Tampereen yliopisto

Sanni-Sisko Onkalo

TIETOTURVALLISUUS JA YKSITYISYYS ÄLYPUHELIMILLA

Ihmisten riskikäsitykset ja ennaltaehkäisevä toiminta

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Joulukuu 2020

TIIVISTELMÄ

Sanni-Sisko Onkalo: Tietoturvallisuus ja yksityisyys älypuhelimilla : Ihmisten riskikäsitykset ja ennaltaehkäisevä toiminta
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Joulukuu 2020

Älypuhelinten käytön lisääntyessä myös niihin kohdistuvat tietoturvariskit lisääntyvät. Yksilön kannalta tietoturvallisuuden edistämisen edellytyksenä ovat ihmisen omat käsitykset ja tietoisuus asiasta. Tämän tutkielman tarkoituksena on selvittää, millaisia käsityksiä ihmisillä on tietoturvallisuudesta ja yksityisyydestä älypuhelimilla sekä sitä, miten nämä käsitykset vaikuttavat ihmisten toimintaan. Sen lisäksi tutkielmassa pohditaan syitä käsityksille sekä käsitysten ja toiminnan suhteelle.

Tutkielma toteutettiin kirjallisuuskatsauksena. Aineisto kerättiin Andorin, IEEE:n ja ScienceDirectin tietokannoista. Kirjallisuuskatsaukseen valikoitiin mukaan julkaisuja vain viimeisen kuuden vuoden ajalta, sillä digitalisaation edetessä ihmisten käsitykset ja toiminta voivat muuttua nopeasti.

Kirjallisuuskatsauksen tulokset osoittavat, että ihmiset ovat yleisesti tietoisia termistä tietoturvallisuus ja ymmärtävät, että älypuhelinten käyttö voi altistaa heidät erilaisille tietoturvariskeille. Suurimpina riskeinä nähtiin yksityisyyttä uhkaavat riskit, kuten identiteettivarkaus. Ihmisten käsitykset eivät kuitenkaan täysin vastaa todellisia riskejä. Lisäksi tulokset osoittavat, että ihmiset suorittavat jonkin verran ennaltaehkäiseviä toimia riskien välttämiseksi. Näytönlukitus suojakoodin avulla todettiin yleisemmäksi toimeksi tietoturvallisuuden edistämiseksi. Näytönlukitusta lukuun ottamatta toimet ovat kuitenkin usein riittämättömiä, jonka vuoksi käsityksissä ja toimissa voidaan sanoa olevan ristiriitaisuutta. Toisin sanoen, vaikka tietoturvallisuutta ja yksityisyyttä pidettiin tärkeänä, eivät käsitykset heijastuneet täysin toimintaan. Tämä ristiriita käsityksissä ja toiminnassa on osa laajempaa yksityisyyden paradoksin ilmiötä.

Tutkielma antaa aihetta tietoturvallisuustietoisuuden lisäämiseen käyttäjien keskuudessa. Lisäksi turvallisuus- ja yksityisyysasetukset olisi syytä tehdä helpommiksi käyttää, ja oletusasetusten tulisi olla nykyistä turvallisempia.

Avainsanat: tietoturvallisuus, yksityisyys, älypuhelimet, käsitykset, yksityisyyden paradoksi

Sisällysluettelo

1 Johdanto

Älypuhelimista on tullut suuri osa ihmisten joka päiväistä elämää. Käytön lisääntyessä myös niihin liittyvät tietoturvariskit ja yksityisyyden suojan riskit lisääntyvät. Älypuhelimet pitävät sisällään suuren määrän henkilökohtaista dataa (Furini et al., 2020), jonka vuoksi ihmisten tulisi suojata laitteensa asianmukaisilla tietoturva-asetuksilla. Tietoturvallisuuden ketjussa heikoin lenkki on inhimillinen virhe (Sasse et al., 2001), joten ihmisten toiminnalla on suuri merkitys. Tässä tutkielmassa tarkastelen ihmisten käsityksiä tietoturvallisuudesta ja yksityisyydestä älypuhelimilla sekä sitä, miten nämä käsitykset vaikuttavat ihmisten toimintaan.

Tietoturvallisuuden edistämisen edellytyksenä yksilön kannalta on käyttäjän käsitykset ja tietoisuus. Jos tietoturvauhilta suojautumista ei pidetä tärkeänä, ei sen eteen luultavasti tehdä tarpeeksi tarvittavia toimenpiteitä. Sen vuoksi on oleellista tutkia nimenomaan käsityksiä ja tietoisuuden tasoa. Toisaalta käyttäjän tietoisuus asian tärkeydestä ei välttämättä takaa muutosta toteutuneessa toiminnassa, jonka vuoksi on tärkeää tutkia myös tietoisuuden ja toiminnan yhteyttä.

Tietoturvallisuuden aihepiiriin nivoutuu tiukasti yhteen yksityisyyden suojaan liittyvät kysymykset. Puhuttaessa yksilöä uhkaavasta tietoturvariskistä, on kyse usein myös yksityisyyden suojaan kohdistuvasta riskistä. Tietoturvan voidaankin ajatella olevan yksi tietosuojan toteuttamisen keino (Morton & Sasse, 2012). Tämän vuoksi käsittelen tutkielmassani ihmisten käsityksiä tietoturvallisuuden lisäksi myös yksityisyydestä ja tietosuojasta. Näin ollen pyrin tutkielmassani vastaamaan seuraaviin kysymyksiin:

1. Miten ihmiset käsittävät älypuhelinten käyttöön liittyvät tietoturvan ja yksityisyyden suojan riskit?
2. Millä tavalla käsitykset vaikuttavat ihmisten toimintaan laitteiden suojaamiseksi?

Toteutin tutkielman kirjallisuuskatsauksena. Valitsin kirjallisuuskatsaukseeni mukaan julkaisuja vain viimeisen kuuden vuoden ajalta, lukuun ottamatta muutamia peruslähteitä, sillä digitalisaation edetessä ihmisten käsitykset ja toiminta voivat muuttua nopeasti (Breitinger et al., 2020). Aineiston keräsin Andorin, IEEE:n ja ScienceDirectin tietokannoista käyttäen erilaisia yhdistelmiä seuraavista hakusanoista:

- tietoturvallisuus (*engl. cybersecurity* tai *cyber security*),
- yksityisyys (*engl. privacy*),
- älypuhelimet (*engl. smartphones*),
- käsitykset (*engl. perceptions*),
- tietoisuus (*engl. awareness*),
- ennaltaehkäisevä toiminta (*engl. precautionary behaviour*)
- yksityisyyden paradoksi (*engl. privacy paradox*),

- tietosuoja (*engl. data protection* tai *data privacy*),
- yksityisyyden suoja (*engl. privacy protection*).

Yleisesti ihmisten tietoisuuden tason voi sanoa olevan kohtuullisen hyvä. Ihmiset ovat tietoisia termistä tietoturvallisuus ja ymmärtävät, että älypuhelinten käyttö voi altistaa heidät erilaisille tietoturvariskeille. Suurimpana riskinä nähdään erilaiset sosiaaliset ja yksityisyyttä uhkaavat riskit. Ihmisten käsitykset eivät kuitenkaan aina vastaa todellisia riskejä.

Hyvä tietoisuuden taso ei täysin heijastu ihmisten toimintaan, sillä ihmisten käyttämät ennaltaehkäisevät toimenpiteet ovat usein yksinkertaisia ja riittämättömiä. Näin ollen käsityksissä ja toiminnassa on havaittavissa ristiriita, jota kutsutaan myös yksityisyyden paradoksiksi. Yleisin syy ristiriitaisuudelle on tiedon puute, jonka vuoksi tietoisuuden lisääminen koulutuksen avulla olisi tärkeää.

Luvussa 2 käsittelen ihmisten käsityksiä tietoturvariskeistä ja yksityisyyden suojan riskeistä. Kerron ensin lyhyesti riskikäsityksen määritelmän. Sen jälkeen esittelen, millaisia tietoturvaan ja yksityisyyteen liittyviä riskejä yksilö kohtaa älypuhelinta käyttäessään. Lopuksi käsittelen sitä, miten ihmiset käsittävät nämä riskit. Luvussa 3 käsittelen ihmisten ennaltaehkäiseviä toimenpiteitä tietoturvaa ja yksityisyyttä uhkaavia riskejä vastaan. Pohdin myös toimenpiteiden suhdetta käsityksiin ja mahdollisia syitä toimenpiteiden puuttumiselle. Luku 4 on keskustelu, jossa pohdin kirjallisuuskatsauksen tuloksia. Viimeisenä lukuna on yhteenveto tutkielman tuloksista.

2 Riskikäsitykset liittyen tietoturvallisuuteen ja yksityisyyteen

2.1 Riskikäsitykset

Riskikäsitys (*engl. risk perception*) on ihmisen uskomus mahdollisesta vahingosta tai menetysmahdollisuudesta. Se on subjektiivinen arvio, jonka ihminen tekee riskin ominaisuuksista ja vakavuudesta. (Darker, 2013)

Käsitteestä *risk perception* käytetään lähteestä riippuen erilaisia suomennoksia, esimerkiksi *riskikäsitys*, *riskin kokeminen* ja *riskien havaitseminen*. Näistä yleisin lienee suomennos *riskikäsitys*, jota myös tässä tutkielmassa käytän.

Ihmisten riskikäsityksiin vaikuttavat monenlaiset tekijät. Riskin arvioinnin voidaan katsoa olevan hyötyjen ja haittojen välillä punnitsemista, jossa riski otetaan silloin, kun hyödyt ovat suuremmat kuin haitat (van Schaik et al., 2017). Tällainen malli olettaa ihmisen rationaalisena päätöksentekijänä, jolla on saatavillaan kaikki päätöksen tekoon tarvittava tieto.

Toisaalta tällaisen rationaalisen pohdinnan lisäksi ihmisen päätöksentekoon vaikuttaa myös suuri määrä erilaisia ihmisen kognitioon liittyviä asioita, kuten tunnereaktiot ja kognitiiviset harhat. Kognitiivinen harha (*engl. cognitive bias*) on psykologian käsite, jolla

tarkoitetaan ihmisen tapaa painottaa tulkintojaan ja havaintojaan tietyllä tavoin, johtaen usein virheellisiin arviointeihin. (Gerber et al., 2018)

2.2 Tietoturvariskit

Tietoturva jaetaan perinteisessä tiedon arvoon perustuvassa määritelmässä kolmeen eri osa-alueeseen: luottamuksellisuuteen, eheyteen ja saatavuuteen. Luottamuksellisuudella (*engl. confidentiality*) tarkoitetaan tiedon olevan vain sellaisten osapuolten saatavissa, joilla on siihen oikeus. Eheys (*engl. integrity*) viittaa tiedon oikeellisuuteen. Tiedon täytyy säilyä luotettavana, oikeana ja ajantasaisena, eivätkä tiedot saa muuttua tai kadota laitteisto- tai ohjelmistovikojen seurauksena. Saatavuudella (*engl. availability*) tarkoitetaan sitä, että järjestelmän tiedot ja palvelut ovat niihin oikeutettujen henkilöiden saatavilla silloin, kun niitä tarvitaan. (Hakala et al., 2006)

Älypuhelinta käyttäessään ihminen altistaa itsensä erilaisille tietoturvariskeille. Tällaisia riskejä ovat muun muassa tietovuoto puhelimen varkauden tai katoamisen seurauksena, suojaamattomat julkiset verkot, tietojenkalastelu, sosiaalinen manipulointi, identiteettivarkaus ja haittaohjelmat.

Tietovuoto varkauden tai katoamisen seurauksena on yksi älypuhelimiin kohdistuva tietoturvariski. Älypuhelimet ovat sekä arvokkaita että pienikokoisia, jonka vuoksi ne ovat alttiita tällaisille tapahtumille. Varastetun tai kadonneen puhelimen kautta hyökkääjä voi päästä käsiksi puhelimen omistajan henkilötietoihin. Tällaisen tietovuodon (*engl. data leakage*) riski kasvaa merkittävästi, jos puhelimeen ei ole asetettu suojakoodia tai biometristä lukitusta, kuten sormenjälkeä. (Hogben & Dekker, 2010)

Julkisiin verkkoihin liittyminen aiheuttaa erilaisia tietoturvan ja yksityisyyden suojan riskejä. Julkisen verkon kautta siirretty suojaamaton tieto voi päätyä rikollisten esimerkiksi mies välissä -hyökkäyksen kautta (Aime et al., 2007). Mies välissä -hyökkäyksessä (*engl. man-in-the-middle attack*) hyökkääjä asettaa itsensä julkisen verkon ja siihen yhdistetyn laitteen väliin siten, että osapuolet luulevat kommunikoivansa toistensa kanssa (ENISA, 2020) ja täten verkkoon yhdistetyn laitteen sisältämiä henkilötietoja voi päätyä rikollisen käsiin.

Tietojenkalastelulla (*engl. phising*) tarkoitetaan toimintaa, jossa hyökkääjä pyrkii saamaan tietoa hyökkäyksen kohteesta. Kalasteltavia tietoja voivat olla esimerkiksi salasana, kotiosoite, puhelinnumero tai maksukortin tiedot. Tietojenkalastelua tapahtuu esimerkiksi massasähköposteilla, tekstiviesteillä, tiedonkeruusivuilla ja sosiaalisessa mediassa. Kalasteluviestissä hyökkääjä pyrkii esiintymään tahona, johon uhri luottaa, kuten polii-

sina, pankkina tai kollegana. Tavoite on saada uhri uskomaan, että häneltä tarvitaan jotain. Viestiin on usein liitetty linkki tiedonkeruusivustolle, joka on naamioitu näyttämään identtiseltä hyökkääjän esittämän tahon oikean nettisivuston kanssa. (ENISA, 2020)

Sosiaalinen manipulointi (*engl. social engineering*) on toimintaa, jossa hyökkääjä pyrkii uhriaan harhauttamalla saamaan hänet tekemään asioita, jotka eivät ole uhrin oman edun mukaisia. Hyökkääjä saattaa esimerkiksi tavoitella uhrin hallussa olevia luottamuksellisia tietoja tai pyytää uhria lähettämään rahaa. Sosiaalista manipulointia esiintyy esimerkiksi kalasteluviesteissä. (ENISA, 2020)

Identiteettivarkaudella (*engl. identity theft*) tarkoitetaan toisen henkilön henkilötietojen oikeudetonta käyttöä. Oikeudeton käyttö voi tarkoittaa toisena henkilönä esiintymistä esimerkiksi sosiaalisessa mediassa tai toisen henkilön nimissä tehtyä lainaa tai kauppaa. Rikoksen uhrille identiteettivarkaudesta voi olla vakavia sosiaalisia, taloudellisia ja henkisiä vaikutuksia. Hyökkääjä voi käyttää henkilötietojen hankkimiseen esimerkiksi sosiaalisen manipuloinnin tai kalastelun keinoja.

Haittaohjelmat (*engl. malware*) ovat ohjelmia, jotka suorittavat uhrin laitteella ei-toivottuja toimintoja, kuten vakoilua tai tiedostojen tuhoamista, tai mahdollistavat oikeudettoman henkilön pääsyn laitteelle. Haittaohjelmat leviävät useimmiten älypuhelimelle ladattavien sovellusten kautta, mutta ne voivat levitä myös muun muassa sähköpostien liitetiedostoissa. (ENISA, 2020)

2.3 Yksityisyyden suojan riskit

Yksityisyys on yksi ihmisen perusoikeuksista. Yksi varhaisimmista määritelmistä yksityisyydelle on ”oikeus tulla jätetyksi yksin” (Warren & Brandeis, 1890).

Yksityisyyden pohjimmainen määritelmä ei ole muuttunut, mutta se on saanut lisää ulottuvuuksia. ATK-sanakirja (2020) määrittelee yksityisyyden luonnollisen henkilön oikeudeksi tai käytännön mahdollisuudeksi suojautua ulkopuoliselta puuttumiselta sekä määrätä itseään koskevien henkilötietojen käytöstä.

Nykypäivän digitalisoituneessa maailmassa yksityisyyden ylläpitäminen käy yhä vaikeammaksi kyberympäristön asettaessa yksityisyydelle uudenlaisia haasteita. Yhteiskunnan erilaisia palveluita käyttäessä henkilötietojen jakamiselta välttyminen on lähes mahdotonta. Henkilötietoja on tallennettuna moniin erilaisiin palveluihin, jonka vuoksi yksityishenkilön on vaikea hallita omien tietojen käyttöä ja näin ollen omaa yksityisyyttään. Kyberkontekstissa yksityisyyden määritelmästä korostuukin oikeus ja käytännön mahdollisuus määrätä henkilötietojen käytöstä.

Luonnollisen henkilön yksityisyyttä kyberympäristössä turvataan tietosuojalla (*engl. data protection*). Suomessa tietosuoja on perustuslain takaama perusoikeus, joka turvataan tietosuojalailla ja sitä täydentävällä EU:n yleisellä tietosuoja-asetuksella. Tietosuojalaki takaa jokaiselle oikeuden tietää, mitä henkilötietoja itsestä on tallennettu, kuka on tietoja hallitseva rekisterinpitäjä ja mihin tietoja käytetään. Henkilötietoja käsiteltäessä on noudatettava laissa määriteltyjä tietosuojaperiaatteita. Tietosuojaperiaatteiden mukaan henkilötietoja on käsiteltävä asianmukaisesti ja asianomaisen kannalta läpinäkyvästi. Asianmukaisuudella tarkoitetaan sitä, että kerättyjä tietoja käytetään vain ennalta määriteltyyn tarkoitukseen. Tietoja sallitaan kerättävän vain tiettyä tarkoitusta varten ja ainoastaan tarpeellinen määrä. Lisäksi tietoja on säilytettävä vain niin kauan, kuin on tarpeellista. (Tietosuojavaltuutettu, 2020)

Erilaisille tietoturvariskeille altistuessaan ihminen altistaa itsensä väistämättä myös yksityisyyttä uhkaaville riskeille. Erityisesti älypuhelimien kontekstissa yksityisyys on uhattuna, koska älypuhelimet pitävät usein sisällään suuren määrän henkilökohtaista dataa käyttäjästään (Furini et al., 2020). Lähes kaikkien edellä mainittujen tietoturvariskien voidaankin sanoa olevan myös yksityisyyden suojan riskejä. Esimerkkinä näistä haittaohjelma, jolla voi olla pääsy vaikkapa käyttäjän puhelinnumeroon, tarkkaan sijaintiin tai muihin henkilötietoihin, vaikka mitään näistä ei tarvittaisi sovelluksen toimintaan (Furini et al., 2020).

Toisaalta myös ihmisten yhteinen käsitys yksityisyyden merkityksestä ja halukkuus jakaa tietoa internetissä vaikuttaa olevan muuttunut viime vuosina. Muutama vuosi sitten ihmiset epäröivät käyttää internetissä edes omaa nimeään, kun nykyisin sosiaalisessa mediassa saatetaan jakaa koko nimen lisäksi hyvinkin yksityiskohtaisia henkilötietoja vapaaehtoisesti. Myös tällainen tietojen jakaminen asettaa yksityisyyden uhatuksi.

2.4 Käsitykset tietoturvariskeistä ja yksityisyydestä

Yleisesti ihmiset ovat tietoisia siitä, että älypuhelinten käyttö altistaa heidät erilaisille tietoturvan ja yksityisyyden suojan riskeille (Bhatnagar & Pry, 2020; Parker et al., 2015; Zwilling et al., 2020). Esimerkiksi Sarathchandran ja muiden (2016) tutkimuksessa suurin osa vastaajista osasi selittää useimpia tietoturvallisuuteen liittyviä termejä, kuten *identiteettivarkaus*, *haittaohjelmat* ja *kalastelu*. Vastaavasti Bhatnagar ja muut (2020) raportoivat ihmisten osaavan antaa hyviä esimerkkejä erilaisista yksityisyyteen kohdistuvista riskeistä. Yleisesti tietoisuuden tason voi siis sanoa olevan suhteellisen hyvä.

Suurimpina riskeinä nähtiin erilaiset sosiaaliset ja yksityisyyttä uhkaavat riskit. Esimerkiksi Bhatnagarin ja Pryn (2020) mukaan 80 % tutkimukseen osallistuneista koki yksityisyyden tärkeäksi tai erittäin tärkeäksi. Niin ikään Furini ja muut (2020) raportoivat suurimman osan ihmisistä pitävän yksityisyyttä tärkeänä älypuhelinta käyttäessä. Huomattavaa on myös se, että kukaan vastaajista ei valinnut yksityisyyden tärkeydelle vaih-

toehtoa ”ei yhtään”, jokainen vastaajista siis antoi yksityisyydelle edes jonkin verran painoarvoa (Furini et al., 2020). Yksityisyyden tärkeänä pitämistä korostaa myös se, että vertaillessa eri tietoturvan ja yksityisyyden suojan riskejä identiteettivarkaus koettiin suurimmaksi yksittäiseksi riskiksi (Sarathchandra et al., 2016; van Schaik et al., 2017). Identiteettivarkauden lisäksi muita suureksi koettuja riskejä olivat sosiaalinen manipulointi (van Schaik et al., 2017), sekä yksityisyyden loukkaukset ja tietojen menetys (Zwilling et al., 2020). Vähemmän uhkaaviksi koettiin erilaiset teknisemmät riskit, kuten kalastelu ja haittaohjelmat (Sarathchandra et al., 2016).

Ihmisten riskikäsityksiin tietoturvallisuuden kontekstissa vaikuttavat useat tekijät. Yhtenä tekijänä on riskien seurausten välittömyys. Toisin sanoen riskit, joiden seuraukset tapahtuvat lähes välittömästi, koetaan suuremmiksi kuin sellaiset riskit, joiden seuraukset toteutuvat pidemmällä aikavälillä. Toisena tekijänä on seurausten tuhoisuus ja vakavuusaste. Riskin suuruutta arvioidessaan ihmiset eivät siis niinkään pohdi toteutumisen todennäköisyyttä, vaan ennemminkin riskin vaikutusten suuruutta ja vakavuutta. Lisäksi riskit, joilla on henkilökohtaisia vaikutuksia, nähdään suurempana. Kolmantena tekijänä riskin kokemiseen vaikuttaa internetkokemus. Tämä tarkoittaa sitä, että ihmiset, joilla on enemmän kokemusta ja tietämystä internetin käytöstä ja sen uhista, kokevat sen riskit suurempina. (van Schaik et al., 2017)

Näiden tekijöiden lisäksi myös riskin vapaaehtoisuus ja hallinnan mahdollisuus vaikuttavat riskikäsityksiin. Ihmiset kokevat sellaiset riskit suurempina, joille altistuminen on vähemmän vapaaehtoista. Toisaalta silloin, kun ihmiset kokevat olevansa hallinnassa sellaisissa tilanteissa, joissa riskeille voi altistua, he kokevat riskit pienemmiksi. (van Schaik et al., 2017)

Joidenkin tutkimusten mukaan käsitykset riskeistä eivät aina vastaa todellisia riskejä. Toisin sanoen ihmiset pelkäävät usein enemmän asioita, jotka ovat vähemmän todennäköisiä sivuuttaen samalla todennäköisemmät riskit (Sarathchandra et al., 2016). Esimerkkinä tästä voidaan pitää identiteettivarkauden ja tietojenkalastelun koettua riskiä. Identiteettivarkaus koettiin huomattavasti suuremmaksi riskiksi kuin tietojenkalastelu, vaikka todellisuudessa tietojenkalastelun uhriksi joutuminen on todennäköisempää. Tätä selittää muun muassa edellä mainittu seikka riskien tuhoisuudesta. Toteutuessaan identiteettivarkaudella voi olla uhrille nimenomaan henkilökohtaisia ja tuhoisia vaikutuksia, jonka vuoksi ihmiset kokevat sen riskin suureksi. Lisäksi identiteettivarkauden esiintyminen laajasti mediassa voi lisätä tietoisuutta ja samalla riskin kokemusta aiheesta (Sarathchandra et al., 2016; van Schaik et al., 2017).

3 Toiminta riskien ehkäisemiseksi

Tietoturvaan ja yksityisyyden suojaan kohdistuvilta riskeiltä suojautuakseen älypuhelimen käyttäjä voi toteuttaa erilaisia ennaltaehkäiseviä toimenpiteitä. Toimenpiteet eivät

ole yksiselitteisiä ja eri riskien ehkäisemiseen voivat vaikuttaa monet erilaiset toimenpiteet. Selkeyden vuoksi taulukkoon 1 on kuitenkin koottu muutamia toimenpiteitä, jotka voivat ehkäistä luvussa 2.2 esitettyjä riskejä.

Tietoturvaan tai yksityisyyteen kohdistuva riski	**Ennaltaehkäisevä toimenpide**
Tietovuoto varkauden tai katoamisen seurauksena	Laitteen lukitus
Julkisiin verkkoihin liittyminen	Julkisten verkkojen välttäminen VPN-yhteyden käyttö
Tietojenkalastelu	Viestin alkuperän tarkastamien
Sosiaalinen manipulointi	Viestin alkuperän tarkistaminen
Identiteettivarkaus	Henkilökohtaisen tiedon jakamisen välttäminen
Haittaohjelmat	Sovellusten lataaminen vain luotetusta lähteestä Sovelluksen lupapyyntöjen lukeminen

Taulukko 1 Riskit ja niitä ennaltaehkäisevät toimenpiteet

Riski tietovuodosta laitteen varkauden tai katoamisen seurauksena kasvaa merkittävästi, jos laitteeseen ei ole asetettu lukitusta esimerkiksi suojakoodin, lukituskuvion tai biometrisen lukituksen avulla (Hogben & Dekker, 2010). Sen vuoksi laitteen lukitus on tärkeä ennaltaehkäisevä toimenpide tietoturvallisuuden edistämiseksi.

Julkisiin verkkoihin liittyviltä riskeiltä voi suojautua välttelemällä niihin liittymistä kokonaan. Etenkin tuntemattomiin verkkoihin liittymistä tulisi välttää. Jos kuitenkin julkisia tai tuntemattomia verkkoja käyttää, voi riskeiltä suojautua VPN-yhteyden (Virtual Private Network) avulla (Breitinger et al., 2020).

Tietojenkalastelulta ja sosiaaliselta manipuloinnilta suojautumiseen yksi keino on erilaisten viestien, kuten teksti- tai sähköpostiviestien, alkuperän tarkastaminen. Tuntemattomasta lähteestä tulleisiin viesteihin tulisi suhtautua varauksella eikä tällaisten viestien sisältämiä linkkejä tulisi avata. Myös tunnetulta vaikuttava viestin lähde voi osoittautua joksikin muuksi, jonka vuoksi viestin alkuperän tarkistaminen on tärkeää. (ENISA, 2020)

Haittaohjelmat leviävät älypuhelimille useimmiten erilaisten sovellusten muodossa. Sen vuoksi haittaohjelmilta suojautumisessa oleellista on ladata sovellukset laitteelle vain luotetusta lähteestä, kuten älypuhelimen sovelluskaupasta (ENISA, 2020). Lisäksi haittaohjelmia voi levitä älypuhelimille sovellusten päivitysten kautta. Sovellus voi siis olla luotetusta lähteestä ladattu ja alkuperäisessä muodossaan harmiton, mutta osoittautua

haittaohjelmaksi päivityksen myötä (Parker et al., 2015). Sen vuoksi sovelluksen lupapyynnöt olisi syytä lukea ennen sovelluksen asennusta sekä päivityksen yhteydessä.

3.1 Toteutettu toiminta ja puutteet toiminnassa

Kaikki tutkimukset osoittivat jonkin verran toimintaa tietoturvallisuuden edistämiseksi. Kuitenkin yleisimmin käytetyt toimet ovat usein yksinkertaisia ja riittämättömiä, jonka vuoksi toiminnassa ja käsityksissä voidaan todeta olevan ristiriitaisuutta. Tässä kappaleessa esittelen riskien ehkäisemiseksi toteutuneet toimenpiteet ja puutteet toiminnassa.

Taulukkoon 2 on koottu yleisimmät toteutuneet toimet riskien ehkäisemiseksi sekä puutteet toimissa. Lisäksi taulukkoon on koottu jokaisesta tutkimuksista ilmenevä yleinen arvio toimenpiteiden riittävyydestä. Muutamissa tutkimuksissa ei täsmällisesti mainittu joko yleistä arviota, toteutuneita toimia tai puutteita toiminnassa, jonka vuoksi taulukko sisältää myös tyhjiä soluja.

	Yleinen arvio toimenpiteiden riittävyydestä	**Toteutetut toimet**	**Toimet, joiden toteutuksessa puutteita**
Bhatnagar & Pry, 2020	Toimenpiteiden taso on hyvä	Henkilökohtaisen tiedon jakamisen välttäminen	–
Breitinger et al., 2020	Toimet eivät ole riittäviä	Älypuhelinten lukitus	Julkisten verkkojen välttäminen VPN-yhteyden käyttö
Imgraben et al., 2014	Toimet eivät ole riittäviä	Sovellusten lataaminen vain luotetusta lähteestä Tuntemattomien verkkojen välttäminen Viestin alkuperän tarkastaminen	Älypuhelinten lukitus
Parker et al., 2015	–	Sovellusten lataaminen vain luotetusta lähteestä Älypuhelinten lukitus	Sovelluksen lupapyyntöjen lukeminen
Sarathchandra et al., 2016	–	–	Julkisten verkkojen välttäminen
Zwilling et al., 2020	Toimet eivät ole riittäviä	Henkilökohtaisen tiedon jakamisen välttäminen	Julkisten verkkojen välttäminen

Taulukko 2 Toteutunut toiminta ja puutteet toiminnassa

Älypuhelinten näytönlukitus suojakoodilla, lukituskuviolla tai biometrisellä lukituksella on nykyisin yleinen tapa suojata laitetta. Näytönlukituksen käyttö on yleistynyt merkittävästi viime vuosikymmenenä (Breitinger et al., 2020). Esimerkiksi Imgrabenin ja muiden (2014) vuosina 2010–2011 kerätty aineisto osoittaa, että jopa 48 % vastaajista ei lukinnut

älypuhelintaan lainkaan. Sen sijaan uudemman tutkimuksen mukaan vastaava lukema oli enää 7,7 % (Breitinger et al., 2020).

Sovelluksia ladataan enimmäkseen vain luotetuista lähteistä, kuten älypuhelimen sovelluskaupasta (Imgraben et al., 2014; Parker et al., 2015). Esimerkiksi Parkerin ja muiden tutkimuksessa jopa 96,9 % vastaajista kertoi lataavansa sovelluksia virallisesta lähteestä. Sen sijaan sovelluksen lupapyyntöjen lukeminen on huomattavasti harvinaisempaa, etenkin sovellusta päivittäessä (Parker et al., 2015).

Henkilökohtaisten tiedon jakamista varotaan (Bhatnagar & Pry, 2020; Zwilling et al., 2020). Zwillingin ja muiden (2020) mukaan ihmiset eivät olleet valmiita jakamaan sosiaalisen median tileillään esimerkiksi kotiosoitetta, puhelinnumeroa tai henkilötunnusta. Ainoastaan ikä oli sellainen tieto, jonka ihmiset olivat valmiita jakamaan. Bhatnagar ja Pry (2020) puolestaan toteavat sosiaalisen median tilin yksityisenä pitämisen olevan yleistä. Kun sosiaalisen median tili on yksityinen, tilin omistaja saa itse päättää, kuka pystyy näkemään tilin sisällön. Tällöin mahdolliset tilillä jaetut henkilökohtaiset tiedot ovat paremmin suojassa.

Julkisten verkkojen välttеleminen on yksi vähemmän suosituista tavoista suojautua tietoturvauhilta. Esimerkiksi Breitingerin ja muiden (2020) tutkimus osoittaa, että vain 22,2 % tutkimukseen osallistuneista ihmisistä vältteli julkisiin verkkoihin liittymistä. Löydökset ovat saman suuntaisia Zwillingin ja muiden (2020) tutkimuksessa, joka listaa julkisten verkkojen välttelyn vain pienen osan suosimaksi keinoksi. Niin ikään Sarathchandra ja muut (2016) raportoivat, että julkisissa verkoissa suoritettiin sekä pankkiasioiden hoitamista että verkko-ostoksia. Lisäksi Breitingerin ja muiden (2020) mukaan suurin osa julkisia verkkoja käyttävistä ihmisistä on aktivoinut laitteellaan asetuksen, joka mahdollistaa laitteen automaattisen yhdistämisen niihin. Myöskään VPN-yhteyden käyttö julkisiin verkkoihin yhdistäessä ei ollut yleistä (Breitinger et al., 2020). Huomattavaa kuitenkin on, että kysyttäessä tuntemattomiin verkkoihin yhdistämisestä, vain 16,4 % osoitti yhdistävänsä sellaisiin (Imgraben et al., 2014).

Kuten taulukosta 2 on havaittavissa, useimpien tutkimusten yleinen arvio toimien tasosta on, etteivät toimet ole riittäviä. Esimerkiksi Breitingerin ja muiden (2020) mukaan älypuhelinten käyttäjät toteuttavat riittämättömästi suojausasetuksia eivätkä usein noudata hyviä suojauskäytäntöjä. Niin ikään Zwillingin ja muiden (2020) mukaan ihmiset toteuttavat vain yksinkertaisia ja riittämättömiä suojaustoimenpiteitä. Useimpien tutkimusten mukaan ihmisten käsityksissä ja toteutuneessa toiminnassa onkin havaittavissa ristiriita (Barth et al., 2019; Parker et al., 2015; Zwilling et al., 2020).

Käsitysten ja toiminnan ristiriidasta voidaan puhua myös yksityisyyden paradoksin ilmiönä. Yksityisyyden paradoksilla (*engl. privacy paradox*) tarkoitetaan juuri tätä ristiriitaa: ihmiset ovat huolissaan omasta yksityisyydestään, mutta tämä huoli ei vaikuta ihmisten toimiin. Ihmiset esimerkiksi antavat itsestään vapaaehtoisesti tietoja julkaisemalla

yksityiskohtia elämästään sosiaalisessa mediassa tai käyttämällä tietoisesti sovelluksia ja sivustoja, jotka keräävät tietoja käyttäjästään. Toisaalta ihmiset myös useimmiten sivuuttavat sovellusten tietosuojaehdot, eivätkä näin ollen ole tietoisia siitä, mitä tietoja sovellus käyttää. Tämän lisäksi ihmiset harvoin suojelevat tietojaan aktiivisesti esimerkiksi säännöllisen evästeiden poiston tai sähköpostisuojauksen avulla. (Gerber et al., 2018)

3.2 Tiedon puute selittävänä tekijänä

Yksi selitys käsitysten ja toiminnan ristiriidalle on tiedon puute: ihmiset haluaisivat suojata laitteitaan, mutta heiltä puuttuvat tarvittavat tiedot ja taidot suojautumiseen (Zwilling et al., 2020). Useissa tutkimuksissa onkin löydetty yhteys paremman tietoturvallisuustietämyksen ja vahvempien tietoturvatoimien käytössä. Tietämyksellä tai tiedolla viitataan tässä yhteydessä englannin kielen termiin *knowledge*, jota ei tule sekoittaa termiin tietoisuus, *awareness*.

Ihmiset, joilla on enemmän tietoa tietoturvallisuudesta, käyttävät vahvempia salasanoja sekä pidempiä suojakoodeja älypuhelimen lukitukseen. Tieto on siis yhteydessä vahvempien lukitusasetusten käyttöön älypuhelimilla. Sen lisäksi korkeampi tietoturvatietämyksen taso on yhteydessä turvallisuuteen liittyvien oletusasetusten muuttamiseen, säännölliseen varmuuskopiointiin sekä tietoturvasovellusten ja -ominaisuuksien laajempaan käyttöön. Enemmän tietoturvallisuudesta tietävät ihmiset käyttävät todennäköisemmin erilaisia tietoturvasovelluksia, kuten viruksentorjuntaohjelmia. Heillä on todennäköisemmin kehittynyt varmuuskopiointisuunnitelma ja he suorittavat varmuuskopioinnin säännöllisemmin ja useammin. (Breitinger et al., 2020)

Lisäksi tietämys erilaisista tietoturvauhista vaikuttaa riskikäsityksiin (van Schaik et al., 2017). Toisin sanoen ihmiset, joilla on enemmän kokemusta ja tietoa kybermaailmasta, kokevat sen riskit suurempina ja käyttävät sen vuoksi myös enemmän ennaltaehkäiseviä toimia. Toisaalta tietämyksen ei tarvitse välttämättä olla syvällistä taitoa ja kokemusta kybermaailmasta, vaan yksinkertainenkin tieto riittää. Tämän osoittaa Furinin ja muiden (2020) tutkimus, jossa ihmisten käsityksiä yksityisyydestä älypuhelimilla mitattiin ennen ja jälkeen sen, kun heille oli annettu lisäinformaatiota aiheesta. Lisäinformaationa ihmisille kerrottiin, millaisia riskejä tietyllä aktiviteetilla voi olla. Tutkimus osoitti merkittävää kasvua riskikäsityksissä tiedon lisääntyessä. Näin ollen tiedon puute voidaan nähdä yhtenä selittävänä tekijänä käsitysten ja toiminnan ristiriitaisuudelle.

3.3 Muiden ominaisuuksien arvottaminen selittävänä tekijänä

Pelkästään tiedon puutteella ei voida kuitenkaan selittää ristiriitaisuutta kokonaan. Tämän osoittaa Barthin ja muiden (2019) tutkimus, jossa myös teknisesti lahjakkaat ihmiset olivat valmiita uhraamaan yksityisyytensä ja arvottamaan muita ominaisuuksia korkeammalle. Yksityisyyttä ja tietoturvaa ei usein pidetäkään sovelluksen ominaisuuksista prio-

riteetteina, vaan muut asiat, kuten käytettävyys, helppokäyttöisyys, toimivuus ja visuaalisuus, ovat tärkeämpiä (Barth et al., 2019). Lisäksi tietoturva-asetusten saatetaan nähdä rajoittavan sovelluksen täyttä toiminnallisuutta (Bhatnagar & Pry, 2020) tai olla liian vaivalloisia edes pohdittavaksi (Sarathchandra et al., 2016).

Myös taloudelliset hyödyt voidaan nähdä yksityisyyttä tärkeämpinä. Esimerkiksi uutta sovellusta valitessa sovelluksen hinta voi olla merkittävä päätöksentekoon vaikuttava tekijä. Ihmiset ovat tottuneet ilmaisiin sovelluksiin, eivätkä näe hyötyjä maksullisissa sovelluksissa. Jos halutusta sovelluksesta on olemassa myös ilmainen versio, on se houkuttelevampi vaihtoehto kuin maksullinen, vaikka ilmaisen version valitessaan joutuisikin tinkimään yksityisyydestään. (Barth et al., 2019)

Muiden ominaisuuksien arvottaminen perustuu riskien ja hyötyjen välillä laskelmointiin. Tämä niin kutsuttu yksityisyyden laskelmoinnin (*engl. privacy calculus*) teoria perustuu ajatukseen rationaalisesta hyötyjen ja haittojen suhdetta pohtivasta ja niiden perusteella päätöksiä tekevästä ihmisestä. Sovellettaessa ajatusta yksityisyyden kontekstiin hyödyiksi katsotaan tietojen luovuttamisesta saavutettavat ominaisuudet ja haitaksi yksityisyyden heikentyminen. Tietojen luovuttamisesta saavutettavat hyödyt voivat olla edellä mainittujen ominaisuuksien lisäksi esimerkiksi käytännöllisyyteen tai sosiaaliseen verkostoitumiseen liittyviä. Jos odotettujen hyötyjen määrä kasvaa suuremmaksi kuin odotettujen haittojen määrä, ovat käyttäjät valmiita luovuttamaan tietojaan vapaaehtoisesti, vaikka käyttäjällä olisi edelleen huoli yksityisyydestä. Ihmiset ovat siis valmiita vapaaehtoisesti luopumaan yksityisyydestään saadakseen vastineeksi muita hyötyjä. (Gerber et al., 2018)

3.4 Tunnereaktiot ja kognitiiviset harhat selittävänä tekijänä

Hyötyjen ja haittojen rationaaliseen punnintaan perustuva malli ei ota huomioon toiminnan aiheuttamia tunnereaktioita tai erilaisia kognitiivisia harhoja. Kognitiivisia harhoja on määritelty psykologian alalla lukuisia erilaisia ja useat niistä voivat osaltaan olla selittävinä tekijöinä käsitysten ja toiminnan ristiriidalle (Gerber et al., 2018). Näistä esiin nousee kuitenkin eniten optimistinen harha ja tunnereaktioharha.

Optimistisella harhalla (*engl. optimistic bias*) tarkoitetaan ihmisen taipumusta uskoa, että itsellä on pienempi riski joutua negatiivisen tapahtuman kohteeksi verrattuna muihin ihmisiin (Gerber et al., 2018). Ilmiö osaltaan selittää ristiriitaa käsitysten ja toiminnan suhteessa. Esimerkiksi Sarathchandran ja muiden (2016) tutkimuksessa 53,66 % vastaajista uskoi itse olevansa vähemmän alttiita tietoturvariskeille kuin ihmiset keskimäärin. Tämä johtaa toiminnan puutteeseen tietoturvariskien ehkäisemiseksi, sillä ihmiset eivät usko, että omalla toiminnan puutteella voisi olla joitain negatiivisia seurauksia itselle, ainoastaan muille. Lisäksi ihmiset kokevat riskit pienempinä silloin, kun he kokevat hal-

litsevansa riskialttiita tilanteita sekä silloin, kun riskille altistumisen koetaan olevan vapaaehtoisempaa. Tämä osaltaan voi johtaa optimistiseen harhaan (van Schaik et al., 2017), kun ihmiset valheellisesti kokevat hallitsevansa riskialttiita tilanteita.

Tunnereaktioharhalla (*engl. affect bias*) tarkoitetaan ihmisten taipumusta tehdä päätöksiä ja arvioida erilaisia tilanteita nopeasti tunteeseen perustuen (Gerber et al., 2018). Tietoturvallisuutta ja yksityisyyttä uhkaavat riskit ovat usein epävarmoja ja monimutkaisia, minkä vuoksi niitä arvioidessa ihmiset luottavat usein rationaalisen punninnan sijaan toiminnan tai riskin aiheuttamaan tunnereaktioon (van Schaik et al., 2020). Tämän tunnereaktioharhan vuoksi ihmiset usein aliarvioivat riskin sellaisille asioille, joista he pitävät ja yliarvioivat sellaisille asioille, joista he eivät pidä (Gerber et al., 2018). Lisäksi positiivinen tunnereaktio riskialttiin toiminnan seurauksena kasvattaa kokemusta toiminnan hyödystä (van Schaik et al., 2020). Tämä koetun hyödyn kasvaminen puolestaan johtaa suurempaan todennäköisyyteen toteuttaa kyseinen riskialtis toiminta ja jättää samalla tarvittavat turvatoimet suorittamatta.

4 Keskustelu

Tarkastelin kirjallisuuskatsauksessani ihmisten käsityksiä tietoturvallisuudesta ja yksityisyydestä älypuhelimilla sekä sitä, miten nämä käsitykset vaikuttavat ihmisten toimintaan laitteiden suojaamiseksi. Tutkimuskysymykset olivat seuraavat: (1) miten ihmiset käsittävät älypuhelinten käyttöön liittyvät tietoturvan ja yksityisyyden suojan riskit ja (2) millä tavalla käsitykset vaikuttavat ihmisten toimintaan laitteiden suojaamiseksi.

Kirjallisuuskatsauksen perusteella ihmiset ovat yleisesti tietoisia termistä tietoturvallisuus, ja ymmärtävät älypuhelinten käytön altistavan heidät erilaisille tietoturvariskeille. Yleisesti tietoturvatietoisuuden tason voi siis sanoa olevan kohtuullisen hyvä. Suurimpana riskinä koettiin identiteettivarkaus ja pienimpinä riskeinä tietojenkalastelu ja haittaohjelmat. Riskit, joilla on välittömiä tai tuhoisia vaikutuksia, koettiin suurempina. Lisäksi riskit, joille altistuminen on vähemmän vapaaehtoista tai joiden suhteen ihminen ei koe olevansa hallinnassa, koettiin suurempina.

Osan tutkimuksista mukaan ihmisten käsitykset ovat todellisista riskeistä poikkeavia. Väitettä perusteltiin esimerkiksi sillä, että identiteettivarkaus koettiin suuremmaksi riskiksi kuin kalastelu, jonka uhriksi joutuminen on huomattavasti todennäköisempää. Itse en kuitenkaan tulkitsisi näitä käsityksiä todellisuudesta poikkeaviksi, sillä kuten luvussa 2.2 totesin, identiteettivarkauden yhteydessä voidaan käyttää muun muassa kalastelun tai sosiaalisen manipuloinnin keinoja, mikä asettaa identiteettivarkauden ikään kuin lopulliseksi päämääräksi, ja muut uhat sen välikeinoiksi.

Kaikki kirjallisuuskatsauksessa tarkastellut julkaisut osoittivat jonkin verran toimintaa laitteiden suojaamiseksi. Yleisin tapa suojata laitteita oli näytön lukitus suojakoodilla, lukituskuviolla tai biometrisellä lukituksella. Myös sovellusten lataaminen vain luotetusta

lähteestä osoittautui laajasti toteutetuksi keinoksi. Sen sijaan julkisten verkkojen välttäminen tietoturvatoimena ei ollut suosittua.

Joitain toimia siis käytettiin, mutta kuitenkin useimpien tutkimusten mukaan toimenpiteet ovat yksinkertaisia ja riittämättömiä. Sen vuoksi useimpien tutkimusten mukaan ennaltaehkäisevät toimet ovat ristiriidassa käsitysten kanssa. Toisin sanoen, vaikka ihmiset pitävät tietoturvallisuutta tärkeänä ja ymmärtävät älypuhelinten käytön altistavan heidät erilaisille tietoturvan ja yksityisyyden suojan riskeille, eivät nämä käsitykset heijastu ihmisten toimintaan. On kuitenkin syytä pohtia, miten riittävyyden taso määritellään suhteessa riskien suuruuteen. Vaikka tietoturvariskeiltä onkin tärkeää suojautua, ei ole myöskään mielekästä toteuttaa ylimitoitettuja toimia.

Yleisimmäksi syyksi ristiriitaisuudelle osoittautui tiedon puute. Siitä johtuen useimmissa tutkimuksissa korostettiin koulutuksen merkitystä ja kannustettiin tietoisuuden lisäämiseen koulutuksen avulla (Bhatnagar & Pry, 2020; Breitinger et al., 2020; Sarathchandra et al., 2016; Zwilling et al., 2020). Muita syitä ristiriitaiselle toiminnalle oli muiden ominaisuuksien arvottaminen, toiminnan aiheuttamat tunnereaktiot sekä erilaiset kognitiiviset harhat, kuten optimistinen harha. Koska ihmisen arviointikyky on rajallinen ja siihen vaikuttavat vahvasti erilaiset kognitioon liittyvät asiat, nostaisin tietoisuuden lisäämisen lisäksi myös tietoturvallisen toiminnan tekemisen helpommaksi käyttäjälle yhdeksi tärkeäksi asiaksi. Näin ehdottavat myös Parker ja muut (2015), joiden mukaan älypuhelinten tietoturvan suunnittelun tulee olla yksinkertaista eikä liian teknistä, jotta se parhaiten palvelisi monipuolista käyttäjäkuntaa. Asiassa on onneksi nähty jo kehitystä: esimerkkinä laitteiden lukituksen yleistyminen asetuksen muututtua oletusasetukseksi. Olettaisin kehityksen jatkuvan saman suuntaisena.

Kirjallisuuskatsauksellani on muutamia rajoitteita. Käytin lähteiden etsimiseen enimmäkseen kahdenlaisia hakulausekkeita: sellaisia, joissa oli mukana hakusana tietoturvallisuus (*cyber security*) sekä sellaisia, joissa oli mukana yksityisyys (*privacy*). Sen vuoksi lähdemateriaali oli melko vaihtelevaa, joka vaikeutti tulosten vertailua esimerkiksi määritellessäni eri riskien koettua suuruutta. Kaikissa julkaisuissa vertailtavana olleet riskit eivät olleet täysin samoja, jonka vuoksi yksimielistä kantaa esimerkiksi suurimmaksi koetusta riskistä ei voinut määritellä. Sen lisäksi jotkut kirjallisuuskatsaukseen valitsemani julkaisut käsittelivät ihmisten käsityksiä yleisesti tietoturvariskeistä esimerkiksi internetiä käyttäessä sen sijaan, että ne olisivat käsitelleet riskejä liittyen erityisesti älypuhelimiin.

Suurimmassa osassa valitsemaani kirjallisuutta tutkimuskohteena oli yliopisto-opiskelijat, jotka olivat pääosin nuoria aikuisia. Myös niissä tutkimuksissa, joissa tutkimuskohteena oli kaikenikäiset ihmiset, oli pääpaino nuorissa aikuisissa. Tutkimustulos saattaisi olla toisen suuntainen, jos tutkimusten kohderyhmänä olisi ollut vaikkapa työelämässä olevat henkilöt, ikäihmiset tai teini-ikäiset. Tilastokeskuksen mukaan (2020) nuoret aikuiset käyttävät älypuhelimia enemmän kuin vanhemman sukupolven edustajat.

Käytön ollessa korkeammalla tasolla myös teknologinen osaaminen voi olla edistyneempää, mikä johtaisi parempaan tietoturvallisuustietoisuuteen, kuten luvussa 3.2 esitin.

Toisaalta teknologian vahva läsnäolo nuorten aikuisten elämässä saattaa johtaa myös löysempään suhtautumiseen tietoturvallisuuteen tai yksityisyyteen liittyvissä asioissa. Tähän suuntaan viittaavat esimerkiksi van Schaik ja muut (2017), joiden mukaan ihmiset, jotka käyttivät internetiä useammin, kokivat sen riskit pienempinä. Sen sijaan teknologiaa vähemmän käyttävät ikäihmiset saattaisivat olla jopa varovaisempia internetissä. Eri ikäryhmien käsitysten vertailu asettakin jatkotutkimuksen aihetta.

5 Yhteenveto

Tässä tutkielmassa tarkastelin ihmisten käsityksiä tietoturvallisuudesta ja yksityisyydestä älypuhelimilla sekä sitä, miten nämä käsitykset vaikuttavat ihmisten toimintaan. Yleisesti ihmiset ovat tietoisia älypuhelinten käyttöön liittyvistä tietoturvallisuuteen ja yksityisyyteen kohdistuvista riskeistä. Osan tutkimuksista mukaan käsityksissä on kuitenkin vielä parannettavaa. Joitain yksinkertaisia tietoturvallisuustoimia käytettiin älypuhelinten suojaamiseksi, mutta toimet ovat usein riittämättömiä. Käsityksissä ja toiminnassa on näin ollen havaittavissa ristiriita, jota kutsutaan myös yksityisyyden paradoksiksi. Yleisimmäksi syyksi toiminnan puutteelle osoittautui tiedon puute, jonka vuoksi tietoisuutta tulisi lisätä koulutuksen avulla. Lisäksi älypuhelinten tietoturva-asetukset tulisi tehdä helppokäyttöisiksi ja oletusasetukset nykyistä turvallisemmaksi.

Lähdeluettelo

ATK-sanakirja (2020). *MOT Tietotekniikan liiton ATK-sanakirja, Kielikone Oy.* (Haettu 27.11.2020)

Aime, M. D., Calandriello, G., & Lioy, A. (2007). Dependability in Wireless Networks: Can We Rely on WiFi? *IEEE Security & Privacy, 5*(1), 23–29. *https://doi.org/*10.1109/MSP.2007.4

Barth, S., de Jong, Menno D. T, Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics, 41*, 55–69. *https://doi.org/*10.1016/j.tele.2019.03.003

Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal, 18*(1), 48.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security, 88*, 101647. *https://doi.org/10.1016/j.cose.2019.101647*

Darker C. (2013). Risk Perception. *In: Gellman M.D., Turner J.R. (eds) Encyclopedia of Behavioral Medicine. Springer, New York, NY. https://doi.org/10.1007/978-1-4419-1005-9_866*

ENISA. (2020). *Euroopan unionin verkko- ja tietoturvavirasto.* (Haettu 21.11.2020) *https://www.enisa.europa.eu/topics/csirts-in-europe/glossary*

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy Perception when Using Smartphone Applications. *Mobile Networks and Applications, 25*(3), 1055–1061. *https://doi.org/10.1007/s11036-020-01529-z*

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226–261. *https://doi.org/*10.1016/j.cose.2018.04.002

Hakala, M., Vainio, M., & Vuorinen, O. (2006). *Tietoturvallisuuden käsikirja*. Docendo.

Hogben, G., Dekker, M. (2010). Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency (ENISA). https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users*

Imgraben, J., Engelbrecht, A., & Choo, K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology, 33*(12), 1347–1360. *https://doi.org/10.1080/0144929x.2014.934286*

Morton, A., & Sasse, M. (2012). Privacy is a process, not a PET: a theory for effective privacy practice. *Proceedings of the 2012 New Security Paradigms Workshop, 2012-09-18, p.87–104*. *https://doi.org/10.1145/2413296.2413305*

Parker, F., Ophoff, J., Van Belle, J., & Karia, R. (2015). Security awareness and adoption of security controls by smartphone users. *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), 2015-11, p.99–104*. *https://doi.org/10.1109/InfoSec.2015.7435513*

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. *2016 Cybersecurity Symposium (CYBERSEC) 2016-04*, 68 73. *https://doi.org/*10.1109/CYBERSEC.2016.018

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal, 19*(3), 122–131. *https://doi.org/10.1023/A:1011902718709*

Tietosuojavaltuutettu. (2020). *Tietosuojavaltuutetun toimisto*. *https://tietosuoja.fi* (Haettu 27.11.2020)

Tilastokeskus. (2020). Väestön tieto- ja viestintätekniikan käyttö, Liitetaulukko 13. Matkapuhelimen käyttö ja internetin käyttö televisiolla 2020, %-osuus väestöstä. *Suomen virallinen tilasto (SVT). http://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tau_013_fi.html*

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547–559. *https://doi.org/*10.1016/j.chb.2017.05.038

van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security, 90*, 101651. *https://doi.org/10.1016/j.cose.2019.101651*

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193–220.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł, Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, ahead-of-print*(-), 1–16. *https://doi.org/10.1080/08874417.2020.1712269*