutkimuksena internetissä. Tällä oli tarkoitus saada mahdollisimman paljon ja kattavasti vastauksia eri taustoista tulevilta yksityishenkilöiltä. Käytännössä tutkimuksen neliosainen kysely toteutettiin jakamalla sosiaalisen median eri kanavilla Google Forms -palvelulla laadittua kyselyä, jolloin on mahdollista saada helposti tavoitettua suuri yleisö. Kyselyn toteutukseen käytetty palvelu tarjoaa myös mahdollisuuden ladata tulokset esimerkiksi laskentataulukkoon, tai tulkita vastauksia itse palvelun tarjoamien grafiikoiden kautta. Lomakkeen laatimisessa keskityttiin luomaan kysymyksiä, joiden perusteella olisi mahdollista vastata seuraavassa osassa esiteltäviin tutkimuskysymyksiin kuitenkaan tutkimuskysymyksiä suoraan kyselyssä esittelemättä. Kyselyssä käytettiin monivalintakysymyksiä, avoimia kysymyksiä sekä erilaisia asteikkoja hyödyntäviä kysymyksiä.

5.1 Tutkimuskysymykset

- Kuinka käyttäjät huomioivat tietoturvallisuuden ja sitä edistävät mekanismit ja niiden käytön?
- Miten käyttäjät edistävät tai vähentävät tietoturvaansa päivittäisessä käytössään?
- Millaisia uhkia ja riskejä käyttävät ovat kokeneet käyttäessään älypuhelinta ja sen palveluita

Koska tutkimus on käyttäjien toimintaa tutkiva on ensimmäisen tutkimuskysymyksen tarkoitus määritellä tutkimuksen perustaa tähän suuntaan. Kysymyksen tarkoitus on tuoda tutkimukseen selkeä käyttäjälähtöinen näkökulma, jota entisestään rajataan yksityiskäyttäjiin tutkimuksen kyselyn jakamisessa. Lisäksi kysymyksessä esitellään sekä

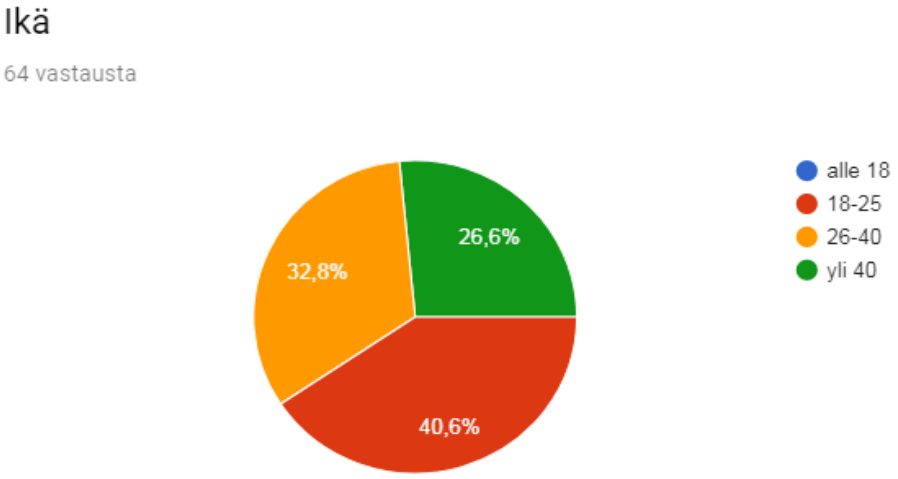
tutkimuksen että teorian näkökulmaa siitä, miten käyttäjien omat toimet vaikuttavat tietoturvaan arkisessa käytössä. Lisäksi on tarkoitus kartoittaa käyttäjien tietämystä älypuhelimen omista tietoturvamekanismeista, kuten esimerkiksi pääsykoodista, laitevalmistajien omista sovelluskaupoista ja mahdollisuudesta valita sovellusten oikeuksia.

Toinen tutkimuskysymyksistä tarkentaa entisestään ensimmäistä tutkimuskysymystä määrittelemällä tutkimuksen arkisiin toimiin kohdistuvia tietoturvariskejä käyttäjän toimien näkökulmasta. Kun ensimmäinen kysymys hakee vastausta siihen, miten paljon käyttäjä tietää erilaisista tietoturvaa edistävistä mekanismeista, toisella kysymyksellä haetaan vastausta siihen, käyttävätkö käyttäjät näitä tietoturvamekanismeja jokapäiväisessä älypuhelimen käytössään.

Kolmannen ja samalla viimeisen tutkimuskysymyksen tarkoitus on tuoda esille käyttäjien kokemuksia siitä, mitä riskejä nämä ovat itse tunteneet kokevansa älypuhelimen käytössä. Kysymyksellä kartoitetaan myös sitä, miten paljon tai vähän käyttäjät tietävät mahdollisista tietoturvariskeistä, ja ovatko nämä itse huomanneet tietoturvaongelmia älypuhelimensa käytössä. Koska kysely keskittyi muutoinkin kokonaan tietoturvaan, tuotiin tämä käyttäjien ennakkotiedot tietoturvasta esiin heti ensimmäisessä osiossa avoimella kysymyksellä siitä, mitä tietoturvariskejä käyttäjät ovat itse kokenee tai huomanneet. Kysymys sijoitettiin alkuun, jotta käyttäjät vastaisivat siihen ennen kuin ovat pohtineet kyselyn avulla omia käyttötottumuksiaan älypuhelimen käytössä.

6 Kyselyn tulokset

Kysely oli avoinna kaksi viikkoa, jonka aikana kyselyä jaettiin sosiaalisessa mediassa aktiivisesti. Vastauksia kyselyyn kertyi kaikenkaikkiaan 64 kappaletta, eikä vastauksista ole nähtävissä erityisiä ongelmia kyselyyn vastaamisessa vastaajien kesken. Kyselyssä ei ollut pakollisia kysymyksiä. Kysymysten muotoilusta kuitenkin tuli itselleni mieleen jo kyselyn julkaisun jälkeen, että vaihtoehto ”en tiedä”, tai ”ei koske minua” -olisi voinut sopia joihinkin monivalintakysymyksiin kartoittamaan vielä lisää käyttäjien tietämystä kyseisestä kyselyn osa-alueesta. Vastaamattomuus joihinkin kysymyksiin joiltain osin voidaan kuitenkin tulkita sopivan tuohon ”en tiedä” tai ”ei koske minua” -vastaustyyppiin.



Kuva 1: Kyselyn vastaajien ikäjakauma

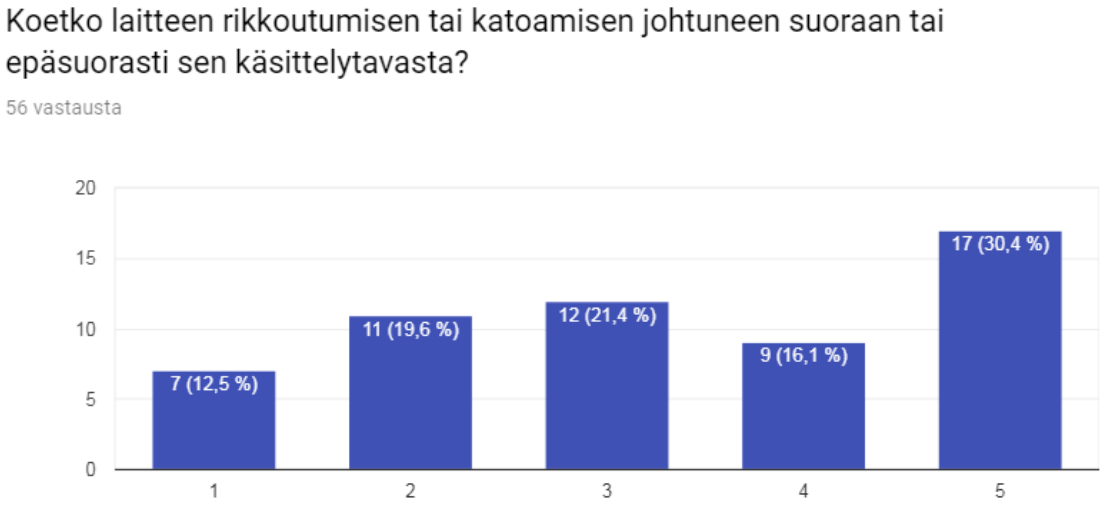
Vastaajien sukupuolijakauma kallistui naisten suuntaan: naisia vastanneista oli 43, ja miehiä 19. Loput vastaajista valitsivat vaihtoehdon ”muu/en halua kertoa”. Ikäjakauma näkyy alla olevasta kuvasta 1, josta ilmenee kaikkien vastaajien olleen täysi-ikäisiä, ja vastaajista suurin osuus osui nuoriin aikuisiin, 18-20-vuotiaisiin. Otannassa on edustettuna alaikäisiä lukuunottamatta kaikkia kyselyssä määriteltyjä ikäryhmiä, jolloin analyysissä ei ole tarvinnut huomioida mahdollista tulosten vääristymistä tietyn ikäryhmän suuntaan.

Ensimmäisen osion viimeinen kysymys oli avoin kysymys siitä, millaisia tietoturvariskejä tai -ongelmia käyttäjä on huomannut tai kokenut omasta mielestään. Se keräsi kaikenkaikkiaan 48 avointa vastausta. Näistä nousevat vastaajien kesken esille erityisesti häiritsevät mainokset ilmaissovelluksissa, sovellusten oikeudet, virukset ja älypuhelinten usein oletuksena päällä olevat sijaintipalvelut. Lisäksi vastaajat olivat huolissaan tietojen mahdollisesta salauksesta arkaluontoisempia tietoja (pankki- ja muut maksutiedot) käsiteltäessä. Käyttäjät eivät kuitenkaan nimenneet suoraan tietoturvariskejä, kuten niitä teoriaosuudessa on esitelty, mutta he olivat huolissaan tietojensa vääriin käsiin joutumisesta. Avointen vastauksien perusteella vaikutti siltä, ettei käyttäjilla välttämättä ole termejä kuvailla tietoturvariskejä, mutta he ovat tietoisia riskien olemassaolosta ja mahdollisuudesta riskien toteutumiseen. Vastaajat ovat myös kohdanneet tai kokeneet tietoturvariskejä älypuhelinta käyttäessään.

6.1 Fyysiset riskit

Kaikki kyselyyn osallistuneet vastasivat kysymykseen siitä, käyttävätkö nämä älypuhelimessaan lukitusta, esimerkiksi pääsykoodia tai sormenjälkitunnistusta. Vastaajista 83% ilmoitti käyttävänsä älypuhelimessaan lukitusta. Kyllä- ja ei-valinnasta ei tule ilmi, onko kyse tietämättömyydestä vai laitteen käytön hidastumisesta lukituskoodin myötä. Kyllä ja ei -vastausvaihtoehdoilla laaditusta kysymyksestä ei voida päätellä, miksi osa vastaajista ei käytä lukitusta laitteessaan. Suurin osa vastaajista kuitenkin käyttää lukituskoodia, mikä itsessään jo edistää tietoturvaa merkittävästi.

Laitteen katoamista tai rikkoutumista koskevaan kysymykseen osallistuneista vastasivat lähes kaikki, 55 henkilöä 64:sta vastaajasta. Vastauksista kävi ilmi, että jotkin älypuhelimen käyttöön liittyvät fyysiset tietoturvariskit olivat toteutuneet. Yleisimmät älypuhelimesta rikkoutuneet osat olivat näyttö (61% vastaajista), sekä kosteusvauriot ja akun ongelmat (22% vastaajista). Älypuhelin oli kadonnut 9%:lla vastaajista, ja varastettu 7%:ssa tapauksista. 9% vastaajista ilmoitti laitteen fyysisten painikkeiden (äänenvoimakkuus-, virta- ja kotipainike) rikkoutuneen. ”Muu” vastaus keräsi muutamia vastauksia, joissa kerrottiin laitteeseen ilmaantuneen haamukosketuksia ja lämpenemistä, sekä käyttöjärjestelmän päivityksen jälkeen laite ei käynnistynyt lainkaan. Laitteen rikkoutuminen vaikuttaa olevan vastaajien kesken yleisin tietoturvariski, ja erityisesti näytön kohdalla sen toteutuminen vaikuttaa liittyvän laitteen käsittelytapoihin.



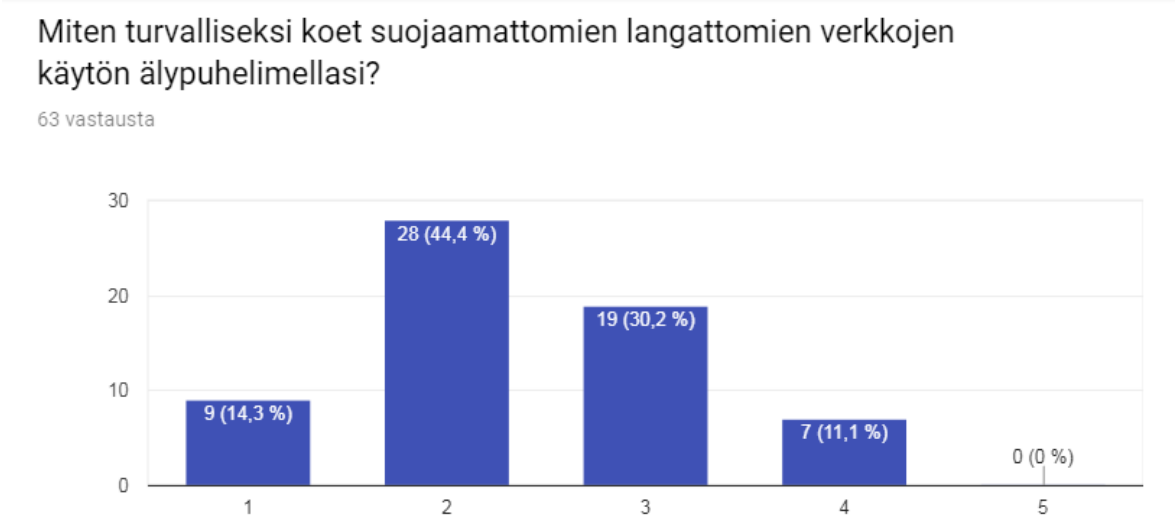
Kuva 2 Asteikko: 1 "en lainkaan" ja 5 "erittäin varmasti"

Yllä olevasta kuvasta 2 näemme, että suurimmat vastausmäärät keränneet pylväät ovat viisi ”erittäin varmasti” ja kolme, joka on vaihtoehtojen keskivaiheilla. Tämä korreloi suoraan edellisen kysymyksen vastausten kanssa, sillä näytön rikkoutuminen oli yleisin

toteutunut tietoturvariski. Tämä myös kertoo, että käyttäjät ovat tietoisia omien toimiensa seurauksista laitetta käsitellessään. Kysymykseen vastaajista vain 12,5% eli 7 henkilöä valitsi vaihtoehdon ”en lainkaan”, mikä voi viitata ”muu” vaihtoehdossa esiin tulleisiin haamukosketuksiin sekä käyttöjärjestelmän omiin ongelmiin. Käyttäjät selkeästi vaikuttavat tunnistavan omien toimien seuraukset. Kysymyksen vastauksista on kuitenkin vaikea tulkita sitä, ovatko käyttäjät ehkäisseet laitteen rikkoutumista käyttämällä esimerkiksi suojakuoria. Kuitenkaan aina älypuhelimen rikkoutumisen syynä ei kyselyn perusteella ollut käyttäjän toiminta, vaan laite on voinut rikkoutua myös vanhuuttaan, tai virheellisten ohjelmistopäivitysten myötä, ja se on varmasti jakanut kokemuksia omien toimien vaikutuksesta vähäisemmiksi ja melko pienessä otannassa nämä vähäisetkin tulokset muuttavat tuloksen painotusta jonkin verran.

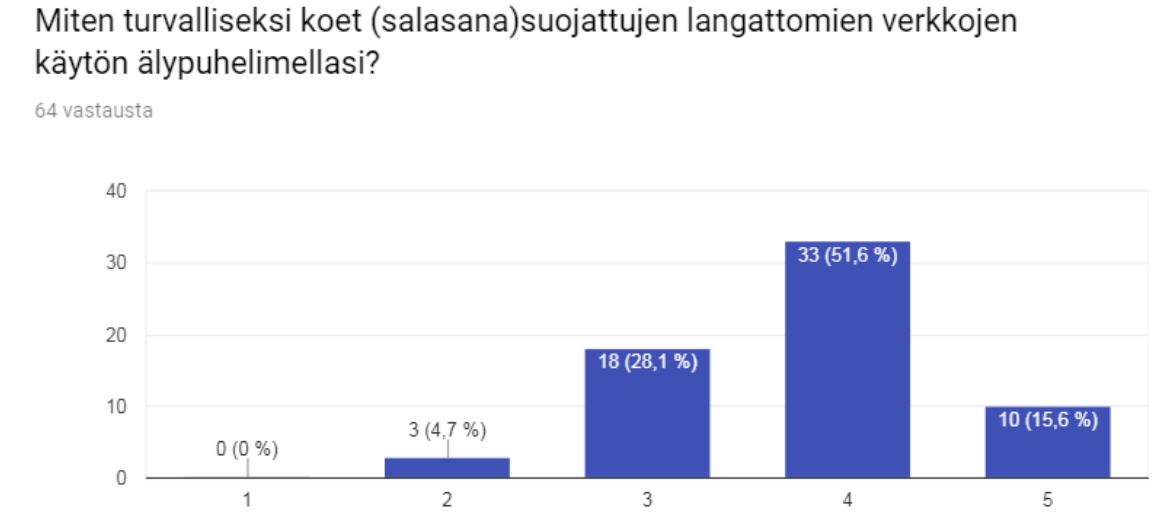
Avoimesta kysymyksestä laitteen katoamisesta, varastamisesta tai rikkoutumisesta ja sen aiheuttamasta haitasta tuli 41 vastausta. Näissä yleisimpänä haittana on taloudellinen menetys uuden laitteen hankinnasta, ja hieman harvemmin rikkoutuneen laitteen korjaamisesta ja tähän kuluvan ajan ja rahan menetys. Korjaaminen koettiin yhtä tai lähes yhtä kalliiksi kuin uuden laitteen hankinta, ja merkittävästi vaivalloisemmaksi. Lisäksi käyttäjät kokivat ongelmalliseksi tiedon menettämisen laitteen rikkoutumisen myötä, mutta taloudellinen ja ajallinen haitta koettiin tiedon menetystä suuremmaksi ongelmaksi. Mikäli uuden älypuhelimen valmistaja oli eri kuin uuden laitteen valmistaja, koettiin tiedonsiirto laitteiden välillä ongelmalliseksi. Muutama vastaajista myös ilmoitti ostaneensa näytönsuojalasin sekä kotelon uudelle laitteelleen suojellakseen sitä edeltävää laitetta paremmin. Vastauksista jää kuva siitä, että käyttäjä on kiinnittänyt huomiota enemmän älypuhelimensa käsittelyyn, kun laite on ensin rikkoutunut käsittelystä johtuvista seikoista. Tämä voi viitata siihen, ettei käyttäjä ole ennen laitteen rikkoutumista käyttänyt esimerkiksi suojalasia tai -kuoria rikkoutumisen ehkäisemiseksi.

6.2 Langattomat yhteydet



Kuva 3 Asteikko: 1 ”erittäin turvattomaksi ja 5 ”erittäin turvalliseksi”

Käyttäjien tietoisuutta langattomien yhteyksien tietoturvariskeistä kartoitettiin kyselyn toisessa osiossa. Ensimmäisessä kysymyksessä kysyttiin, miten turvallisiksi suojaamattomat langattomat verkot koettiin. Kuvasta 3 huomaamme, miten yksikään kysymykseen vastanneista ei kokenut suojaamattomia langattomia verkkoja erittäin turvallisiksi. Suurin osa vastauksista painottui asteikon vaihtoehtoihin kaksi ja kolme, eli asteikon keskivaiheille ja sen alle. Tämä jakautuminen kertoo, että käyttäjillä on epäilyksiä suojaamattomia langattomia verkkoja kohtaan. Kukaan vastaajista ei kokenut suojaamattomia langattomia verkkoja erittäin turvallisiksi, mikä viittaa käyttäjien tietoisuuteen tietoturvariskeistä niiden käyttämisessä.



Kuva 4 Asteikko: 1 ”erittäin turvattomaksi ja 5 ”erittäin turvalliseksi”

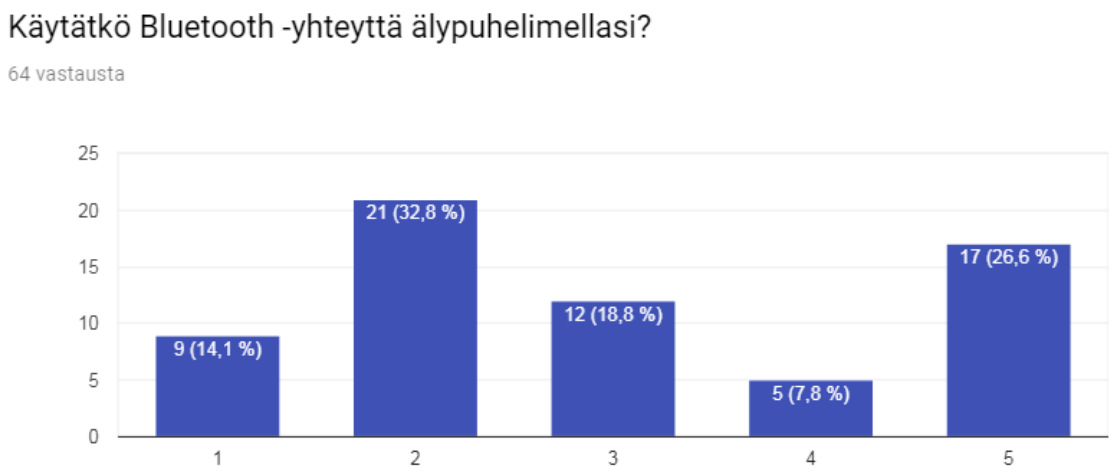
Kuvassa 4 esitetään vastauksien jakautuminen suojattujen langattomien verkkojen käyttöä koskevan kysymyksessä. Vastauksien jakaantuminen on lähes peilikuva siitä, miten suojaamattomia langattomia verkkoja koskevassa kysymykseksä kuvassa 3 oli. Vastauksien perusteella suurin osa käyttäjistä tunsi suojattujen langattomien verkkojen olevan melko turvallisia. Vain 10 vastaajista koki suojatut langattomat verkot erittäin turvallisiksi. Tämä voisi viittata siihen, että käyttäjät kokevat langattomissa verkoissa olevan mahdollinen tietoturvariski salasanasuojauksesta huolimatta.

Kuvista 3 ja 4 on erotettavissa, että yleinen käsitys vastaajien keskuudessa on se, että suojaamattomat langattomat verkot ovat turvattomimpia kuin suojatut langattomat verkot. Yksikään vastaajista ei kokenut suojaamattomia langattomia verkkoja erittäin turvallisiksi, mikä viittaa käyttäjien tietoon mahdollisista riskeistä, kun käytetään kaikille avoimia verkkoja.

Langattomien verkkojen asetuksista tiedustelevaan monivalintakysymykseen vastasi 63 vastaajista, eli lähes kaikki. Vastaajista 71% ilmoitti käyttävänsä pääsääntöisesti mobiilidataa internetyhteytenään. Julkisissa paikoissa käytettävissä olevista langattomista Wi-Fi-yhteyksistä salasanasuojatut verkot olivat suositumpia: salasanasuojattuja langattomia verkkoja käytti vastaajista 64%, kun suojaamattomia langattomia yhteyksiä ilmoitti käyttävänsä 35%. Vain 3% vastaajista ilmoitti älypuhelimensa liittyvän automaattisesti uusiin suojaamattomiin langattomiin verkkoihin, mutta 54% käyttäjistä vastasi laitteen yhdistävän automaattisesti jo tunnettuihin verkkoihin.

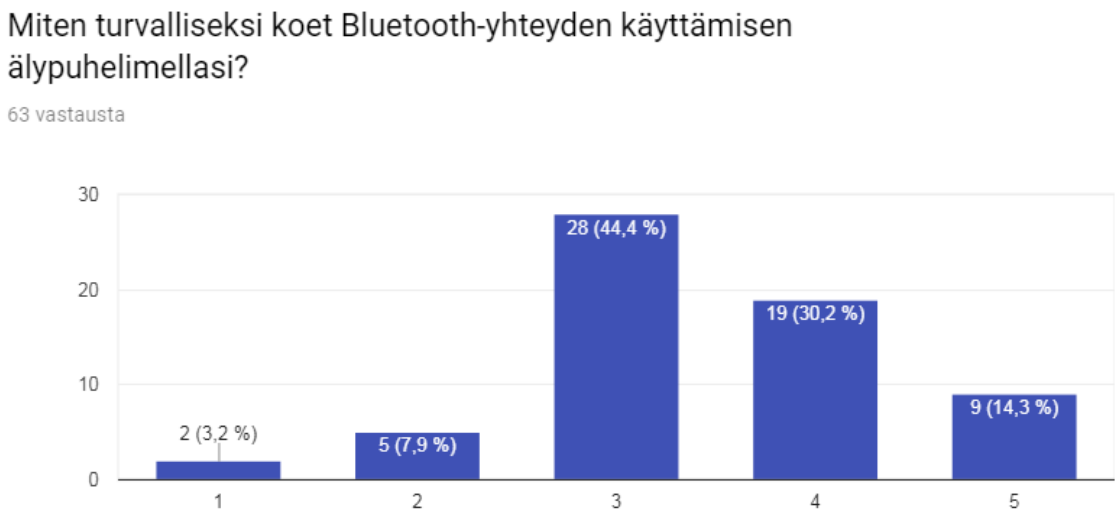
Aiempien kysymysten vastauksiin nähden vastaukset ovat linjassa toistensa kanssa. Suojaamattomia langattomia verkkoja käytetään vastaajien mukaan vähemmän kuin salasanasuojattuja verkkoja. Vastauksista voidaan myös arvioida, että käyttäjät tietävät langattomiin yhteyksiin sisältyvistä tietoturvariskeistä ainakin jonkin verran, sillä niin moni vastaajista suosii mobiilidatan tai suojattujen verkkojen käyttöä. Lisäksi pieni 3%:n osuus älypuhelimen automaattisesta langattomiin verkkoihin yhdistämisestä viittaa siihen, että käyttäjät katsovat ja valvovat, mihin ja millaisiin langattomiin verkkoihin liittyvät. Yksi vastaajista ilmoitti käyttävänsä VPN:ää, kun käyttää langattomia yhteyksiä muualla kuin luotetuissa verkoissa.

6.3 Bluetooth



Kuva 5 Asteikko: 1 ”en koskaan” ja 5 ”lähes päivittäin”

Bluetoothin käyttöä koskevaan kysymykseen olivat vastanneet kaikki kyselyyn osallistuneet. Yllä olevasta kuvasta 5 näkee, ettei vastauksien kesken ole selkeää jakoa siitä, käytetäänkö Bluetooth-yhteyttä vai ei. Tämä vaikuttaa olevan käyttäjäkohtainen mieltymys. 52 vastaajista vastasi monivalintakysymykseen älypuhelimen Bluetooth-asetuksista ja älypuhelimeen yhdistettävissä Bluetoothia käyttävistä laitteista. Näistä vastaajista 48% käyttää Bluetooth-kuulokkeita tai kaiuttimia, ja 42% käyttää Bluetoothia laitteiden väliseen tiedonsiirtoon tai synkronoitiin. Kaksi vastaajista ilmoitti Bluetooth-yhteyden olevan aina aktiivisena älypuhelimessa, mutta vain yksi vastaajista ilmoitti älypuhelimensa yhdistäneen vieraaseen tai väärään Bluetooth-verkkoon käyttäjän sitä haluamatta.



Kuva 6 Asteikko: 1 ”erittäin turvattomaksi ja 5 ”erittäin turvalliseksi”

Koska Bluetooth-yhteyttä käytetään kyselyn perusteella vaihtelevasti, ei vastauksista nouse esille erityisiä tietoturvariskejä käyttäjien kohdalla lukuunottamatta väärään Bluetooth-verkkoon yhdistämistä. Käyttäjillä ei vaikuta olevan niin tarkkaa käsitystä Bluetooth-yhteyksien tietoturvariskeistä, mitä langattomien verkkojen kohdalla oli nähtävissä vastauksien jakaantumisesta. Kuvasta 6 nähdään, miten käyttäjät kokevat Bluetoothin käytön, ja suurin osa vastaajista on turvallisuudentunteen osalta keskivaiheilla vastauksissaan. Tämä tukee päätelmää siitä, että käyttäjät eivät tiedä Bluetooth-yhteyksien tietoturvariskeistä ja kokevat sen keskimäärin turvalliseksi yhteystyypiksi.

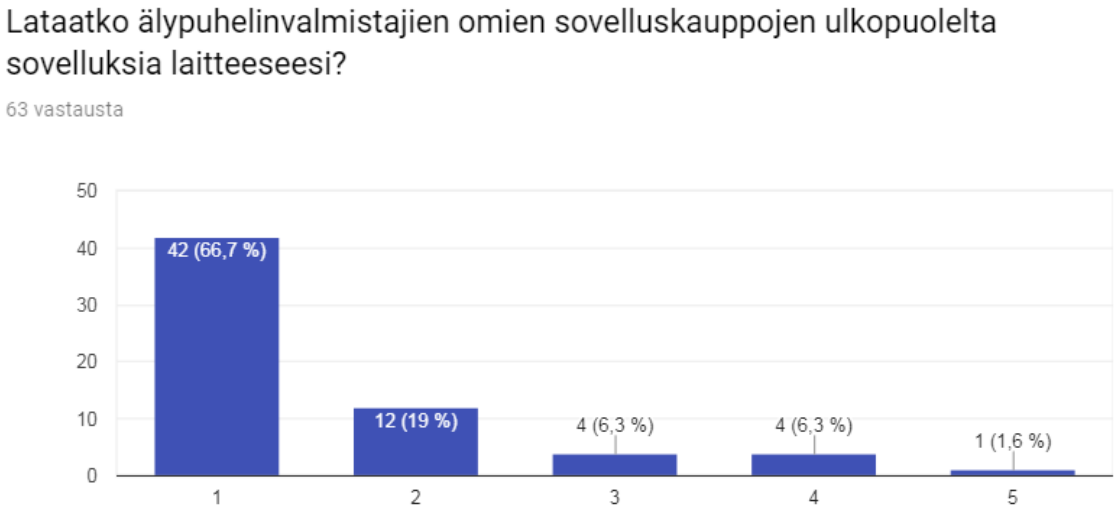
6.4 Near Field Communcation eli NFC

Kaikki kyselyyn vastanneet vastasivat kysymykseen siitä, ovatko he käyttäneet älypuhelimen lähimaksuominaisuutta. Näistä 83% ei ollut koskaan käyttänyt lähimaksua älypuhelimella. Vain 6% vastaajista ilmoitti, että käyttää usein lähimaksuominaisuutta. NFC-yhteyden käyttö mobiilimaksamisessa on Suomessa melko uutta, mikä voi selittää lähimaksuominaisuuden vähäistä käyttöä. Käyttäjät eivät välttämättä ole tutustuneet yhteystyyppiin, tai heillä saattaa olla älypuhelin, joka ei tue NFC-yhteyden käyttöä.

Kuva 7 Asteikko: 1 ”erittäin turvattomaksi ja 5 ”erittäin turvalliseksi”

Kuvassa 7 esitellyt vastaukset NFC-yhteyden turvallisuudentunteesta käyttäjien kesken nähdään, että vastaukset jakautuvat turvattomuuden puolelle. Käyttäjät näyttävät kokevan lähimaksun melko turvattomaksi, sillä suurin osa vastauksista sijoittuu asteikon keskimmäisen vaihtoehdon alapuolelle. Vastauksista ja kysymyksestä ei voida päätellä, tietävätkö käyttäjät yhteystyypin tietoturvariskeistä, eikä kysymyksessä esitelty muita käyttötarkoituksia NFC-yhteydelle. Käyttäjät kuitenkin vaikuttavat olevan tietoisia lähimaksun käyttömahdollisuudesta, sillä kaikki kyselyyn osallistuneet vastasivat kysymykseen.

6.5 Haittaohjelmat



Kuva 8 Asteikko: 1 "en koskaan" ja 5 "lähes aina"

Sovelluksien aiheuttamia ongelmia koskeva monivalintakysymys keräsi 59 vastausta, eli lähes kaikki vastasivat tähän. 80% näistä vastaajista oli kohdannut häiritsevää mainontaa, ja 60% oli huomannut sovelluksilla olevan erikoisia käyttöoikeuspyyntöjä. Sovelluksen poistamisessa ongelmia oli kohdannut 19% vastaajista, ja 45%:ssa vastauksista sovellus oli merkittävästi vähentänyt akunkestoa. 10% vastaajista oli kohdannut ongelmia ylimääräisten maksujen tai luottokorttitietojen kyselyn muodossa. Edellä kuvatut avoimet vastaukset, ja kuva 8:n kuvaama diagrammi sovellusten latauspaikoista tuntuvat olevan jopa hieman ristiriidassa toistensa kanssa. Laitevalmistajat toivovat käyttäjien käyttävän omia sovelluskauppoja, mutta vastausten mukaan myös näissä sovelluksissa on ollut mm. häiritseviä mainoksia ja erikoisia käyttöoikeuspyyntöjä. Voisi olla tutkimisen arvoista, millaisia kriteerejä eri sovelluskaupoilla on sovelluksilta, jotka sinne voidaan hyväksyä. Kyselyssä ei eritellä vastaajien älypuhelinten käyttöjärjestelmiä, joten emme voi arvioida eri valmistajien sovelluskauppojen eroja.

Sovellusten käyttöoikeuksia koskevaan kysymykseen avoimia vastauksia tuli 39:ltä vastaajalta. Vastauksissa yleisenä teemana olivat oikeudet, joita sovellus tarvitsee välttämättömiin, tarkoituksensa mukaisiin toimiin, ja sovelluksen on esitettävä käytännössä tämä tarve. Ylimääräiset sovelluksen toiminnasta riippumattomat oikeudet nähtiin turhiina. Esimerkkeinä epäselvistä oikeuspyynnöistä annettiin esimerkiksi taskulamppusovellus, joka vaati oikeuksia yhteystietoihin, mutta hyväksyttävistä kuvien ja kameran käyttöoikeus erilaisissa sosiaalisen median sovelluksissa. Ominaisuus sovellusten käyttöoikeuksien laajentamisen kysymisestä vaikuttaa vastauksien perusteella olevan käyttäjille hyvin tietoturvaa edistävä ominaisuus, ja käyttäjät osaavat tarkastella sovellusten käyttöoikeuksia.

31 vastaajista vastasi avoimeen kysymykseen siitä, miten he kuvailisivat ongelmia aiheuttaneita sovelluksia, ja nämä sovellukset vastaajien mukaan useimmiten olivat pelejä tai muita sovelluksia, jotka voi ladata sovelluskaupoista ilmaiseksi. Ongelmiksi kuvattiin myös jatkuva päivittämisen tarve, mainokset päivitysten jälkeen sekä suuri internetkaistan tai akun kulutus myös sovelluksen ollessa suljettuna. Vaikuttaa siltä, että käyttäjät ovat tietoisia haittaohjelmien riskeistä, ja ovat kohdanneet näitä jonkin verran. On kuitenkin kysymysten perusteella epäselvää, onko tietämys kertynyt kokemuksen kautta, vai muista lähteistä.

7 Päätelmät ja oma oppiminen

7.1 Teoriaosuus

Opinnäytetyön teoriaosuus on kattanut erilaisia tietoturvariskejä, joita älypuhelinta käyttäessä voi kohdata. Lisäksi opinnäytetyössä esitellään tapoja suojautua näiltä tietoturvariskeiltä yksinkertaisin keinoin. Lopputuloksena oli kooste yleisimmistä älypuhelinten tietoturvariskeistä.

Fyysisiin uhkiin valikoituivat esimerkiksi laitteen eri osien rikkoutuminen ja varkaudet, jotka molemmat voivat aiheuttaa merkittävää haittaa käyttäjälleen. Näihin liittyy riskejä niin tietoturvan kuin tiedon säilymisenkin osalta aina tietojen pysyvästä katoamisesta pieneen tai suurempaan taloudelliseen haittaan. Riskeiltä suojautuminen kaikessa yksinkertaisuudessaan kiteytyy laitteen huolelliseen käsittelyyn ja sen suojaamiseen mahdollisilta kolhuilta. Lisäksi on hyvä tietää oman älypuhelimen IMEI-numero, jotta sen käyttöä ja jälleenmyyntiä voidaan katoamisen tai varkauden yhteydessä rajoittaa.

Toinen pääluku teoriaosuudessa oli langattomat yhteydet. Näiden välttämättömyys ja yleisyys älypuhelinten käytössä olivat syy sille, miksi se päätyi pääotsikoksi. Luvussa käsiteltiin eri yhteystyyppien tietoturvallisuutta uhkien ja suojautumisen näkökulmasta. Nämä riskit sisältävät esimerkiksi mm. mies välissä -hyökkäyksen ja Bluetoothin osalta Denial of Service eli DoS -hyökkäyksen. Niiden tavoite voi olla salakuuntelu, tiedonsiirto tai laitteen käytön hidastaminen tai kokonaan sen estäminen. Salakuuntelun uhriksi on mahdollista joutua myös Near Field Communications eli NFC-yhteyttä käyttäessä. Tämä yhteystyyppi on varsin uusi, ja useimmille tunnettu käyttötarkoituksestaan mobiilimaksamisessa.

Suojautumiskeinoihin langattomien yhteyksien tapauksessa sisältyvät erityisesti älypuhelimen asetukset, joissa on hyvä kieltää laitteen automaattista verkkoihin yhdistämistä. Lisäksi on suotavaa käyttää vain tunnettuja salasanasuojattuja verkkoja, ja välttää suojaamattomia verkkoja julkisilla alueilla. Bluetoothin osalta tunnettujen laitteiden lista on hyvä pitää ajantasalla ja vain laitteissa, jotka käyttäjä tunnistaa itse. Lähiverkkoja turvallisemman mobiilidatan tai matkapuhelinverkon käyttö on Suomessa edullista ja kilpailukykyistä nopeuden suhteen, joten se on varteenotettava tietoturvallisempi vaihtoehto erityisesti tuntemattomille langattomille lähiverkoille.

Viimeinen teoriaosuuden pääluku oli haittaohjelmat. Luvussa käsitellään lyhyesti eri haittaohjelmatyyppejä: viruksia, troijalaisia ja matoja, joiden tavoite on nimensä

mukaisestikin aiheuttaa erilaista haittaa laitteen käyttäjälle esimerkiksi tietojen vakoilusta niiden levittämiseen. Lisäksi luvissa käsiteltiin ei-toivottuja sovelluksia (Potentially Unwanted Applications), jotka näyttävät esimerkiksi häiritseviä mainoksia tai, ohjaavat käyttäjän turvattomille verkkosivuille. Näiden haittaohjelmien ja ei-toivottujen sovellusten ehkäisyssä keskeisessä asemassa ovat käytetyt latauslähteet, ja onkin suositeltavaa käyttää vain laitevalmistajien omia sovelluskauppoja ja seurata käyttäjien arvioita sekä latausmääriä. Usein suosituimmat ja hyvät arviot saaneet sovellukset ovat myös ongelmattomia käyttää.

Lähteiden etsimisessä ongelmaksi muodostui se, miten uusi aihe älypuhelinten tietoturva on. Erilaisia artikkeleita löytyy jonkin verran, mutta vain hyvin harva tutkimus tai artikkeli tuo esille käyttäjän toimien seurauksia muutoin kuin sivulauseissa. Toisaalta kirjojen vähyys johdatti useiden erilaisten lähteiden äärelle ja sai aikaan useista eri lähteistä kootun teoriataustan käyttäjän ja tietoturvan näkökulmasta. Kuitenkin kirjojen vähyys on johtanut hyvin monien lähteiden käyttöön, jotta kirjojen vähyyttä on voitu kompensoida. Eri lähteillä olen myös tarkistanut ristiin lähteiden faktoja niin, että useammassa lähteessä on kerrottu teoria samantyylisesti faktojen varmistamiseksi.

Teoriaosuuden rakenteen ja sisällön suunnittelu oli yllättävän helppoa. Aihealue oli looginen jaettavaksi eri yläkäsitteisiin, ja siitä vähitellen muuttaa lähestymistä yksityiskohtaisemmaksi. Koska aihealue oli kohtalaisen laaja, ei yhtä osa-aluetta ole voitu käsitellä erityisen laajasti. Pyrin teoriaosuudessa tuomaan eri tietoturvariskejä kattavasti ja helposti lähestyttävässä muodossa esille.

7.2 Kyselytutkimus

Kyselyn suunnittelu ja toteutus oli melko mutkantonta. Sosiaalisessa mediassa kyselyn jakaminen osoittautui hyväksi vaihtoehdoksi, ja sillä vastauksia kertyi mukava määrä. Kyselyssä ei vaikuttanut olevan erityisiä ongelmia, mutta näin jälkeenpäin ajateltuna sitä olisi voinut hieman lyhentää. Vastausaktiivisuus laski hieman loppua kohden, mikä viittaa siihen, että kysely saattoi olla liian pitkä. Kysymysten muotoilu tuntui olevan vastaajille riittävän selkeä.

Oli mielenkiintoista, miten käyttäjät kyselyn perusteella tuntuvat useimmiten tunnistavan tietoturvariskejä päivittäisessä älypuhelimen käytössään, mutta eivät vältämättä tee erityisiä toimia niiden ehkäisemiseksi. Lisäksi käyttäjät eivät osanneet nimetä tietoturvauhkia, vaikka olivat niistä tietoisia. Lisäksi vastauksien perusteella joidenkin uhkien toteutuminen (esimerkiksi varkaus, rikkoutuminen) muutti usein älypuhelimen

käyttöä tietoturvallisempaan suuntaan. Vähiten käyttäjät tiesivät langattomien yhteyksien ja haittaohjelmien tuomista riskeistä. Haittaohjelmien aiheuttamat riskejä tunnistettiin, mutta kyselystä ja sen vastauksista ei voida päätellä, oppivatko käyttäjät kokemuksen kautta näistä riskeistä.

Langattomia verkkoja koskevan kyselyn osion myötä heräsi kysymys siitä, miten käyttäjät käyttävät langattomia verkkoja, ja luottavatko nämä julkisissa paikoissa sijaitseviin suojattuihin verkkoihin vain salasanan vuoksi? Salasana saattaa kuitenkin olla koko yhteyden käytössäoloajan sama, mikä lisää itsessään riskiä välimieshyökkäykselle tilanteessa, jossa salasanan on lähes julkinen kaikille verkon käyttäjille.

Bluetooth-yhteyksiä koskevasta osuudesta kyselystä jäi paljon lisäkysymyksiä auki: suhtautuvatko käyttäjät Bluetooth-yhteyteen kevyemmin ja huolettomammin kuin esimerkiksi langattomiin lähiverkkoihin? Vastaukset kyselyssä olivat Bluetooth-yhteyden kohdalla hajaantuneempia, mitä langattomien lähiverkkoyhteyksien kohdalla oli. Tämä voi viitata siihen, ettei käyttäjillä ole selkeää käsitystä tietoturvauhkista tai yhteyden erityispiirteistä. Onko käyttäjillä siis tietoa Bluetooth-yhteyden riskeistä? Miten tämä mahdollinen tietämys näkyy käytössä?

Haittaohjelmien yleisyydestä kertovat myös kyselyn tulokset. Sovelluskauppoihin hyväksyttävien sovellusten sisältämistä ongelmallisista mainoksista ja muista ongelmista voisi olla hyvä tehdä lisätutkimusta. Vaikuttavatko eri valmistajien sovelluskauppojen kriteerit sovellusten hyväksymisessä haittaohjelmien ja erityisesti ongelmallisten sovellusten määrään? Miten tietyn älypuhelinmallin tai -käyttöjärjestelmän yleisyys vaikuttaa haittaohjelmien määrään, ja suunnataanko tietylle käyttöjärjestelmälle erilaisia haittaohjelmia kuin muihin?

Tulokset olivat kokonaisuudessaan vähintäänkin mielenkiintoisia, ja jättävät useita uusia kysymyksiä jälkeensä. Miten esimerkiksi käyttäjät voisi saada huomioimaan tietoturvan paremmin? Miten tietoturvaa edistävät mekanismit saataisiin paremmin käyttäjien tietoisuuteen ja erityisesti käyttöön? Älypuhelinten yleistyminen ja teknologian kehittyminen tuo jatkossa varmasti lisää tietoturvauhkia ja -ongelmia jo tiedettyjen ja tiedostettujen tietoturvariskien lisäksi.

7.3 Oma oppiminen

Näinkin laaja projekti kuin opinnäytetyö vaatii aina hyvää projektinhallintaa, edistymisen seurantaa sekä omien työtapojen tuntemista. On myös tärkeää tehdä työ aiheesta, joka

on kiinnostava. Se oli mielenkiintoisempi mitä alunperin ajatellin, eikä opinnäytetyöprojektin aikana tullut ajatuksia aiheen vaihtamisesta tai muuttamisesta. Aiempien tietojen pohjalta työtä oli mukava tehdä, mutta työn aikana tuli opittua paljon lisää aihealueesta, erityisesti yksityiskohtia ja syventävää tietämystä erityisesti tietoturvan näkökulmasta.

Projektinhallintaa on koko opintojen ajan erityylisissä ja -kokoisissa projekteissa harjoiteltu, joten se itsessään ei ollut uutta. Usein kuitenkin kouluprojektit on tehty joko pareittain tai ryhmässä, mutta näin opinnäytetyön aikana se toisten oppilaiden tuki jää merkittävästi vähäisemmäksi ja korostaa itsenäistä projektinhallintaa. Opinnäytetyölle omistetun ajan käyttö vain opinnäytetyöhön osoittautui kaikkein haastavimmaksi projektinhallinnan osalta. Lisäksi usein työskentelyn aloitus usein venyi, vaikka kalenterista oli varattu aikaa opinnäytetyön tekemiselle. Muilta osin en nähnyt haasteita projektinhallinnassa, sillä aikataulussa pysymistä ja itse projektinhallintaa aina suunnittelusta varsinaiseen toteutukseen oli niin usein harjoiteltu opintojen ja töiden ohessa.

Kielellisesti en kokenut, että minulla olisi ollut ongelmia. Lähteiden kieli on pääsääntöisesti englanti, jota olen käyttänyt niin töissä kuin vapaa-ajallakin. Ongelmia toisinaan tuotti käsitteiden kääntäminen suomeksi. Osalle käsitteistä on vakiintuneet suomenkieliset termit, mutta osa on tulkinnanvaraisia kontekstista riippuen. Joissain kohdin lisäsin vielä sulkuihin englanninkielisen käsitteen selventämään sitä, mistä on kyse. Kaikenkaikkiaan opinnäytetyö edistyi yllättävän ongelmattomasti, ja työtahti pysyi suhteellisen tasaisena.

8 Lähdeluettelo

Anderson, J., Nampalli, J., Nykamp, D., Speed, T. 2013. Mobile Security: How to secure, privatize and recover your devices. Packt Publishing

Athow, D. 2017. What is VPN? Luettavissa: https://www.techradar.com/news/what-is-a-vpn Luettu: 11.5.2018

Chen, L., Padgette, J., Scarfone, K. 2012. Guide to Bluetooth Security. Luettavissa: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf. Luettu: 21.3.2018

F-Secure. 2013. Mobile Threat Report Q3 2013. Luettavissa: https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q3_2013.pdf Luettu: 15.3.2018

Gritzalis, D., Mylonas, A., Theoharidou, M. A Risk Assesment Method for Smartphones. Luettavissa: https://pdfs.semanticscholar.org/03f4/b494d47b402d6e84decbf4e96694ad94d5ef.pdf Luettu 15.3.2018

Haataja, K. 2009. Security Threaths and Countermeasures in Bluetooth-Enabled Systems. Luettavissa: http://epublications.uef.fi/pub/urn_isbn_978-951-27-0111-7/urn_isbn_978-951-27-0111-7.pdf Luettu 21.3.2018

Imei.info. 2018. What is imei number? Luettavissa: http://www.imei.info/faq-what-is-IMEI/ Luettu: 16.3.2018

Imei.info. 2018. What is phone blacklist? Luettavissa: http://www.imei.info/faq-what-is-phone-blacklist/ Luettu: 16.3.2018

Javaid, Q., Kamran, M., Shah, M., Zaidi, S., Zhang, S. 2016. A Survey on Security for Smartphone Device. International Journal of Advanced Computer Science and Applications, 7, 4. Luettu 7.3.2018

Kasperky Lab. 2016. Mobile Malware Evolution 2016. Luettavissa: https://securelist.com/files/2017/02/Mobile_report_2016.pdf Luettu: 7.3.2018

Mooney, P. 2013. Effective Physical Security of a Mobile Device Luettavissa: http://www.infosectoday.com/Articles/Physical_Security_Mobile_Device.htm. Luettu 15.3.2018

Paganini, P. 2012. NFC, business opportunities, security and privacy issues. Luettavissa: http://securityaffairs.co/wordpress/5090/hacking/nfc-business-opportunities-security-and-privacy-issues.html. Luettu. 10.4.2018.

Paganini, P. 2013. Nier Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema. Luettavissa: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/#gref Luettu: 10.4.2018

Radio-Electronics.com. NFC Security. Luettavissa: http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php Luettu: 4.5.2018

Schmidt, A. 2011. Detection of Smartphone Malware. Luettavissa: https://depositonce.tu-berlin.de/bitstream/11303/3182/1/Dokument_8.pdf Luettu 20.3.2018

Srikanth, R. 2012. Mobile Malware Evolution, Detection and Defence. Luettavissa: http://blogs.ubc.ca/computersecurity/files/2012/04/SRamu_EECE572_SurveyPaper-SrikanthRamu.pdf Luettu: 10.4.2018

Statista.com. 2018. Global mobile OS market share in sales to end users from 1st quarter 2009 to 2nd quarter 2017. Luettavissa: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. Luettu 7.3.2018

Taanila, A. 2014. Luettavissa: https://tilastoapu.wordpress.com/2012/03/13/kyselytutkimuksen-luotettavuus/ Luettu: 20.4.2018

Triggs, R. 2018. What is NFC & how does it work? Luettavissa: https://www.androidauthority.com/what-is-nfc-270730/. Luettu: 10.4.2018

Vahtiohje 2008. Valtionhallinnon tietoturvasanasto. Luettavissa: https://www.vahtiohje.fi/web/guest/maaritelmat-t Luettu: 14.3.2018

Verkkokauppa.com. 2018. Luettavissa: https://www.verkkokauppa.com/fi/catalog/660b/Kotelot-ja-suojakuoret/products/1 Luettu: 15.3.2018

Viestintävirasto. 2015. Suojaamattoman WLAN:n käyttö. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409171602.html Luettu: 15.3.2018

9 Liitteet

9.1 Älypuhelimen käytettävyys ja tietoturva -kysely

9.1.1 Perustiedot

Ikä (monivalinta, jossa voi valita yhden vaihtoehdon)

- Alle 18
- 18-25
- 26-40
- yli 40

Sukupuoli (monivalinta, jossa voi valita yhden vaihtoehdon)

- Nainen
- Mies
- Muu/en halua kertoa

Millaisia tietoturvariskejä, tai -ongelmia olet kokenut, huomannut tai ehkäissyt käyttäessäsi älypuhelinta? Millaisia kokemuksia sinulla on tietoturvaan ja älypuhelimiin liittyen? (avoin vastausteksti)

9.1.2 Laitteen fyysinen käsittely

Käytätkö laitteessasi jotakin lukitusta (esim. pääsykoodi, sormenjälki- tai kasvontunnistus)? (monivalinta, jossa voi valita yhden vaihtoehdon)

- Kyllä
- Ei

Onko älypuhelimesi kadonnut tai rikkoutunut, ja jos on, miten tai mitkä osat laitteesta? (monivalinta, jossa voi valita usean vaihtoehdon ja lisätä vastauksen ”muu”)

- Näytön rikkoutuminen putoamisen tai kolhujen johdosta
- Laite on kadonnut (esim. jäänyt johonkin, tippunut)
- Vesivahinko, jonka seurauksena laite on käyttökelvoton
- Kuuloke- tai latausliitännät
- Virta-, äänenvoimakkuus tai koti-painikkeet
- Laitteen muiden osien rikkoutuminen (esim. akku)
- Laite on varastettu
- Muu

Koetko laitteen rikkoutumisen tai katoamisen johtuneen suoraan tai epäsuorasti sen käsittelytavasta? (Asteikko yhdestä viiteen, jossa yksi on ”en lainkaan”, ja viisi on ”erittäin varmasti”)

Mikäli laitteesi on kadonnut, varastettu tai rikoutunut, niin mitä haittaa siitä seurasi (esimerkiksi tiedon menetys, taloudelliset haitat korjauksesta tai uudesta laitteesta)? (avoin vastausteksti)

9.1.3 Langattomat yhteydet

Miten turvalliseksi koet suojaamattomien langattomien verkkojen käytön älypuhelimellasi? (Asteikko yhdestä viiteen, jossa yksi on ”erittäin turvattomaksi” ja viisi on ”erittäin turvalliseksi”)

Miten turvalliseksi koet (salasana)suojattujen langattomien verkkojen käytön älypuhelimellasi? (Asteikko yhdestä viiteen, jossa yksi on ”erittäin turvattomaksi” ja viisi on ”erittäin turvalliseksi”)

Mitkä kohdat pätevät laitteesi Wi-Fi -yhteyksienasetuksiin ja yhteyksien käyttöön koti- tai ulkomailla? (monivalinta, jossa voi valita useamman vaihtoehdon tai lisätä vastauksen ”muu”)

- Käytän suojaamattomia langattomia verkkoja esimerkiksi kahviloissa tai hotelleissa
- Käytän (salasana)suojattuja langattomia verkkoja esimerkiksi kahviloissa tai hotelleissa
- Älypuhelimeni liittyy automaattisesti langattomiin verkkoihin, joihin se on ollut yhdistettynä aiemmin
- Pääsääntöisesti käytän mobiilidataa
- Langattomien verkkojen etsintä on laitteessa aina tai lähes aina aktiivinen (laite voi esimerkiksi ehdottaa saatavilla olevia langattomia verkkoja)
- Muu

Käytätkö Bluetooth -yhteyttä älypuhelimellasi? (Asteikko yhdestä viiteen, jossa yksi on ”en koskaan”, ja viisi on ”lähes päivittäin”)

Miten turvalliseksi koet Bluetooth-yhteyden käyttämisen älypuhelimellasi? (Asteikko yhdestä viiteen, jossa yksi on ”erittäin turvattomaksi”, ja viisi on ”erittäin turvalliseksi”)

Mikäli käytät Bluetooth-yhteyksiä laitteessasi, millaiset asetukset tai laitteet ovat käytössä älypuhelimessasi? (monivalinta, jossa voi valita useamman vaihtoehdon tai lisätä vastauksen ”muu”)

Bluetooth-kuulokkeet

- Laitteen synkronointi toisen laitteen kanssa Bluetoothia käyttäen (esim. varmuuskopiointi, tiedon siirto laitteiden välillä)
- Bluetooth on laitteessa lähes aina tai aina aktiivinen/päällä
- Bluetooth-yhteys hakee automaattisesti uusia laitteita, joihin yhdistää

- Laite liittyy automaattisesti samaan Bluetooth-verkkoon aiemmin yhdistettyjen laitteiden (esim. kuulokkeet) kanssa
- Älypuhelin on yhdistänyt ei-toivottuun Bluetooth-verkkoon (esimerkiksi muiden henkilöiden laitteet)

Oletko käyttänyt älypuhelimen lähimaksuominaisuutta?
(Asteikko yhdestä viiteen, jossa yksi on ”en lainkaan”, ja viisi on ”erittäin varmasti”)

Miten turvalliseksi koet lähimaksuominaisuuden älypuhelimessasi? (Asteikko yhdestä viiteen, jossa yksi on ”erittäin turvattomaksi” ja viisi on ”erittäin turvalliseksi”)

9.1.4 Haittaohjelmat

Lataatko älypuhelinvalmistajien omien sovelluskauppojen ulkopuolelta sovelluksia laitteesesi? (Asteikko yhdestä viiteen, jossa yksi on ”en koskaan” ja viisi ”lähes aina”)

Millaisia käyttöoikeuksia mielestäsi muihin sovelluksiin ja puhelimen tietoihin ladatuilla sovelluksilla saa olla? (avoin vastausteksti)

Millaisia ongelmia olet kohdannut sovelluksien käytössä? (monivalinta, jossa voi valita useamman vaihtoehdon tai lisätä vastauksen ”muu”)

- Häiritsevä mainonta (ponnahdusikkunat, ilmoitukset yms.)
- Ongelmia sovelluksen poistamisessa
- Erikoisia käyttöoikeuspyyntyöjä esimerkiksi osoitekirjaan tai viesteihin
- Keskivertoa suurempi akunkulutus myös sovelluksen ollessa suljettuna
- Luottokorttitietojen tai muiden maksutietojen kysely tai ylimääräiset maksut
- Muu

Miten kuvailisit sovelluksia, jotka ovat aiheuttaneet ongelmia käytössä? (avoin vastausteksti)