Pyry Seppänen

ÄLYPUHELINKÄYTTÄJÄN TIETOTURVA-AIKOMUS HENKILÖKOHTAISEN DATAN SUOJAAMISESSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2018

TIIVISTELMÄ

Seppänen, Pyry
Älypuhelinkäyttäjän tietoturva-aikomus henkilökohtaisen datan suojaamisessa
Jyväskylä: Jyväskylän yliopisto, 2018 , 67 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko; Rönkkö, Mikko

Tässä pro gradu –tutkielmassa käsitellään älypuhelinkäyttäjien aikomusta käyttää älypuhelinten tietoturvaominaisuuksia henkilökohtaisen älypuhelimensa suojauksessa. Tutkielma selvittää millaisia uhkia älypuhelimiin ja niiden sisältämiin tietoihin kohdistuu. Uhkien lisäksi esitellään älypuhelimiin kuuluvia tietoturvaominaisuuksia, joita käyttämällä käyttäjä voi itse vaikuttaa laitteensa tietoturvaan.

Uhkien ja ominaisuuksien lisäksi käyttäjien tietoturvakäytöstä ja siihen liittyvää aikomusta tarkastellaan tietoturvakäytänteiden noudattamisen yhtenäismallin, eli Unified Model of Information Security Policy Compliance:n avulla, jonka avulla on tarkoitus selvittää, mitkä tekijät vaikuttavat kyseiseen aikomukseen. Tämän lisäksi aikomukseen liittyvää teoriaa täydennetään aiemmalla tutkimuksella aiheeseen liittyen, jotta malli saadaan asetettua älypuhelinkontekstiin.

UMISPC-mallin ja aiemman tutkimuksen perusteella on luotu määrällinen kyselytutkimus, jonka avulla mallin soveltuvuutta älypuhelinkontekstiin testataan. Mallin testaamisen lisäksi tavoitteena on vastata tutkimuskysymykseen ”Mitkä ennalta määritellyt tekijät vaikuttavat älypuhelinkäyttäjän tietoturva-aikomukseen?”

Asiasanat: älypuhelin, käyttäjä, tietoturva, aikomus, tietoturvakäyttäytyminen, yhtenäismalli

ABSTRACT

Seppänen, Pyry
Smartphone user's information security intention in protecting personal data
Jyväskylä: University of Jyväskylä, 2018, 67 p.
Information Systems Science, Master's Thesis
Supervisor: Siponen, Mikko

This master's thesis discusses the intention of a smartphone user using the information security features in securing their personal smartphone. The thesis examines the threats smartphones and the personalized data within them are facing. Along with the introduction of threats towards smartphone security, features that help the users in securing their phones against such threats are examined.

Along with threats and smartphone security features, the users' intentions of securing their devices are studied through the Unified Model of Information Security Policy Compliance. The model helps to clarify the factors that influence the users' intention of engaging in safe information security behavior. In addition, prior research on the topic of intention is examined in order to make the UMISPC fit better in the context of smartphone users.

An online survey was created using the model, its theories and prior studies which all were used as the basis of the survey. The aim of the survey is to test the validity of the UMISPC. In addition, the goal is to answer the research question: "Which predefined factors affect the smartphone user's intention of security compliance?"

Keywords: smartphone, user, information security, intent, information security behavior, unified model

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Erilaisten älylaitteiden, kuten älypuhelinten ja tablettien käyttö yleistyy jatkuvasti. Käyttäjät käyttävät laitteita usein esimerkiksi internetin selaamiseen, pikaviestittelyyn sekä sosiaalisen median alustojen hyödyntämiseen niin vapaa-ajalla kuin työssäkin. Älypuhelinten yleistyminen on edelleen nopeaa, ja esimerkiksi Suomessa älypuhelin oli käytössä jo 60 prosentilla väestöstä vuonna 2014. Kasvu on jatkunut noin viidellä prosenttiyksiköllä vuosittain ja vuonna 2017 alle 55-vuotiaista suomalaisista 94 %:lla oli jo käytössään älypuhelin. Samalla myös tablettitietokoneiden käyttö on lisääntynyt, vuonna 2014 tablettitietokone löytyi 32 %:sta kotitalouksista, ja vuonna 2017 luku oli jo yli 50 %. (Tilastokeskus, 2014; Tilastokeskus, 2018a.)

Älylaitteiden yleistyessä myös niihin liittyvien riskien ja ongelmien voidaan olettaa samalla lisääntyvän. Laitteiden muuttuessa entistä enemmän käyttäjiensä persoonallisuuden jatkeeksi, laitteeseen tallennetut tiedot ja sen käyttötavat voivat paljastaa käyttäjästään hyvinkin paljon: valokuvat, sosiaaliset verkostot, pankkipalvelut, sähköposti, viihde ja muut kulkevat nyt helposti lähes jokaisen mukana taskussa paikasta toiseen. Jatkuvasti lisääntyvät ominaisuudet, käytön yleistyminen sekä liikkuvuus lisäävät samalla myös laitteeseen ja sen sisältöön kohdistuvia riskejä. Näitä riskejä ovat esimerkiksi haitta- ja huijausohjelmat, tietojen urkinta ja varastaminen, tietojenkalastelu, verkkohyökkäykset sekä esimerkiksi laitteen haltuunotto käyttäjän huomaamatta, joko verkkoyhteyksiä hyödyntäen tai fyysisesti (Leavitt, 2011).

Tutkimuksen tavoitteena on selvittää, millaiset tekijät vaikuttavat älypuhelinkäyttäjien aikomukseen suojata oma laitteensa siihen kohdistuvilta uhilta. Tätä aikomusta tarkastellaan Moody, Siponen & Pahnilan (2018) luoman tietoturvakäytänteiden noudattamisen yhtenäismallin, eli Unified Model of Information Security Policy Compliance:n, lyhyemmin UMISPC:n, avulla. Malli kokoaa yhteen 11 eri aikomukseen ja tietoturvakäyttäytymisen tutkimuksessa käytettävää teoriaa, jonka tuloksena on syntynyt nämä teoriat yhdistävä yhtenäismalli. Tässä tutkielmassa tutkitaan tämän yhtenäismallin soveltuvuutta älypuhelinkäyttäjien kontekstissa.

UMISPC-mallin lisäksi käyttäjien toimintaa tarkastellaan loppukäyttäjien tietoturvakäyttäytymistä kuvaavan analyysin perusteella, jonka Stanton, Stam, Mastrangelo, & Jolton (2005) ovat luoneet. Analyysin perusteella käyttäjät voidaan toimintansa perusteella sijoittaa kaksitasoiseen matriisiin, jonka tasot ovat osaaminen (expertise) ja aikomus (intentions). Käyttäjän sijoittuminen matriisissa määrittää sen, millaiseen tietoturvakäyttäytymisen päätyyppiin hän kuuluu. Analyysissä esitetyt kuusi käyttäytymisen päätyyppiä määräytyvät osaamisen ja aikomuksen tasojen, matala-korkea ja haitallinen-hyödyllinen mukaan vastaavasti.

Stanton:in et al. (2005) Tietoturvakäyttäytymistä kuvaava teoria ei kuitenkaan pääosin kuvaa kyseistä käyttäytymistä älypuhelinten osalta, joten tässä tutkimuksessa tarkastellaan tätä (2005) teoriaa hieman eri näkökulmasta. Oman versionsa teoriasta ovat koostaneet Ngoqo & Flowerday (2015), jossa teoriaa on muokattu vastaamaan paremmin älypuhelinkäyttäjien kontekstia. Merkittävimpänä erona alkuperäiseen on matriisirakenteen muokkaus, jolloin jäljelle ovat jääneet kuusi eri ryhmää, joihin käyttäjät sijoitetaan tietoturvakäyttäytymisensä perusteella.

Aiheeseen liittyvän aiemman tutkimuksen tarkastelun lisäksi tutkielmaa varten suoritetaan määrällinen kyselytutkimus, jonka tavoitteena on vastata seuraavaan tutkimuskysymykseen:

1) ”Mitkä ennalta määritellyt tekijät vaikuttavat älypuhelinkäyttäjän tietoturva-aikomukseen?”

Tutkielma rakentuu viidestä osiosta. 1. luku sisältää johdannon ja tutkimuskysymyksen. Luku 2 sisältää tutkielman kannalta tärkeiden käsitteiden määrittelyn, älypuhelimiin kohdistuvien riskien esittelyn sekä älypuhelinten sisältämät tietoturvaominaisuudet. Luku 3 käsittelee tutkielmassa käytettävät mallit ja teoriat. Luku 4 sisältää tutkielman tutkimusosuuden esittelyn, tutkimuskysymyksen, aineiston keräämisen ja kohteen sekä tutkimukseen käytetyn kyselyn sisällön. Luku 5 käsittää tutkimuksen tulokset, tutkimuksen analyysit ja lopulta vastaa tutkimuskysymykseen. Luku 6 sisältää johtopäätökset, jotka tutkimustuloksista voidaan mahdollisesti päätellä, ja luvun lopussa esitellään jatkotutkimusehdotukset.

2 ÄLYPUHELINTEN TURVALLISUUS

2.1 Käsitteiden määrittely

Tietoturvasta puhuttaessa on tärkeää määritellä käytettävät käsitteet niin, että niiden käyttö on yhdenmukaista ja selkeää. Käsitteille on usein myös useita eri määritelmiä, jotka eroavat vaihtelevissa määrin toisistaan. Käsitteiden määritelmät on usein esitetty aineiston lähdekielellä, joka on yleensä englanti, mikä luo oman haasteensa käsitteiden määrittelyyn, sillä ne on käännettävä suomeksi. Kaikille käsitteille ei myöskään aina löydy suomenkielistä vastinetta, joten tässä kappaleessa määritellyt käsitteet pätevät parhaiten juuri tämän tutkielman sisällä.

Tietoturva (engl. information security): suojakeinot, joiden avulla yritetään suojata ja varmistaa yksilön tai organisaation omistaman datan yhtenäisyys, saatavuus sekä oikeellisuus, samalla estäen datan luvaton käyttö, muokkaus, sekä hävittäminen tai tuhoutuminen. Datan yhtenäisyys tarkoittaa sitä, että dataa ei voi ja ei ole muokannut kukaan ulkopuolinen taho. (BusinessDictionary.com, 2015.)

Tietoturvakäyttäytyminen (engl. security behavior): millä tavoin loppukäyttäjät toimivat tietoturvaan liittyvissä tilanteissa. Toiminta voidaan sijoittaa kahden akselin matriisiin, jotka ovat asiantuntemus (ekspertti – vasta-alkaja) sekä tarkoitusperä (hyväntahtoinen – tahallinen haitanteko). (Stanton et al., 2005.)

Mobiiliturvallisuus (engl. mobile security): mobiililaitteeseen, kuten älypuhelimeen tai tablettitietokoneeseen liittyvä tietoturva. Mitä uhkia mobiililaitteisiin kohdistuu, miten ne eroavat perinteisiin päätelaitteisiin kohdistuviin uhkiin verrattuna, ja mitä haittaa nämä uhat voivat aiheuttaa (Becher et al., 2011). Tutkielmassa mobiiliturvallisuudesta puhuttaessa kyseessä on aiheen rajauksen mukaisesti juuri älypuhelimiin liittyvä turvallisuus, vaikka ne pääasiallisesti pätevät myös tablettitietokoneiden parissa.

Aikomus (engl. intention): toimintaan vaikuttavat tekijät, ja se mitkä tekijät vaikuttavat aikomuksen muodostumiseen. Aikomukseen vaikuttavat asenne

aiottua toimintaa kohtaan, subjektiiviset normit eli ympäristön suhtautuminen sekä tietoinen käytöskontrolli, eli miten kohde itse kokee pystyvänsä kontrolloimaan aikomustaan. (Ajzen, 1991.)

Mobiililaite (engl. mobile device): Kaplan (2012) määrittelee mobiililaitteen laitteena, joka pystyy olemaan yhteydessä langattomiin verkkoihin ja internettiin paikkariippumattomasti, eli laitteen käyttö ei rajoitu vain yhteen tiettyyn paikkaan. Älypuhelin (engl. smartphone) täyttää siis mobiililaitteen määritelmän, mutta sisältää samalla myös perinteisten matkapuhelinten sisältämät ominaisuudet, kuten mahdollisuuden soittaa ja vastaanottaa puheluita ja tekstiviestejä. Lisäksi älypuhelin sisältää ominaisuuksia, joita löytyy myös tietokoneista, kuten käyttöjärjestelmä, sovellukset, internetyhteys ja multimediaominaisuudet (Oxfordictionaries.com, 2016).

Näiden määriteltyjen käsitteiden lisäksi tutkielmassa käytetään useita mobiililaitteisiin ja tietotekniikkaan liittyviä käsitteitä sekä konsepteja. Suurin osa käsitteistä on varmasti lukijalle tuttuja, joten kaikkein perustavanlaatuisimpia tietoteknisiä käsitteitä ei välttämättä jokaista määritellä erikseen. Tutkimuksen kannalta tärkeimmät käsitteet ja niiden englanninkieliset vastineet käydään kuitenkin läpi asiayhteyksissään ymmärrettävyyden parantamiseksi ja lukemisen helpottamiseksi.

2.2 Älypuhelimiin kohdistuvat uhkat

Osa älypuhelimiin kohdistuvista uhkista ovat samoja tai samankaltaisia kuin muuhunkin tietotekniikkaan kohdistuvat uhkat. Näitä uhkia ovat esimerkiksi tietojen kalastelu, haittaohjelmat, häiritsevät mainokset ja roskaposti sekä erilaiset verkkohyökkäykset ja virukset (Khan, Abbas, & Al-Muhtadi, 2015). Kuitenkin älypuhelinten käyttöön usein liittyvä liikkuva, mobiili, käyttötapa asettaa älypuhelimet alttiiksi myös useille muille uhkille, joita perinteiset työasemat eivät useinkaan kohtaa. Erityisesti mobiili- ja älylaitteisiin kohdistuvia uhkia ovat esimerkiksi laitteen kadottaminen tai varastaminen ja tästä koituvat haitat, kuten henkilökohtaisten tietojen häviäminen tai päätyminen vääriin käsiin, langattomaan tiedonsiirtoon kohdistuvat uhat (bluetooth, NFC, wi-fi, GPS jne.) sekä puhelin- ja viestiominaisuuksien väärinkäyttö, esimerkiksi viestien lähettely maksullisiin palvelunumeroihin (He, Chan, & Guizani, 2015; Khan et al., 2015; Li & Clark, 2013).

Tässä kappaleessa käsitellään käyttäjien älypuhelimiin kohdistuvia uhkia tarkemmin, ja tämän jälkeen esitellään älypuhelinten sisältämiä turvallisuusominaisuuksia ja miten käyttäjät voivat hyödyntää näitä ominaisuuksia oman laitteensa suojaamiseksi.

Älypuhelinkäyttäjiä haastattelemalla Chin, Sekar, Wagner & Felt (2012) selvittivät käyttäjiä itseään huolestuttavia uhkia, jotka liittyivät heidän käyttämiinsä älypuhelimiin. Haastateltavat mainitsivat useimmiten laitteen kadottamisen tai varastamisen, laitteen rikkoutumisen sekä henkilökohtaisten tietojen katoamisen uhkana yksityisyydelle ja tietoturvalle. Älypuhelimen kadottami-

sen aiheuttamien kustannuksien lisäksi käyttäjät kokivat ongelmalliseksi myös laitteeseen tallennetut tunnistetiedot, kuten henkilötunnukset, luottokorttitiedot ja muut henkilökohtaiset tiedot, kuten valokuvat ja kontaktiluettelot, joiden pelättiin joutuvan epäluotettavien tahojen käyttöön. (Chin et al., 2012.)

Älypuhelinten sisältämät lukuisat erityyppiset tiedot sekä tiedostot ovatkin usein hyökkääjien listalla: laitteiden sisältämät tiedot ovat usein käyttäjäkohtaisia ja laitteiden personointi on korkealla tasolla. Henkilökohtaisten tietojen lisäksi laitteissa on mahdollisesti myös käyttäjän työhön liittyviä tietoja, jolloin laitteen kadotessa haitat voivat olla hyvinkin suuria esimerkiksi tietojen määrästä ja arkaluonteisuudesta riippuen. Varastettujen tietojen avulla hyökkääjä voi esimerkiksi varastaa uhrin identiteetin ja luottokorttitiedot, jolloin uhrin tietoja ja identiteettiä saatetaan käyttää esimerkiksi petoksissa ja huijauksissa. Hyökkääjä voi myös halutessaan myydä sekä laitteen että sen sisältämät tiedot eteenpäin hyötyjen saamiseksi. (Khan et al., 2015; La Polla, Martinelli, & Sgandurra, 2013.)

Hyökkääjiä motivoivat yleensä rahallinen hyöty, arkaluonteisen datan kerääminen sekä pääsyn takaaminen suojattuihin verkkoihin. Rahallista hyötyä hyökkääjä voi saada esimerkiksi käyttämällä uhrin älylaitetta tekstiviestien lähettämiseen tai puheluiden soittamiseen maksullisiin palvelunumeroihin, joiden avulla hyökkääjä saa kerättyä rahaa uhrilta. Samalla hyökkääjä voi myös yrittää levittää haittaohjelmaa hyödyntämällä uhrin älylaitteen kontaktitietoja, jolloin hyökkääjä voi lähettää esimerkiksi latauslinkkiä haittaohjelmaan esittäen samalla olevansa luotettava lähettäjä, kun vastaanottaja saa viestin suoraan kontaktiltaan. Arkaluonteisen datan keräämisellä puolestaan tavoitellaan esimerkiksi tunnistetietoja, pankkitunnuksia, salasanoja ja muita tärkeitä tietoja, joita hyökkääjä voi käyttää hyväkseen. Esimerkiksi sähköpostiosoitteen ja tähän liittyvän salasanan avulla hyökkääjä voi potentiaalisesti aiheuttaa merkittävää haittaa päästyään uhrin sähköpostitilille, jolloin usein myös pääsy muihin uhrin käyttämiin palveluihin ja sivustoihin tulee hyökkääjälle mahdolliseksi. Pääsy suojattuihin verkkoihin tarkoittaa hyökkääjälle mahdollista pääsyä kyseisessä verkossa liikkuviin tietoihin ja dataan, tai esimerkiksi kyseiseen verkkoon liitettyihin verkkolevyihin ja muihin verkkoresursseihin. Hyökkääjä voi mahdollisesti myös käyttää uhrin verkkoa välikätenä erilaisissa verkkohyökkäyksissä, jolloin alkuperäinen uhri saattaa näyttäytyä hyökkääjänä toiseen kohteeseen, vaikka hyökkäyksen taustalla on jokin muu taho. Myös tietojen urkinta ja niiden varastaminen saattaa olla hyvinkin vahingollista, esimerkiksi jos hyökkääjän haltuun ottama laite on yhdistettyä työpaikan tai muun organisaation verkkoon. (Penning, Hoffman, Nikolai, & Wang, 2014.)

Fyysisen varkauden lisäksi hyökkääjillä on käytössään useita eri tapoja päästä käsiksi käyttäjän älypuhelimen sisältämiin tietoihin. Näihin tapoihin kuuluvat esimerkiksi verkkopohjaiset hyökkäykset, kuten suojaamattomien langattomien verkkojen hyödyntäminen, älypuhelinten bluetooth-ominaisuuden haavoittuvuudet ja verkkohyökkäykset, kuten palvelunesto-hyökkäys (Khan et al., 2015; Leavitt, 2011). Verkkohyökkäyksien lisäksi uhrin älypuhelin voidaan yrittää asettaa haavoittuvaiseksi haittaohjelmille useilla eri

tavoilla, jotka hyödyntävät laitteen käyttämiä sovelluksia ja ominaisuuksia. Haittaohjelmalla tarkoitetaan mitä tahansa haitallista sovellusta ja koodia, jonka tarkoituksena on käyttää uhrin laitetta ilman tämän lupaa. Haittaohjelman tarkoitus voi olla esimerkiksi seurata käyttäjää, kerätä tältä tietoja, käyttää laitetta verkkohyökkäyksissä tai roskapostin lähteenä. Käyttäjä yritetään saada lataamaan haittaohjelma esimerkiksi internetselaimen kautta, saamalla käyttäjä lataamaan ja asentamaan saastutettu sovellus tai levittämällä haittaohjelmaa teksti-, multimedia- ja sähköpostiviestien avulla. (La Polla et al., 2013.)

Usein haittaohjelma ujutetaan luotettavalta vaikuttavan sovelluksen sisälle, jolloin käyttäjä saadaan helpommin asentamaan saastutettu sovellus laitteeseensa. Vastaavasti haittaohjelmaa voidaan myös yrittää levittää verhottuna päivitykseksi viralliselle sovellukselle, jolloin haittaohjelma asentuu samalla, kun käyttäjä hyväksyy päivityksen asentamisen. Käyttäjä voidaan yrittää saada myös vahingossa asentamaan saastutettu sovellus, esimerkiksi lataamalla sovelluksen asennuspaketti automaattisesti laitteeseen, kun käyttäjä vierailee tietyllä verkkosivulla. Automaattisen latauksen lisäksi saastunutta sovellusta voidaan yrittää myös markkinoida erilaisilla hyödyllisiltä kuulostavilla ominaisuuksilla, kuten tallennustilan säästöllä tai laitteen nopeuttamisella, jotta käyttäjä asentaisi sovelluksen entistä todennäköisemmin. (Zhou & Jiang, 2012.) Saastuneet ja haittaohjelmia sisältävät älypuhelinsovellukset ovatkin hyvin yleisiä: tietoturvayhtiö Symantec:in raportin (2015) mukaan vuonna 2014 analysoidusta 6,3 miljoonasta mobiiliapplikaatiosta noin 17 % voitiin luokitella haittaohjelmaksi. Saman raportin mukaan myös 36 % kaikista analysoiduista applikaatioista sisälsi jotain ei-toivottuja ominaisuuksia (engl. grayware), kuten häiritsevää mainontaa, laitteen asetuksia muuttavia ominaisuuksia (esimerkiksi taustakuva, soittoääni jne.) tai käyttäjätietojen kalastelua.

Älypuhelimiin ja älylaitteisiin kohdistuvat uhkat ovat moninaisia, ja niiden välttäminen ja jopa tunnistaminen voivat olla vaikeaa jopa edistyneemmille käyttäjille. Laitteet ovat alttiina sekä perinteisemmälle fyysisille varkaudelle tai haitalle, ja tämän lisäksi oman uhkansa luovat kommunikaatioon ja ohjelmistoihin kohdistuvat hyökkäykset. Uhkien myötä käyttäjille aiheutuu haittoja ja kustannuksia, jos älylaite tai sen data joutuu hyökkääjän armoille.

2.3 Älypuhelinten turvallisuusominaisuudet

Älypuhelimet eivät kuitenkaan ole täysin hyökkääjien vapaasti hyödynnettävissä, sillä laite- sekä sovellusvalmistajat ovat ottaneet suuren osan tunnetuista riskeistä huomioon. Älypuhelimiin on sisällytetty useita erilaisia ominaisuuksia, joiden tarkoitus on suojata käyttäjän dataa ja tietoja hyökkääjiltä. Osa ominaisuuksista ja niiden käyttötavoista vaihtelee hieman eri mobiilikäyttöjärjestelmien, kuten Android:in, iOS:n ja Windows Phone:n välillä, mutta pääosin käyttäjälle tarjottavat ominaisuudet ovat hyvinkin samankaltaisia (Oh et al., 2012). Tässä kappaleessa käsitellään yleisesti tietoturvaa parantavia ominaisuuksia, joiden avulla käyttäjä voi itse vaikuttaa laitteensa tietoturvaan. Turvaominai-

suuksien käytössä on kuitenkin huomioitava, että eri mobiilikäyttöjärjestelmien ja käyttäjien tietoteknisen osaamisen välillä on merkittäviä eroja (Mylonas, Kastania, & Gritzalis, 2013), eivätkä tietoturvaratkaisut aina ole identtisiä eri käyttöalustoilla.

Yksi yleisimmistä ja perustavanlaatuisimmista turvaominaisuuksista on älypuhelimen näyttölukko. Näyttölukko on hyvin samantyyppinen kuin salasanasuojaus erimerkiksi tietokoneessa, jolle kirjautuessa käyttäjältä kysytään salasanaa, jotta tietokonetta ja sen sisältöjä sekä ohjelmistoja voidaan käyttää. Älypuhelinten näyttölukko toimii samalla periaatteella, mutta mobiilialustalle sopivassa muodossa (Van Bruggen et al., 2013). Vaihtoehtoina näyttölukolle (Kuvio 1) ovat esimerkiksi (a) PIN-koodi, (b) salasana ja (c) piirrettävä kuvio. Ilman näyttölukkoa (d) älypuhelimen sisältöön pääsee käsiksi täysin vapaasti esimerkiksi liu'uttamalla sormea laitteen näytöllä.

(a) PIN-koodi (b) Salasana

(c) Piirrettävä kuvio (d) Ei näyttölukkoa

Kuvio 1. Android älypuhelimen näyttölukot

Näyttölukko suojaa tehokkaimmin käyttäjän dataa fyysiseltä hyökkäysyritykseltä esimerkiksi jos laite on varastettu tai hävinnyt. Liian monta kertaa väärin syötetty salasana tai koodi voi esimerkiksi lukita puhelimen, jolloin laitteen saa avatuksi vain kirjautumalla laitteessa käytössä olevaan tiliin jollain muulla alustalla, esimerkiksi tietokoneella. (Oh et al., 2012.) Erityyppisten näyttölukkojen

välillä on kuitenkin myös eroa suojauksen tehokkuudessa. Esimerkiksi piirtokuviolla suojattu laite saattaa olla fyysiselle hyökkäykselle haavoittuvampi salasanasuojaukseen verrattuna: piirtämällä lukituskuvio laitteen näyttöön, saattaa näyttöön jäädä näkyviä rasvajälkiä kuviota piirrettäessä sormessa ja ihossa olevan öljyn takia (Aviv, Gibson, Mossop, Blaze, & Smith, 2010). Kuvion piirtämiseen perustuva näyttölukko on saanut kritiikkiä myös helposta arvattavuudestaan (Andriotis, Tryfonas, Oikonomou, & Yildiz, 2013). Ilman näyttölukkoa oleva, tai pelkkää pyyhkäisylukitusta käyttävä älypuhelin ei luonnollisestikaan suojaa käyttäjän tietoja lainkaan, sillä hyökkääjän ei tarvitse tehdä mitään puhelimen avaamiseksi ja tietoihin pääsemiseksi.

Riskeistä huolimatta merkittävä osa älypuhelinten käyttäjistä ei käytä minkäänlaista näyttölukkoa laitteissaan. Aiempien tutkimusten perusteella 32 % - 40 % (Van Bruggen et al., 2013), 48 % (Imgraben, Engelbrecht, & Choo, 2014), 29 % (N=28) (Egelman et al., 2014) ja 35,6 % (Mylonas et al., 2013) tutkimuksiin osallistuneista eivät käyttäneet minkäänlaista näyttölukkoa älypuhelimissaan. Syitä älypuhelimen lukitsematta jättämiseksi ovat esimerkiksi huono tietoisuus turvaominaisuuksien olemassaolosta tai huono tietotekninen osaaminen (Mylonas et al., 2013; Ngoqo & Flowerday, 2015). Lisäksi syyt kuten halu jakaa älypuhelin lähipiirin, esimerkiksi ystävien tai perheenjäsenten kanssa vaikuttaa haluun jättää älypuhelin ilman lukitusta. Osa käyttäjistä myös pitää laitettaan epäkiinnostavana kohteena hyökkääjille tai eivät muuten pidä älypuhelimeen tallennettuja tietoja tärkeinä tai suojaamisen arvoisina. Näyttölukon käyttö on myös osan käyttäjistä mukaan epäkäytännöllistä tai laitteen käyttöä hankaloittavaa. (Egelman et al., 2014; Karlson, Brush, & Schechter, 2009.)

Älypuhelinten ja suojaustapojen kehittyessä näyttölukoille on kehitetty myös muita vaihtoehtoja aiemmin tässä kappaleessa esiteltyjen lukitusten lisäksi. Esimerkiksi laitteen lukitseminen biometrisellä mekanismilla, kuten sormenjäljellä tai silmän skannauksella, on jo mahdollista uusimmilla laitteilla. Biometriset lukitsemiskeinot saattavat olla myös ratkaisu nykyisten näyttölukkojen käytettävyysongelmaan (Zirjawi, Kurtanovic, & Maalej, 2015).

Näyttölukituksen lisäksi mobiilikäyttöjärjestelmät sisältävät useita käyttäjän datan turvaamiseen soveltuvia ominaisuuksia. Yleisimmät näistä ovat laitteen ja sen sisältämien tietojen salaus (engl. encryption), tietojen etätyhjennys laitteen kadotessa ja tietojen varmuuskopiointi. Tietojen salauksella tarkoitetaan älypuhelimen tietojen muuttamista salattuun muotoon. Tietojen salauksen voi purkaa vain salauksessa käytetyllä avaimella, joka vaikeuttaa hyökkääjän pääsyä tietoihin. Käytännössä salaus esimerkiksi suojaa laitteen sisältämiä tietoja, kun laite on yhdistettynä tietokoneeseen. (Wang, Streff, & Raman, 2012.) Laitteen suojaus myös vähentää tietojen varastamisen riskiä huomattavasti, jos käyttäjän älypuhelin joutuu hyökkäyksen kohteeksi (Mylonas et al., 2013).

Käyttäjän kadottaessa älypuhelimensa, on hänen myös mahdollista pyyhkiä laitteestaan kaikki henkilökohtaiset tiedot käyttämällä mobiilialustoista löytyviä työkaluja. Laitteen kadotessa myös laitteen mahdollinen paikallistaminen on mahdollista, jos käyttäjä on kytkenyt kyseiset ominaisuudet laitteessaan päälle. Mobiilikäyttöjärjestelmien eroista johtuen kaikissa alustoissa kyseiset

ominaisuudet eivät välttämättä ole valmiiksi asennettuina, mutta käyttäjä voi ladata ne esimerkiksi käyttämänsä alustan sovelluskaupasta. Näiden turvaominaisuuksien käyttö myös vähentää käyttäjän tietojen väärinkäytön mahdollisuutta, ja mahdollisesti auttaa käyttäjää myös löytämään kadonneen laitteensa, jolloin laitteen rahallista arvoakaan ei menetetä. (Mylonas et al., 2013.)

Merkittävän uhkan käyttäjän älypuhelimelle aiheuttavat myös haittaohjelmat, jotka usein aiheuttavat haittaa joko hyväksikäyttämällä laitteeseen tallennettuja henkilökohtaisia tietoja tai hyödyntämällä älypuhelimen ominaisuuksia rahallisen hyödyn saavuttamiseksi (Penning et al., 2014). Haittaohjelmien uhriksi joutuminen onkin lukujen perusteella jokseenkin todennäköistä, sillä lähes joka viides käytetty mobiilisovellus on luokiteltu haittaohjelmaksi (Symantec, 2015). Mobiilialustat sisältävätkin ominaisuuksia, joiden tarkoituksena on yrittää estää haitallisten sovellusten asentuminen käyttäjien laiteisiin joko automaattisesti tai käyttäjän itse asentamina.

Suurimmat älypuhelimilla toimivat sovelluskaupat, Google Play Store Android laitteilla ja App Store Applen iOS laitteilla, suodattavat haitalliset sovellukset sovelluskaupoistaan erilaisten tunnistusalgoritmien avulla. Ennaltaehkäisevä sovellusten tarkistus vähentää loppukäyttäjille päätyviä haitallisia sovelluksia heikentämällä niiden leviämismahdollisuuksia, kun saastuneita sovelluksia ei päästetä alustojen virallisiin sovelluskauppoihin. Älypuhelimet jotka toimivat iOS -alustalla (Apple) myös estävät kaikkien ulkopuolisten sovellusten asentamisen laitteeseen, joita ei ole ladattu suoraan App re -sovelluskaupasta. (He et al., 2015.) Android-käyttöjärjestelmä puolestaan mahdollistaa käyttäjälle sovellusten lataamisen ja asentamisen myös muista kuin virallisista lähteistä, kuten Play Store:sta, mutta kyseinen asennusominaisuus on otettava erikseen käyttöön laitteella käyttäjän toimesta. Jos käyttäjä lataa ja asentaa sovelluksia myös epävirallisista lähteistä, on älypuhelimeen kohdistuva haittaohjelmien aiheuttama saastumisen riski korkea. Käyttäjän on myös mahdollista asettaa tuntemattomista lähteistä ladattujen sovellusten asentamiselle rajoituksia Android-järjestelmän asetuksista. (Oh et al., 2012.)

Mobiilikäyttöjärjestelmät ovat myös asettaneet sovelluksille oikeuksia, joita sovellus yleensä pyytää asennuksen yhteydessä. Näiden oikeuksien tavoitteena on suojata laitetta sovelluksilta, jotka pyytävät käyttöönsä epäilyttäviä oikeuksia joiden salliminen saattaa altistaa laitteen hyökkäykselle tai hyväksikäytölle. (Liu, Lin, & Sadeh, 2014.) Käyttöoikeuksia ovat esimerkiksi lupa lukea laitteen sisältämiä tiedostoja, sisältäen esimerkiksi musiikkitiedostot, valokuvat ja niin edelleen, tai lupa käyttää laitteeseen tallennettuja kontaktitietoja, esimerkiksi sosiaalisen median sovellusten avulla ystävien ja tuttujen löytämisen helpottamiseksi. Oikeuksien valtava määrä ja tarpeellisuus ovat kuitenkin osittain kyseenalaisia, sillä ei ole realistista olettaa loppukäyttäjän tietävän, mitä toimintaa kymmenet, jopa sadat eri oikeudet mahdollistavat sovellusten suorittaa (Liu et al., 2014). Oikeuksien hallinnasta entistä vaikeampaa tekee se, että aina sovelluskehittäjätkään eivät itse tiedä, mitä oikeuksia sovelluksen tulisi saada käyttöönsä toimiakseen normaalisti – eivätkä aina itse laitevalmistajatkaan ole oikeuksien hallinnassa ajan tasalla, jolloin liialliset ja turhat sovellusoikeudet voivat

aiheuttaa ongelmia (Wu, Grace, Zhou, Wu, & Jiang, 2013). Jos käyttäjä kokee sovellusta asentaessa sovelluksen pyytämät oikeudet luotettaviksi ja oikeellisiksi, ja hyväksyy ne, ei sovellus voi enää myöhemmin pyytää lisää oikeuksia käyttöönsä (Shabtai, Fledel, Kanonov, Elovici, & Dolev, 2009). Esimerkiksi jos sovellus ei ole asennuksen yhteydessä pyytänyt käyttöoikeutta käyttää laitteen kameraa tai mikrofonia, ei sovellus voi toimiessaan niitä käyttää.

Älypuhelimet ja niiden käyttöjärjestelmät sisältävät usein myös muita perustavanlaatuisia turvaominaisuuksia, jotka eivät välttämättä ole käyttäjälle helposti nähtävissä. Sovellusten suoritus mobiilikäyttöjärjestelmissä on esimerkiksi rajattu niin sanottuihin hiekkalaatikoihin (engl. sandboxing), joka estää sovelluksia käyttämästä muita sovelluksia ja niiden käsittelemiä tietoja. Ellei sovellus ole pyytänyt lupaa muiden resurssien tai sovellusten käyttöön, kuten tekstiviestisovellus oikeutta käyttää laitteen kontaktiluetteloa, ei se saa resursseja tai tietoja käytettäväkseen – kyseinen sovellus ei myöskään voi pyytää oikeutta toiselta sovellukselta, jolle kyseinen oikeus on myönnetty. Tämäntyyppisellä sovellusten suorittamisen rajaamisella kyseisiin hiekkalaatikoihin pyritään estämään haittaohjelmien leviäminen ja niiden pääsy hyväksikäyttämään käyttäjän henkilökohtaisia tietoja joko suoraan laitteesta itsestään tai muiden sallittujen sovellusten kautta. (Shabtai et al., 2010.)

3 TEORIAT JA AIKAISEMPI TUTKIMUS

Tutkielman tavoitteena on selvittää, miten ennalta määritellyt tekijät vaikuttavat älypuhelinkäyttäjän aikomukseen hyödyntää älypuhelimiin sisäänrakennettuja tietoturvaominaisuuksia oman datansa ja tietojensa suojaamiseksi niihin kohdistuvilta uhilta. Sekä aikomukseen yleisesti, että aikomukseen tietoturvan kannalta on jo olemassa aikaisempaa tutkimustietoa laajasti. Tutkielman kantavaksi viitekehykseksi on valittu *tietoturvakäytänteiden noudattamisen yhtenäismalli*, alkuperäiseltä nimeltään **Unified Model of Information Security Policy Compliance** (jatkossa lyhenteenä UMISPC). Kyseinen viitekehys kokoaa yhteen lukuisia teorioita ja malleja käyttäjien tietoturvakäyttäytymiseen liittyen. UMISPC-malli sisältää myös osuuden käyttäjien tietoturvakäyttäytymisestä sekä hyvien tietoturvakäytänteiden noudattamisen aikomuksen, jota tarkastellaan tämän tutkielman tutkimusosuudessa.

Tässä luvussa esitellään UMISPC-malli ja sen viitekehys, samalla läpikäyden teoriat, joiden pohjalta malli on rakennettu. Tämän tutkielman rajauksen kannalta merkittävimmät teoriat esitellään laajasti, ja loput UMISPC:n sisältämistä teorioista hieman suppeammin.

3.1 Tietoturvakäytänteiden noudattamisen yhtenäismalli, Unified Model of Information Security Policy Compliance

Unified Model of Information Security Policy Compliance, suomennettuna *tietoturvakäytänteiden noudattamisen yhtenäismalli*, on malli joka esittelee viitekehyksen, jonka tavoitteena on koota yhteen useita eri tietoturvakäyttäytymiseen liittyviä, yleisesti hyväksyttyjä ja tunnettuja malleja sekä teorioita (Moody et al., 2018). Tietoturvakäyttäytymiseen, ja käyttäytymiseen yleensä, liittyviä teorioita on lukuisia, eikä niiden seasta aina onnistuta löytämään sitä tärkeintä tai osuvinta mallia käyttäytymisen ja aikomuksen tutkimiseen. UMISPC-malli kokoaa tietoturvakäyttäytymisen kannalta merkittävimmät teoriat ja niiden esittämien mallien osat yhteen. Samalla UMISPC yhdistää samankaltaiset teoriat ja muut-

tujat kontruktioihin, sekä poistaa tarpeettomimmat ja heikoimmin tietoturvakäyttäytymistä kuvaavat muuttujat (Moody et al., 2018).

UMISPC-malli käsittää 11 eri teoriaa, joita on joko aikaisemmin käytetty tietoturvakäyttäytymisen tutkimuksessa, tai niiden voidaan olettaa soveltuvan sen tutkimiseen. Näiden teorioiden toimivuutta mallissa on tutkittu empiirisesti kyselytutkimuksella. Mallin teoriat edustavat hyvin laaja-alaisesti eri tieteenaloja, kuten kriminologiaa, psykologiaa, sosiaalipsykologiaa sekä terveyspsykologiaa, joista kaikista löytyy teorioita, joiden avulla tietoturvakäyttäytymistä on yritetty tutkimuksen kautta selittää. Malliin sisällytetyt 11 teoriat ovat seuraavat:

1) Suunnitellun käyttäytymisen teoria (Ajzen, 1985)
2) Ihmistenvälisen käyttäytymisen teoria (Triandis, 1977)
3) Peloteteoria (Gibbs, 1975) ja rationaalisen valinnan teoria (G. S. Becker, 1968; Paternoster & Simpson, 1996)
4) Protection Motivation -teoria (Rogers, 1975)
5) Kontrollitasapainoteoria (Tittle, 1995)
6) Perustellun toiminnan teoria (Fishbein & Ajzen, 1977)
7) Itsesäätelyteoria (Bagozzi, 1992)
8) Neutralisaatiotekniikat ts. neutralisaatioteoria (Sykes & Matza, 1957)
9) Terveysuskomusmalli (M. H. Becker, 1974)
10) Extended Protection Motivation -teoria (Maddux & Rogers, 1983)
11) Laajennettu rinnakkaisprosessointimalli (Witte, 1992)

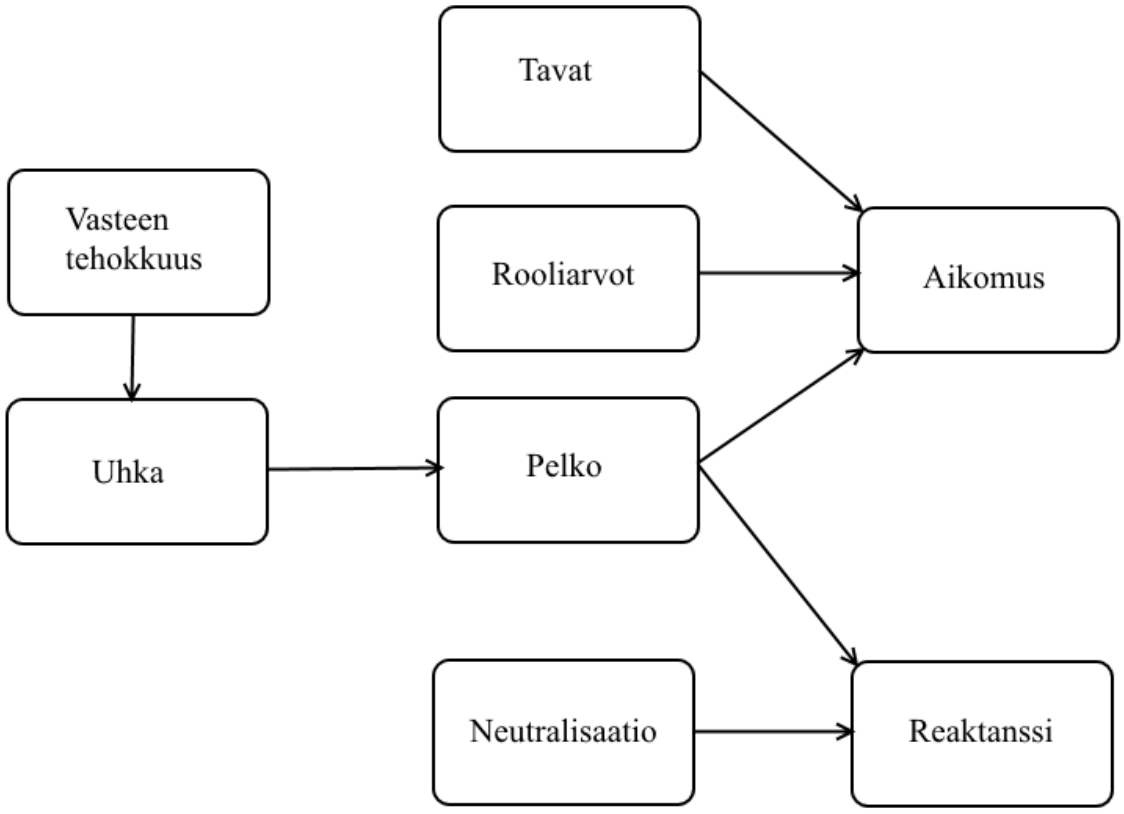
Moody, Siponen & Pahnila (2018) ovat koonneet näistä teorioista yhteen käsitteistön, jonka avulla teorioita on pyritty yhdistämään UMISPC-mallin luomiseksi. Käsitteistön tavoitteena on ollut löytää teorioiden välisiä yhteneväisyyksiä ja tiivistää yhteiset konstruktiot kyseisten käsitteiden alle. UMISPC-malliin on valittu 29 tarkasteltujen teorioiden sisältämää käsitteillä kuvattua konstruktiota, joista tämän tutkimuksen kannalta merkittävimmät on esitelty taulukossa 1.

Taulukko 1. Konstruktioiden käsitteet ja niiden kuvaukset. Mukaillen (Moody et al., 2018).

Käsite	**Kuvaus**
Affekti	Emotionaalinen reaktio tiettyyn tilanteeseen, joka perustuu vaistonvaraisiin ja alitajuisiin prosesseihin
Pelko	Negatiivinen tunnereaktio koettuun merkittävään tai oleelliseen uhkaan, joka aiheuttaa kiihtymystä
Tavat	Käyttäytyminen, joka on tai josta on tullut automaattista siinä määrin, että toimintaa ei tarvitse erityisesti ajatella
Aikomus	Aikomus ryhtyä tiettyyn käyttäytymiseen tai toimintaan
Koettu käytöskontrolli	Toimijan oma käsitys omasta kykeneväisyydestään suorittaa haluttu tai aiottu toiminta
Roolit	Sosiaalinen asema, johon toimija kuuluu tälle tärkeiden sosiaalisten ryhmien sisällä

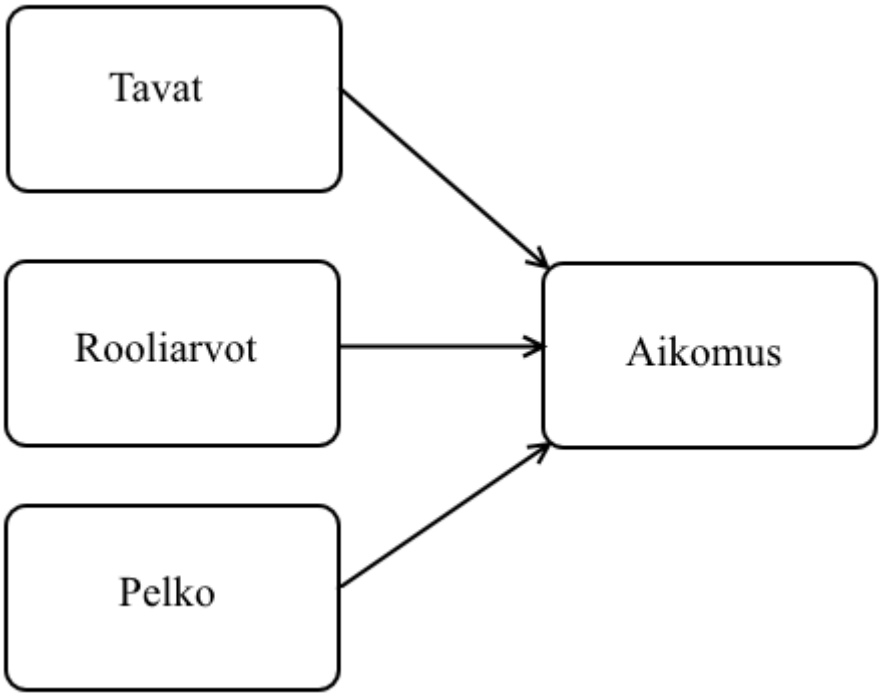
Minäkäsitys	Kokemus siitä, miten hyvin toiminta sopii henkilön omaan käsitykseen itsestään
Subjektiiviset normit	Toimijan käsitys siitä, onko toiminta sopivaa tai hyväksyttyä toimijan lähipiirin mielestä
Vasteen tehokkuus (engl. response efficacy)	Toimijan käsitys siitä, miten hyvin vaste, eli ehdotettu ”hyvä” tapa toimia tilanteessa, vähentää uhkan aiheuttamaa koettua riskiä (Witte, 1992)

UMISPC:n luomisessa Moody, Siponen & Pahnila (2018) kävivät läpi usean mallin iteraation ennen lopullisen UMISPC-mallin esittämistä. Malli koki muutoksia etenkin tutkimuksen eri vaiheissa, jolloin konstruktioiden sisältämät muuttujat muotoutuivat kohti lopullista esitettyä mallia. Lopullisessa mallissa (kuvio 2) 11 käsitellystä teoriasta on löydetty merkittävimmät konstruktiot ja niiden väliset vaikuttavuudet.



Kuvio 2. UMISPC-malli. Mukaillen (Moody et al., 2018).

Tämä tutkielma tarkastelee juurikin UMISPC:stä löytyvää aikomuksen konstruktiota, joten tutkielman laajuuden kannalta käsiteltävää mallia on rajattu. Tässä tutkielmassa käsitellään siis vain aikomusta, ja siihen suoraan liittyviä konstruktioita. Nämä aikomukseen suoraan liittyvät konstruktiot ovat pelko, rooliarvot, tavat sekä luonnollisesti aikomus. Tutkielman käyttämä rajaus löytyy myös kuviosta 3.



Kuvio 3. Tutkielman rajaama UMISPC-mallin osuus. Mukaillen (Moody et al., 2018)

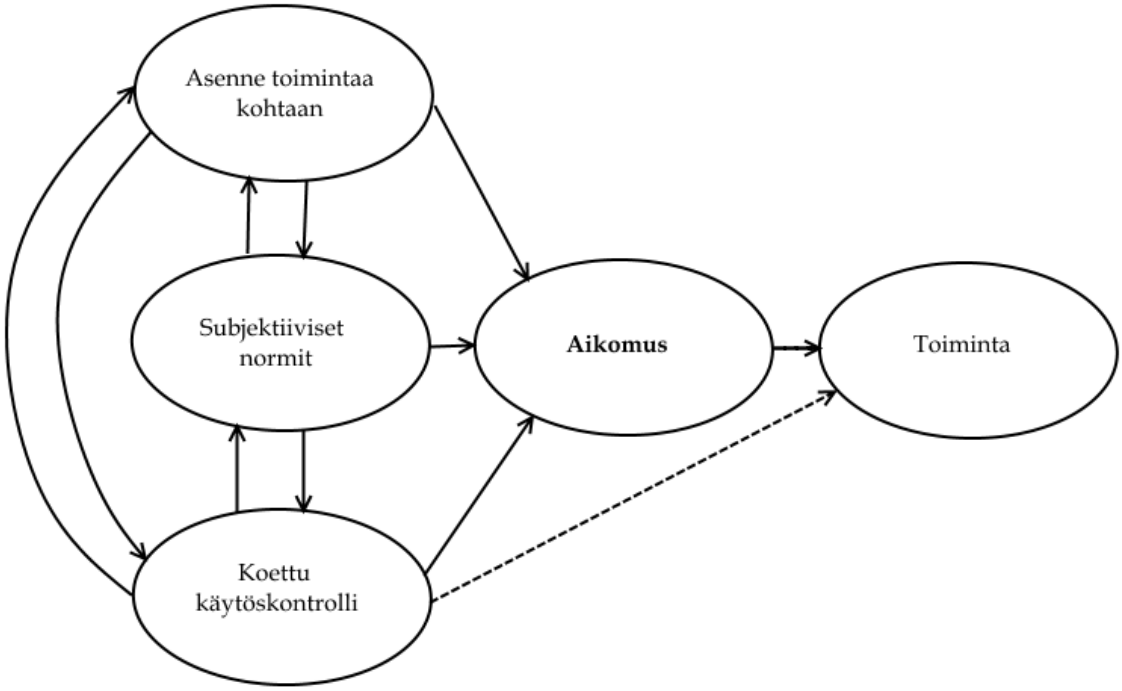
Tämän luvun seuraavissa kappaleissa käydään läpi UMISPC:n sisältämä teoriapohja, joiden avulla malli on rakennettu. UMISPC-mallin konstruktiot sisältävät muuttujia kaikista näistä teorioista, joten niiden läpikäynti on sekä perusteltua että mallin ymmärtämisen kannalta tärkeää. Tutkielman käyttämät konstruktiot, sekä niihin liittyvät teoriat ja muuttuja käydään yksityiskohtaisesti läpi luvussa 4, joka käsittelee tutkielman empiiristä osuutta.

3.1.1 Suunnitellun käyttäytymisen teoria

Eräs aikomukseen ja sen mittaamiseen keskittynyt teoria on Ajzen:in (1991) luoma viitekehys, joka tarkastelee aikomukseen liittyviä tekijöitä. Aikomuksen lisäksi viitekehyksen avulla voidaan arvioida sitä, millä todennäköisyydellä aikomus johtaa varsinaiseen toimintaan. Tämän tutkielman keskittyy juuri UMISPC-mallin *aikomukseen*, sekä siihen vaikuttaviin tekijöihin. Tutkielman empiirisessä tutkimusosuudessa tarkastellaan näiden aikomukseen vaikuttavien tekijöiden suhdetta itse aikomukseen, ja yritetään selvittää, onko malli pätevä myös älypuhelimen suojausaikomuksen kontekstissa. Aikomuksen käsitteen ollessa tutkielman kannalta äärimmäisen merkittävä, sitä käsittelevät teoriat esitellään laajemmin, joihin myös Ajzen:in (1991) suunnitellun käyttäytymisen teoria lukeutuu.

Ajzen:in (1991) suunnitellun käyttäytymisen teoria (engl. theory of planned behaviour, TBP) on hyvin tunnettu viitekehys psykologian alalta. Viitekehys kuvaa henkilön, aktorin eli toimijan, käyttäytymistä tiettyä toimintaa kohtaan. Yksi viitekehyksen tärkeimmistä osatekijöistä on henkilön aikomus suorittaa toiminta: aikomuksen on käsitetty sisältävän henkilön motivaatioon liittyvät tekijät, eli tekijät, jotka lopulta vaikuttavat toiminnan suorittamiseen. Motivaatio kuvaa sitä, kuin paljon henkilö on valmis ponnistelemaan lopullisen toiminnan suorittamiseksi.

Kuvio 4 sisältää kuvauksen Ajzen:in (1991) viitekehyksestä. Muut henkilön aikomukseen liittyvät osatekijät ovat kyseisen henkilön asenne tarkasteltavaa toimintaa kohtaan, subjektiiviset normit sekä koettu käytöskontrolli. Näistä koetun käytöskontrollin on myös huomattu vaikuttavan suoraan toiminnan suorittamiseen.



Kuvio 4. Suunnitellun käyttäytymisen teoria. Mukaillen Ajzen (1991).

Asenteella toimintaa kohtaan tarkoitetaan henkilön kokemaa ajatusta siitä, onko tällä toimintaa kohtaan suotuisa vai epäsuotuisa tuntemus. Asenteen vaikutus aikomukseen on yleisesti ottaen aina positiivinen, jos toiminnalla koetaan olevan positiivinen tai hyödyllinen lopputulos. Samalla asenteen vaikutus aikomukseen ja tätä kautta toimintaan on negatiivinen, jos toiminnan oletetaan olevan haitallinen tai aiheuttavan epäsuotuisan lopputuloksen. Tämän tutkielman kontekstissa esimerkiksi asenne näyttölukon käyttöä kohtaan voi vaikuttaa aikomukseen positiivisesti tai negatiivisesti älypuhelinkäyttäjän katsontakannasta riippuen: näyttölukon voidaan kokea parantavan tietoturvaa, joten asenteen vaikutus aikomukseen on positiivinen. Toisaalta jos näyttölukon käyttö koetaan hankalaksi tai häiritseväksi, voidaan vaikutuksen aikomukseen olettaa olevan negatiivinen. (Ajzen, 1991.)

Subjektiivisilla normeilla tarkoitetaan ulkoista sosiaalista painetta suorittaa toiminta, tai olla suorittamatta tarkasteltava toiminta. Nämä normit voivat olla esimerkiksi toimijan lähipiirin, kuten perheen ja ystävien asenne tarkasteltavaa toimintaa kohtaan. Vaikutus voi tulla myös yleisemmältä tasolta, kuten yhteiskunnalta tai asiantuntijoilta, jotka voivat vaikuttaa henkilön toimintaan. Subjektiiviset normit edustavat sidosryhmien asenteen lisäksi sitä, millainen toiminta toimijan lähiympäristössä koetaan oikeaksi tai oikeelliseksi. Samoin

kuin asenteen osalta, myös subjektiivisten normien positiivinen ja negatiivinen vaikutus toiminnan aikomukseen on havaittavissa. Jos nämä normit suhtautuvat positiivisesti toimintaa kohtaan, on vaikutus aikomukseen yleensä myös positiivinen. Näin ollen normien negatiivinen suhtautuminen toimintaan vaikuttaa aikomukseen yleensä negatiivisesti. Tutkielman kontekstissa älypuhelinkäyttäjään voi vaikuttaa positiivisesti esimerkiksi asiantuntijoiden kehotukset näyttölukon käyttöön tietoturvaseminaarin luennolla tai tietoiskussa. Vastaavasti negatiiviset subjektiiviset normit voivat syntyä esimerkiksi, jos älypuhelinkäyttäjän ystäväpiiri ei pidä näyttölukon käyttöä tarpeellisena tai pitää sen käyttöä jopa haitallisena: näyttölukon käyttö voidaan kokea haitalliseksi sosiaalisen kanssakäymisen kannalta, jos esimerkiksi ystävykset eivät helposti pysty käyttämään toistensa älypuhelimia. On kuitenkin huomioitava, että ulkoisen sosiaalisen paineen vaikutus toiminnan suorittamiseen ei aina toteudu, vaan toimijan oman harkinnan on huomattu olevan lopullisen päätöksen kannalta merkittävämpi osatekijä. (Ajzen, 1991.)

Koettu käytöskontrolli (engl. perceived behavioural control) sisältää toimijan kokemat uskomukset siitä, miten hyvin tai huonosti tämä pystyy toiminnan toteuttamaan. Koettu käytöskontrolli voidaan edelleen jakaa kahteen erilliseen osaan, koettuun minäpystyvyyteen (engl. self-efficacy) ja koettuun kontrolliin (engl. controllability) (Ajzen, 1985). Koettu minäpystyvyys sisältää henkilön kokeman sisäisen käsityksen siitä, miten hyvin tai huonosti tämä pystyy toiminnan toteuttamaan. Esimerkiksi jos älypuhelinkäyttäjä kokee ymmärtävänsä ja osaavansa käyttää älypuhelinsovellusten oikeuksienhallintaa, hän todennäköisemmin käyttää tätä tietoturvaominaisuutta, kuin jos hän kokisi toiminnan vaikeana ja itsensä osaamattomana kyseisen ominaisuuden käyttöön. Koettu kontrolli puolestaan kuvaa henkilön ulkoisia mahdollisuuksia toiminnan suorittamiseen. Ulkoisia mahdollisuuksia, tai resursseja, ovat esimerkiksi sormenjälkitunnistuksella toimiva näyttölukko: vaikka henkilön asenne ja pystyvyyden kokemus olisivatkin positiivisia sormenjälkitunnistusta kohtaan, ei henkilön älypuhelimessa välttämättä ole kyseistä ominaisuutta, joten toiminnan suorittaminen on resurssien puutteen vuoksi mahdotonta. Näin ollen koettu käytöskontrolli vaikuttaa aikomuksen lisäksi suoraan toiminnan toteutumiseen (ks. Kuvio 2). (Ajzen, 1991.)

Viitekehyksen mukaan kaikki aikomukseen vaikuttavat tekijät vaikuttavat myös toisiinsa. Asenne toimintaa kohtaan, subjektiiviset normit ja koettu käytöskontrolli ovat vuorovaikutuksessa keskenään. Useimmissa tapauksissa yhden tekijän positiivinen vaikutus peilautuu positiivisesti myös toiseen tekijään. Vastaavasti negatiivinen vaikutus saattaa näkyä negatiivisena vaikutuksena toiseen tekijään. Tekijöiden vaikutus toisiinsa ei kuitenkaan ole absoluuttinen: yhden tekijän negatiivinen vaikutus muihin saattaa olla hyvinkin pieni, tai sen vaikutus ei näy käytännössä lainkaan. Esimerkiksi resurssien puute, kuten sormenjälkitunnistuksen puuttuminen, ei välttämättä vaikuta lainkaan henkilön asenteeseen näyttölukon käyttöä kohtaan, eikä sen puuttuminen myöskään tee siitä huonompaa tai epähyväksyttävämpää subjektiivisten normien osalta. (Ajzen, 1991.)

3.1.2 Ihmistenvälisen käyttäytymisen teoria

Triandiksen (1977) ihmistenvälisen käyttäytymisen teorian (engl. theory of interpersonal behavior, TIB) mukaan ihmisten käyttäytymistä ei voida tarpeeksi tarkasti arvioida pelkkien normien, asenteiden ja aikomuksen pohjalta. Triandis puolestaan esittää mallia, johon on valittu myös tunteellinen komponentti. Tunteellisen komponentin lisäksi mallissa on mukana myös sosiaalisia osatekijöitä, asenteen ennusteita ja muita tekijöitä, kuten *tavat,* jotka saattavat myös ennustaa ihmisten toimintaa. (Moody et al., 2018; Triandis, 1977.)

Teoria esittää, että ihmisen asenteeseen toimintaa kohtaan vaikuttaa merkittävästi toimijan kokemat hyödyt ja kustannukset, jotka toiminnan suorittaminen saattaa aiheuttaa. Hyötyjen ja kustannusten lisäksi toiminnan suorittamisen ennustamisessa tulee ottaa huomioon toimijan yleinen tuntemus tai tuntemukset toimintaa kohtaan, jotka eivät aina perustu loogisiin tai rationaalisiin osatekijöihin. (Triandis, 1977.) Tämä tuntemus, *affekti*, on yksi teorian esittämistä osatekijöistä, jonka osuutta aikomukseen toimintaa kohtaan tulisi tarkastella.

Teoria esittelee myös sosiaalisia vaikuttumia, jotka ovat yhteydessä toiminnan aikomukseen. Sosiaalisilla vaikuttimilla Triandis (1977) tarkoittaa minäkäsitystä (engl. self-concept) ja roolia. Nämä sosiaaliset vaikuttimet voivat muuttaa toimijan käytökseen liittyvää aikomusta (Moody et al., 2018). Toimijan minäkäsitys sekä toimijan rooli sosiaalisissa piireissään ovat molemmat sosiaalisia tekijöitä, joiden uskotaan vaikuttavan toimijan aikomukseen ryhtyä tarkasteltuun toimintaan. Minäkäsityksellä tarkoitetaan toimijan käsitystä itsestään ja siitä, miten hyvin toiminnan suorittaminen, tai suorittamatta jättäminen, sopii toimijan omaan käsitykseen siitä, millainen toiminta on hänelle itselleen sopivaa. (Triandis, 1977) Esimerkiksi vahvasti tietoturvastaan kiinnostunut ja puhelimensa suojaamiseen pyrkivä toimija saattaa kokea, ettei epämääräisiltä vaikuttavien ilmaisten puhelinsovellusten asentaminen ole turvallista, jättää hän sovellukset asentamatta, sillä toiminta ei sovi hänen omiin arvoihinsa.

Aikomukseen vaikuttaa myös toimijan *rooli* sosiaalisten piiriensä sisällä, kuten esimerkiksi perheen, työpaikan tai ystävien kesken. Roolilla tarkoitetaan toimijan sosiaalista sijaintia sosiaalisten piirien sisällä. (Triandis, 1977.) Esimerkkinä roolista perheen sisällä ”teknologianero”, jolta koko perhe kysyy ohjeita, ja joita tämä henkilö auttaa tietoteknisissä ongelmissa. Kyseisessä tilanteessa toimija saattaa kokea painetta toimia tietyllä tavalla, esimerkiksi pitää huolta omasta ja muiden tietoturvasta osaamisensa puitteissa, jolloin kyseisen ”teknologianeron” rooli saattaa vaikuttaa toimijan aikomukseen käyttää tietoturvaa parantavia ominaisuuksia tai toimintatapoja. Roolit ryhmien sisällä voivat vaikuttaa henkilön toimintaa niin, että normit sekä sosiaalinen paine ryhmän sisällä voivat kannustaa henkilöä toimimaan omaan rooliinsa sopivalla ja johdonmukaisella tavalla (Moody et al., 2018).

Sosiaalisten osatekijöiden lisäksi Triandis (1977) esittää *tapojen* sekä *vaikuttavien olosuhteiden* olevan yhteydessä toimintaan ja sen aikomukseen. Tavat tarkoittavat käyttäytymistä, josta on tullut toimijalle automaattista, eikä sen suorittamiseen tarvita tietoista käskyä toiminnan tekemiseksi (Verplanken, 2006).

Toisaalta tapoihin perustuva toiminta voidaan suorittaa ilman tietoista ajatustyötä (engl. conscious), joka ei enää sisälly ihmistenvälisen käyttäytymisteorian esittämän tietoisesti tarkoituksellisen prosessin piiriin (Moody et al., 2018).

Vaikuttavien olosuhteiden vaikutus aikomukseen ja toimintaan esitellään myös osana Triandiksen (1977) teoriaa. Näillä olosuhteilla tarkoitetaan toimijaan kohdistuvaa ulkoista vaikutusta, joka voi ohjata toimijan kokonaan pois aiotusta toiminnasta, tai tehdä siitä vaikeampaa koettuja kustannuksia lisäämällä (Triandis, 1977). Ulkoinen vaikutin voi olla esimerkiksi aiemmin mainitun ”teknologianeron” tapauksessa kyseisen neron ystävän pyyntö auttaa tätä puhelimensa tietojen varmuuskopioinnissa. Vaikka toimija haluaisikin auttaa ystäväänsä, ei tämä välttämättä aio tehdä niin, esimerkiksi jos ystävä asuu kaukana toisella paikkakunnalla, jolloin toimijan kokemat kustannukset (kirjaimelliset ja/tai henkiset) toimintaan nähden saattavat olla kohtuuttomat.

Ihmistenvälisen toiminnan teorian merkittävin anti tähän tutkielmaan on affektin sekä roolin käsite, sekä niiden vaikutus toiminnan aikomukseen. Myös minäkäsityksen konsepti on merkittävässä osassa UMISPC-mallissa, jonka pohjalta aikomusta myös tarkastellaan. UMISPC-malli käsittelee myös tapoja (engl. habits), jotka pohjautuvat UMISPC:ssä Verplanken & Orbell:in (2003) kaksitoista kysymystä sisältävään indeksiin tapojen voimakkuudesta (alkup. Self-report Index of Habit Strength, SRHI).

3.1.3 Peloteteoria ja rationaalisen valinnan teoriat

Gibbsin (1975) peloteteoria (engl. deterrence theory, DT) on tunnettu teoria kriminologian alalta, jota on käytetty useasti myös tietoturvakäyttäytymistä tutkittaessa. Peloteteorian mukaan toimija, peloteteorian kontekstissa rikollinen, ryhtyy rikokseen, kun sen aiheuttamat hyödyt ajavat oletettujen kustannusten ohitse (Gibbs, 1975). Peloteteorian nimen mukaisesti näiden kustannusten on tarkoitus toimia pelotteena, jotta rikollinen ei ryhtyisi rikokseen nostamalla mahdolliset kustannukset rikoksesta saatavia hyötyjä korkeammiksi (Gibbs, 1975).

UMISPC-malli laajentaa kustannusten käsitettä laajentamalla sen käsitettä myös rationaalisen valinnan teorioilla (engl. rational choice theory, RCT), joita löytyy usealta eri tutkimus- ja tieteenalalta. UMISPC:n käyttämät rationaalisen valinnan teoriat ovat Beckerin (1968) sekä Paternoster & Simpsonin (1996), jotka ovat tuttuja myös kriminologian alalta, joiden mukaan toimijat (rikolliset) ovat rationaalisesti toimivia yksilöitä, jotka laskelmoivat rikoksesta saatavat hyödyt ja kustannukset ennen siihen ryhtymistä. Paternoster & Simpsonin (1996) mukaan toiminnan kustannuksiksi lasketaan myös toiminnasta saatavat viralliset sekä epäviralliset sanktiot, kuten esimerkiksi sakot tai vankeustuomio, jotka toimija ottaa huomioon ennen toimintaan ryhtymistä.

UMISPC olettaa näiden teorioiden perusteella, että näitä toiminnan kustannuksia tulee pitää tarpeeksi vakavina seuraamuksina toimijan kannalta tarkasteltuna, jotta tosiasiallinen pelotevaikutus voisi syntyä ja näin ollen vaikuttaa toimijan aikomukseen (Moody et al., 2018). Aiemmin mainitut koetut kustannukset tai pelotteet, kuten viralliset rangaistukset, voidaan kuitenkin nähdä

liian voimakkaina toimina tietoturvakäyttäytymisen kontekstissa. Tämän vuoksi UMISPC-malli tarkastelee toiminnan kustannuksia myös häpeän kannalta, jonka on huomattu olevan tehokas epämuodollinen keino tietoturvakäyttäytymisen kontrolloinnissa. Häpeän aiheuttamia kustannuksia ovat esimerkiksi syyllisyydentunne tai kiusaantuminen, joita toimija kokee tehtyään jotain tilanteeseen tai sosiaaliseen rooliinsa sopimatonta, joka pätee myös tietoturvarikkeisiin. (Moody et al., 2018; Siponen & Vance, 2010.)

Esimerkiksi tietoturvastaan kiinnostunut henkilö saattaa yhdistää puhelimensa ulkomailla tuntemattomaan langattomaan verkkoon verkkosivuja selatakseen: toimija kokee saavansa hyötyä siitä, ettei tämän tarvitse maksaa kalliita datamaksuja ulkomailla, mutta saattaa samalla kokea syyllisyyttä tietoturvarikkeestään, sillä tuntemattomien langattomien verkkojen käyttö voi olla vaarallista. Esimerkissä toimija kokee tietoturvarikkeestään saatavan hyödyn olevan mahdollisia kustannuksia suurempi, ja näin ollen suorittaa rikkeen puhelimensa vaarantumisen pelotteesta huolimatta.

UMISPC-mallin mukaan sekä peloteteorian että rationaalisen toiminnan teorian esittelemien kustannusten tulee olla toimijan mielestä tarpeeksi vakavia ja merkittäviä. Kustannusten merkittävyys toimijalle on tärkeää, jotta kustannus voi toimia todellisena pelotteena, ja näin vaikuttaa toimijan käyttäytymiseen ja aikomukseen. (Moody et al., 2018.)

3.1.4 Protection Motivation –teoria

UMISPC-malli esittää myös pelon olevan vaikutin tietosuojakäyttäytymiseen aikomuksessa. Malli pohjaa pelkoon liittyvän teorian Rogersin (1975) Protection Motivation –teoriaan (PMT), joka käsittelee ihmisten toimintaa ja aikomusta terveyteen liittyvien uhkien perusteella. PMT selittää ihmisten toimintaa pelkoa aiheuttavien tilanteiden ja tapahtumien aiheuttaman kognitiivisen prosessin perusteella, jolloin toiminta aiheutuu reaktiosta pelkoa aiheuttavaan tapahtumaan tai tilanteeseen. Pelkoon perustuvaa toimintaa voidaan pitää rationaalisesta toiminnasta poikkeavana, jolloin toiminta saattaa perustua tunteeseen eikä järjelliseen, suunniteltuun aikomukseen. (Rogers, 1975.) Myös PMT:n kohdalla, samoin kuin peloteteorian ja rationaalisen toiminnan teorian yhteydessä, uhan tai pelotteen tulee olla toimijan mielestä tarpeeksi merkittävä, jotta teorian esittämä pelkovaste voi syntyä, ja näin vaikuttaa toimijan käyttäytymiseen (Moody et al., 2018).

Vaikka PMT:tä on alun perin käytetty ihmisten terveyteen liittyvien uhkien kontekstissa, on sitä käytetty aiemmin myös tietoturvakäyttäytymisen tutkimuksessa (Moody et al., 2018). Teoria esittelee myös selviytymiskeinoja (engl. coping mechanism), joita toimijat käyttävät koettua uhkaa vastaan ehkäistäkseen sekä uhkan toteutumista että sen toteutumisen aiheuttamaan pelkoa (Rogers, 1975). Näin ollen toimijan käytökseen vaikuttaa tämän kokema minäpystyvyys: toimija yrittää vaikuttaa omalla toiminnallaan uhkan toteutumiseen, joko sen vaikutuksia lieventämällä, tai yrittäen kokonaan estää uhkan toteutuminen. On kuitenkin huomioitava, että terveystieteen ja tietoturvakäyttäytymi-

sen kontekstissa käytettävät määritteet pelolle ovat samat. Tämän käsitteiden yhteneväisyyden vuoksi ei voida olla varmoja siitä, ovatko terveyteen kohdistuvat pelot täysin samanlaisia kuin tietoturvaan liittyvät pelot. (Moody et al., 2018.)

UMISPC-mallin luomisen empiirisessä osuudessa on käytetty PMT:hen perustuvaa Pain Anxiety Symptoms Scale –kyselymittaristoa (PASS), joka on alun perin luotu mittaamaan krooniseen kipuun liittyvää pelkoa ja sen aiheuttamaa ahdistuneisuutta (McCracken, Zayfert, & Gross, 1992). UMISPC-mallin luomiseen käytetyssä kyselyssä kysymykset on johdettu Osman, Barrios, Osman, Schneekloth, & Troutman:in (1994) käyttämästä PASS-mittaristosta, joka on sovitettu tietoturvakäyttäytymisen kontekstiin ja sen mittaamiseen (Moody et al., 2018).

3.1.5 Kontrollitasapainoteoria

Kontrollitasapainoteoria (engl. control balance theory, CBT) on myös tuttu kriminologian alalta. Tittle:n (1995) esittämä teoria tarkastelee ihmisten käyttäytymistä niin kutsutun kontrollitasapainon näkökulmasta. Kontrollitasapainoteorian mukaan tämän tasapainon järkkyminen saa aikaan poikkeavaa käyttäytymistä. Tällä järkkymisellä tarkoitetaan koetun kontrollin ylijäämää (engl. surplus) ja alijäämää (engl. deficit), jotka saavat toimijat käyttäytymään poikkeavasti. Tällä poikkeavalla toiminnalla, esimerkiksi rikoksella, toimija pyrkii joko tasaamaan kokemansa kontrollin epätasapainoa, tai edelleen lisätäkseen kontrolliaan muista. (Tittle, 1995.) Kontrollin ylijäämän tilanteessa toimijalla on korkeampi insentiivi kontrolloida muita ja muiden toimintaa, samalla edelleen lisäten omaa kontrollin ylijäämäänsä. Kontrollin alijäämä puolestaan saa toimijan toimimaan poikkeavasti lisätäkseen kokemaansa kontrollin tunnetta, jonka tavoitteena on vähentää jonkin ulkoisen tahon kontrolloitavana olemisen tunnetta. Sekä ylijäämän että alijäämän tilanteessa toimijat käyttäytyvät poikkeavalla tavalla lisätäkseen kontrolliylijäämäänsä, ja alijäämän tapauksessa päästäkseen koetun kontrollin tasapainoon, tai tasapainon ylijäämään. (Tittle, 1995.) Esimerkiksi koettu kontrollin ylijäämä saa toimijan antamaan työpaikalla alaiselleen moraalisesti tai eettisesti arveluttavia tehtäviä, kuten tilastomanipulointi tai harhaanjohtavan tiedon levittäminen. Alijäämäisessä tilanteessa työntekijät saattavat esimerkiksi mennä lakkoon tai mustamaalata auktoriteetteja tai vallanpitäjiä, jolloin toiminnan tavoitteena on lisätä koettua kontrollia sen alijäämän pienentämiseksi. (Piquero & Piquero, 2006; Tittle, 1995.)

Piquero & Piquero (2006) tarkastelevat kontrollitasapainoteoriaa organisatorisessa kontekstissa, josta UMISPC-malli edelleen johtaa sen tietoturvakäyttäytymisen piiriin. Teoriaa ei myöskään ole käytetty tietoturvakäyttäytymisen tutkimuksessa, ja UMISPC yrittää osaltaan vastata tähän puutteeseen samalla testaten teorian toimivuutta tietoturvakäyttäytymisen kontekstissa (Moody et al., 2018).

3.1.6 Muut UMISPC-mallin teoriat

Tässä kappaleessa käydään läpi loput UMISPC-mallin luomisessa käytetyt teoriat lyhyesti läpi. Tämän tutkielman kannalta kyseiset teoriat eivät ole pääosassa, mutta niiden esittely on tärkeää UMISPC-mallin toiminnan ja rakenteen ymmärtämisen kannalta. Kyseiset teoriat ovat myös olleet merkittävässä asemassa UMISPC:n eri iteraatioissa, joten niiden esittelyä ei voi sivuuttaa.

Perustellun toiminnan teoriaa (engl. theory of reasoned action, TRA) voidaan pitää suunnitellun toiminnan teorian (TPB) esiasteena. Fishbein & Ajzen (1977) esittelivät teoriassaan käsityksen siitä, että käyttäytyminen on aikomuksellista (engl. intentional). Tämä aikomuksellisuus on ennustettavissa toimijan asenteesta aiottua toimintaa kohtaan, ja mikä tahansa toimijan subjektiivisesti kokema normi voi vaikuttaa toiminnan suorittamiseen (Fishbein & Ajzen, 1977). TRA:n pohjalta luotu ja laajasti tunnettu aikomusta tarkasteleva suunnitellun toiminnan teoria (engl. theory of planned behavior, TBP) käytiin perusteellisemmin läpi aiemmin tässä kappaleessa, ja se sisältääkin suurilta osin samat komponentit kuin TRA.

Itsesäätelyteoria (engl. theory of self-regulation) jatkaa perustellun toiminnan teorian (TRA) jalanjäljissä ja lisää tähän *halun* (engl. desire) käsitteen. Bagozzi (1992) määrittelee teoriassa halun kognitiivisena tai emotionaalisena taipumuksena sille, miten toimija käyttäytyy. Bagozzi (1992) kritisoi TRA:ta siitä, että asenne toimintaa kohtaan ei välttämättä ole ainoa, joka vaikuttaa lopulliseen käyttäytymiseen. Teorian mukaan toimijalla saattaa olla myönteinen asenne toimintaa kohtaan, mutta toiminnan kanssa ristiriidassa oleva halu, joka voi estää toimintaan ryhtymisen (Bagozzi, 1992). Vaikka teorian esittämä teoreettinen selitys halun vaikutuksesta lopulliseen käyttäytymiseen on vahva, ei sitä ole aiemmin käytetty tietoturvakäyttäytymisen tutkimuksessa (Moody et al., 2018).

Neutralisaatiotekniikat tai *neutralisaatioteoria* (engl. theory of neutralization) selittää toimijan poikkeavaa käyttäytymistä tarkastelemalla sitä, miten toimija selättää normit ja pelotteet, jotka liittyvät tarkasteltavana olevaan poikkeavaan toimintaan. Teorian mukaan toimija selittää tai järkeistää itselleen syitä, joilla tämä käyttäytyy poikkeavalla tavalla, esimerkiksi rikkomalla sääntöjä, käytäntöjä tai lakeja. (Siponen & Vance, 2010; Sykes & Matza, 1957.) Neutralisaatiotekniikoita ovat esimerkiksi vastuun kieltäminen tai sen välttely, toiminnasta aiheutuneen haitan vähättely ja toiminnan oikeuttaminen tilanteen perusteella (Sykes & Matza, 1957). UMISPC:n mukaan neutralisaatiotekniikat lisäävät ymmärrystä siitä, miten toimijat selittävät tai järkeistävät tietoturvaa heikentäviä toimiaan itselleen (Moody et al., 2018).

Terveysuskomusmalli (engl. health benefit model) selittää alun perin toimijan käytöstä terveyteen kohdistuvaa uhkaa kohtaan. Beckerin (1974) mukaan toimija pyrkii pienentämään koettua ja mahdollista uhkaa toimimalla tavalla, joka vähentää uhkan mahdollisuutta realisoitua. Turvallisesti toimimalla toimija hyötyy riskin pienentymisellä, joka edelleen johtaa koetun uhkan toteutumisen pienentymiseen. Vastaavasti turvallinen toiminta ei saa aiheuttaa toimijalle

liikaa kustannuksia, parhaimmassa tapauksessa ei lainkaan: jos turvallisena pidetty toiminta on toimijalle liian kallista, ei tämä välttämättä toimi turvallisella tavalla. (M. H. Becker, 1974; Moody et al., 2018.)

Extended Protection Motivation –teoria (PMT2) nimensä mukaisesti laajentaa Rogersin (1975) protection motivation –teoriaa (PMT) lisäämällä siihen toimijan kokemat hyödyt ja kustannukset toimintaa kohtaan. Hyödyillä tarkoitetaan toimijalle toiminnasta aiheutuvia positiivisia vaikutuksia, ja kustannuksilla negatiivisia vaikutuksia. Sekä toiminnasta saatavat hyödyt että toiminnan mahdolliset kustannukset vastaavasti lisäävät ja vähentävät toimintaan ryhtymisen todennäköisyyttä. (Maddux & Rogers, 1983.)

Laajennettu rinnakkaisprosessointimalli (engl. extended parallel processing model, EPPM) on Witte:n (1992) esittelemä malli, joka selittää toimijan suhtautumista terveyskampanjoihin, tarkemmin joko niiden hyväksymiseen tai hylkäämiseen. Mallin mukaan toimija joko muokkaa käyttäytymistään terveyskampanjan ajamaan terveellisempään suuntaan, tai hylkää kampanjan ja jatkaa epäterveellistä elämäntapaansa.

EPPM olettaa pelon tunteen syntyvän, kun koettu uhka on suurempi kuin pystyvyyden tunne uhkaa vastaan (Witte, 1992). Tällä tarkoitetaan esimerkiksi, jos henkilö kokee pakollisen pankkisovelluksen käytön vaarallisena, minkä vuoksi hän kokee mahdollisen rahan menetyksen konkreettisena uhkana. Tässä tilanteessa toimija kokee, ettei hän itse pysty vaikuttamaan uhkan realisoitumiseen merkittävästi sovelluksen pakollisuuden takia, minkä vuoksi hän saattaa tuntea pelkoa.

Mallin mukaan toimijalla on merkittävä halu vähentää pelon aiheuttamaa epämukavuutta, jolloin tämä ottaa käyttöönsä emotionaaliset selviytymistekniikat. Nämä tekniikat ovat välttäminen ja reaktanssi, jotka ovat myös niin kutsuttuja pelon kontrollivasteita (engl. fear control response). Välttämisellä tarkoitetaan uhkaan liittyvien vihjeiden tai tiedon välttelyä joko tietoisesti tai tiedostamattomasti, jolloin pelontunne ei pääse syntymään. Reaktanssi puolestaan tarkoittaa uhkaan liittyvien asioiden tarkoituksellista hylkäämistä, esimerkiksi pitämällä uhkaa epäuskottavana tai merkityksettömänä, jolloin pelkoa ei myöskään pääse syntymään. (Moody et al., 2018.)

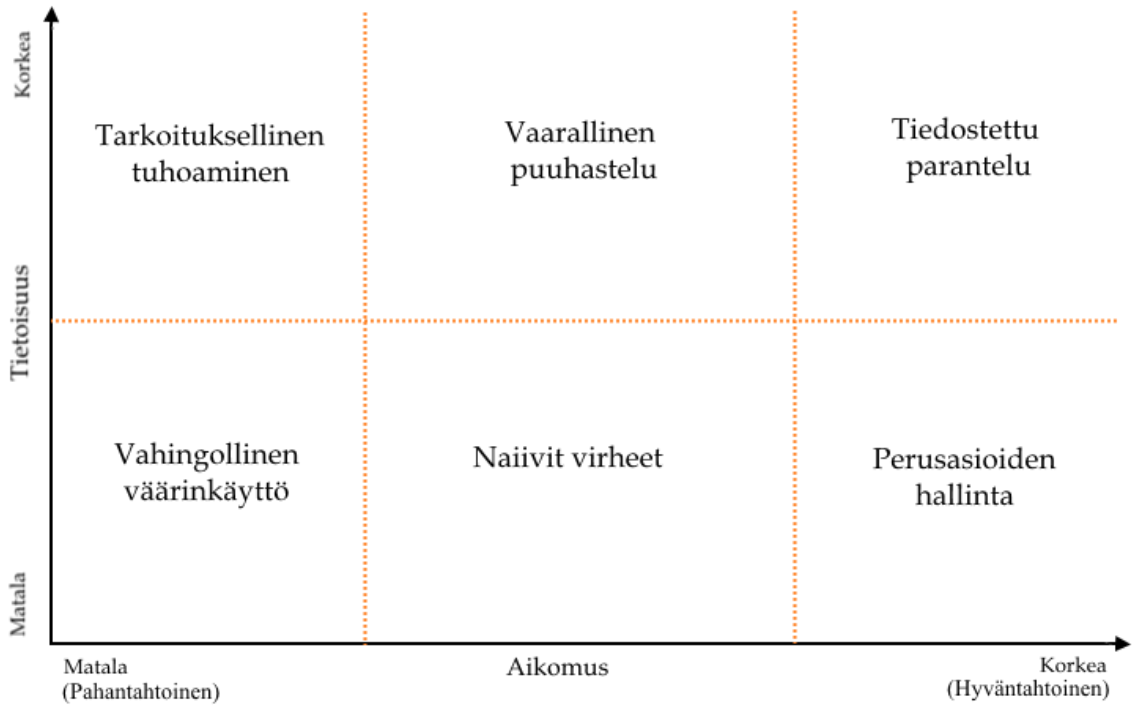
3.2 Loppukäyttäjän tietoturvakäyttäytyminen

UMISPC-mallin lisäksi tutkielmassa käsitellään myös muuta aikaisempaa kirjallisuutta tietoturvakäyttäytymiseen liittyen tutkielman empiirisen tutkimusosuuden perustelemiseksi. Tutkielman konteksti poikkeaa merkittävästi UMISPC:stä, joten tässä kappaleessa esiteltävien teorioiden tavoitteena on siirtää konteksti älypuhelimen käyttäjiä koskevaksi. Tähän tarkoitukseen valittiin loppukäyttäjien tietoturvakäyttäytymistä käsittelevä Stanton, Stam, Mastrangelo & Jolton:in (2005) viitekehys, jonka Ngoqo & Flowerday (2015) ovat muokanneet älypuhelinkontekstiin sopivaksi.

Stanton et al. (2005) ovat analysoineet loppukäyttäjien tietoturvakäyttäytymistä organisaatioissa. Tutkimuksensa perusteella he ovat luoneet viitekehyksen, joka jakaa loppukäyttäjien käyttäytymisen kahden muuttujan perusteella. Nämä muuttujat ovat asiantuntemus (engl. expertise) sekä aikomus (engl. intention). Asiantuntemus on viitekehyksessä jaettu alkamaan vasta-alkajasta ja päättymään eksperttiin, ja aikomus haitallisesta hyödylliseen.

Viitekehyksen perusteella tutkijat ovat päätyneet kuuteen eri kategoriaan, joihin loppukäyttäjä voidaan tietoturvakäyttäytymisensä perusteella sijoittaa. Nämä kategoriat ovat alkaen alhaisesta asiantuntemuksesta ja haitallisesta aikomuksesta korkeaan asiantuntemukseen ja hyödylliseen aikomukseen: vahingollinen väärinkäyttö, tarkoituksellinen tuhoaminen, naiivit virheet, vaarallinen puuhastelu, perusasioiden hallinta ja tiedostettu parantelu.

Stanton:in et al. (2005) viitekehys on kuitenkin luotu loppukäyttäjien käytöksen perusteella organisatoriseen ja tietotekniseen kontekstiin, joten se ei välttämättä vastaa yksilöllistä tietoturvakäyttäytymistä älypuhelinten käyttäjissä. Tutkielman kannalta on tarpeellista etsiä tapoja muuttaa tietoturvakäyttäytymisen konteksti organisatorisesta näkökulmasta, joka usein liittyy myös pelkästään perinteisiin tietokoneisiin, älypuhelinnäkökulmaan. Oman versionsa kyseisestä viitekehyksestä älypuhelinkontekstiin ovat luoneet Ngoqo & Flowerday (2015), jotka ovat sovittaneet sen älypuhelinkäyttäjien toimintaan sopivaksi (kuvio 5).



Kuvio 5. Älypuhelinkäyttäjien tietoturvakäyttäytyminen. Mukaillen Ngoqo & Flowerday (2015).

Ngoqo & Flowerday (2015) ovat vaihtaneet alkuperäisen viitekehyksen (Stanton et al., 2005) muuttujan asiantuntijuudesta tietoisuuteen (engl. awareness) joka viittaa älypuhelinkäyttäjien tietoturvakäyttäytymiseen, sen osaamiseen ja asenteeseen tietoturvakäyttäytymistä kohtaan. Samalla Ngoqo & Flowerday (2015) ovat muuttaneet hieman aikomuksen merkitystä: mitä korkeampi aikomus, sitä suurempi aikomus käyttäjällä on toimia hyvien tietoturvatapojen mukaisesti. Näin ollen tietoturvakäyttäytymisen osalta paras tilanne on silloin, kun käyttäjä on korkealla tasolla sekä tietoturvaan liittyvässä tietoisuudessa (osaaminen ja asenne) että aikomuksessa toimia tietoturvaa edistävällä tavalla.

Viitekehyksen kuusi kategoriaa auttavat käyttäjien kategorisoimisessa tietoturvakäyttäytymisensä perusteella tietyin ehdoin. Vahingolliseen väärinkäyttöön syyllistyvät käyttäjät, jotka ovat matalalla tasolla sekä tietoisuudessa että aikomuksessa hyvien tietoturvakäytäntöjen noudattamiseksi (Ngoqo & Flowerday, 2015). Tässä kategoriassa käyttäjä esimerkiksi ei suojaa älypuhelintaan

lainkaan, asentaa sovelluksia kiinnittämättä huomiota niiden vaatimiin oikeuksiin tai lähteeseen, josta sovellus on ladattu, tai ei ylipäätään välitä tai ole kiinnostunut laitteensa tietoturvasta.

Tarkoituksellinen tuhoaminen eroaa edellisestä kategoriasta siinä, että käyttäjän tietoisuus ja osaaminen ovat molemmat korkealla tasolla. Käyttäjä on siis tietoinen tietoturvauhista, joille laitteensa toiminnallaan altistaa, mutta ei lopulta välitä laitteensa tietoturvasta. (Ngoqo & Flowerday, 2015.) Esimerkiksi älypuhelinten tietoturvaominaisuuksien muokkaaminen tai poistaminen kokonaan käytöstä, tai jopa itse käyttöjärjestelmän suojauksien poistaminen voidaan laskea tähän kategoriaan.

Naiivit virheet sekä vaarallinen puuhastelu kuuluvat aikomuksen osalta neutraaliin kategoriaan, jolloin toimijalla ei ole selkeää aietta toimintaa kohtaan. Tämä tarkoittaa sitä, että käyttäjä ei välttämättä toimi tietoturvaa vaarantavasti eikä sitä parantavasti. Naiivit virheet eivät vaadi korkeaa tietoisuutta tietoturvaominaisuuksista, ja ne ovatkin usein niin sanottuja tekemättä jättämisiä. (Ngoqo & Flowerday, 2015.) Esimerkiksi näyttölukon käyttäminen laitteen suojauksessa, mutta koodin ollessa ”1234” käyttäjän voidaan sanoa tekevän naiivin virheen, sillä koodi on helposti arvattavissa. Vaarallinen puuhastelu puolestaan vaatii korkeampaa osaamista kuin naiivit virheet (Ngoqo & Flowerday, 2015). Vaarallista puuhastelua voi olla esimerkiksi käyttöjärjestelmän tiedostojen poistaminen lisätallennustilan saavuttamiseksi tai epävirallisesti muokatun kolmannen osapuolen sovelluksen asentaminen laitteeseen, jolloin varsinainen tarkoitus ei ole edistää eikä huonontaa tietoturvaa.

Perusasioiden hallinta vaatii käyttäjältä korkeaa aikomusta toimia tietoturvakäytäntöjen mukaisesti, mutta se ei kuitenkaan vaadi korkeaa tietoisuutta tietoturvaominaisuuksista. Tähän kategoriaan kuuluvat käyttäjät, jotka toimivat parhaan kykynsä mukaan tavoitteenaan suojata laitteensa siihen kohdistuvilta uhkilta. (Ngoqo & Flowerday, 2015.) Käyttäjä ei esimerkiksi tallenna pankkitietojaan tai luottokortin numeroaan laitteeseensa, käyttää jonkin tasoista suojausta, kuten näyttölukkoa, ei avaa epäilyttäviä tekstiviestejä tai linkkejä eikä asentele epävirallisia sovelluksia. Tiedostettu parantelu eroaa perusasioiden hallinnasta siten, että se vaatii käyttäjältä korkeaa osaamista sekä aikomusta toimia tietoturvan parantamiseksi omilla toimillaan (Ngoqo & Flowerday, 2015). Esimerkiksi haavoittuvien ja turhien järjestelmäominaisuuksien ja sovellusten poisto tai sovelluksien manuaalinen oikeuksienhallinta kuuluvat tähän kategoriaan.

3.3 Mallin hyödyntäminen tässä tutkimuksessa

UMISPC-malli (2018) on uusi tietoturvakäyttäytymistä tarkasteleva viitekehys. Mallia ei ole testattu merkittävästi tutkielmaa kirjoittaessa, joten tutkielman tutkimusosuudella on mahdollisuus luoda lisää pohjaa mallille, sen käytölle ja toimivuudelle. Myös mallin luoneet Moody et al. (2018) painottavat, että mallia tulee testata, sekä selvittää miten hyvin se soveltuu eri konteksteihin ja tietotur-

varikkeisiin. UMISPC sisältää myös määrällisen tutkimusosuuden, jonka avulla tutkielman kyselytutkimus on luotu, ja jonka avulla mallia voidaan luonnollisesti testata.

UMISPC-malliin perustuva kyselytutkimus tulee myös asettaa älypuhelinkontekstiin. Tähän tarkoitukseen käytetään aikaisempaa tutkimusta aiheesta, kuten Stanton:in et al. (2005) luomaa viitekehystä loppukäyttäjien tietoturvakäyttäytymisestä, ja tästä edelleen muokattua Ngoqo & Flowerday:n (2015) versiota, joka käsittelee tietoturvakäyttäytymistä älypuhelinkäyttäjien näkökulmasta. Tämän viitekehyksen avulla tutkimusosuudessa saatuja tuloksia voidaan tarkastella ja verrata aiempiin tutkimuksiin älypuhelinkäyttäjien tietoturvakäyttäytymisestä.

4 TUTKIMUSMENETELMÄT

4.1 Tutkimuksen tarkoitus ja tutkimuskysymys

Tämän tutkielman tarkoituksena on tarkastella älypuhelinkäyttäjien aikomusta käyttää laitteistaan löytyviä tietoturvaominaisuuksia oman datansa suojaamiseksi. Aikomukseen ja käyttäytymiseen liittyvää tutkimusta on jo olemassa laajasti, mutta sen soveltaminen eri tutkimusaloilla ja konteksteissa on vaihtelevaa. Tähän tutkielmaan on valittu UMISPC-malli, jonka tavoitteena on luoda yhtenäinen malli, joka pyrkii yhdistelemään useita eri tietoturvan ja tietoturvakäyttäytymisen tutkimuksessa käytettyjä teorioita ja malleja yhteen (Moody et al., 2018).

UMISPC-malli on tutkielmaa kirjoittaessa uusi, ja tämä tutkielma pyrkiikin osaltaan vastaamaan mallin luojien haasteeseen mallin testaamiseksi (Moody et al., 2018). Tutkielma tarkastelee mallia myös eri näkökulmasta, jolloin sen soveltuvuutta eri kontekstissa voidaan arvioida. UMISPC-malli on luotu organisaation sisällä ja tarkastelun kohteena ovat olleet työntekijät sekä heidän harjoittamansa tietoturvakäyttäytyminen sekä tietoturvarikkeet, erityisesti perinteisten tietokoneiden parissa (Moody et al., 2018). Tämä tutkielma tarkastelee tietoturvakäyttäytymistä älypuhelinkäyttäjän näkökulmasta, sekä heidän aikomustaan pitää oman, henkilökohtaisen laitteensa tietoturvan kunnossa. Tutkielman konteksti on siis henkilökohtainen tietoturva sekä älypuhelimen, kun UMISPC-mallissa konteksti on organisatorinen sekä vahvasti tietokonepainotteinen (Moody et al., 2018).

Tutkimuksella on tarkoitus vastata kysymykseen ”Mitkä ennalta määritellyt tekijät vaikuttavat älypuhelinkäyttäjän tietoturva-aikomukseen?”. Nämä tekijät ovat UMISPC:stä valitut tavat, rooliarvot, pelko sekä aikomus.

4.2 Kyselyn laatiminen ja testaus

Kyselyn sisältö laadittiin UMISPC-mallin pohjalta, sillä tutkimuksen tavoitteena on testata älypuhelinkäyttäjien aikomusta käyttää laitteidensa tietoturvaominaisuuksia. UMISPC-malli valittiin kyselyn pohjaksi myös siksi, että mallia ei ole testattu älypuhelin- ja mobiililaitekontekstissa, jolloin mallin sopivuutta eri konteksteihin voidaan samalla testata. UMISPC-mallin kehittäjät myös toivoivat tulevien tutkimusten tarkastelevan mallia eri konteksteissa, samalla selvittäen mallin toimivuutta erilaisissa ja erityyppisissä tilanteissa (Moody et al., 2018). Mallin toimivuutta, tai mahdollista toimimattomuutta, älypuhelinkontekstissa voidaan tarkastella kerätyllä aineistolla, jolloin ero kohdenkontekstissa on merkittävä alkuperäiseen malliin. Tutkimuksen kysely eroaa kontekstissaan edellä mainitun lisäksi myös käyttöympäristöllään: kyselyssä tarkastellaan käyttäjien toimia henkilökohtaisen älypuhelimensa käytöllä. UMISPC-mallissa käyttäjien toiminta tapahtuu organisatorisessa ympäristössä, jossa tarkasteltavat laitteet itsessään sekä niiden sisältämä data ei ole käyttäjän kannalta henkilökohtaisia (Moody et al., 2018).

Tutkimuksessa käytettiin samaa skenaario- eli tarinapohjaista lähestymistapaa kuin UMISPC:ssä, mutta tarinoiden konteksti ja sisältö on luotu käyttäjien henkilökohtaisen älypuhelimen käytön pohjalta. Tarinapohjaisen kyselyn tavoitteena on saada kerättyä dataa laitteen erilaisista käyttötilanteista, jolloin mallin toimivuutta voidaan testata eri näkökulmista. Eri näkökulmien tarkastelun lisäksi tarinapohjaisuudella saadaan kuvattua laitteen käyttötilannetta tarkasti, realistisesti ja kyselyyn vastaajille tutulla tavalla. Kyselyn tarinoissa toimijana toimi kuvitteellinen henkilö, jonka toimintaa vastaajat arvioivat omien periaatteidensa pohjalta, jolloin vastaajien ei tarvitse vastata oman toimintansa pohjalta. Kuvitteellisen henkilön käyttämisen tarinoissa on tarkoitus saada vastaajat vastaamaan kysymyksiin mahdollisimman totuudenmukaisesti, jos kysymyksessä käsitellään tapahtunutta virhettä tai muuta mahdollisesti sosiaalisia normeja rikkovaa tapahtumaa (Moody et al., 2018; Pogarsky, 2004).

Kyselyyn luotiin kaksi erilaista tarinaa, joissa molemmissa kuvitteellinen toimija oli sama henkilö. Molempia tarinoita edelsi lyhyt kuvaus tarinoissa toimivasta henkilöstä ja tämän tavasta käyttää omaa älypuhelintaan. Tämän lyhyen kuvauksen tavoitteena oli luoda kuva toimijasta oikeana älypuhelimen käyttäjänä, jonka pohjalta kyselyyn vastaaja pystyi käsittelemään henkilön toimintaa ja sen mahdollisia syitä. Kuvauksessa kerrottiin lyhyesti toimijan tavasta käyttää älypuhelintaan, mitä tietoja ja dataa puhelin sisältää, sekä toimijan aito halu pitää älypuhelimensa turvallisena.

Kuvauksen jälkeen kyselyssä kerrottiin kaksi erillistä lyhyttä tarinaa toimijasta erilaisissa älypuhelimenkäyttötilanteissa, joissa molemmissa toimija toimi jollain tavalla älypuhelimen tietoturvaa uhkaavalla tavalla. Tarinoissa korostettiin toimijan suorittamaa tietoturvarikkomusta, sekä sitä, mitä hyötyjä käyttäjä odotti kyseisen rikkomuksen tuovan. Toimijan kuvauksen ja tarinoiden perusteella kyselyyn vastaajille kerrottiin kuvitteellisen toimijan *rooli* älypuhe-

limen käyttäjänä, toimijan tavoitteet älypuhelimensa turvassa pitämiseksi *toimintatavoillaan* (engl. policy), suoritettu *tietoturvarike* sekä mahdollinen *hyöty* joka tietoturvarikkeestä oletettiin saatavan.

UMISPC-mallin tarinat sijoittuvat organisatoriseen kontekstiin, jossa kuvitteellinen toimija toimii oman roolinsa perusteella organisaation sisällä. UMISPC-mallin alkuperäisissä tarinoissa tietoturvarikkeet valittiin organisaatioiden johtajien raportoimien yleisimpien tietoturvarikkeiden pohjalta. Tarinoista ilmenee myös toimijan *rooli* organisaation toimijana, organisaation *toimintatapa* tietoturvan suhteen, sekä toimijan suorittama *tietoturvarike* sekä tietoturvarikkeestä saatava mahdollinen *hyöty*. (Moody et al., 2018.) Tässä tutkimuksessa tarinoiden tietoturvarike on perusteltu älypuhelinten tietoturvaan liittyvällä aiemmalla tutkimuksella.

Molempia tarinoita sekä kyselyn kysymyksiä tarkastellaan yksityiskohtaisemmin seuraavissa kappaleissa.

4.2.1 Kyselyn kuvitteellisen toimijan kuvaus

Tutkimuksen kyselyssä käytettiin samanlaista tarinapohjaista lähestymistapaa kuin UMISPC-mallissa (Moody et al., 2018). Kriminologian ja moraalipsykologian aloilla tällaista niin kutsuttua tarinapohjaisuutta kutsutaan skenaarioksi (Siponen & Vance, 2014). Molemmissa tarinoissa käytettiin samaa lyhyttä kuvausta tarinan toimijasta, ”Jokinen”, ja tämän roolista sekä toimintatavoista älypuhelimen käyttöön ja tietoturvaan liittyen:

> ”Jokinen on ahkera älypuhelimen käyttäjä ja hän *haluaa pitää laitteensa tietoturvan kunnossa*. Hän käyttää älypuhelintaan useita tunteja päivässä, ja käyttää sillä erityisesti sosiaalista mediaa sekä pikaviestisovelluksia. Jokinen käyttää puhelintaan myös valokuvaamiseen, sähköpostiin, pelien pelaamiseen, ja joskus myös kävely- ja juoksulenkkiensä matkan ja keston seuraamiseen GPS-paikannuksen avulla.”

Kuvauksen tavoitteena oli kertoa vastaajille toimijan tavasta käyttää älypuhelintaan henkilökohtaisessa käytössään. Myös toimijan halu pitää puhelimensa tietoturva kunnossa oli selkeästi ilmaistu. Kuvauksessa kerrottiin vastaajille myös siitä, mitä henkilökohtaisia tietoja ja dataa tarinan toimijan älypuhelin sisältää (kuvat, sähköposti jne.). Kuvauksesta ilmenee myös toimijan *rooli* älypuhelimen käyttäjänä: toimija käyttää puhelintaan ahkerasti ja tallentaa siihen huomattavan määrän henkilökohtaisia tietojaan. Toimijan henkilökohtainen *toimintatapa* (engl. policy) tietoturvan suhteen ilmenee tämän halussa pitää laitteensa tietoturva kunnossa.

4.2.2 Kyselyn tarina 1 (näyttölukko)

Kyselyn ensimmäinen tarina toimijasta kuvaa tilannetta, jossa toimija on turhautunut puhelimensa näyttölukkoon. Tarinassa kuvataan ympäristö, jossa toimija on ja jossa tämä suorittaa tietoturvarikkeen. Tietoturvarikkeeksi ensimmäiseen tarinaan valittiin näyttölukon käyttämättömyys tai sen puute, jonka käyttö usein koetaan häiritsevänä tai sen tietoturvahyötyjä ei tunneta (Harbach,

Von Zezschwitz, Fichtner, De Luca, & Smith, 2014). Näyttölukkoa voidaan myös pitää suurimmalle osalle vastaajista tuttuna tietoturvaominaisuutena, ja sen käyttö voidaan laskea kuuluvan perusasioiden hallintaan, jolloin toiminnan aikomus on parantaa tietoturvaa, mutta se ei vaadi käyttäjältä korkeaa teknistä osaamista (Ngoqo & Flowerday, 2015).

> ”Jokinen suuntaa kesälomallaan toiselle puolelle maata, ja matkustaa kohteeseensa junalla. Matka kestää useita tunteja, jonka aikana Jokinen käyttää puhelintaan aktiivisesti lähes koko matkan ajan. Jonkin ajan kuluttua matkan alkamisesta Jokista alkaa ärsyttää toistuva näyttölukon avaaminen ja hän päättää *poistaa puhelimen näyttölukon kokonaan käytöstä* säästääkseen aikaa ja hermojaan. Jokinen tietää, että kuka tahansa voi käyttää puhelinta ja selata sen sisältämiä tietoja näyttölukon ollessa kokonaan pois käytöstä.”

Tarinassa kerrotaan toimijan tietoturvarikkeestä, jonka toimija tunnistaa *toimintatapansa* vastaiseksi. Toimija poistaa älypuhelimensa näyttölukon käytöstä säästääkseen aikaa ja hermojaan, joka on tietoturvarikkeen syy ja samalla odotettu *hyöty.* Toimija myös tunnistaa tietoturvarikkeen aiheuttaman riskin laitteella ja samalla sen sisältämille tiedoille, mutta hän suorittaa rikkeen riskeistä huolimatta.

4.2.3 Kyselyn tarina 2 (ulkopuoliset sovellukset)

Kyselyn toisessa tarinassa toimija etsii korvaavaa sovellusta toimimattoman sovelluksen tilalle. Toimijan tilanne ja sen hetkinen tilanne on jälleen avattu vastaajille, sekä tietoturvarike ja tämän aiheuttamat mahdolliset riskit. Tietoturvarikkeeksi toiseen tarinaan valittiin virallisten sovelluskauppojen ulkopuoliset sovellukset, jotka usein sisältävät haitta- tai vakoiluohjelmia (Harris, Furnell, & Patten, 2014). Ulkopuolisten sovellusten asentaminen voidaan laskea vaarallisen puuhastelun kategoriaan, sillä tarkoituksena ei ole erityisesti parantaa eikä vahingoittaa tietoturvaa. Ulkopuolisten sovellusten asentaminen vaatii kuitenkin perustasoa parempaa teknistä osaamista, jonka vuoksi toimintaa ei lasketa naiiviksi virheeksi (Ngoqo & Flowerday, 2015).

> ”Jokinen käyttää puhelimessaan kuvankäsittelysovellusta, joka jostain syystä ei enää suostu käynnistymään sovellukseen tulleen uusimman päivityksen jälkeen. Jokinen olisi halunnut lähettää ystävälleen hauskan muokatun valokuvan onnitellakseen tätä tämän syntymäpäivänä. Jokinen etsii korvaavaa sovellusta kuvien muokkaamiseksi, mutta ei sellaista puhelimensa sovelluskaupasta löydä. Jokinen jatkaa ohjelman etsintää netistä, ja löytää tätä kautta ilmaisen korvaavaan kuvankäsittelyohjelman. Sovelluksen nettisivu vaikuttaa tarpeeksi luotettavalta, ja Jokinen asentaa puhelimeensa netistä lataamansa sovelluksen. Jokinen tietää, että virallisen sovelluskaupan ulkopuolelta ladatut sovellukset saattavat olla haitallisia ja aiheuttaa ongelmia.”

Samoin kuin kyselyn ensimmäisessä tarinassa, toisessa tarinassa toimija toimii jälleen oman *toimintatapansa* vastaisesti ja asentaa virallisen sovelluskaupan ulkopuolisen sovelluksen laitteeseensa, ollen samalla tietoinen sen mahdollisista riskeistä. Tarinassa toimijan odottama *hyöty* tietoturvarikkeestä on saada haluttu valokuvanmuokkaus tehtyä, jotta voisi lähettää tämän ystävälleen.

4.2.4 Kyselyn sisältö, kysymykset ja kyselyn testaaminen

Kyselyn luomisessa käytettiin samaa kyselypohjaa, jota käytettiin UMISPC-mallin luomisessa. Kyselypohjaa kuitenkin muokattiin niin, että se vastasi tutkielman rajausta, sekä osa kysymyksistä muutettiin vastaamaan älypuhelinkontekstia, esimerkiksi alkuperäinen kysymys muutettiin muodosta ”tietokoneeni saattaa vaarantua” muotoon ”älypuhelimeni saattaa vaarantua”. Kyselyn kysymykset myös käännettiin englannista suomeksi, sillä alkuperäisiä suomenkielisiä kysymyksiä ei ollut saatavilla. Kysely testattiin ennen lopullisen kyselyn julkistamista seitsemällä henkilöllä, joilta kerättiin palautetta kyselyn ymmärrettävyydestä, kieliasusta sekä vastaamisen helppoudesta. Testistä kerätty palaute oli epäformaalia, ja sen perusteella tehtiin pieniä muokkauksia kysymysten kieliasuun, eikä ongelmia kyselyyn vastaamisessa ilmennyt.

Kysely alkoi saatekirjeellä, jossa vastaajille kerrottiin lyhyesti kyselyn tavoitteesta ja mitä kerätyillä vastauksilla tehdään. Saatekirjeessä annettiin myös vastaamisohjeet, sekä painotettiin ettei kerättyjä tietoja anneta tutkimukseen liittymättömille tahoille. Kyselyyn vastaamalla oli myös mahdollista osallistua elokuvalippujen arvontaan, johon osallistumisen ohjeet annettiin saatekirjeen lopussa. Arvontaa varten halukkailta kerättiin sähköpostiosoite. Sähköpostiosoitetta ei missään vaiheessa käytetty datan analysoinnissa, eikä vastaajia voitu tunnistaa vastausten perusteella, sillä henkilötietoja ei kerätty. Yleisistä demografiatiedoista vastaajilta kerättiin vain ikä ja sukupuoli. Molempien tarinoiden jälkeen vastaajilta kysyttiin myös, kuinka realistisena he tarinan tilannetta pitivät, näin ollen antaen yleisen käsityksen siitä, voidaanko tarinaa pitää uskottavana. Tarinan realistisuuden kysymys löytyy myös UMISPC-mallin kyselylomakkeesta, joka oli syy kysymyksen lisäämiselle (Moody et al., 2018). Kyselyn lopussa vastaajat saivat halutessaan osallistua arvontaan, jonka jälkeen heitä kiitettiin vastauksesta kiitossivulla.

Jokainen kysymyksistä liittyi tiettyyn UMISPC-mallin esittämään konstruktioon. Kysymykset valittiin niin, että ne sopivat tutkielmaan valittuun rajaukseen käyttäen UMISPC-mallin esittämiä konstruktioita. Kyselyn molempiin tarinoihin liitettiin kontekstisidonnaiset kysymykset laajempien tulosten saamiseksi. Tapaan liittyvät kysymykset koskivat vastaajia itseään, ja ne eivät olleet yhteydessä luotuihin tarinoihin, joten kysymykset kysyttiin vain kerran tarinasidonnaisten kysymysten jälkeen. Vastaajia ei myöskään haluttu rasittaa liikaa, joten tarinoita ei luotu enempää. Liian pitkät kyselyt myös saattavat vähentää vastausprosenttia tai aiheuttaa keskeneräisiä vastauksia (Hoerger, 2010). Valitut kysymykset, niiden UMISPC:tä vastaavat konstruktiot sekä kysymysten teoriapohja löytyvät seuraavasta taulukosta 2. Kysymysten numero viittaa kyselypohjassa käytettyihin kysymysnumeroihin (ks. liite 1).

Kysym. #	UMISPC #	UMISPC konstruktio	Kysymys engl. (UMISPC)/ suomennokset	Kysymyksen teoriapohja ja lähde
4. / 19.	selfcon1	Rooliarvot	*I would feel guilty if I did what Mattila did./* Tuntisin syyllisyyttä, jos tekisin niin kuin Jokinen teki	Ihmistenvälisen käyttäytymisen teoria (TIB) (Gagnon et al., 2003)
5. / 20.	selfcon2	Rooliarvot	*What Mattila did is consistent with my principles. /* Jokinen toimi henkilökohtaisten periaatteideni mukaan johdonmukaisesti	Ihmistenvälisen käyttäytymisen teoria (TIB) (Gagnon et al., 2003)
6. / 21.	selfcon3	Rooliarvot	*It is acceptable to do what Mattila did. /* On hyväksyttävää toimia niin kuin Jokinen toimi tarinassa	Ihmistenvälisen käyttäytymisen teoria (TIB) (Gagnon et al., 2003)
7. / 22.	roles2	Rooliarvot	*What Mattila did fits with his/her work style. /* Mitä Jokinen teki sopi hänen tapaansa käyttää älypuhelintaan	Suunnitellun käyttäytymisen teoria (TPB) ja ihmistenvälisen käyttäytymisen teoria (TIB) (Bamberg & Schmidt, 2003)
8. / 23.	roles3	Rooliarvot	*What Mattila did can be justified due to the nature of Mattila's work. /* Mitä Jokinen teki oli oikeutettua tarinan käyttötilanteen perusteella	Suunnitellun käyttäytymisen teoria (TPB) ja ihmistenvälisen käyttäytymisen teoria (TIB) (Bamberg & Schmidt, 2003)
9. / 24.	affect1	Rooliarvot	*What Mattila did is smart./* Mitä Jokinen teki oli fiksua	Suunnitellun käyttäytymisen teoria (TPB) (Limayem & Hirt, 2003)
10. / 25.	affect4	Rooliarvot	*What Mattila did is pleasant./* Mitä Jokinen teki oli miellyttävää	Suunnitellun käyttäytymisen teoria (TPB) (Limayem & Hirt, 2003)
11. / 26.	moral1	Rooliarvot	*How morally wrong would it be to do what the person did in the scenario? /* Kuinka moraalisesti oikein olisi toimia samoin kuin Jokinen toimi tilanteessa?	Peloteteoria (DT) ja rationaalisen valinnan teoria (RCT) (Paternoster & Simpson, 1996; Vance, Siponen, & Pahnila, 2012)
12. / 27.	percbehcont2	Rooliarvot	*If you were Mattila, how much would you feel able to not do as he did? /* Koetko, että pystyisit olemaan toimimatta samoin kuin Jokinen kuvatussa tilanteessa?	Suunnitellun käyttäytymisen teoria (TPB) (Ajzen, 1985; Ajzen, 2002)
13. / 28.	fear10	Pelko	*My computer might become unusable if I did what Mattila did./* Älypuhelimeni saattaa muuttua käyttökelvottomaksi, jos teen niin kuin Jokinen teki	Protection Motivation –teoria (PMT) (McCracken et al., 1992; Osman et al., 1994)
14. / 29.	fear7	Pelko	*My computer might be compromised if I did what Mattila did./* Älypuhelimeni saattaa vaarantua, jos teen niin kuin Jokinen teki	Protection Motivation –teoria (PMT) (McCracken et al., 1992; Osman et al., 1994)

Kysym. #	UMISPC #	UMISPC konstruktio	Kysymys engl. (UMISPC)/ suomennokset	Kysymyksen teoriapohja ja lähde
15. / 30.	fear11	Pelko	*My computer might become slower if I did what Mattila did./* Älypuhelimeni saattaa hidastua, jos teen niin kuin Jokinen teki	Protection Motivation –teoria (PMT) (McCracken et al., 1992; Osman et al., 1994)
16. / 31.	intent1	Aikomus	*What is the chance that you would do what Mattila did in the described scenario?/* Miten todennäköistä on, että itse toimisit kuvatussa tilanteessa samoin kuin Jokinen	Kontrollitasapainoteoria (CBT) (Piquero & Piquero, 2006)
17. / 32.	intent2	Aikomus	*I would act in the same way as Mattila did if I were in the same situation./* Toimisin samalla tavalla kuin Jokinen, jos olisin samassa tilanteessa	Kontrollitasapainoteoria (CBT) (Piquero & Piquero, 2006)
33.	habit1	Tavat	*Complying with information security procedures is something I do frequently./* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä teen usein	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)
34.	habit2	Tavat	*Complying with information security procedures is something I do automatically. /* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä teen automaattisesti	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)
35.	habit3	Tavat	*Complying with information security procedures is something I do without having to consciously remember. /* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä minun ei tarvitse tietoisesti erikseen muistaa	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)
36.	habit5	Tavat	*Complying with information security procedures is something I do without thinking. /* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä teen ajattelematta	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)
37.	habit7	Tavat	*Complying with information security procedures is something that belongs to my (daily, weekly, monthly) routine./* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mikä kuuluu rutiiniini (päivittäin, viikoittain, kuukausittain)	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)

38.	habit8	Tavat	*Complying with information security procedures is something I start doing before I realize I'm doing it./* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä aloitan tekemään ennen kuin edes huomaan tekeväni niin	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)
39.	habit11	Tavat	*Complying with information security procedures is something that's typically "me." /* Älypuhelimen tietoturvaominaisuuksien käyttö on minulle tyypillistä	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)
40.	habit12	Tavat	*Complying with information security procedures is something I have been doing for a long time. /* Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä olen tehnyt jo pitkään	Ihmistenvälisen käyttäytymisen teoria (TIB) (Verplanken & Orbell, 2003)

Taulukko 2. Kyselyn kysymykset, UMISPC-konstruktit sekä teoriapohjat

4.3 Tutkimusaineiston keruu ja kohde

Tutkimuksen tavoitteena oli kerätä määrällistä dataa UMISPC-mallin testaamiseksi sekä älypuhelimen käyttäjien tietoturvaominaisuuksien käytön aikomuksen tarkastelemiseksi. Tämän tavoitteen saavuttamiseksi kysely suoritettiin internetissä, ja sen alustana käytettiin Webropol 3.0 kyselyohjelmistoa. Internetpohjainen kysely valittiin tutkimukseen, jotta vastaajien ja vastauksien kerääminen ja käsittely olisi mahdollisimman tehokasta.

Kysely oli vastattavissa kaksi viikkoa, ja kyselyyn pääsi vastamaan avoimen internetlinkin kautta. Kyselylinkkiä jaettiin useilla sähköpostilistoilla Jyväskylä yliopiston tiedekuntien kautta, sekä suorana linkkinä muille sidosryhmille. Kyselylinkki oli avoin kaikille, ja kyselyyn pystyi vastaamaan kuka tahansa kyselylinkin vastaanottanut.

Kyselyn vastaamiseen oli asetettu muutama ehto, jotka vastaajien tuli täyttää. Vastaajien tuli omistaa älypuhelin, jota käyttäjä käytti henkilökohtaisten asioidensa hoidossa. Kyselyyn hyväksyttiin myös vastaajat, joilla on käytössään työpuhelin, jota vastaaja käyttää vapaa-ajallaan henkilökohtaisten asioidensa hoidossa. Kysely suoritettiin ainoastaan suomeksi, joten vastaajien tuli pystyä vastaamaan kysymyksiin kyseisellä kielellä. Kyselyllä ei myöskään ollut ikärajaa, sillä mitään henkilökohtaista tai arkaluonteista dataa ei kerätty. Vastaajien kesken arvottiin kaksi elokuvalippua, jonka tavoitteena oli houkutella ja motivoida kyselyyn lisää vastaajia. Elokuvalippuarvontaan osallistuminen oli vapaaehtoista, ja halukkailta osallistujilta kerättiin sähköpostiosoite lipun lähettämistä varten.

Kyselyn saatekirjeessä vastaajille kerrottiin lyhyesti kyselyn tavoitteista ja sisällöstä. Saatekirjeessä annettiin vastaajille myös ohjeet kyselyyn vastaamiseen sekä painotettiin ettei vastaajien vastauksia yksilöidä ja että annetuista vastauksista ei voida tunnistaa yksittäistä vastaajaa. Kyselyn dataa ei myöskään luovuteta tutkimuksen ulkopuolisille tahoille. Valittu internetpohjainen kyselyalusta myös mahdollisti sen, että jokaisen vastaajan tuli vastata jokaiseen kysymykseen, eikä keskeneräisiä tai osittain vastattuja vastauksia pystynyt lähettämään. Kyselyyn saatiin yhteensä 485 vastausta.

4.4 Tutkimuksen analyysimenetelmät

Kyselyllä kerättyä dataa analysoitiin faktorianalyysillä. Faktorianalyyseistä valittiin eksploratiivinen faktorianalyysi, sillä tutkielman kontekstin muutos alkuperäisestä on merkittävä. Tutkielman konteksti on muutettu tietokonepainoitteisesta ja organisatorisesta henkilökohtaiseen älypuhelinkontekstiin. Tutkielman tutkimusosuudessa tutkikaan myös vain rajattua osuutta UMISPC-mallista, jolloin osa alkuperäisen mallin konstruktioista jäi tämän rajauksen ulkopuolelle. Eksploratiivista faktorianalyysia voidaan käyttää, jos ajatus teoriapohjasta on olemassa, mikä on tässä tutkielmassa perusteltua (Metsämuuro-

nen, 2011, s. 667). Jatkossa eksploratiivisesta faktorianalyysistä käytetään yleistä termiä faktorianalyysi.

Faktorianalyysissä muuttujien välillä oletetaan olevan korrelaatioita. Myös tutkimuksen otoskoon tulisi olla tarpeeksi suuri, noin 300 vastaajaa, jolloin faktorianalyysin käyttö on mielekästä. Pienempikin vastaajien määrä voi olla riittävä, jos havaitut korrelaatiot ovat korkeita. (Metsämuuronen, 2011, s. 667.) Tässä tutkielmassa kyselyyn saatiin 485 vastaajaa, joten nämä faktorianalyysin käytön yleiset ehdot on täytetty.

Faktorianalyysi suoritettiin Webropol Professional Statistics –ohjelmistolla. Faktorien latausten selvittämiseksi analyysissä käytettiin vinokulmaista PROMAX-rotaatiota. Vinokulmaiseen rotaatioon päädyttiin, sillä käytetyn mallin ja teoriapohjan mukaan faktorit voivat korreloida keskenään, jonka vinokulmaisuus mahdollistaa (Metsämuuronen, 2011, s. 669). Faktorianalyysissä on tarkoitus löytää muuttujien pohjalta kokonaisuuksia, ja antaa löydetyille kokonaisuuksille eli faktoreille sisällöllisesti merkittävät nimet (Metsämuuronen, 2011, s. 671). Faktorianalyysin löydökset esitellään seuraavassa luvussa, jossa esitellään myös muut kyselytutkimuksen tulokset.

4.5 Tutkimuksen luotettavuus

Tutkielman empiirisen tutkimusosuuden luotettavuutta tulee myös tarkastella tulosten uskottavuuden lisäämiseksi. Sisällön validiteettia eli uskottavuutta voidaan arvioida esimerkiksi sillä, vastaavatko tutkimuksessa käytetyt mallit ja käsitteet käytettyä teoriapohjaa tai mallia. (Metsämuuronen, 2011, s. 126.)

Tutkimuksessa käytetty kyselypohja on luotu tutkielmassa käytetyn UMISPC-mallin mukaan, ja se sisältää samoja elementtejä. UMISPC-mallin on todettu mittaavan tarkasteltavaa tutkimuskohdetta hyvin, joten sen käyttöä voidaan pitää luotettavana (Moody et al., 2018). Vaikka käytettyä teoriapohjaa voidaan pitää luotettavana, on tutkimuksen toteuttamisessa käytettyjä metodeja tarkasteltava kriittisesti.

Tutkimuksen kyselyosuus suoritettiin anonyyminä, joten vastaajia ei pystytty tunnistamaan heidän vastauksiensa perusteella. Kysely oli kuitenkin kenen tahansa vastattavissa, jos heillä oli pääsy kyselyssä käytettyyn nettilinkkiin, eikä vastaajia näin ollen voitua seuloa tarkemmin. Kyselyssä myös luotettiin vastaajien omaan päätösvaltaan ja siihen että vastaajilla oli käytössään henkilökohtainen älypuhelin. Tilastokeskuksen (2018a) mukaan vuonna 2017 alle 55-vuotiaista suomalaisista 94 %:lla oli käytössään älypuhelin, joten tutkimukseen vastanneiden demografioiden perusteella tätä oletusta voidaan pitää luotettavana. Tutkimuksessa myös oletettiin vastaajien vastaavan kysymyksiin rehellisesti, ja tätä painotettiinkin kyselyn saatekirjeessä. Kyselyn vastausprosenttia ei voida kuitenkaan määrittää, sillä kyselyllä ei ollut tarkasti määriteltyä kohdetta, vaan kyselyyn pystyi osallistumaan kuka tahansa. Kyselyyn saatiin kuitenkin huomattava määrä vastauksia (N=485), joten kerätty aineisto on riittävän suuri analysoitavaksi. Yksikään kerätty vastaus ei myöskään ollut keskeneräinen tai

muuten puutteellinen, joten jokainen kerätty vastaus pystyttiin hyödyntämään analyyseissä.

Kyselyn luomisessa alkuperäisen UMISPC-mallin kysymykset sekä tarinat tuli kääntää englanninkielestä suomeksi, joka saattoi vaikuttaa mittariston tarkkuuteen ja havaittuihin tuloksiin. Kääntämisen lisäksi kysymysten konteksti tuli vaihtaa älypuhelinkontekstiin, jonka perusteena käytettiin aiempaa tutkimusta älypuhelimista ja niiden turvallisuudesta. Kyselyssä käytetyt tarinat luotiin käyttämällä UMISPC-mallin luomisessa käytettyjä skenaarioita, joista eroteltiin kolme merkittävää päätekijää: tarinassa esiintyvän henkilön rooli, käytetty tietoturvakäytänne ja sen rikkominen, sekä henkilön toiminnasta olettama hyöty (Moody et al., 2018). Kyselyn tarinat luotiin näiden kolmen osuuden pohjalta, ja tietoturvarike sekä -käytänne luotiin aiemman älypuhelinturvallisuuden kirjallisuuden perusteella.

Kuten kyselytutkimuksissa yleensä, on kerättyä dataa tarkasteltava kriittisesti myös mahdollisten mittausvirheiden osalta. Empiirisissä tutkimuksissa, joissa tutkitaan esimerkiksi ihmisten käyttäytymistä tai asenteita, on huomattu, että usein mittausvirheet ja ongelmat esimerkiksi mittaustyökaluissa voivat aiheuttaa merkittäviä muutoksia dataa analysoitaessa. Nämä mittausvirheet voivat joko keinotekoisesti nostaa tai laskea esimerkiksi havaittujen yhteyksien voimakkuutta muuttujien välillä. (Podsakoff, MacKenzie, Lee, Podsakoff, 2003.)

Tässä tutkimuksessa voidaan olettaa myös olevan mittausvirheitä, jotka voivat johtua useista eri syistä. Esimerkiksi on mahdollista, että vastaajat eivät ole vastanneet kysymyksiin totuudenmukaisesti, tai vastaaja on saattanut tietoisesti vastata erityisen yhdenmukaisesti samantyyppisiin kysymyksiin, vaikka vastaus muuten olisi ollut toinen. Myös kysymyksenasettelussa ja kieliasussa on mahdollista luoda vastaajalle esimerkiksi positiivinen tai negatiivinen mielikuva tutkimusaiheesta tai alueesta, jota kysely on käsitellyt. Vastaajat myös saattavat yrittää miellyttää tutkijaa, tai vastata kysymyksiin niin sanotusti ”yleisesti hyväksyttävästi”, jossa vastaaja vastaa kysymyksiin niin, että yleisesti sosiaalisesti hyväksytyt vastausvaihtoehdot painottuvat. (Podsakoff et. al, 2003.)

Podsakoff et. al (2003) myös esittelevät keinoja mittausvirheiden vähentämiseksi, kuten esimerkiksi jättämällä ajallinen tauko kyselyjen välille, tai lisädatan käyttö tutkimuksen ohessa, jos sellaista on saatavilla. Tässä tutkimuksessa olisi voitu esimerkiksi testata tarinoita erillisinä kyselyinä, jolloin tarinan 1 vastauksilla ei olisi ollut vaikutusta tarinan 2 vastauksiin, jotka tässä tutkimuksessa kysyttiin samassa kyselyssä. Kysely testattiin myös etukäteen muutamalla vastaajalla, joilta kysyttiin, aiheuttivatko kysymykset esimerkiksi positiivisia tai negatiivisia tuntemuksia, tai koettiinko kysymykset johdatteleviksi. Kyselyn testaamisen tarkoituksena oli siis parantaa kyselyn ja sen tulosten oikeellisuutta vähentämällä mahdollisia mittausvirheitä. Tutkimuksen skaalan vuoksi esimerkiksi pitkän aikavälin jättäminen kyselyiden väliin tai erillisten kyselyiden toteuttaminen ei ollut mielekästä.

Tutkielman tavoitteena on tarkastella älypuhelinkäyttäjien tietoturvaaikomusta, ja UMISPC-mallista on valittu vain aikomukseen liittyvät osiot aiheen rajauksen perusteella (ks. kuvio 3). Koska tutkimusosuudessa ei ole käy-

tetty UMISPC-mallia täydellisessä muodossaan, tulee tämä ottaa huomioon tutkimustuloksia tulkittaessa. Tutkimuksen luotettavuutta voidaankin siis pitää hyvänä, sillä käytössä on osuus luotettavasta mittaristosta, ja kerättyjen vastausten määrä oli hyvä määrällisen tutkimuksen suorittamiseksi.

5 TUTKIMUKSEN TULOKSET JA ANALYYSIT

Tässä luvussa käsitellään kyselytutkimuksen tulokset. Ensimmäisenä tuloksista käydään läpi vastaajien yleiset demografiat ja verrataan otosta todelliseen väestörakenteeseen. Tämän jälkeen tulokset käydään läpi tarinakohtaisesti, ja molemmat tarinat sekä havaitut tulokset esitellään yksityiskohtaisesti. Havaittuja tuloksia verrataan myös UMISPC:n rakentamisessa saatuihin tuloksiin. Ensimmäisenä tulokset esitellään tarinaan 1, jossa tarkasteltavana tietoturvaominaisuutena oli älypuhelimen näyttölukko. Seuraavana tulokset esitellään tarinaan 2, joka puolestaan käsittelee virallisen sovelluskaupan ulkopuolisten sovellusten asentamista.

5.1 Tutkimuksen demografiat ja yleistettävyys

Kyselyn vastausaikana (14 päivää) kyselyyn saatiin yhteensä 485 vastausta (N=485). Kyselyn pystyi lähettämään vain, jos jokaiseen kysymykseen oli vastattu, joten jokainen kerätty vastaus on käyttökelpoinen, eikä keskeneräisiä tai puutteellisia vastauksia kerätty lainkaan. Kyselyn ollessa internetpohjainen, toteutettiin edellä kuvattu täydellisen vastauksen rajoitus teknisesti Webropol-kyselyalustaa käyttämällä.

Kyselyn 485 vastaajasta 295 ilmoitti sukupuolekseen nainen, 186 ilmoitti sukupuolekseen mies. Sukupuolen vaihtoehdoissa oli myös vaihtoehto ”muu”, jonka valitsi 4 vastaajaa. Vastaajista 60,8 % olivat naisia (N=295), 38,4 % miehiä (N=186) ja muita 0,8 % (N=4). Lukemisen helpottamiseksi, nämä demografiat ovat kuvattuna myös taulukossa 3.

Taulukko 3. Kyselyn demografiat

Sukupuoli	**Lukumäärä (N)**	**Osuus vastaajista (%)**
Nainen	295	60,8
Mies	186	38,4
Muu	4	0,8
Kaikki vastaajat yhteensä	485	100

Kyselyyn vastaajille ei asetettu ala- eikä yläikärajaa, sillä kyselyssä ei kerätty henkilökohtaista eikä arkaluontoista dataa. Kyselyn vastaajien ikä vaihteli 18-vuotiaasta 93-vuotiaaseen. Kaikkien vastaajien keski-ikä oli 27,3 vuotta, ja mediaani 25 vuotta. Kyselyyn vastanneiden naisten keski-ikä oli 26,7 vuotta, miesten 28,3 vuotta ja muiden 26,8 vuotta. Taulukosta 4 löytyvät vastaajien keski-iät.

Taulukko 4. Vastaajien keski-ikä

Sukupuoli	**Keski-ikä**
Nainen	26,7
Mies	28,3
Muu	26,8
Kaikki vastaajat yhteensä	27,3

Tutkimuksen kohteena olivat suomea puhuvat henkilöt, eikä muita rajoituksia kyselyyn vastaamiselle asetettu. Näin ollen tutkimuksen kohteena voidaan pitää koko Suomea, jolloin vastaajien soveltumista maan väestörakenteeseen tulee arvioida tutkimuksen yleistettävyyden vuoksi. Tutkimuksen kyselyyn vastanneet olivat keski-iältään huomattavasti nuorempia kuin koko väestön keski-ikä Suomessa. Tilastokeskuksen (2018b) mukaan Suomessa naisten keski-ikä on 44,0 vuotta, ja miesten 41,3 vuotta, mikä eroaa merkittävästi vastaajien 26,7:sta naisten ja 28,3:sta miesten osalta.

Vastaajista myös huomattavan suuri osa oli naisia, mikä ei myöskään vastaa väestön normaalia rakennetta Suomessa. Naisten osuus väestöstä on Tilastokeskuksen (2018b) mukaan 50,7 % ja miesten 49,3 % - muihin sukupuoliin kuuluvien määrää ei erikseen kerrota. Kyselyyn vastanneista 60,8 % oli naisia ja 38,4 % miehiä, joten ero todelliseen populaatioon on huomattava. Kyselyyn vastasi siis huomattavasti normaalipopulaatiota nuorempi ja naisvaltaisempi joukko.

5.2 Tutkimuksen vastausten erittely

Tässä kappaleessa esitellään tutkimusainestossa ilmenneitä tuloksia. Tulosten erittelyn tavoitteena on sekä esittää kerättyä dataa ennen analyysejä että tuoda esille tutkimuksessa käsiteltyjen tarinoiden välisiä eroavaisuuksia. Tarinakohtaisten kysymysten lisäksi taulukosta löytyvät vastaajien tietoturvakäyttäytymistapoihin liittyvät kysymykset, jotka kysyttiin erikseen tarinoista, ja niitä sovelletaan molempien tarinoiden analyyseissä. Kysymykset löytyvät kokonai-

suudessaan ja numeroituna kappaleesta 4.2.4, jossa kysymyslomake esiteltiin. Kaikkiin kysymyksiin vastattiin Likert-asteikolla välillä 1-7, jossa arvo 1 vastasi ”täysin eri mieltä”, kun taas arvo 7 puolestaan ”täysin samaa mieltä”. Seuraavassa taulukossa (taulukko 5) esitellään tutkimuksessa kerättyjen vastausten keskiarvot, mediaanit sekä keskihajonnat tarinakohtaisesti.

Taulukko 5. Kyselyn vastausten erittely

	Tarina 1 (näyttölukko)				**Tarina 2 (ulkop. sovellukset)**		
Kysymys	**Keskiarvo**	**Mediaani**	**Keskihajonta**		**Keskiarvo**	**Mediaani**	**Keskihajonta**
selfcon1	3.56	3	2.02		4.55	5	1.89
selfcon2	3.51	3	1.77		3.35	3	1.71
selfcon3	4.57	5	1.84		4.01	4	1.71
roles2	4.04	4	1.85		3.82	4	1.69
roles3	4.46	5	1.82		3.94	4	1.66
affect1	2.40	2	1.48		2.15	2	1.24
affect4	3.93	4	1.84		3.33	4	1.54
moral1	4.39	4	1.64		3.76	4	1.55
percbehcont2	6.03	7	1.61		5.96	7	1.52
fear10	2.88	2	1.82		5.71	6	1.49
fear7	5.62	6	1.59		6.25	7	1.09
fear11	2.33	2	1.58		5.99	6	1.24
intent1	2.55	2	1.89		2.20	2	1.52
intent2	2.47	2	1.83		2.19	2	1.51
	Tapoihin liittyvät kysymykset						
Kysymys	**Keskiarvo**	**Mediaani**	**Keskihajonta**				
habit1	4.80	5	1.74				
habit2	4.83	5	1.74				
habit3	4.57	5	1.72				
habit5	4.56	5	1.71				
habit7	4.59	5	1.92				
habit8	4.05	4	1.87				
habit11	4.67	5	1.83				
habit12	4.80	5	1.89				

Tutkimuksessa kerättyjen vastauksen numeerisen ilmaisun lisäksi on hyvä esitellä myös kysymysten korrelaatiomatriisit tarinakohtaisesti. Korrelaatiomatriisin avulla aineiston soveltumista faktorianalyyseihin voidaan arvioida, ja jos korrelaatioita on olemassa, on faktorianalyysiä mahdollista käyttää teorian tai mallin tutkimisessa (Metsämuuronen, 2011, s. 684). Korrelaatiomatriiseista on poistettu alhaisen korrelaation arvot ($<|0.20|$) lukemisen helpottamiseksi. Kaikki esitetyt arvot ovat myös tilastollisesti merkitseviä ($p<0.05$). Tarinan 1 korrelaatiomatriisi löytyy taulukosta 6, ja tarinan 2 taulukosta 7.

Taulukko 6. Tarinan 1 korrelaatiomatriisi

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
1. selfcon1	1	-0,44	-0,56	-0,26	-0,52	-0,46	-0,38	-0,51		0,27	0,37		-0,42	-0,42	0,3	0,27			0,26	0,26	0,29	0,29
2. selfcon2	-0,44	1	0,58	0,46	0,57	0,58	0,42	0,47	-0,27		-0,31		0,53	0,52	-0,25	-0,27			-0,21		-0,29	-0,29
3. selfcon3	-0,56	0,58	1	0,37	0,66	0,54	0,41	0,64		-0,28	-0,33		0,43	0,42	-0,22	-0,23					-0,25	-0,24
4. roles2	-0,26	0,46	0,37	1	0,52	0,38	0,3	0,33	-0,22		-0,25		0,36	0,37							-0,24	-0,25
5. roles3	-0,52	0,57	0,66	0,52	1	0,55	0,5	0,59		-0,28	-0,32		0,47	0,49		-0,22					-0,25	-0,25
6. affect1	-0,46	0,58	0,54	0,38	0,55	1	0,47	0,49	-0,3	-0,24	-0,46		0,53	0,54	-0,23	-0,25					-0,26	-0,29
7. affect4	-0,38	0,42	0,41	0,3	0,5	0,47	1	0,4	-0,23	-0,24	-0,25		0,47	0,46								
8. moral1	-0,51	0,47	0,64	0,33	0,59	0,49	0,4	1		-0,28	-0,27		0,35	0,36							-0,21	
9. percbeh-cont2		-0,27		-0,22		-0,3	-0,23		1				-0,57	-0,58		0,23					0,23	0,24
10. fear10	0,27		-0,28		-0,28	-0,24	-0,24	-0,28		1	0,33	0,54										
11. fear7	0,37	-0,31	-0,33	-0,25	-0,32	-0,46	-0,25	-0,27		0,33	1		-0,3	-0,28								0,28
12. fear11										0,54		1										
13. intent1	-0,42	0,53	0,43	0,36	0,47	0,53	0,47	0,35	-0,57		-0,3		1	0,93	-0,34	-0,37		-0,26	-0,3	-0,3	-0,39	-0,41
14. intent2	-0,42	0,52	0,42	0,37	0,49	0,54	0,46	0,36	-0,58		-0,28		0,93	1	-0,34	-0,36		-0,26	-0,29	-0,29	-0,38	-0,4
15. habit1	0,3	-0,25	-0,22			-0,23							-0,34	-0,34	1	0,84	0,44	0,6	0,75	0,65	0,79	0,74
16. habit2	0,27	-0,27	-0,23		-0,22	-0,25			0,23				-0,37	-0,36	0,84	1	0,55	0,71	0,79	0,71	0,82	0,78
17. habit3															0,44	0,55	1	0,67	0,48	0,56	0,53	0,46
18. habit5													-0,26	-0,26	0,6	0,71	0,67	1	0,63	0,72	0,68	0,63
19. habit7	0,26	-0,21											-0,3	-0,29	0,75	0,79	0,48	0,63	1	0,71	0,81	0,77
20. habit8	0,26			-0,2									-0,3	-0,29	0,65	0,71	0,56	0,72	0,71	1	0,77	0,71
21. habit11	0,29	-0,29	-0,25	-0,24	-0,25	-0,26		-0,21	0,23				-0,39	-0,38	0,79	0,82	0,53	0,68	0,81	0,77	1	0,87
22. habit12	0,29	-0,29	-0,24	-0,25	-0,25	-0,29			0,24		0,28		-0,41	-0,4	0,74	0,78	0,46	0,63	0,77	0,71	0,87	1

Matalat <|0.20| korrelaatiot poistettu, kaikki arvot tilastollisesti merkitseviä ($p<0.05$).

Taulukko 7. Tarinan 2 korrelaatiomatriisi

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
1. selfcon1	1	-0,48	-0,57	-0,29	-0,45	-0,48	-0,32	-0,51	0,3	0,37	0,39	0,34	-0,48	-0,48								
2. selfcon2	-0,48	1	0,56	0,43	0,57	0,56	0,39	0,46	-0,28	-0,25	-0,26	-0,24	0,53	0,48								
3. selfcon3	-0,57	0,56	1	0,33	0,65	0,5	0,35	0,68	-0,21	-0,27	-0,26	-0,22	0,49	0,47								
4. roles2	-0,29	0,43	0,33	1	0,45	0,29	0,22	0,3					0,25	0,23								
5. roles3	-0,45	0,57	0,65	0,45	1	0,55	0,41	0,62	-0,23	-0,27	-0,27	-0,23	0,49	0,48								
6. affect1	-0,48	0,56	0,5	0,29	0,55	1	0,41	0,49	-0,4	-0,39	-0,46	-0,38	0,61	0,59								
7. affect4	-0,32	0,39	0,35	0,22	0,41	0,41	1	0,37		-0,24	-0,28	-0,23	0,36	0,36								
8. moral1	-0,51	0,46	0,68	0,3	0,62	0,49	0,37	1		-0,29	-0,25	-0,24	0,42	0,4								
9. percbeh-cont2	0,3	-0,28	-0,21		-0,23	-0,4	-0,19	-0,16	1	0,26	0,32	0,23	-0,55	-0,58								
10. fear10	0,37	-0,25	-0,27		-0,27	-0,39	-0,24	-0,29	0,26	1	0,7	0,66	-0,36	-0,4								
11. fear7	0,39	-0,26	-0,26		-0,27	-0,46	-0,28	-0,25	0,32	0,7	1	0,68	-0,37	-0,43								0,23
12. fear11	0,34	-0,24	-0,22		-0,23	-0,38	-0,23	-0,24	0,23	0,66	0,68	1	-0,27	-0,34								
13. intent1	-0,48	0,53	0,49	0,25	0,49	0,61	0,36	0,42	-0,55	-0,36	-0,37	-0,27	1	0,91								
14. intent2	-0,48	0,48	0,47	0,23	0,48	0,59	0,36	0,4	-0,58	-0,4	-0,43	-0,34	0,91	1								
15. habit1															1	0,84	0,44	0,6	0,75	0,65	0,79	0,74
16. habit2															0,84	1	0,55	0,71	0,79	0,71	0,82	0,78
17. habit3															0,44	0,55	1	0,67	0,48	0,56	0,53	0,46
18. habit5															0,6	0,71	0,67	1	0,63	0,72	0,68	0,63
19. habit7															0,75	0,79	0,48	0,63	1	0,71	0,81	0,77
20. habit8															0,65	0,71	0,56	0,72	0,71	1	0,77	0,71
21. habit11															0,79	0,82	0,53	0,68	0,81	0,77	1	0,87
22. habit12											0,23				0,74	0,78	0,46	0,63	0,77	0,71	0,87	1

Matalat <|0.20| korrelaatiot poistettu, kaikki arvot tilastollisesti merkitseviä ($p<0.05$).

5.3 Tarinan 1 (näyttölukko) tulokset

Kyselyssä molempien tarinoiden kohdalla vastaajilta kysyttiin, kuinka realistisena he tarinaa pitivät. Vastaajat arvioivat tarinan realistisuutta 7-kohtaisella likert-asteikolla, jonka arvot olivat 1-7. Asteikon numero 1 vastasi väittämää ”täysin eri mieltä” ja arvo 7 ”täysin samaa mieltä”. Vastaajille ei esitetty vaihtoehtoa ”en tiedä” lainkaan, jotta jokaiselle vastaukselle saataisiin luotettava arvo. Myöskään vaihtoehtoa ”ei samaa eikä eri mieltä” vaihtoehtoa ei erikseen esitetty, joskin asteikon arvo 4 sijoittui molempien ääripäiden keskelle.

Kaikkien vastaajien keskiarvo tarinan 1 realistisuudesta oli 5,04 ja mediaani 5. Arvo 1 vastaa täysin epärealistista ja arvo 7 täysin realistista, joten tulosten perusteella kuvattua tarinaa voidaan pitää jokseenkin realistisena kuvauksena älypuhelimen käyttötilanteesta. Vastaajista miehet pitivät tarinaa hieman muita epärealistisempana (keskiarvo 4,8), naisiin (ka. 5,2) ja muihin verrattuna (ka. 5,3). Taulukosta 8 löytyvät tarinan realistisuutta mittaavat arvot.

Taulukko 8. Tarinan 1 realistisuus

Sukupuoli	**Tarinan realistisuus (1- täysin epärealistinen, 7-täysin realistinen), keskiarvo**
Nainen	5,2
Mies	4,8
Muu	5,3
Kaikki vastaajat yhteensä	5,04

Tutkimuksen faktorianalyysin tavoitteena oli tarkastella UMISPC-mallin kuvailemia konstruktioita ja niiden vaikutusta toisiinsa. Erityisen tarkastelun kohteena tutkielmassa on aikomus, tarkemmin tietoturvaominaisuuksien käytön aikomus. Faktorianalyysillä nähdään myös UMISPC-mallin toimivuus, kun tutkimuksen konteksti on vaihdettu organisatorisesta henkilökohtaiseen älypuhelinkäyttöön. Taulukon 9 sarakkeessa ”Kysymys UMISPC” tarkoittaa kyselypohjassa käytettyjä UMISPC-mallin kysymyksiä (ks. taulukko 2). Muuttujien lataukset on asetettu löydetyille faktoreille. Vain muuttujat joiden lataukset ovat suurempia kuin |0.30| on esitetty taulukossa lukemisen helpottamiseksi. Muuttujia, joiden latauksen arvo on alle |0.30| voidaan pitää turhina, ja ne voidaan kokonaan poistaa löydetyistä faktoreista (Metsämuuronen, 2011, s. 670). Muuttujan kommunaliteetti kuvaa sitä, miten hyvin muuttuja latautuu faktorille. Mitä lähempänä arvoa 1 kommunaliteetti on, sitä voimakkaammin se latautuu kyseiselle faktorille. (Metsämuuronen, 2011, s. 670.) Tarinan 1 faktorianalyysin tulokset näkyvät taulukossa 9.

Taulukko 9. Tarinan 1 faktorianalyysin tulokset

Kysymys UMISPC	**Faktori 1**	**Faktori 2**	**Faktori 3**	**Faktori 4**	**Kommunaliteetti**
selfcon1					0,379
selfcon2				0,666	0,474
selfcon3				0,887	0,802
roles2				0,484	0,242
roles3				0,829	0,688
affect1				0,612	0,408
affect4				0,459	0,271
moral1				0,807	0,673
percbehcont2					0,510
fear10	1,018				1,041
fear7					0,155
fear11	0,543				0,298
intent1			0,898		0,817
intent2			0,902		0,825
habit1		0,843			0,715
habit2		0,898			0,807
habit3		0,620			0,400
habit5		0,781			0,619
habit7		0,891			0,800
habit8		0,828			0,687
habit11		0,915			0,840
habit12		0,851			0,729

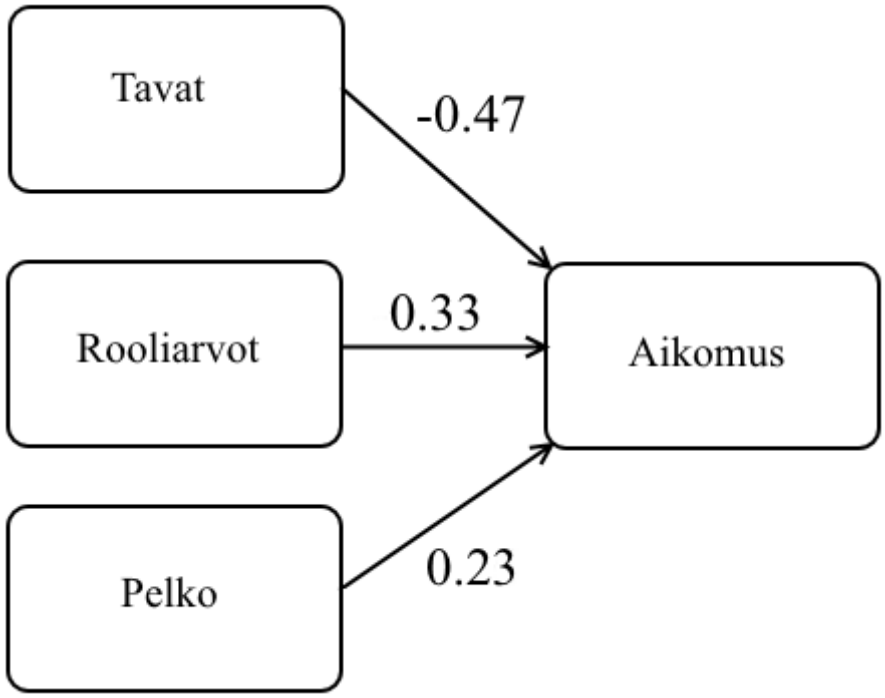
Tarinan 1 faktorianalyysin perusteella huomataankin, että UMISPC:n kysymykset *selfcon1*, *fear7*, ja *percbehcont2* eivät sijoitu millekään faktoreista. Kysymys *selfcon1* eli ”Tuntisin syyllisyyttä, jos tekisin niin kuin Jokinen teki”, *fear7* eli ”Älypuhelimeni saattaa vaarantua, jos teen niin kuin Jokinen teki” ja kysymys *perchbehcont2* eli ”Koetko että pystyisit olemaan toimimatta samoin kuin Jokinen kuvatussa tilanteessa?” ja eivät siis ole kerätyn datan perusteella merkittäviä, ja ne poistetaan tarinan 1 jatkoanalyyseistä.

Faktorianalyysin perusteella muuttujat voidaan jakaa 4 faktoriin, jotka sopivatkin hyvin UMISPC-mallin tarkasteltavana olevaan osuuteen. Löydetyt faktorit nimettiin UMISPC:n konstruktioiden mukaan, jotka ovat pelko, tavat, aikomus sekä rooliarvot. Faktorin selitysaste kuvaa sitä, miten hyvin faktori selittää muuttujien hajontaa, joka on tarinan 1 faktorianalyysin perusteella yhteensä 59,9 %, mikä tarkoittaa sitä, että löydetyt faktorit selittävät yhteensä 59,9 % muuttujien hajonnasta (Metsämuuronen, 2011, s. 662). Taulukossa 10 näkyvät nimetyt faktorit, niiden selitysaste sekä reliabiliteettia kuvaava Cronbach:in alfan arvo. Cronbach:in alfan arvoa voidaan pitää hyväksyttävänä, jos se on suurempi kuin 0,60 (Metsämuuronen, 2011, s. 467).

Taulukko 10. Tarinan 1 löydetyt faktorit

Faktori	**Muuttujien määrä**	**Selitysaste**	**Reliabiliteetti (Cronbach α)**
Tavat	8	25,4 %	0,946
Rooliarvot	7	17,9 %	0,867
Aikomus	2	10,3 %	0,961
Pelko	2	6,3 %	0,694

Faktorien löytämisen ja nimeämisen jälkeen faktoreille suoritettiin regressioanalyysi konstruktioiden (ts. faktorien tai summamuuttujien) yhteyksien löytämiseksi. Regressioanalyysissä käytettiin lineaarista regressioanalyysiä, joka sopii sen tutkimiseen, miten hyvin selittävät muuttujat selittävät kriteerimuuttujaa, eli miten pelko, tavat ja rooliarvot ovat yhteydessä aikomukseen (Metsämuuronen, 2011, s. 710). Kuviossa 6 kuvataan faktorien (summamuuttujien) välillä löydetyt yhteydet.



Kuvio 6. Tarinan 1 summamuuttujien yhteys aikomukseen

Regressioanalyysissä huomattiin, että kaikilla faktorianalyysissä havaituilla summamuuttujilla oli selittävä yhteys aikomukseen. Summamuuttujien yhteyttä kuvaa regressioanalyysin β-kerroin hieman korrelaatiokertoimen tavoin, ja B-arvo kertoo sen, miten selittävä muuttuja käyttäytyy, kun kriteerimuuttuja (aikomus) nousee yhdellä (Metsämuuronen, 2011 s. 715-716). Tapojen merkitystä aikomusta selittävänä tekijänä voidaan pitää kohtalaisena (-0.47), ja pelon vaikutusta aikomukseen vähäisenä (0.26). Rooliarvot selittävät aikomusta myös hieman (0.33), mutta ei läheskään yhtä merkittävästi kuin UMISPC-mallissa (Moody et al., 2018).

Regressioanalyysin perusteella tarinassa 1 selittävät muuttujat selittävät kriteerimuuttujaa selitysosuudella $R^2 = 0.4$, mikä tarkoittaa sitä, että yhteensä summamuuttujat selittävät aikomuksesta 40 prosenttia. Yksittäisen summamuuttujan aikomuksen selittävyys saadaan kertomalla kunkin muuttujan arvo r itsellään. Kaikki regressioanalyysin tulokset olivat tarinan 1 kohdalla myös tilastollisesti merkittäviä, joten niitä voidaan pitää vaihtelua selittävinä (Metsämuuronen, 2011, s. 720). Tarinan 1 regressionanalyysin tuloksen löytyvät taulukosta 11.

Taulukko 11. Tarinan 1 summamuuttujien yhteys aikomukseen

	B	**β-kerroin**	**r**	**p-arvo**	**t**
Tavat	-0.47	-0.47	-0.414	<0.001***	-12.97
Rooliarvot	0.36	0.33	0.370	<0.001***	9.19
Pelko	0.26	0.23	0.139	<0.001***	6.37
Selitysosuus $R^2 = 0.4$, SSE = 436.73, F = 258.64					

5.4 Tarinan 2 (ulkopuoliset sovellukset) tulokset

Samoin kun tarinan 1 kohdalla, myös tarinassa 2 kysyttiin vastaajilta arviota tarinan realistisuudesta. Tarina 2 koettiin yleisesti realistisempana kuin tarina 1. Tarinan 2 realismi sai keskiarvokseen 5,47, ja mediaani arvoille oli 6. Näiden arvojen perusteella tarinaa voidaan jo pitää hyvin todellisuutta vastaavana, mikä parantaa tutkimuksen validiteettia. Sukupuolten välillä oli jälleen hieman eroja, naisten keskiarvo tarinan realismille oli 5,6, miesten 5,3 ja muiden (N=4) 7. Naiset pitivät siis jälleen tarinaa miehiä realistisempana, kun taas muut pitivät tarinaa täysin realistisena – tosin tulee huomioida, että muihin kuuluvien vastaajien määrä oli hyvin pieni. Taulukosta 12 löytyvät vastaajien tarinan realismille antamat keskiarvot.

Taulukko 12. Tarinan 2 realistisuus

Sukupuoli	**Tarinan realistisuus (1- täysin epärealistinen, 7-täysin realistinen), keskiarvo**
Nainen	5,6
Mies	5,3
Muu	7
Kaikki vastaajat yhteensä	5,47

Myös tarinalle 2 suoritettiin sama faktorianalyysi, kuin tarinalle 1. Taulukosta on jälleen poistettu muuttujien lataukset, jotka ovat alle $|0.30|$. Taulukossa 13 kuvataan tarinan 2 faktorianalyysin tulokset.

Taulukko 13. Tarinan 2 faktorianalyysin tulokset

Kysymys UMISPC	**Faktori 1**	**Faktori 2**	**Faktori 3**	**Faktori 4**	**Kommunaliteetti**
selfcon1					0,297
selfcon2				0,635	0,429
selfcon3				0,870	0,763
roles2				0,505	0,272
roles3				0,836	0,710
affect1				0,440	0,290
affect4				0,403	0,184
moral1				0,848	0,735
percbehcont2					0,399
fear10			0,829		0,688
fear7			0,875		0,771
fear11			0,877		0,782
intent1	0,936				0,904
intent2	0,911				0,836
habit1		0,847			0,719
habit2		0,906			0,822
habit3		0,605			0,394
habit5		0,768			0,601
habit7		0,866			0,759
habit8		0,824			0,686
habit11		0,930			0,866
habit12		0,873			0,772

Faktorianalyysin perusteella jälleen huomataan, että UMISPC:n kysymykset *selfcon1* ja *perchbehcont2* eivät sijoitu millekään faktorille. Kysymys *selfcon1* eli ”Tuntisin syyllisyyttä, jos tekisin niin kuin Jokinen teki ja kysymys *perchbehcont2* eli ”Koetko että pystyisit olemaan toimimatta samoin kuin Jokinen kuvatussa tilanteessa?” eivät siis tässäkään tarinassa ole merkittäviä muuttujia.

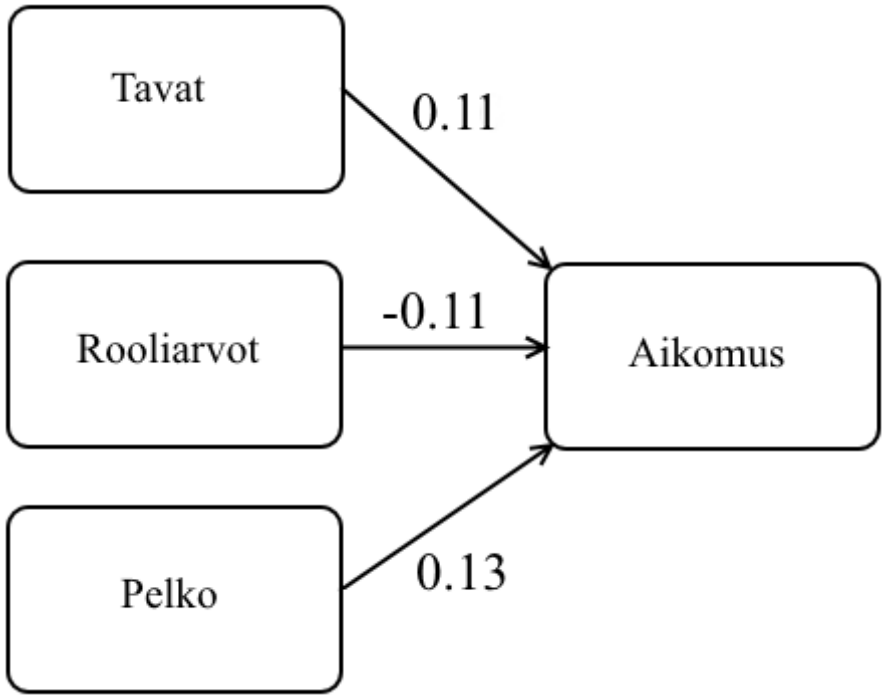
Tarinasta 1 poiketen kysymys *fear7* eli ”Älypuhelimeni saattaa vaarantua, jos teen niin kuin Jokinen teki” sijoittuu yhdelle faktoreista. Muuttujan lataus sekä kommunaliteetti ovat molemmat myös korkeita, joka eroaa merkittävästi tarinan 1 faktorianalyysistä kyseisen muuttujan kohdalla. Regressioanalyysin mielekkyyden ja tarinoiden vertailun oikeellisuuden kannalta *fear7* poistettaan kuitenkin lopullisista faktoreista.

Faktorit pystyttiin jälleen nimeämään UMISPC:n esittämien konstruktioiden mukaan samoin kun tarinan 1 kohdalla. Tarinassa 2 faktorien yhteinen selitysaste oli 62,4 %, joka oli hieman tarinaa 1 korkeampi. Tarinasta 1 poiketen pelon faktorin selitysaste nousi aikomuksen vastaavaa korkeammaksi, mikä nostaa pelon faktorin vaikutusta muuttujien hajonnan selittävänä tekijänä. Kaikkien löydettyjen faktorien Cronbach:in alfan arvot olivat myös hyvät. Tarinan 2 faktorianalyysistä löydettyjen faktorien nimet ja selitysasteet näkyvät taulukossa 14.

Taulukko 14. Tarinan 2 löydetyt faktorit

Faktori	**Muuttujien määrä**	**Selitysaste**	**Reliabiliteetti (Cronbach α)**
Tavat	8	26,6 %	0,946
Rooliarvot	7	17,1 %	0,853
Pelko	2	7,7 %	0,789
Aikomus	2	11,0 %	0,954

Faktorien luomisen jälkeen suoritettiin niille myös lineaarinen regressioanalyysi. Tarinan 2 kohdalla havaittiin, että kaikilla summamuuttujilla oli hyvin matala yhteys aikomukseen. Nämä havaitut yhteydet olivat kuitenkin kaikki tilastollisesti merkitseviä ($p<0.05$). Tarinan 2 summamuuttujien yhteys aikomukseen näkyvät kuviossa 7.



Kuvio 7. Tarinan 2 summamuuttujien yhteys aikomukseen

Samoin kuin tarinassa 1, tarinassa 2 regressioanalyysin tulosten perusteella selittävillä summamuuttujilla on yhteys aikomukseen. Vaikka yhteydet ovat havaittavissa, ja ne ovat kaikki tilastollisesti merkitseviä, voidaan yhteyksien arvoja yhteyttä aikomukseen pitää matalina. Tarinasta 1 poiketen, tarinassa 2 tavoilla on matala positiivinen yhteys aikomukseen, kun yhteys tarinassa 1 oli kohtailainen sekä negatiivinen. Rooliarvoilla havaittiin olevan tarinassa 2 heikko negatiivinen yhteys aikomukseen arvolla -0.11, mikä kuitenkin tarinassa 1 oli kohtalainen arvolla 0.33. Tarinassa 2 huomionarvoista on myös se, että selitysosuudeksi R^2 saatiin 0 %, mikä tarkoittaa sitä, että summamuuttujat eivät selitä kriteerimuuttujan vaihtelua lainkaan. Havaittuja yhteyksiä summamuuttujien välillä käsitellään tulosten analyysiosiossa tarkemmin seuraavassa luvussa. Taulukossa 15 esitellään tarinan 2 regressioanalyysin tulokset.

Taulukko 15. Tarinan 2 summamuuttujien yhteys aikomukseen

	B	β-kerroin	r	p-arvo	t
Tavat	0.09	0.11	-0.02	<0.017***	2.39
Rooliarvot	-0.10	-0.11	-0.09	<0.006***	-2.55
Pelko	0.10	0.13	0.08	<0.011***	2.78
Selitysosuus R^2 = 0.0, SSE = 467.59, F = 6.79					

5.5 Tutkimuksen tulosten analyysi

Tutkimuksen kyselyosuudessa kyselyyn kaikki vastanneet vastasivat sekä tarinaan 1 että tarinaan 2 liittyviin väittämiin. Tarinoiden pääasiallisina eroina oli käyttötilanne, jossa tarinan henkilö käytti älypuhelintaan, ja jossa henkilö rikkoi yleisiä älypuhelimen käyttöön liittyviä tietoturvakäytänteitä. Tarinassa 1 tarkasteltiin näyttölukon käyttöä, ja tarinassa 2 ulkopuolisten sovellusten asentamista. Tässä kappaleessa käydään läpi tarinoiden välillä havaittuja eroja ja yhtäläisyyksiä, sekä verrataan tuloksia UMISPC-mallin tuloksiin.

Kyselyssä tarinan toimijan ja tarinan esittelyn jälkeen vastaajilta kysyttiin, miten realistisina vastaajat tarinoita pitivät. Kysymyksen tavoitteena oli yleisesti kartoittaa sitä, miten hyvin tarinat sopisivat käytännölliseen älypuhelimenkäyttötilanteeseen. Kerättyjen vastausten perusteella molempia tarinoita voidaan pitää realistisina, ja niiden realistisuudelle annetut arvot olivat 5,04 tarinalle 1 ja 5,47 tarinalle 2, jossa arvo 1 vastaa täysin epärealistista ja arvo 7 täysin realistista, arvon 4 sijoittuessa asteikon keskelle.

Faktorianalyysillä pyrittiin selvittämään muuttujien sopivuutta aineiston mittaamiseen. Faktorianalyysissä löytyneet faktorit vastasivat tarinoiden välillä hyvin toisiaan, mutta pieniä eroja oli havaittavissa. Jokainen muuttuja oli merkittävä UMISPC-mallissa (Moody et al., 2018), joten eroja malliin löydettiin. Faktorianalyysissä havaitut faktorit (ts. konstruktiot) vastasivat sisällöiltään täysin UMISPC-mallin esittämiä ja tarkastelun kohteina olleita: tavat, pelko, rooliarvot ja aikomus olivat kaikki havaittavissa, ja niille sijoittuneet muuttujat vastasivat faktorien tosiasiallista sisältöä.

Faktorianalyysissä kuitenkin huomattiin, että osa muuttujista ei sijoittunut millekään faktorille, joten niitä voidaan pitää huonoina kerätyn aineiston kuvaajina. Tarinassa 1 UMISPC muuttujat *selfcon1*, *fear7*, ja *percbehcont2* eivät sijoittuneet löydetyille faktoreille, ja ne poistettiin. UMISPC-mallissa *selfcon1* ja *percbehcont2* sijoittuivat molemmat rooliarvojen konstruktioon, ja *fear7* pelon konstruktioon (Moody et al., 2018). Tarinan 2 muuttujat *selfcon1* ja *percbehcont2* poistettiin myös faktorianalyysin perusteella, sillä ne eivät sijoittuneet löydetyille faktoreille. Tarinasta 1 poiketen *fear7* kuitenkin sijoittui pelon faktorille tarinassa 2, joten tarinan 2 kontekstissa muuttuja oli merkittävä – *fear7* kuitenkin poistettiin summamuuttijista, jotta regressioanalyysin tuloksia voidaan verrata tarinoiden välillä. Näiden erojen mahdollisia syitä käsitellään seuraavassa johtopäätöksiä käsittelevässä luvussa.

Tarinoiden faktorianalyysissä löydettyjen faktorien selitysosuudet olivat tarinalle 1 yhteensä 59,9 % ja tarinalle 2 62,4 %. Selitysosuudet kuvaavat sitä, kuinka paljon faktorit selittävät kaikkien muuttujien varianssia (Metsämuuronen, 2011, s. 662). Molemmissa tarinoissa aineistoa parhaiten selitti tavat-faktori.

UMISPC:n mukaan rooliarvot ovat löydetystä aikomukseen yhteydessä olevista konstruktioista kaikkein merkittävin. Moody, Siponen & Pahnila (2018) kuitenkin painottavat rooliarvojen olevan merkittäviä juuri työkontekstissa, jossa työntekijä joko noudattaa tai rikkoo voimassaolevia tietoturvakäytänteitä. Myös tapojen ja pelon konstruktiot yhdistyivät aikomukseen merkittävästi. (Moody et al., 2018.) Tämän tutkimuksen tulokset eroavat kuitenkin merkittävästi UMISPC:hen verrattuna: tarinassa 1 rooliarvojen yhteys aikomukseen oli 0,33, jota voidaan pitää matalana tai enintään kohtalaisena, ja tarinassa 2 arvolla -0,11, joka puolestaan on hyvin matala. Kaikki havaitut yhteydet olivat kuitenkin tilastollisesti merkitseviä, joka osaltaan viittaa mallin yleispätevyyteen.

Tutkimuksessa havaittiin sekä yhtäläisyyksiä että eroja kerätyn datan ja UMISPC-mallin välillä. Esimerkiksi UMISPC-mallin esittämät konstruktiot (faktorit) olivat sisällöllisesti helposti löydettävissä kerättyä dataa analysoimalla. Molempien tarinoiden kohdalla kuitenkin muuttujat ”tuntisin syyllisyyttä” ja ”koetko, että pystyisit olemaan toimimatta samoin” eivät sijoittuneet faktoreille, eivätkä näin ollen selittäneet dataa hyvin. Löydettyjen faktorien selitysosuudet olivat myös kohtalaiset, noin 60 % molemmissa tarinoissa.

Merkittävimmät erot UMISPC:hen verrattuna löytyivätkin summamuuttujien yhteyksistä keskenään. UMISPC-malli painottaa rooliarvojen yhteyttä aikomukseen työkontekstia tarkastellessa huomattavasti (Moody et al., 2018), mutta tässä tutkimuksessa rooliarvojen merkitys oli verrattain vähäinen.

Vastaukset tutkimuskysymykseen ”mitkä ennalta määritellyt tekijät vaikuttavat älypuhelinkäyttäjän tietoturva-aikomukseen?” tutkimusosuuden perusteella ovatkin siis seuraavat:

> Tarinassa 1 (näyttölukko) tietoturva-aikomukseen vaikuttivat tavat (-0,47), rooliarvot (0,33) ja pelot (0.23).
>
> Tarinassa 2 (ulkopuoliset sovellukset) tietoturva-aikomukseen vaikuttivat pelot (0,13), tavat (0,11) ja rooliarvot (-0,11).

Seuraavassa luvussa käsitellään mahdollisia syitä havaituille eroille UMISPC-mallin ja tutkimustulosten välillä, jossa esille nousevatkin erityisesti erot tutkimusten konteksteissa, ja yksittäisiä muuttujia tarkastellessa.

6 JOHTOPÄÄTÖKSET

Tässä tutkielmassa käsiteltiin älypuhelinkäyttäjien tietoturvakäyttäytymistä ja aikomusta tietoturvarikkeisiin liittyen. Tarkastelimme tutkielman alkupuolella mitä erilaisia tietoturvaominaisuuksia älypuhelimissa on käyttäjien käytettävissä, ja millaisia uhkia älypuhelimiin kohdistuu. Tämän jälkeen esittelimme tutkielmassa tutkielman aiheen kannalta relevantteja teorioita, sekä kävimme läpi UMISPC-mallin ja sen luomisessa käytetyt teoriat. UMISPC-mallia käytettiin myös tutkielman empiirisen tutkimusosuuden rakentamisessa, jonka tavoitteena oli tarkastella UMISPC-mallin soveltuvuutta älypuhelinkäyttäjien tietoturva-aikomuksen kuvaamisessa. Tutkimusosuuden avulla selvitettiin UMISPC-mallin soveltuvuutta älypuhelinkontekstiin selvitettiin, ja tuloksia löydettiin.

Edellisessä luvussa käsiteltiin tutkimuksen keskeisimmät tutkimustulokset ja lopuksi tuloksia analysoitiin kyselyssä käytettyjen tarinoiden sekä tutkimuksen luomisessa käytetyn UMISPC-mallin välillä. Kerättyä dataa analysoitiin faktorianalyysillä, sekä löydettyjä faktoreita regressioanalyysillä yhteyksien löytämiseksi summamuuttujien ja aikomuksen välillä. Faktorianalyysissä löydetyt faktorit sopivat UMISPC-mallin esittämiin konstruktioihin hyvin, ja regressioanalyysillä saatiin selvyys, miten hyvin summamuuttujilla voidaan aikomusta selittää tämän tutkielman kontekstissa.

Tutkimuksen tuloksia täytyy kuitenkin tarkastella kriittisesti, sillä kuten usein kyselytutkimuksissa, on mahdollista, etteivät kerätty data ja siitä löydetyt tulokset vastaa täysin todellisuutta. Tuloksiin ja vastaajien vastauksiin voi syntyä mittausvirhettä useilla eri tavoilla, joita on kuitenkin yritetty vähentää testaamalla kyselylomaketta etukäteen, sekä käyttämällä jo aiemmin testattuja kyselylomakkeita mallina tutkimuksen kyselyn luomisessa.

Tässä luvussa käsitellään tutkimuksen ja UMISPC-mallin välisien yhtäläisyyksien ja eroavaisuuksien mahdollisia syitä. Johtopäätöksiä voidaan pitää jokseenkin spekulatiivisina, mutta niille voidaan löytää myös mahdollisia syitä aikaisempaa tutkimusta hyödyntämällä, sekä tutkimuksessa käytettyjen yksittäisten muuttujien (ts. kysymysten) vastausten perusteella.

Ensimmäinen ja kenties merkittävin johtopäätös tulosten ja käytetyn mallin välillä on tarkasteltava konteksti. UMISPC-mallin on luotu organisatoriseen työkontekstiin, jossa toimijoilla on aina jonkinlainen sosiaalinen rooli työpaikan sisällä, jonka vuoksi malli painottaakin rooliarvojen tärkeyttä tietoturva-

aikomuksen selittävänä tekijänä (Moody et al., 2018). Tutkimuksessa tarkasteltiin älypuhelinkäyttäjien toimintaa henkilökohtaisen datansa suojaamiseksi, jolloin työpaikan luomat sosiaaliset roolit jäävät puuttumaan. Tarinoissa toimijan rooliin kuului halu pitää laitteensa tietoturva kunnossa, mutta silti rooliarvojen vaikutus aikomukseen jäi jokseenkin vähäiseksi. Voidaankin olettaa, että tilanteessa, jossa toimija on ns. ”oman itsensä herra”, ei konkreettista uhkaa tai koettuja kustannuksia tai haittoja synny yhtä helposti tai paljon kuin organisatorisessa kontekstissa. Esimerkiksi työpaikan tietoturvaa rikkomalla toimija saattaa aiheuttaa merkittävää haittaa yrityksen imagolle tietovuodon muodossa, kun puolestaan henkilökohtaisessa kontekstissa haitta saattaa olla toimijalle lähes merkityksetön, esimerkiksi puhelimen väliaikainen hidastuminen asennetun roskasovelluksen muodossa. Henkilökohtaisessa käytössä myös mahdolliset sanktiot ovat lähes olemattomat, kun taas puolestaan työpaikalla pienestäkin rikkeestä epämuodollisena sanktiona saattaa olla paheksunta, pahimmassa tapauksessa jopa työpaikan menetys (Moody et al., 2018; Siponen & Vance, 2010).

Molemmissa tutkimuksen tarinoissa myös poistettiin UMISPC-mallin mukaisia muuttujia tarkastelusta, sillä ne eivät sijoittuneet faktorianalyyseissä millekään faktorille. Eräs poistetuista muuttujista oli kysymys ”tuntisin syyllisyyttä, jos tekisin niin kuin Jokinen teki”, jonka huonon mittaavuuden syitä voidaan arvioida. Kyselyyn vastanneilla henkilöillä oli käytössään henkilökohtainen älypuhelin, eikä heillä tutkimuksen rajauksessa ollut mitään virallista roolia, toisin kuin UMISPC:ssä, jossa toimijoilla oli rooli organisaation työntekijänä. On mahdollista, että tietoturvarikkeestä ei synny vastaajille syyllisyydentunnetta, sillä tietoturvarikkeen sattuessa rikkeen seurauksista vastaa vain rikkeen tekijä itse. Organisatorisessa kontekstissa sekä sanktiot että mahdolliset muut aiheutuneet haitat saattavat aiheuttaa enemmän syyllisyyttä kun henkilökohtaisessa käytössä.

Kontekstin merkittävyydestä UMISPC-mallia tarkastellessa puhuu myös tutkimuksen yksittäisten kysymysten vastaukset. Kyselyn tarinoissa tarkasteltiin kahta eri tietoturvaominaisuutta, näyttölukkoa sekä ulkopuolisten sovellusten asentamista. Molemmat tarinat koskivat älypuhelinkäyttäjien omaa toimintaa oman datansa suojaamisessa, mutta esimerkiksi pelkoa käsittelevien kysymysten vastaukset olivat mielenkiintoisia. Tarinassa 1, jossa käsiteltiin näyttölukkoa, vastaajat pitivät laitteensa tietoturvan vaarantumista mahdollisena (5,62), mutta vastaajat eivät uskoneet tämän tietoturvarikkeen tekevän laitteesta käyttökelvotonta (2,89), eikä siihen, että laite hidastuisi (2,33). Vastaavasti tarinassa 2 ulkopuolisten sovellusten asentamista tarkastellessa vastaajien vastausten keskiarvot laitteen mahdolliselle vaarantumiselle (6,25), käyttökelvottomaksi muuttumiselle (5,70) ja hidastumiselle (5,98) olivat huomattavasti korkeammat. Tuloksista huomaamme, että esimerkiksi pelon faktoria tarkastellessa tulokset pelkkää tietoturvarikettä muuttamalla ovat merkittävät, joka edelleen kertoo siitä, että kontekstilla on suuri merkitys UMISPC-mallin kannalta.

Regressioanalyysin tuloksia vertailemalla voidaan myös yrittää selittää tarinoiden tulosten eroja. Merkittävää näissä tuloksissa oli esimerkiksi muuttijien

selittävyysasteen erot tarinoiden välillä, tarinassa 1 selittävyysaste oli 40 %, kun taas tarinassa 2 tuloksena selitysasteelle oli 0 %. Selittävyysasteen ero on tarinoiden välillä suuri, joten tietoturvakäyttäytymisen konteksia voidaan pitää UMISPC-malliin vaikuttavana tekijänä. Tarinassa 2 kaikki summamuuttujat kuitenkin olivat regressioanalyysin perusteella tilastollisesti merkitseviä, samoin kuin tarinassa 1, joten tuloksia saatiin, mutta erot konteksteissa on saattanut vaikuttaa niin paljon, että aikomusta ei voitu selittää summamuuttujilla UMISPC-mallin mukaisesti.

Näin merkittävät erot käyttäjien vastauksissa tarinoiden välillä älypuhelimen vaarantumiselle, hidastumiselle ja käyttökelvottomaksi muuttumiselle voidaan näin ollen väittää olevan riippuvaisia tarkasteltavasta tietoturvaominaisuudesta. Riskien ja mahdollisten haittojen tunteminen ei kuitenkaan takaa tietoturvan kannalta turvallisesti toimimista, sillä on mahdollista että käyttäjä ottaa tietoisen riskin ja rikkoo tarkoituksellisesti hyvää tietoturvakäytäntöä (Ngoqo & Flowerday, 2015). Eri tietoturvaominaisuudet myös suojaavat käyttäjiä erilaisilta uhkilta, esimerkiksi näyttölukon käyttö suojaa käyttäjän laitetta pääosin fyysisen varkauden aiheuttamilta haitoilta (Oh et al., 2012), jolloin koettu uhka voidaan tuntea merkittömänä jos varkautta ei pidetä todennäköisenä. Koetun uhkan onkin oltava käyttäjän mielestä tarpeeksi merkittävä, jolloin uhkan aiheuttama pelko saattaa vaikuttaa käyttäjän toimintaan – jos uhkaa ja pelkoa ei tunneta, ei käyttäjä todennäköisesti aio toimia uhkaa ehkäisevällä tavalla (Moody et al., 2018).

UMISPC-mallin ollessa vielä tuore, tulee sen soveltuvuutta tietoturva-aikomuksen tutkimuksessa testata jatkossakin. Mahdollisia konteksteja joihin mallin soveltuvuutta voidaan testata on lukemattomat määrät. Tämä tutkimus raapaisi vain pintaa mallin toiminnasta henkilökohtaisen älypuhelimenkäytön näkökulmasta, mutta joitain mielenkiintoisia tuloksia oli kuitenkin havaittavissa. Jatkotutkimuksissa voitaisiin esimerkiksi tutkia tietoturva-aikomuksen tahallisuuden luonnetta tarkemmin; sekä UMISPC että tämä tutkimus tarkastelivat vain tapahtunutta tietoturvarikettä ja siitä odotettua hyötyä, mutta odotettu hyöty voi olla myös pahantahtoinen ja tarkoituksellisesti tietoturvaa rapauttava. Vastaavasti mallia voitaisiin testata mobiililaitteilla, eli älypuhelimilla ja tableteilla organisatorisessa kontekstissa, jolloin tulokset saattavat hyvinkin olla erilaiset.

LÄHTEET

Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior* Springer.

Ajzen, I. (1991). *The theory of planned behavior.* Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Ajzen, I. (2002). *Residual effects of past on later behavior: Habituation and reasoned action perspectives.* Personality and Social Psychology Review, 6(2), 107-122.

Andriotis, P., Tryfonas, T., Oikonomou, G., & Yildiz, C. (2013). (2013). *A pilot study on the security of pattern screen-lock methods and soft side channel attacks.* Paper presented at the Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, 1-6.

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). *Smudge attacks on smartphone touch screens.* WOOT, 10, 1-7.

Bagozzi, R. P. (1992). *The self-regulation of attitudes, intentions, and behavior.* Social Psychology Quarterly, 178-204.

Bamberg, S., & Schmidt, P. (2003). I*ncentives, morality, or habit? predicting students' car use for university routes with the models of Ajzen, Schwartz, and Triandis.* Environment and Behavior, 35(2), 264-285.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). (2011). *Mobile security catching up? revealing the nuts and bolts of the security of mobile devices.* Paper presented at the Security and Privacy (SP), 2011 IEEE Symposium On, 96-111.

Becker, G. S. (1968). *Crime and punishment: An economic approach. The economic dimensions of crime* (pp. 13-68) Springer.

Becker, M. H. (1974). *The health belief model and sick role behavior.* Health Education Monographs, 2(4), 409-419.

BusinessDictionary.com. (2015). *What is information security? Definition and meaning. BusinessDictionary.com.* Noudettu 12.12.2015 osoitteesta http://www.businessdictionary.com/definition/information-security.html

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). *Measuring user confidence in smartphone security and privacy.* Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security, 1.

Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., & Wagner, D. (2014). (2014). *Are you ready to lock?* Paper presented at the Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 750-761.

Fishbein, M., & Ajzen, I. (1977). *Belief, attitude, intention, and behavior: An introduction to theory and research.*

Gagnon, M., Godin, G., Gagné, C., Fortin, J., Lamothe, L., Reinharz, D., & Cloutier, A. (2003). *An adaptation of the theory of interpersonal behaviour to the study of telemedicine adoption by physicians.* International Journal of Medical Informatics, 71(2), 103-115.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence.* Elsevier: New York.

Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A., & Smith, M. (2014). (2014). *It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception.* Paper presented at the Symposium on Usable Privacy and Security (SOUPS), 213-230.

Harris, M. A., Furnell, S., & Patten, K. (2014). *Comparing the mobile device security behavior of college students and information technology professionals.* Journal of Information Privacy and Security, 10(4), 186-202.

He, D., Chan, S., & Guizani, M. (2015). *Mobile application security: Malware threats and defenses.* Wireless Communications, IEEE, 22(1), 138-144.

Hoerger, M. (2010). *Participant dropout as a function of survey length in internet-mediated university studies: Implications for study design and voluntary participation in psychological research.* Cyberpsychology, Behavior, and Social Networking, 13(6), 697-700.

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.

Kaplan, A. M. (2012). *If you love something, let it go mobile: Mobile marketing and mobile social media 4x4.* Business Horizons, 55(2), 129-139.

Karlson, A. K., Brush, A., & Schechter, S. (2009). *Can I borrow your phone?: Understanding concerns when sharing mobile phones.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1647-1650.

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). *Survey on mobile user's data privacy threats and defense mechanisms.* Procedia Computer Science, 56, 376-383.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). *A survey on security for mobile devices.* Communications Surveys & Tutorials, IEEE, 15(1), 446-471.

Leavitt, N. (2011). *Mobile security: Finally a serious problem?* Computer, 44(6), 11-14.

Li, Q., & Clark, G. (2013). *Mobile security: A look ahead.* Security & Privacy, IEEE, 11(1), 78-81.

Limayem, M., & Hirt, S. G. (2003). *Force of habit and information systems usage: Theory and initial validation.* Journal of the Association for Information Systems, 4(1), 3.

Liu, B., Lin, J., & Sadeh, N. (2014). *Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?* Paper presented at the Proceedings of the 23rd International Conference on World Wide Web, 201-212.

Maddux, J. E., & Rogers, R. W. (1983). *Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change.* Journal of Experimental Social Psychology, 19(5), 469-479.

McCracken, L. M., Zayfert, C., & Gross, R. T. (1992). *The pain anxiety symptoms scale: Development and validation of a scale to measure fear of pain.* Pain, 50(1), 67-73.

Metsämuuronen, J. (2011). *Tutkimuksen tekemisen perusteet ihmistieteissä.* Helsinki: International Methelp Oy.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). *Toward a Unified Model of Information Security Policy Compliance.* MIS Quarterly, 42(1)

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). *Delegate the smartphone user? security awareness in smartphone platforms.* Computers & Security, 34, 47-66.

Ngoqo, B., & Flowerday, S. V. (2015). *Information security behaviour profiling framework (ISBPF) for student mobile phone users.* Computers & Security, 53, 132-142.

Oh, T., Stackpole, B., Cummins, E., Gonzalez, C., Ramachandran, R., & Lim, S. (2012). *Best security practices for android, blackberry, and iOS.* Paper presented at the Enabling Technologies for Smartphone and Internet of Things (ETSIoT), 2012 First IEEE Workshop On, 42-47.

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., & Troutman, J. A. (1994). *The pain anxiety symptoms scale: Psychometric properties in a community sample.* Journal of Behavioral Medicine, 17(5), 511-522.

Oxforddictionaries.com. (2016). *Definition of smartphone.* Oxforddictionaries.com. Noudettu 1.3.2016, osoitteesta http://www.oxforddictionaries.com/definition/english/smartphone

Paternoster, R., & Simpson, S. (1996). *Sanction threats and appeals to morality: Testing a rational choice model of corporate crime.* Law and Society Review, 549-583.

Penning, N., Hoffman, M., Nikolai, J., & Wang, Y. (2014). *Mobile malware security challeges and cloud-based detection.* Paper presented at the Collaboration Technologies and Systems (CTS), 2014 International Conference On, 181-188.

Piquero, N. L., & Piquero, A. R. (2006). *Control balance and exploitative corporate crime.* Criminology, 44(2), 397-430.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). *Common method biases in behavioral research: A critical review of the literature and recommended remedies.* Journal of applied psychology, 88(5), 879.

Pogarsky, G. (2004). *Projected offending and contemporaneous rule-violation: Implications for heterotypic continuity.* Criminology, 42(1), 111-136.

Rogers, R. W. (1975). *A protection motivation theory of fear appeals and attitude change.* The Journal of Psychology, 91(1), 93-114.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., & Dolev, S. (2009). *Google android: A state-of-the-art review of security mechanisms.* arXiv Preprint arXiv:0912.5101

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). *Google android: A comprehensive security assessment.* IEEE Security & Privacy, (2), 35-44.

Siponen, M., & Vance, A. (2010). *Neutralization: New insights into the problem of employee information systems security policy violations.* MIS Quarterly, 487-502.

Siponen, M., & Vance, A. (2014). *Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations.* European Journal of Information Systems, 23(3), 289-305.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). *Analysis of end user security behaviors.* Computers & Security, 24(2), 124-133.

Sykes, G. M., & Matza, D. (1957). *Techniques of neutralization: A theory of delinquency.* American Sociological Review, 22(6), 664-670.

Symantec. (2015). *2015 Internet Security Threat Report, Volume 20*. Noudettu 2.3.2016 osoitteesta http://www.symantec.com/security_response/publications/threatreport.jsp

Tilastokeskus (2014). *Väestön tieto- ja viestintätekniikan käyttö 2014*. Noudettu 10.7.2018 osoitteesta https://www.stat.fi/til/sutivi/2014/sutivi_2014_2014-11-06_kat_001_fi.html

Tilastokeskus (2018a). *Internetin käyttö mobiililaitteilla.* Noudettu 10.7.2018 osoitteesta https://www.stat.fi/til/sutivi/2017/13/sutivi_2017_13_2017-11-22_kat_002_fi.html

Tilastokeskus (2018b). *Väestö.* Noudettu 9.7.2018 osoitteesta https://www.tilastokeskus.fi/tup/suoluk/suoluk_vaesto.html

Tittle, C. R. (Ed.). (1995). *Control balance: Toward a general theory of deviance.* USA: Westview Press.

Triandis, H. (Ed.). (1977). *Interpersonal behavior.* USA: Brooks/Cole Publishing Company.

Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C. R., & D'Arcy, J. (2013). (2013). *Modifying smartphone user locking behavior.* Paper presented at the Proceedings of the Ninth Symposium on Usable Privacy and Security, 10.

Vance, A., Siponen, M., & Pahnila, S. (2012). *Motivating IS security compliance: Insights from habit and protection motivation theory.* Information & Management, 49(3), 190-198.

Vassekov, A., Hämmäinen, H. (2015). *Mobile Handset Population in Finland 2005-2014,* Aalto University School of Electrical Engineering.

Verplanken, B. (2006). *Beyond frequency: Habit as mental construct.* British Journal of Social Psychology, 45(3), 639-656.

Verplanken, B., & Orbell, S. (2003). *Reflections on past behavior: A Self-Report index of habit strength.* Journal of Applied Social Psychology, 33(6), 1313-1330.

Wang, Y., Streff, K., & Raman, S. (2012). *Smartphone security challenges.* Computer, 45(12), 0052-58.

Witte, K. (1992). *Putting the fear back into fear appeals: The extended parallel process model.* Communications Monographs, 59(4), 329-349.

Wu, L., Grace, M., Zhou, Y., Wu, C., & Jiang, X. (2013). *The impact of vendor customizations on android security.* Paper presented at the Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, 623-634.

Zhou, Y., & Jiang, X. (2012).. *Dissecting android malware: Characterization and evolution.* Paper presented at the Security and Privacy (SP), 2012 IEEE Symposium On, 95-109.

Zirjawi, N., Kurtanovic, Z., & Maalej, W. (2015). *A survey about user requirements for biometric authentication on smartphones.* Paper presented at the Evolving Security and Privacy Requirements Engineering (ESPRE), 2015 IEEE 2nd Workshop On, 1-6.

LIITE 1. KYSELYLOMAKE

1. Ikäsi vuosina *

Esim. 51, 19, ##	

2. Sukupuoli *

- ◯ Nainen
- ◯ Mies
- ◯ Muu

Lue lyhyt tarina Jokisen älypuhelimen käytöstä, ja vastaa tarinan perusteella esitettyihin kysymyksiin. Molemmissa tarinoissa Jokinen on sama henkilö. Tarinoita on kaksi, A) ja B), ja molempiin tarinoihin on samat kysymykset.

Jokinen on ahkera älypuhelimen käyttäjä ja hän *haluaa pitää laitteensa tietoturvan kunnossa*. Hän käyttää älypuhelintaan useita tunteja päivässä, ja käyttää sillä erityisesti sosiaalista mediaa sekä pikaviestisovelluksia. Jokinen käyttää puhelintaan myös valokuvaamiseen, sähköpostiin, pelien pelaamiseen, ja joskus myös kävely- ja juoksulenkkiensä matkan ja keston seuraamiseen GPS-paikannuksen avulla.

Tarina A)

Jokinen suuntaa kesälomallaan toiselle puolelle maata, ja matkustaa kohteeseensa junalla. Matka kestää useita tunteja, jonka aikana Jokinen käyttää puhelintaan aktiivisesti lähes koko matkan ajan. Jonkin ajan kuluttua matkan alkamisesta Jokista alkaa ärsyttää toistuva näyttölukon avaaminen ja hän päättää *poistaa puhelimen näyttölukon kokonaan käytöstä* säästääkseen aikaa ja hermojaan. Jokinen tietää, että kuka tahansa voi käyttää puhelinta ja selata sen sisältämiä tietoja näyttölukon ollessa kokonaan pois käytöstä.

3. Mielestäni yllä kuvattu tarina A) on realistinen *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

4. Tuntisin syyllisyyttä, jos tekisin niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

5. Jokinen toimi henkilökohtaisten periaatteideni mukaan johdonmukaisesti *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

6. On hyväksyttävää toimia niin kuin Jokinen toimi tarinassa *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

7. Mitä Jokinen teki sopi hänen tapaansa käyttää älypuhelintaan *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

8. Mitä Jokinen teki oli oikeutettua tarinan käyttötilanteen perusteella *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

9. Mitä Jokinen teki oli fiksua *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

10. Mitä Jokinen teki oli miellyttävää *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

11. Kuinka moraalisesti oikein olisi toimia samoin kuin Jokinen toimi tilanteessa? *

	1	2	3	4	5	6	7	
Täysin väärin	◯	◯	◯	◯	◯	◯	◯	Täysin oikein

12. Koetko, että pystyisit *olemaan toimimatta* samoin kuin Jokinen kuvatussa tilanteessa? *

	1	2	3	4	5	6	7	
En pystyisi lainkaan	◯	◯	◯	◯	◯	◯	◯	Pystyisin täysin

13. Älypuhelimeni saattaa muuttua käyttökelvottomaksi, jos teen niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

14. Alypuhelimeni saattaa vaarantua, jos teen niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

15. Alypuhelimeni saattaa hidastua, jos teen niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

16. Miten todennäköistä on, että itse toimisit kuvatussa tilanteessa samoin kuin Jokinen *

	1	2	3	4	5	6	7	
Hyvin epätodennäköistä	◯	◯	◯	◯	◯	◯	◯	Hyvin todennäköistä

17. Toimisin samalla tavalla kuin Jokinen, jos olisin samassa tilanteessa*

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

Lue lyhyt tarina Jokisen älypuhelimen käytöstä, ja vastaa tarinan perusteella esitettyihin kysymyksiin. Molemmissa tarinoissa Jokinen on sama henkilö. Tarinoita on kaksi, A) ja B), ja molempiin tarinoihin on samat kysymykset.

Jokinen on ahkera älypuhelimen käyttäjä ja hän *haluaa pitää laitteensa tietoturvan kunnossa*. Hän käyttää älypuhelintaan useita tunteja päivässä, ja käyttää sillä erityisesti sosiaalista mediaa sekä pikaviestisovelluksia. Jokinen käyttää puhelintaan myös valokuvaamiseen, sähköpostiin, pelien pelaamiseen, ja joskus myös kävely- ja juoksulenkkiensä matkan ja keston seuraamiseen GPS-paikannuksen avulla.

Tarina B)

Jokinen käyttää puhelimessaan kuvankäsittelysovellusta, joka jostain syystä ei enää suostu käynnistymään sovellukseen tulleen uusimman päivityksen jälkeen. Jokinen olisi halunnut lähettää ystävälleen hauskan muokatun valokuvan onnitellakseen tätä tämän syntymäpäivänä. Jokinen etsii korvaavaa sovellusta kuvien muokkaamiseksi, mutta ei sellaista puhelimensa sovelluskaupasta löydä. Jokinen jatkaa ohjelman etsintää netistä, ja löytää tätä kautta ilmaisen korvaavaan kuvankäsittelyohjelman. Sovelluksen nettisivu vaikuttaa tarpeeksi luotettavalta, ja Jokinen asentaa puhelimeensa netistä lataamansa sovelluksen. Jokinen tietää, että virallisen sovelluskaupan ulkopuolelta ladatut sovellukset saattavat olla haitallisia ja aiheuttaa ongelmia.

18. Mielestäni yllä kuvattu tarina B) on realistinen *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

19. Tuntisin syyllisyyttä, jos tekisin niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

20. Jokinen toimi henkilökohtaisten periaatteideni mukaan johdonmukaisesti *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

21. On hyväksyttävää toimia niin kuin Jokinen toimi tarinassa *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

22. Mitä Jokinen teki sopi hänen tapaansa käyttää älypuhelintaan *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

23. Mitä Jokinen teki oli oikeutettua tarinan käyttötilanteen perusteella *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

24. Mitä Jokinen teki oli fiksua *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

25. Mitä Jokinen teki oli miellyttävää *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

26. Kuinka moraalisesti oikein olisi toimia samoin kuin Jokinen toimi tilanteessa? *

	1	2	3	4	5	6	7	
Täysin väärin	◯	◯	◯	◯	◯	◯	◯	Täysin oikein

27. Koetko, että pystyisit *olemaan toimimatta* samoin kuin Jokinen kuvatussa tilanteessa? *

	1	2	3	4	5	6	7	
En pystyisi lainkaan	◯	◯	◯	◯	◯	◯	◯	Pystyisin täysin

28. Älypuhelimeni saattaa muuttua käyttökelvottomaksi, jos teen niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

29. Alypuhelimeni saattaa vaarantua, jos teen niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

30. Alypuhelimeni saattaa hidastua, jos teen niin kuin Jokinen teki *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

31. Miten todennäköistä on, että itse toimisit kuvatussa tilanteessa samoin kuin Jokinen *

	1	2	3	4	5	6	7	
Hyvin epätodennäköistä	◯	◯	◯	◯	◯	◯	◯	Hyvin todennäköistä

32. Toimisin samalla tavalla kuin Jokinen, jos olisin samassa tilanteessa*

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

Tämän sivun kysymykset koskevat Sinun henkilökohtaista älypuhelimen käyttöäsi ja tapaasi käyttää sen tietoturvaa parantavia ominaisuuksia.

Kysymykset koskevat yleisesti kaikkia ominaisuuksia, jotka jollain tavalla parantavat älypuhelinten tietoturvaa ja auttavat pitämään laitteesi tietoturvan kunnossa. Kyseisiä tietoturvaa parantavia ominaisuuksia ovat esimerkiksi tiedostojen salaus, varmuuskopiointi ja näyttölukon käyttö (koodi, piirtokuvio, sormenjälki jne.). Tietoturvaa parantava ominaisuus voi olla myös jokin muu ominaisuus, jota käytät tietoisesti laitteesi tietoturvan parantamiseksi.

33. Alypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä teen usein *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

34. Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä teen automaattisesti *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

35. Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä minun ei tarvitse tietoisesti erikseen muistaa*

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

36. Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä teen ajattelematta *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

37. Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mikä kuuluu rutiiniini (päivittäin, viikoittain, kuukausittain) *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

38. Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä aloitan tekemään ennen kuin edes huomaan tekeväni niin*

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

39. Alypuhelimen tietoturvaominaisuuksien käyttö on minulle tyypillistä *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

40. Älypuhelimen tietoturvaominaisuuksien käyttö on jotain, mitä olen tehnyt jo pitkään *

	1	2	3	4	5	6	7	
Täysin eri mieltä	◯	◯	◯	◯	◯	◯	◯	Täysin samaa mieltä

41. Haluatko osallistua leffalippujen arvontaan? *

Sähköpostiosoitekenttä arvontaa varten tulee näkyviin, kun valitset "Kyllä". Jos et halua osallistua lippujen arvontaan, valitse "En".

◯ Kyllä

◯ En