Anna Nemtsinkoff-Rajala

KRIITTISTEN KÄYTTÖKOKEMUSTEN VAIKUTUS F-SECUREN FREEDOME-MOBIILISOVELLUKSEN OMAKSUMISEEN JA JATKUVAAN KÄYTTÖÖN

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Nemtsinkoff-Rajala, Anna
Kriittisten käyttökokemusten vaikutus F-Securen Freedome-mobiilisovelluksen omaksumiseen ja jatkuvaan käyttöön
Jyväskylä: Jyväskylän yliopisto, 2015, 64 s.
Tietojärjestelmätiede, pro gradu –tutkielma
Ohjaaja: Frank, Lauri

Tässä tutkimuksessa pyritään selvittämään miten kriittiset käyttökokemukset vaikuttavat F-Securen Freedome-mobiilisovelluksen omaksumiseen ja jatkuvaan käyttöön. Tutkimus jakautuu kahteen osaan: kirjallisuuskatsaukseen ja empiriaan. Aluksi käydään läpi mitä mobiililaitteiden kyberturvallisuus on sekä mitkä kyberuhkat uhkaavat mobiililaitteita ja miten uhkia voidaan hallita. Kirjallisuuskatsauksen loppuosassa käydään läpi aihepiirin aikaisempia tutkimuksia ja käsitellään teknologian omaksumista selittäviä teorioita. Empiriaosuus sisältää tutkimuksen taustat ja tutkimuksen kulun sekä käy läpi tutkimustulokset ja niiden analysoinnin. Empiirinen tutkimusaineisto kerättiin puolistrukturoidulla puhelinhaastattelulla. Tutkimusaineiston keräämisessä ja analysoinnissa käytettiin viitekehyksenä Rogersin innovaation diffuusioteoriaa ja kriittisten käyttökokemusten tutkimiseen kehitettyä CIT-menetelmää. Tutkimustuloksissa nousi esiin, että positiivisina koetut käyttökokemukset vaikuttavat eniten omaksumispäätöksiin. Negatiivisesti omaksumispäätöksiin vaikutti hinta ja sovelluksesta saadun näkyvän hyödyn puute.

Asiasanat: Kyberturvallisuus, tietoturva, mobiililaitteet, mobiilisovellukset, käyttöönotto, omaksuminen

ABSTRACT

Nemtsinkoff-Rajala, Anna
Research of how critical user experiences affect to adapting and usage of F-Secure Freedome mobile application
Jyväskylä: University of Jyväskylä, 2015, 64 p.
Information Systems, Master's Thesis
Supervisor: Frank, Lauri

The purpose of this thesis is to examine how critical user experiences affect to adapting and usage of F-Secure Freedome mobile application. This thesis has two parts: the literature review and the empirical study. The literature review contains information about what are mobile cyber security and its current state, what cyber threats mobile devices have and how you can manage them. The literature review contains also information about the earlier researches of the mobile cyber security and introduces the diffusion of innovations theory what was used as the frame of reference in the empirical study. The empirical part contains research backgrounds, -progress, -results and -analysis. The research data were collected by using half-structured theme interview used together with the critical incident technique. The empirical study showed that positive user experiences affect the most of adopting decisions. Price and the lack of the visible benefits of the application affected negatively in adopting decisions.

Keywords: cyber security, mobile devices, mobile applications, implementation, acceptance

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Nykyään yli 65 prosenttia suomalaisista omistaa älypuhelimen, 31 prosenttia tabletin ja yli puolet suomalaista käyttää internetiä liikkeellä ollessaan. Suomalaisista 63 prosenttia käyttää matkapuhelimen internetyhteyttä säännöllisesti. (TNS Gallup Digital, 2014) Älypuhelimia käytetään henkilökohtaisiin asioihin sekä työasioihin ja niihin tallennetaan tärkeitä salasanoja sekä tietoja, joiden vuotaminen vääriin käsiin voisi aiheuttaa harmia monilla tavoin. Internetin käyttö älypuhelimissa tuo valtavasti hyötyä, mutta sen kääntöpuolena on kasvava riski altistua tietoturvarikollisuudelle.

On erittäin tärkeää ymmärtää käyttäjien asenteita mobiililaitteiden tietoturvaa ja yksityisyyttä kohtaan, jotta voidaan rakentaa tehokasta ja turvallista mobiiliekosysteemiä. Tässä pro gradussa tutkittavana kohteena on mobiililaitteiden kyberturvallisuus, sekä tieto- ja yksityisyydenhallintaan kehitetty F-Securen Freedome-mobiilisovellus.

Kyber tarkoittaa tässä tutkimuksessa sähköisessä muodossa olevan informaation käsittelyä. Kyberturvallisuus on tila, jossa digitaalisesta ympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallittuja. Kyberturvallisuuden hallinnalla pyritään hallitsemaan ja ennakoimaan erilaisia tietoturvaa uhkaavia toimia ja tapahtumia. (Sanastokeskus TSK ry, 2014) Kyberturvallisuuden merkitys korostui voimakkaasti kesällä ja syksyllä 2013, kun NSA:n entinen työntekijä Edvard Snowden luovutti The Guardian ja The Washington Post –lehdille tietoa, jossa kerrottiin Yhdysvaltojen turvallisuuspalvelun harjoittavan internetin käyttäjien salakuuntelua ja henkilökohtaisten tietojen keräämistä.

Mobiililaitteet ovat mukana kuljetettaviksi tarkoitettuja laitteita, joihin voidaan asentaa sovelluksia tai joissa on internetselain. (JUHTA – Julkisen hallinnon tietohallinnon neuvottelukunta, 2014) Tyypillisesti mobiililaitteiksi voidaan luokitella älypuhelimet, tabletit, niiden välille asettuvat taskukokoiset älylaitteet sekä e-lukulaitteet. Mobiililaitteiden kyberturvallisuus tarkoittaa mukana kuljetettavaksi suunniteltujen laitteisiin tallennettuja tietoja uhkaavien tekijöiden ja riskien hallintaa. Kun henkilökohtainen mobiililaite yhdistetään internetiin, siitä tulee haavoittuvampi ja tietojen suojaamisen merkitys korostuu.

Tämän tutkimuksen teoriaosuudessa käsitellään mobiililaitteiden kyberturvallisuutta ja miten sitä voidaan hallita sekä esitellään empiirisen tutkimuksen perustana käytetty teoreettinen viitekehys. Empiirinen osuus pyrkii selittämään miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön sekä mahdolliseen käytön lopettamiseen.

Tutkimusongelma:

- Miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön?

Tutkimusongelmaa tukevat tutkimuskysymykset:

- Mitä on mobiililaitteiden kyberturvallisuus ja miten sitä voidaan hallita?
- Minkälaisia kriittisiä käyttökokemuksia esiintyy Freedomen käytössä ja miten ne vaikuttavat sovelluksen omaksumiseen ja jatkuvaan käyttöön?

Empiirisen tutkimuksen tutkimusmenetelmäksi valittiin tapaustutkimus, koska haluttiin saada tietoa ainoastaan Freedomesta. Tutkimuksella ei pyritty tarkoituksella saamaan tietoa, joka olisi yleistettävissä kaikkiin tieto- ja yksityisyydensuojapalveluihin. Tiedonkeruun ja -analysoinnin tukena käytettiin The Critical Incident Technique-menetelmää (myöhemmin. CIT-menetelmä), joka on kehitetty nimenomaan kriittisten kokemusten havainnoimiseen. Tiedonkeruu toteutettiin haastattelemalla puhelimitse Freedomen käyttäjiä.

2 MOBIILILAITTEIDEN KYBERTURVALLISUUS

Jotta voidaan ymmärtää mitä kyberturvallisuus tarkoittaa, selvitetään ensin mitä on turvallisuus ja mitä kyber-käsite tarkoittaa. Kyberturvallisuuden määritelmän jälkeen käydään läpi mitä ovat mobiililaitteet. Seuraavissa alaluvuissa käsitellään tarkemmin mobiililaitteiden kyberturvallisuuden nykytila, millaisia kyberuhkia mobiililaitteissa esiintyy ja miten niitä voidaan hallita sekä esitellään tarkemmin Freedome ja käydään läpi aiempia mobiililaitteiden tieto- ja yksityisyydensuojasovelluksia käsitelleitä tutkimuksia.

Limnellin, Majewskin ja Salmisen (2014) mukaan yhdeksi ihmisen perustarpeista voidaan määritellä turvallisuus. Turvallisuuskäsitys on muuttunut maailman muuttuessa ja esimerkiksi viime vuosisadan alussa ihmisen turvallisuustarpeet olivat aivan erilaisia kuin nykypäivänä. Limnell ym. (2014) kirjoittavat, että muuttuvan maailman mukana turvallisuus on saanut uusia ulottuvuuksia ja on määritelty erilaisia turvallisuudenaloja kuten elintarviketurvallisuus, ympäristöturvallisuus, energiaturvallisuus ja kyberturvallisuus. On kuitenkin tärkeää muistaa, että täydellistä turvallisuutta ei ole, eikä sen saavuttaminen ole edes mahdollista.

Limnell ym. (2014) luokittelevat olevan kaksi eri maailmaa, joista toinen on fyysinen maailma, eli atomien maailma. Fyysinen maailma on kaikkea konkreettista ja silmin havaittavaa. Fyysisen maailman lisäksi on olemassa ihmisen luoma keinotekoinen maailma, eli digitaalinen maailma, johon kuuluu internet, erilaiset tietoverkot ja -järjestelmät sekä esimerkiksi älypuhelimen ohjelmistot. Limnell ym. (2014) määrittelevät kyber-etuliitteen tarkoittavan digitaalisen maailman ilmiöitä, tapahtumia, toimijoita, toimintoja, toimintatapoja ja normeja. Kyber-etuliitettä vodaan käyttää hyvin monessa eri yhteydessä, esimerkiksi kyberuhka, kybertoimintaympäristö ja kybersota. Kyber-etuliitteelliset sanat saavat vielä nykyään osakseen paljon ihmettelyä, eikä moni tekniikkaan perehtymätön ihminen osaa määritellä mitä tarkoitetaan, kun puhutaan esimerkiksi kyberturvallisuudesta.

Kyberturvallisuus on tietoturvallisuutta, verkkoturvallisuutta ja laiteturvallisuutta. Käsitteiden määrittelyssä on paljon päällekkäisyyksiä ja kyberkäsitteelle löytyy maailmalla satoja eri määritelmiä. Limnell ym. (2014) tiivistä-

vät, että kyberturvallisuus-käsite syntyi, kun tarvittiin käsite, joka kattoi sisäisen tiedon ohella sen liikkeen turvaamisen niin käyttäjän omissa järjestelmissä, kuin niiden ulkopuolella. Kyber kuvaa myös fyysisen ja digitaalisen rajapintaa, eli kyberfyysistä maailmaa, jossa elämme. Nykyään fyysisen ja digitaalisen maailman toiminnot voidaan nähdä hyvin pitkälle toisistaan riippuvaisina, jolloin kyberturvallisuuden merkitys korostuu entisestään. (Limnell ym., 2014 s. 30-34) Esimerkiksi nykyään hyvin monet älylaitteet helpottavat ihmisen arkea, mutta niiden kääntöpuolena tulee eteen yksityisyydensuojakysymykset kuten mihin vedetään raja mitkä kuluttajan tiedot ovat eettisesti hyväksyttäviä seurata ja tallentaa.

Mobiililaitteet ovat JUHTA - julkisen hallinnon tietohallinnon neuvottelukunnan (2014) mukaan mukana kuljetettaviksi suunniteltuja laitteita, joihin voidaan asentaa sovelluksia, tai joissa on käytössä internetselain. Mobiililaitteita ovat älypuhelimet, tabletit, näiden välille asettuvat taskukokoiset älylaitteet sekä e-kirjojenlukulaitteet, joille on tyypillistä pienempi näyttökoko ja kosketusnäyttö.

Mobiililaitteiden kyberturvallisuus on tila, jossa mobiililaitteeseen kohdistuvat uhkat ja riskit ovat hallittuja. Koska kyber kuvaa myös fyysisen ja digitaalisen maailman toimintoja, mobiililaitteiden kyberturvallisuus on myös osittain laiteturvallisuutta, eli laitteen suojaamista, jotta siihen tallennetut tiedot eivät pääse tuhoutumaan. Mobiililaitteiden kyberturvallisuus on mukana kuljetettavaksi suunniteltujen laitteiden tietojen turvaamista niin laitteessa itsessään, kuin verkossa.

2.1 Nykytila

Mobiililaitteiden kyberturvallisuuden nykytila on jatkuvasti muuttuva. Mobiililaitteita myydään huimaa tahtia, uusia sovelluksia kehitetään jatkuvasti ja näin ollen myös turvallisuuden tila muuttuu ja laajenee. Suomen Tilastokeskuksen (2014) mukaan Suomessa vuonna 2014 tabletti oli käytössä 32 prosentilla kotitalouksista, kun vuonna 2013 niitä oli vain 19 prosentilla. Älypuhelinten määrä on kasvanut Suomessa vuodesta 2013 vuoteen 2014 kymmenen prosenttiyksikköä 60 prosenttiin. Kannettavat tietokoneet ovat jo pitkään korvanneen pöytäkoneita ja 2014 pöytäkoneet harvenivat kahden prosenttiyksikön verran. Yllättävää tuloksissa kuitenkin oli, että kannettavien tietokoneiden yleistyminen pysähtyi. Kotitaloudet hankkivat kannettavien tietokoneiden sijasta tabletteja. (Tilastokeskus, 2014) Mobiililaitteiden määrän kasvu on merkittävää ja kasvuvauhti on niin huimaa, että käyttäjien on vaikea pysyä laitteiden kyberturvallisuuden mukana.

It-Viikko (2013) uutisoi virussuojan puuttuvan monista mobiililaitteista Kaspersky Labin teettämän tutkimuksen muukaan. Kaspersky Lab tutki 2400:n henkilön otoksella pohjoismaisten, hollantilaisten ja belgialaisten kuluttajien tietoturvakäytäntöjä. Suomalaisista 56 prosenttia oli ilmoittanut suojaavansa kaikki laitteensa salasanalla ja salaavansa henkilökohtaiset tiedot ja 48 prosent-

tia kertoi ottavansa varmuuskopiota tiedostoista. Suomalaishaastatelluista 86 prosenttia suojasi tietokoneensa virusskannerilla ja 63 prosenttia käytti tietokoneen suojaukseen myös salasanaa. Vaikka suomalaiset suojaavat tietokoneensa suhteellisen hyvin, niin tämän tutkimuksen mukaan 80 prosentissa mobiililaitteita ei ollut mitään virussuojaa. It-Viikon (2013) mukaan eniten haittaa aiheuttaisi suomalaisille pankkitietojen, salasanojen ja henkilökohtaisten sähköpostien vuotaminen kolmannelle osapuolelle. Kaspersky Labin tutkimuksen valossa voidaan todeta, että mobiililaitteiden tietosuoja nykytila on Suomessa hyvin heikko.

Yksi mobiililaitteiden kyberturvallisuuden suuri ja kasvava osa-alue on Bring Your Own Device -malli (myöh. BYOD). Gilbert (2012) määrittelee, että BYOD tarkoittaa työntekijöiden henkilökohtaisten mobiililaitteiden tuomista työpaikalle, sekä niiden käyttämistä työasioissa työpaikalla tai kotona. Työntekijät käyttävät esimerkiksi yrityksen sähköpostia, tiedostopalvelimia ja tietokantoja omilla henkilökohtaisilla laitteilla. Kun oma laite yhdistetään langattomasti tai langallisesti organisaation tietoverkkoon, siitä voi siirtyä haittaohjelma organisaation laitteisiin verkon yli. (Miller, Voas & Hurlburt, 2012) Haittaohjelmat, jotka varastavat henkilökohtaisia tietoja, aiheuttavat taloudellisia vahinkoja esimerkiksi maksullisilla tekstiviesteillä tai tekevät palvelunestohyökkäyksiä, eli estävät esimerkiksi jonkin tietyn verkkosivun tarkoituksenmukaisen käytön. Haittaohjelmat eivät ole aivan tavattomia, sillä heinäkuussa 2012 Androidille haittaohjelmia oli n. 45 000 ja tammikuussa 2014 niitä oli havaittu jo n. 650 000. (Chang, Ho & Chang, 2014)

F-Securen (2015b) tekemän tutkimuksen mukaan sadasta suosituimmasta linkistä, vain 15 prosenttia oli kuluttajien käyttämiä ja loput 85 prosenttia oli kolmannen osapuolen nettisivustoja, joita käytetään sivuilla vierailleiden seurantaan. Yli puolet kolmannen osapuolen sivustoista ovat pelkästään käyttäjien seurantaan ja profilointiin tarkoitettuja. Rikolliset eivät siis ole ainoita, joita kiinnostaa kuluttajien verkkoselaaminen, niistä on kiinnostunut hyvin moni muukin taho. (F-Secure, 2015b) Tämä tarkoittaa muun muassa kohdennettua mainontaa ja käyttäjien profilointia.

Yhteenvetona voidaan todeta, että tutkimusten mukaan mobiililaitteiden tietojen suojaaminen viruksentorjunnalla on heikkoa, mutta toisaalta yli puolet ilmoittivat suojaavansa kaikki laitteensa salasanalla. Mobiililaitteiden kyberturvallisuuden tila nykypäivänä kuitenkin on alati muuttuva ja henkilökohtaisia laitteita liitetään myös yritysten tietoverkkoihin (BYOD), jolloin myös henkilökohtaisten laitteiden tulisi olla yhtä hyvin tietosuojattuja kuin yrityksen laitteidenkin. Kuitenkaan suurinta osaa mobiililaitteista ei ole suojattu virustorjunnalla ollenkaan.

2.2 Mobiililaitteiden kyberuhkat

Mobiililaitteita uhkaavat samat kyberuhkat kuin tietokoneitakin. Mobiililaitteiden määrän kasvaessa räjähdysmäisesti, myös uhkien määrä kasvaa samaa tah-

tia. Kyberuhkat ovat muun muassa haittaohjelmia ja sovelluksia, jotka käyttävät laitteen käyttäjän tietoja väärin, tai lähettävät niitä kolmannelle osapuolelle. Uhkiksi voidaan luokitella myös laitteeseen fyysisesti kohdistuvat uhkat ja käyttäjän huolimattomuudesta johtuneet uhkat, kuten laitteen katoaminen.

F-Secure (2015c) luokittelee tietoturvauhkat seuraavanlaisesti (taulukko 1):

TAULUKKO 1 Tietoturvauhkat (F-Secure, 2015c)

Haittaohjelmat	- virukset - madot - rootkit-ohjelmat - piilohallintaohjelmat - takaportit - troijalaiset - pelotteluohjelmat (engl. rogue) - haavoittuvuutta hyväksikäyttävät ohjelmat (engl. exploit) - pakatut ohjelmat ja apuohjelmat joita käytetään rakentamaan haittaohjelmia (engl. constructor)
Vakoiluohjelmat	- vakoilemiseen käytetyt ohjelmat - seurantaan käytetyt ohjelmat - mainosohjelmat
Riskiohjelmat	- seurantatyökalut, jotka kirjaavat ylös laitteen käyttöä - ns. hack-tools, jotka mahdollistavat käyttäjälle normaalia enemmän oikeuksia laitteeseen - sovellukset jotka väärinkäytettynä voivat aiheuttaa turvallisuusriskin
Ei-toivotut sovellukset	- sovellukset tai sen osat, jotka ovat tungettelevia tai voi aiheuttaa yksityisyydensuoja- ja tietoturvallisuusriskejä

2.3 Mobiililaitteiden turvallisuuden hallinta

Kyberturvallisuuden hallinta mobiililaitteissa on yhtä tärkeää kuin tietokoneessakin. On olemassa erilaisia työkaluja, joiden avulla voidaan huolehtia tieto- ja yksityisyydensuojasta. Myös käyttäjän omalla käytöksellä voidaan estää monia turvallisuusriskejä toteutumasta.

2.3.1 Mobiililaitteen turvallinen käyttö

Käyttäjä voi vaikuttaa paljon omalla toiminnallaan mobiililaitteensa tietojen turvaamiseen. Viestintävirasto (2014) kehottaa ensimmäisenä ottamaan käyttöön automaattisen käyttöliittymänlukituksen, eli niin sanotun näytönlukituksen. Laitteen merkistä ja mallista riippuen näytönlukituksen suojakoodi voi olla numerosarja, piirrettävä kuvio tai kirjoitettava salasana, jonka valinnassa kannattaa käyttää mielikuvitusta, jotta se olisi mahdollisimman suojaava. Kun lukitusta avaa, tulee olla tarkka kuka avauskoodin näkee.

Tietoturvapäivitysten asentaminen sekä sovellusten- ja käyttöjärjestelmän päivittäminen on tärkeää, jotta ne ovat ajantasaisia. (Viestintävirasto, 2014) Kuten aiemmin on jo mainittu, uusia uhkia kehitetään ja havaitaan jatkuvasti, joten on tärkeää, että myös laite on päivitetty torjumaan niitä. Sovellusten lataaminen vain luotettavista lähteistä auttaa turvallisten sovellusten etsimisessä, mutta se ei kuitenkaan ole tae, ettei sieltä löydy myös haitallisia sovelluksia. Viestintävirasto (2012) muistuttaa, että erityisen tarkka kannattaa olla räätälöityjen ohjelmien ja käyttöjärjestelmien (engl. firmware) sekä lisäturvallisuutta lupaavien sovellusten kanssa, koska ne eivät välttämättä ole sitä mitä lupaavat.

Mobiililaitteisiin tallentuu lukuisia tietoja ja oletusyhteyksiä, jolloin laitteenvaihdon yhteydessä voi tulla ongelmia vanhalle omistajalle, jos uusi omistaja päättääkin käyttää näitä tietoja väärin. Esimerkiksi pilvipalveluista on suuri hyöty mobiililaitteen käyttäjälle, mutta niidenkin käytössä tulee olla tarkka, jotta kirjautumistiedot eivät jää avoimeksi minnekään toiseen laitteeseen, jossa palvelua on käyttänyt. Viestintävirasto (2014) ohjeistaa, että laitteenvaihdon yhteydessä onkin hyvin tärkeää muistaa poistaa pilvipalveluissa käytetty laite pois pilvipalvelun laitelistalta, tyhjentää puhelimen muisti ja muistikortti sekä palauttaa puhelin tehdasasetuksiin. Tehdasasetusten palauttamista suositellaan myös käytetyn laitteen käyttöönotossa, jotta edellinen omistaja ei pysty seuraamaan jonkin pilvipalvelun kautta uuden käyttäjän tietoja tai esimerkiksi etälukitsemaan laitetta.

Haittaohjelmien havaitseminen ajoissa ja niiden poistaminen luotettavilla ohjelmistoilla on tärkeää, jos laiteeseen jostain syystä jokin haitallinen ohjelma pääsee. Mobiililaitteiden kehitys on nykypäivänä todella nopeatahtista ja joissain tapauksissa valmistaja lopettaa kokonaan vanhojen laitemallien päivitykset, jolloin laitteesta tulee haavoittuvampi. Viestintäviraston (2014) mukaan viimeistään siinä vaiheessa kun valmistaja lopettaa päivitysten tuottamisen, tulisi harkita uuden laitteen hankintaa.

2.3.2 Viruksentorjuntaohjelmat ja muut valmiit ratkaisut

On olemassa erilaisia maksullisia ja maksuttomia ohjelmia, jotka auttavat käyttäjää pitämään laitteen puhtaana haittaohjelmista. Viruksentorjuntaohjelmat ovat ohjelmia, joilla pyritään estämään haittaohjelmien pääsyä järjestelmään ja tunnistamaan saastuneet tiedostot sekä poistamaan, puhdistamaan tai eristämään ne (Sanastokeskus TSK ry, 2014).

Haittaohjelmat kehittyvät jatkuvasti, joten ajantasaista viruksentorjuntaohjelmaa päivitetään ja kehitetään jatkuvasti. Jos haittaohjelmaa ei ole listattu ja päivitetty viruksentorjuntaohjelman virustietokantaan, se jää tunnistamatta ja poistamatta. Käyttäjä voi valita haluaako käyttää ohjelmaa manuaalisesti vain silloin kun itse haluaa, vai automaattisesti, jolloin ohjelma skannaa laitetta jatkuvasti haittaohjelmien varalta. Viruksentorjuntaohjelmissa on eroja niin ominaisuuksissa kuin hinnassakin ja valinta sekä ominaisuuksien arviointi jää käyttäjän omalle vastuulle. Ilmaiset ohjelmat yleensä sisältävät vain tärkeimmät toiminnot laitteen suojaamiseksi ja maksullisissa ohjelmissa on enemmän ominaisuuksia.

Mobiililaitteiden kyberturvallisuuden hallintaan on olemassa myös valmiita tietosuojaratkaisuja, jotka sisältävät virustorjunnan sekä yksityisyydensuojan. Valmiita tietosuojaratkaisuja on todella paljon hieman erilaisilla ominaisuuksilla, mutta lähtökohtaisesti kaikki tunnetuimmat yritykset tarjoavat maksullisia ratkaisuja. Pelkän virustorjunnan moni tarjoaa maksutta, mutta yksityisyyden suojaavat ominaisuudet ovat maksullisia.

2.3.3 VPN-suojaus

Internetin käyttö perustuu tiedon lähettämiseen ja vastaanottamiseen, tietoliikenne tapahtuu käyttäen tietosähkeitä eli paketteja. Kaikenlainen sisällön siirto internetin kautta tapahtuu pakettien välityksellä. Kun laite yhdistetään internetiin julkisen WiFi-verkon kautta, tiedonsiirto on salaamatonta, jolloin tieto on helposti kolmannen osapuolen saavutettavissa. Normaalisti kuin laite yhdistetään internetiin, tiedonsiirto on salattua, mutta julkinen WiFi-verkko ei käytä salaustekniikoita. Esimerkiksi julkisen verkon kautta verkkopankkiin kirjautuessa hakkerit voivat päästä helposti käsiksi kaikkeen tietoon, mitä verkkopankin ja laitteen välillä siirtyy. (Tricks Window, 2012)

Virtuaalinen yksityisverkko (engl. virtual private network, VPN) on tietoverkon kautta muodostettu suojattu verkkoyhteys, jossa verkon päätelaitteet toimivat aivan kuin olisivat samassa, muilta tietoverkon käyttäjiltä suljetussa lähiverkossa. VPN toteutetaan yleensä internetin kautta salattuna yhteytenä ja siinä käytetään erilaisia pääsynvalvonnan menetelmiä. (Sanastokeskus TSK ry, 2014) Jos mobiililaitteessa ei ole käytössä matkapuhelinverkon kautta tapahtuvaa tiedonsiirtoa, tai jostain muusta syystä on käytettävä julkista WiFi-verkkoa, VPN-yhteydellä voidaan muodostaa suojattu yhteys internetpalvelimiin.

2.3.4 F-Secure Freedome -sovellus

Freedome on yksityisyydensuojaratkaisu älypuhelimille, tableteille ja PC:lle. Se salaa tietoja, suojaa verkkoyhteyden ja torjuu seurantaa, jolloin arkaluontoisia tietoja ei pääse vuotamaan nettiin. (F-Secure, 2015b) Freedome on yhdistelmä yksityisyyden suojaamista, tietojensuojaamista sekä perinteistä viruksentorjuntaa.

KUVIO 1 Kuvakaappaus: Freedomen päävalikko

Freedome on ulkoasultaan selkeä ja neutraali (kuvio 1), jossa ominaisuuksien lisätiedot avautuvat etusivulla. Freedome sisältää seuraavat ominaisuudet: App Security, seurannan esto, selaussuojaus sekä yhteyksiensuojaus.

- Turvallisuus ja yksityisyys: jolloin hakkerit eivät pääse tietoihin käsiksi, eivätkä mainostajat voi seurata
- WiFi-tietoturva: suojaa yhteyden VPN-tekniikalla, jolloin julkisten langattomien verkkojen käyttö on turvallista
- Poistaa maantieteelliset rajoitukset: käyttäjä voi asettaa virtuaalisen sijaintinsa toiseen maahan, jolloin maantieteellisesti rajattujen sisältöjen selaaminen mahdollistuu mistä vain
- Yksinkertaisuus: lupaus, että yksityisyys ja turvallisuus verkossa on taattu yhdellä napinpainalluksella (F-Secure, 2015a)

Kun laite muodostaa yhteyden internetiin, sille määritellään yksilöllinen IP-osoite. IP-osoite on numeerinen tunniste, joka on kaikilla internetprotokollaa käyttävällä laitteella. Tunnistetta tarvitaan laitteen tunnistamiseen ja kommunikaation ohjaamiseen oikeaan osoitteeseen. (Limnell ym., 2014 s. 238) Freedomen yksi ominaisuus on peittää tämä IP-osoite, jolloin nettiselailusta ei jää yksilöllistä jälkeä tietojen kerääjille. IP-osoitteen peittäminen tapahtuu käyttämällä F-Securen Cloud-pilveä, jolloin laite muodostaa ensin yhteyden pilveen ja sen läpi muodostuu yhteys internetiin. (F-Secure, 2015a) IP-osoitteen muuttaminen mahdollistaa myös käyttäjän sijainnin muuttamisen esimerkiksi toiseen maahan. Esimerkiksi käyttäjä pystyy muuttamaan sijaintinsa toisessa maassa sijaitsevalle pilvipalvelimelle ja näin ollen saada erilaisia hintoja lentotarjouksista, tai vaikka

katsoa kotimaan sisälle rajattua nettitelevisiota ulkomailta muutettuaan virtuaalisijaintinsa kotimaahan.

Internetin käytön seurantaa ja tietojen myymistä harjoitetaan paljon. Freedome suojaa laitetta tällaisilta seurantayrityksiltä. Freedome tunnistaa haittaohjelmat ja seurantaevästeet ja estää niitä keräämästä ja lähettämästä tietoja. (F-Secure, 2015a) Viestintäviraston (2014b) mukaan eväste on pieni tekstitiedosto joka voi sisältää tietoja kuten käyttäjän IP-osoite, kellonaika, käytetyt sivut, selaintyyppi, mistä osoitteesta käyttäjä on tullut kyseiselle verkkosivustolle, miltä palvelimelta käyttäjä on tullut sivuille sekä mistä verkkotunnuksesta käyttäjä on tullut verkkosivuille. Internetselain tallentaa evästeen käyttäjän laitteeseen ja niitä käytetään esimerkiksi kun halutaan säilyttää käyttäjän tietoja tämän siirtyessä internetpalvelun sivuilta toiselle. Viestintävirasto (2014b) mainitsee lisäksi, että evästeiden käyttö vaatii aina käyttäjän suostumuksen ja että palveluntarjoajan tulee noudattaa sähkökauppalakia ja siinä määriteltyä tiedonantovelvollisuutta jos se tallentaa verkkopalvelun käyttöä kuvaavia tietoja tai hyödyntää verkkopalvelun käyttöä kuvaavia tietoja.

WiFi-yhteydensuojaus tapahtuu myös F-Securen Cloud-pilven avulla, joka tekee laitteen internetyhteydestä näkymättömän. Laite muodostaa salatun yhteyden F-Securen pilven kautta internetiin. Pilvi tekee tiedostoista lukukelvottomia, jos joku yrittää lukea laitteen tietoja WiFi-verkon kautta. (F-Secure, 2015a) Kun laite ilman tällaista suojaa yhdistetään avoimeen WiFi-verkkoon, se luovuttaa tietoja laitteesta verkon haltijalle, sekä antaa verkon haltijalle mahdollisuuden päästä käsiksi laitteen tietoihin ilman tietojen salauksia.

F-Secure (2015d) kertoo myös, että käyttäjälle annetaan Freedomen mobiilisovelluksen mukana ilmainen App Security, joka kuuluu virusskanneri, joka suojaa haitallisilta sovelluksilta, viruksilta, vakoiluohjelmilta sekä muilta haitallisilta ohjelmilta. F-Securen (2015d) mukaan App Security on ns. seuraavan sukupolven virusskanneri, joka on aikaisempia virustorjuntaohjelmia kevyempi, nopeampi sekä vähemmän akkua kuormittava.

2.4 Tutkimuksia mobiililaitteiden kyberturvallisuudesta

Aiempia tutkimuksia mobiilisovellusten omaksumisesta on tehty, mutta tutkimuksia, joissa kohteena olisi nimenomaan tietoturva- tai tietosuojasovelluksen omaksuminen ei juuri löydy. Kuitenkin käyttäjien asenteita yleisesti mobiilisovelluksia ja niiden tietoturvapolitiikkaa kohtaan on tutkittu. Tutkimukset ovat todistaneet muun muassa että mobiilisovelluksia ladataan älypuhelimiin tutustumatta tarkemmin niiden alkuperään tai tietosuojakäytäntöihin. Seuraavissa kappaleissa käydään läpi aiemmista tutkimuksista saatuja tuloksia.

Chin, Porter, Sekar & Wagner (2012) ovat tutkineet älypuhelinten käyttäjien asenteita mobiilisovellusten tietoturvaa kohtaan ja havaitsivat muun muassa, että käyttäjät olivat enemmän huolissaan puhelintensa, kuin kannettavien tietokoneidensa yksityisyydestä. Riippuen käyttöliittymästä ja miten turvalliseksi käyttäjät kokivat puhelimensa, he eivät yleisesti halunneet tehdä ostoksia tai

hoitaa arkaluontoisia asioita puhelimella. Toisaalta taas tutkimus osoitti, että suurin osa tutkittavista koki luontevana käyttää sijaintipalveluja koska ne nähtiin hyödyllisinä ominaisuuksina. Lisäksi tutkijat havaitsivat, että jotkin käyttäjien pelot johtuivat todennäköisesti väärinymmärryksistä sovellusten turvallisuuteen liittyen. Tutkimuksessa havaittiin myös, että käyttäjät lataavat enemmän sovelluksia älypuhelimiinsa kuin kannettaviin tietokoneisiinsa. Älypuhelimiin ladattavat sovellukset ovat useasti pelejä tai viihteellisiä sovelluksia, ja niiden asentamisen suhteen ei olla niin merkki- ja hintatarkkoja, kuin tietokonesovellusten suhteen. Tutkimuksen mukaan älypuhelinsovellusten käyttöehdot ja palvelusopimukset usein sivuutetaan. (Chin ym., 2012) Myös Leavittin (2011) mukaan monet käyttäjät lataavat älypuhelimiin sovelluksia huomioimatta niiden tietoturvaa ja samaan aikaan käsittelevät puhelimillaan arkaluontoisia tietoja kuten pankkipalveluja, maksutapahtumia ja lähettävät luottamuksellisia yritystietoja. Tällaiset käyttäjät, joiden laitteita ei ole suojattu, ovat erittäin houkuttelevia kohteita hakkereille.

Mylonas, Kastania ja Gritzalis (2012) tutkivat kuinka tietoisia turvallisuudesta älypuhelinten käyttäjät ovat kun he lataavat sovelluksia virallisista sovelluskaupoista kuten Google Play ja Applen App Store. Tutkimustulokset viittasivat siihen, että käyttäjät luottivat sovelluskauppoihin ja käyttäjät ohittivat tietoturvaperiaatteet valitessaan ja asentaessaan sovellusta. Tutkimus osoitti, että käyttäjät eivät ole niin tietoturvatietoisia, kuin heidän on oletettu olevan, ja että he eivät ole tarpeeksi valmiita tekemään asianmukaisia turvallisuuspäätöksiä. Suuri osa älypuhelinten käyttäjistä uskoi, että sovelluksen lataaminen virallisesta sovelluskaupasta on riskitöntä. On epäselvää mistä tämä turvallisuudentuntu käyttäjissä johtuu. Tutkijat epäilivät, että se voi johtua käyttäjien luottamuksesta viralliseen sovelluskauppaan tai siitä että käyttäjät eivät täysin ymmärrä, että heidän käytössään oleva laite ei ole pelkkä puhelin. (Mylonas ym., 2012)

Mylonas ym. (2012) tekivät myös saman havainnon kuin Chin ym. (2012) ja Leavitt (2011), että älypuhelinten käyttäjät usein sivuuttavat sovellusten tietoturvakäytänteet sovellusta ladattaessa. Mylonas ym. (2012) havaitsivat lisäksi, että osa käyttäjistä sivuuttaa kaikki sovelluksen antamat ilmoitukset. Tutkijat havaitsivat, että ilmoitusten huomioimatta jättäminen on haavoittuvuus, joka kasvaa sovellusten lisääntyessä, koska myös sovelluskehittäjät ovat huomanneet tämän. Yhä useammat sovellukset pyytävät lupaa käyttää tietoja, joita ne eivät toiminnassaan edes tarvitse. Käyttäjän salliessa tällaisten tietojen keräämisen, he tulevat antaneeksi luvan myös sovelluksen yhteistyötahoille (esimerkiksi mainostajille), jotka voivat aiheuttaa esimerkiksi häiritsevää mainontaa. (Mylonas ym., 2012).

Turvatoimenpiteiden käytön omaksuminen näyttää olevan yhteydessä käyttäjän tekniseen osaamiseen. Teknisesti osaavammat käyttäjät ottavat huomioon salauksen, tietojen poistamisen ja laitteen paikannuksen etänä. Toisaalta taas käyttäjän teknisellä osaamisella ei ollut yhteyttä puhelimen salasanalla suojaamiseen. (Mylonas ym., 2012).

Mylonas ym. (2012) havaitsivat tutkimuksessaan, että suurin osa älypuhelinten käyttäjistä ei suojannut puhelinta millään kolmannen osapuolen tarjoa-

malla tietoturvasovelluksella. Käyttäjät kuitenkin mainitsivat suojaavansa tietokoneensa tietoturvaohjelmistolla. Tässä on selvä epäsymmetria miten käyttäjät näkevät tietokoneen ja älypuhelimen tietoturvallisuuden. Lisäksi huomattava määrä käyttäjistä oli sitä mieltä, että älypuhelinten tietoturvasovellukset eivät ole välttämättömiä. Tutkijat epäilevät, että välinpitämätön asenne tietoturvapalveluja kohtaan voi johtua laitteen teknisistä ominaisuuksista, kuten huonosta akunkestävyydestä, laitteen yleisen suorituskyvyn heikkoudesta, olemassa olevien tietoturvauhkien tietämättömyydestä tai väärästä tiedosta tai psykologisista muuttujista, eli esimerkiksi luottamuksesta sovelluskauppoihin. (Mylonas ym., 2012).

Aiempien tutkimusten valossa voidaan muodostaa hypoteesi, että tieto- ja yksityisyydensuojapalveluiden käyttöönoton omaksuminen on heikkoa, vaikka käyttäjät kuitenkin ovat enemmän huolissaan älypuhelintensa suojaamisesta kun kannettavien tietokoneidensa suojaamisesta. Tutkimukset osoittivat, että monet lataavat puhelimiinsa sovelluksia ja hyväksyvät käyttöehdot niihin kuitenkaan perehtymättä, koska luottavat sovelluskauppoihin tai eivät täysin ymmärrä joidenkin haitallisten sovellusten tietoturvariskejä.

2.5 Yhteenveto

Kyberturvallisuus on tietoturvallisuutta, verkkoturvallisuutta ja laiteturvallisuutta. Mobiililaitteiden kyberturvallisuus on turvallisuuden uusi ulottuvuus, joka tarkoittaa mukana kuljetettavaksi suunniteltujen laitteiden tietojen turvaamista laitteessa ja verkossa.

Tutkimusten mukaan mobiililaitteiden määrän kasvu on ollut viime vuosina merkittävää, mutta esimerkiksi Kaspersky Labin tutkimuksen mukaan niiden tietosuojan nykytila on Suomessa hyvin heikko. Mobiililaitteita uhkaa haittaohjelmat, vakoiluohjelmat, riskiohjelmat, ei-toivotut sovellukset sekä fyysiset uhat. Laitteisiin kohdistuvia uhkia voidaan hallita käyttämällä laitetta turvallisesti, viruksentorjuntaohjelmilla ja muilla valmiilla ratkaisuilla sekä VPN-suojauksella. Tässä tutkimuksessa tutkimuskohteena oleva Freedome-sovellus on yksityisyydensuojaratkaisu, jossa on yhdistetty yksityisyydensuoja, tietosuoja sekä viruksentorjunta yhteen sovellukseen.

Aiempien tutkimusten mukaan mobiililaitteiden tieto- ja yksityisyyssuojasovellusten omaksuminen on heikkoa. Käyttäjät kuitenkin ovat huolissaan mobiililaitteidensa suojaamisesta, mutta eivät kuitenkaan toimi sen mukaisesti.

3 TEKNOLOGIAN OMAKSUMISPROSESSI

Teknologian omaksumista voidaan tutkia ja tulkita monen eri teorian pohjalta. Tässä luvussa käsitellään teknologian hyväksymistä selittäviä teorioita teemoittain, sekä käydään läpi tutkimukseen valittu viitekehys.

Everett Rogersin (2003) mukaan innovaation omaksuminen on osa innovaation diffuusiota, eli innovaation ja sitä koskevan tiedon leviämistä markkinoille. Tässä tutkimuksessa innovaation omaksumisprosessia käsitellään käyttäen viitekehyksenä Rogersin innovaation diffuusioteoriaa.

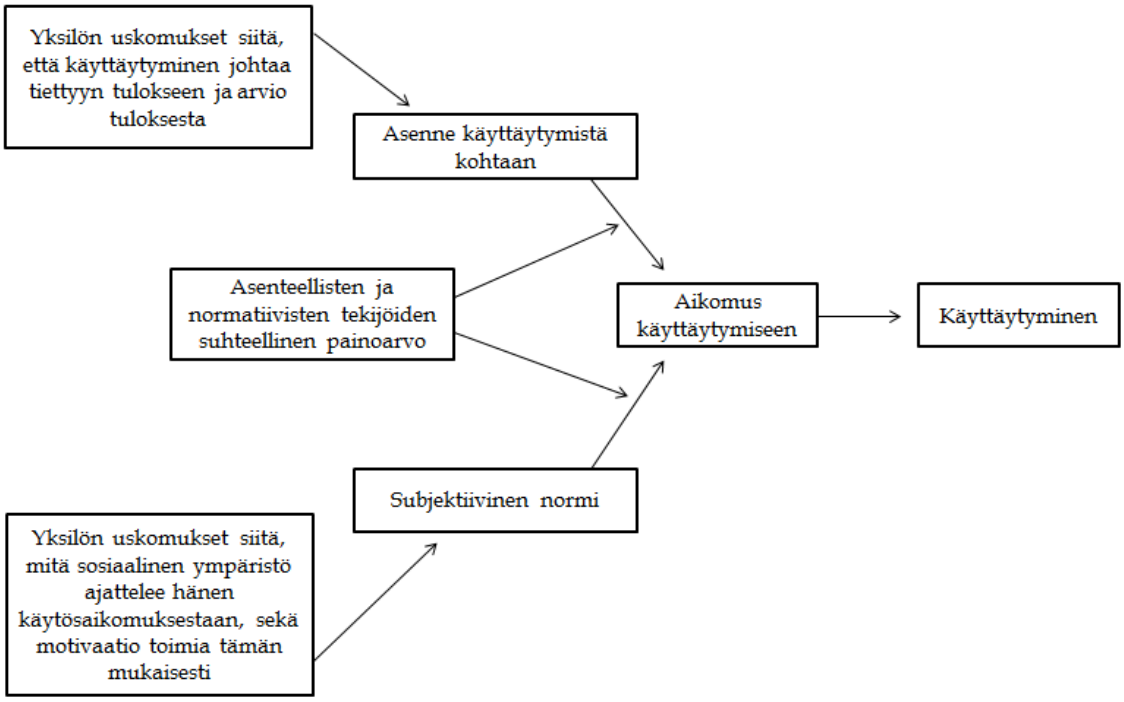
Omaksumisprosessi (engl. the innovation-decision process) alkaa siitä hetkestä, kun henkilö saa tiedon innovaatiosta. Tiedon saamisen jälkeen henkilö muodostaa oman suhtautumisensa innovaatioon ja sen jälkeen tekee päätöksen omaksua tai hylätä innovaation. Omaksumisprosessi päättyy innovaation käyttöönottoon ja sen hyväksymisen tai hylkäämisen vahvistamiseen. (Rogers 2003, 216-217)

3.1 Teknologian omaksumisprosessia selittäviä teorioita

Tunnetuimpia teknologian omaksumista ja hyväksymistä tutkivia malleja ovat perustellun toiminnan teoriamalli (engl. theory of reasoned action, myöh. TRA), laajennettu teknologian hyväksymismalli (engl. technology acceptance model, myöh. TAM2), suunnitellun käyttäytymisen teoria (engl. theory of planned behavior, myöh. TPB), yhdistetty teoria teknologian hyväksynnästä (engl. unified theory of acceptance and use of technology, myöh. UTAUT) sekä innovaation diffuusioteoria.

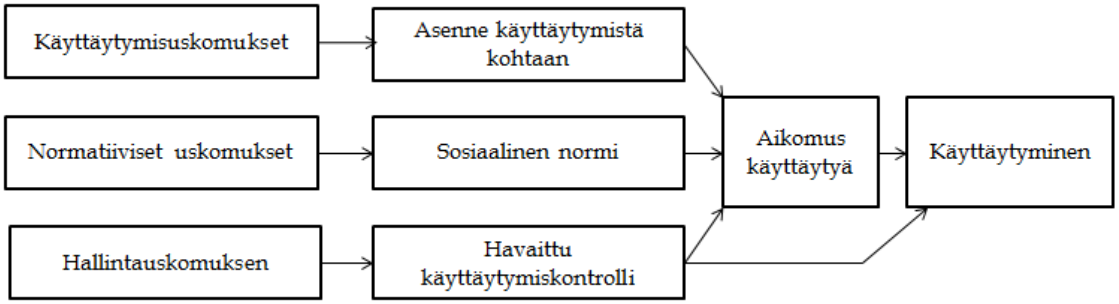
Ajzenin ja Fishbeinin (1980) kehittämän TRA on kehitetty yksilön käyttäytymisen ymmärtämiseksi ja ennakoimiseksi. Tämän mallin mukaan omaksumisprosessi alkaa henkilön aikomuksesta tehdä tai jättää tekemättä jotain ja se aikomus määrittää lopullisen toiminnan. Ajzen & Fishbein (1980) määrittelevät, että henkilön käyttäytymiseen vaikuttaa kaksi muuttujaa: (1) asenne käyttäytymistä kohtaan sekä (2) subjektiivinen normi. TRA teorian mukaan asenne

käyttäytymistä kohtaan tarkoittaa henkilön arvoja jotka määrittelevät hänen arvionsa siitä onko käyttäytymisen toteuttaminen hyvä vai huono asia. Subjektiivinen normi taas tarkoittaa sosiaalista painetta, eli olisiko henkilön hyvä toteuttaa aiottu käyttäytyminen vai jättää se toteuttamatta. Kuviossa 2 on kuvattu yksilön käyttäytymiseen vaikuttavat tekijät TRA:n mukaan.



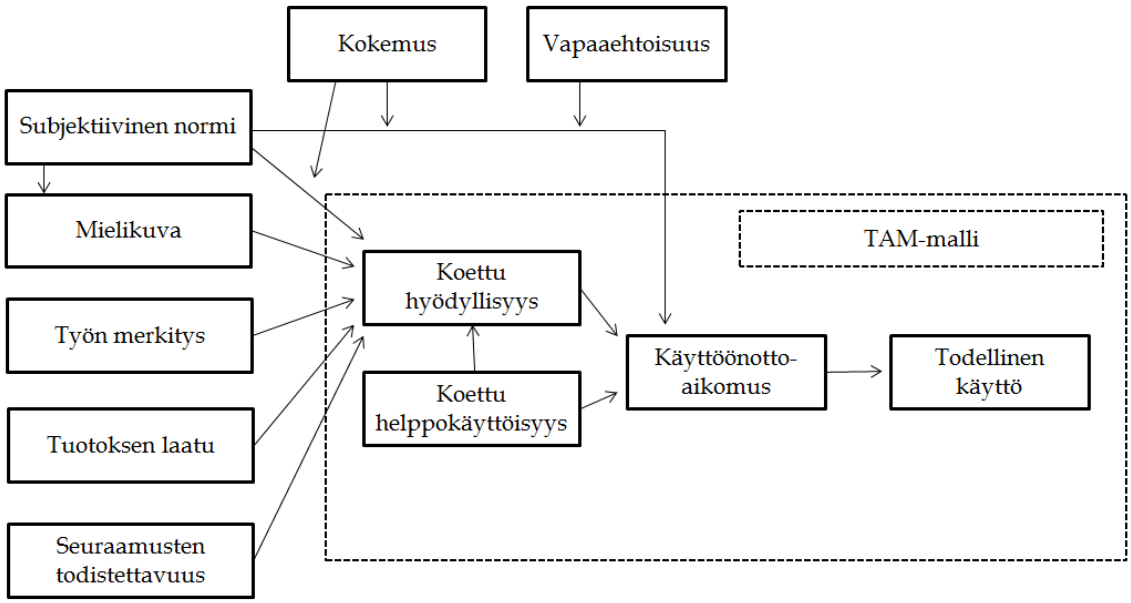
KUVIO 2 TRA-malli (Ajzen & Fishbein, 1980)

TPB, eli suunnitellun käyttäytymisen teoria perustuu TRA-malliin. TPB on esitetty kuviossa 3. Ajzenin (1991) mukaan ihmisen käyttäytymisaikomus muodostuu kolmesta tekijästä joita ovat (1) asenne käyttäytymistä kohtaan, (2) subjektiivinen normi sekä (3) käyttäytymisen hallinta. Kuten TRA-mallissa, myös TPB-mallissa käyttäytymisaikomukseen vaikuttaa asenteeseen liittyvät uskomukset ja arviointi sekä normatiiviset uskomukset ja motivaatio niiden noudattamiseen. Ajzen (1991) määrittelee, että käyttäytymisaikomuksen lisäksi tärkeä vaikuttava tekijä on käyttäytymisen hallinta, johon vaikuttaa ihmisen aikaisemmat kokemukset ja arvio kokeeko hän käyttäytymisen helppona vai vaikeana. Näiden tekijöiden vaikutus näkyy käyttäjän kokemana itsevarmuutena, joka suurella todennäköisyydellä johtaa käytöksen parempaan onnistumiseen.



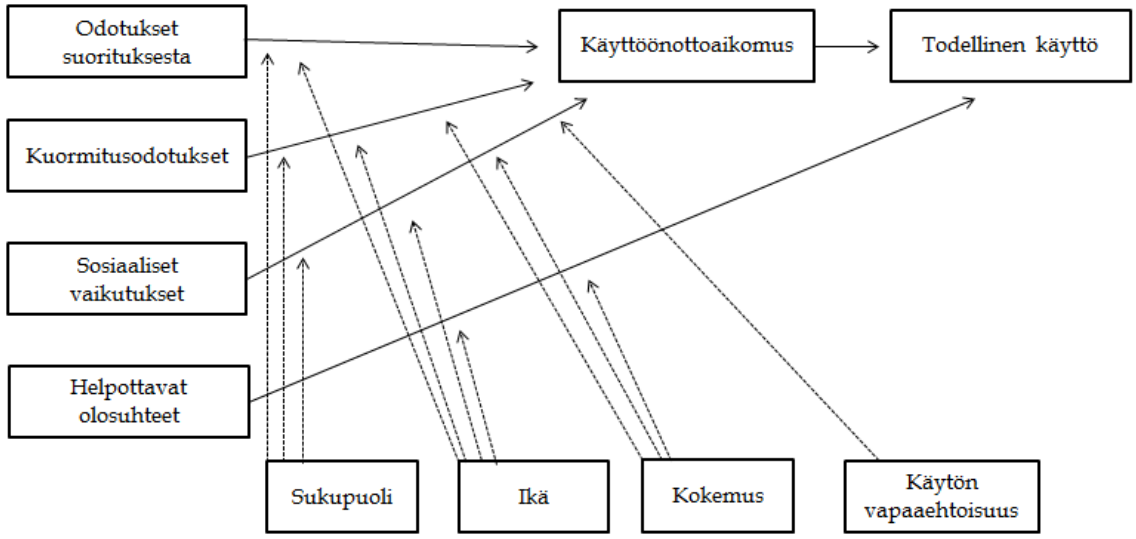
KUVIO 3 TBP-malli (Ajzen, 1991)

TAM2-malli on kehitetty TAM-mallista, jonka perusideana on että koettu hyödyllisyys ja helppokäyttöisyys vaikuttavat käyttöönottoaikomukseen, joka johtaa todelliseen käyttöön, eli omaksumiseen. Venkatesh ja Davis (2000) kehittivät TAM2-mallin, koska alkuperäinen TAM-malli sai paljon kritiikkiä muun muassa sen yksinkertaisuudesta tunnistaa koettuun hyödyllisyyteen vaikuttavia tekijöitä. TAM2 on kuvattu kuviossa 4, jossa alkuperäinen TAM-malli näkyy oikealla katkoviivoin merkityssä laatikossa ja laatikon ulkopuoliset tekijät ovat TAM2 laajennuksia. Venkateshin ja Davisin (2000) mukaan koettuun hyödyllisyyteen vaikuttaa sosiaalisia ja kognitiivisia tekijöitä. Kognitiivisia tekijöitä ovat yhteys työtehtäviin (engl. job relevance), tuloksen laatu (engl. output quality) ja tulosten esitettävyys (engl. result demonstrability). Sosiaalisia tekijöitä ovat TAM2-mallissa subjektiivinen normi (engl. subjective norm) sekä imago (engl. image). Käyttäjän kokemus sekä vapaaehtoisuus vaikuttavat subjektiivisen normin kautta koettuun hyödyllisyyteen.



KUVIO 4 TAM2-malli (Venkatesh & Davis, 2000)

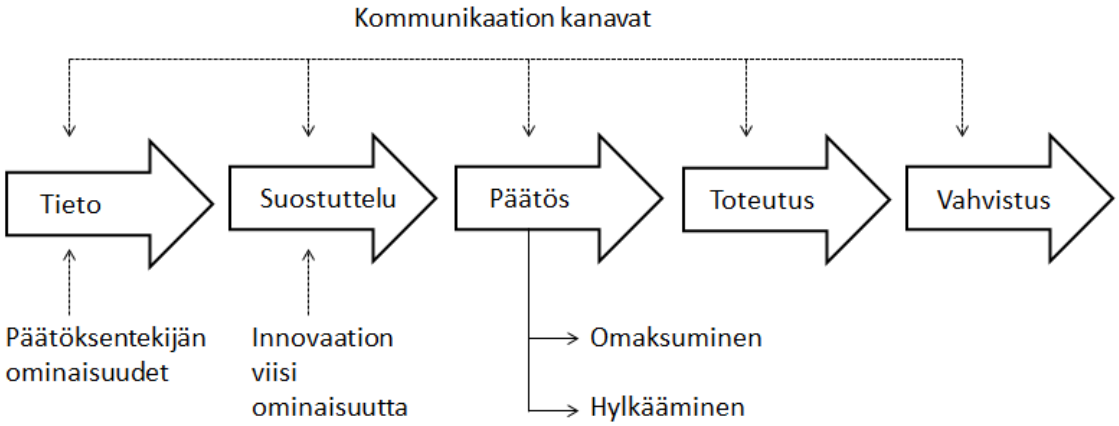
Venkatesh, Morris, Davis ja Davis (2003) kehittivät kuviossa 5 esitetyn UTAUT-mallin kahdeksan eri teknologian hyväksymismallin pohjalta. Venkateshin ym. (2003) mukaan UTAUT-malli pystyy selittämään teknologian omaksumiseen vaikuttavia tekijöitä paremmin kuin aikaisemmat mallit. UTAUT-mallissa kolme tekijää vaikuttaa käyttöaikomukseen: (1) odotukset suorituksesta, (2) kuormitusodotukset ja (3) sosiaaliset vaikutukset ja yksi tekijä, joka vaikuttaa suoraan todelliseen käyttöön: helpottavat olosuhteet. Em. tekijöiden voimakkuuteen vaikuttaa niiden taustalla yksilön ominaisuudet: sukupuoli, ikä ja kokemus sekä käytön vapaaehtoisuus. Venkatesh, Thong ja Xu (2012) ovat kehittäneet UTAUT-mallin pohjalta UTAUT2-mallin, johon on lisätty käyttäytymisaikomukseen vaikuttavina tekijöinä hedoninen motivaatio, hinta sekä tavat ja tottumukset. Hedoninen motivaatio on teknologian käytöstä koituvaa mielihyvää, jolla on Venkateshin ym. (2012) mukaan suuri vaikutus käyttöaikomukseen ja suoraan käyttöön. Hinnan merkitys nähtiin myös vaikuttavana tekijänä nimenomaan yksilön omaksumisprosessia tutkittaessa, jolloin käyttäjä joutuu itse maksamaan käyttämänsä tuotteen tai palvelun. UTAUT2- mallissa lisänä ovat myös tavat ja tottumukset, jotka aikaisempien tutkimusten mukaan ovat vaikuttaneet yksilön käyttäytymiseen omaksumisprosessissa.



KUVIO 5 UTAUT-malli (Venkatesh ym., 2003)

Innovaation diffuusioteoria tutkii innovaatioiden leviämistä ja innovaatioiden omaksumisen alkuvaiheen mittaamista. Innovaation diffuusioteorian mukaan käyttöönottoon ja omaksumisprosessiin vaikuttavan innovaation viisi ominaisuutta: suhteellinen hyöty, yhteensopivuus, monimutkaisuus, kokeiltavuus ja havaittavuus.

Kuviossa 6 on esitetty miten innovaation diffuusioteoria selittää käyttöönotto-prosessin. Ensimmäisenä yksilö saa tiedon innovaatiosta ja luo ymmärryksen sen toiminnasta, jonka jälkeen hän muodostaa innovaation ominaisuuksien perusteella sitä kohtaan suosivan tai hylkäävän asenteen. Näiden jälkeen tulee päätösvaihe, jossa toteutetaan toimenpiteet innovaation hyväksymiseen tai hylkäämiseen. Toteutusvaihe sisältää innovaation käyttöönoton ja kokeilun. Vahvistusvaiheessa päätös vakiinnutetaan hankkimalla innovaatiosta lisää tietoa. Innovaation diffuusioteoria on selitetty tarkemmin seuraavassa alaluvussa.



KUVIO 6 Päätösprosessi innovaation diffuusioteorian mukaan (Rogers, 2003)

Tähän tutkimukseen viitekehykseksi valikoitiin innovaation diffuusioteoria, koska muut teknologian omaksumista selittävät mallit pyrkivät tutkimaan enemmän yksilön toimintaa ja historiaa ennen käyttöönottoa. Tässä tutkimuksessa mielenkiinnon kohteena on omaksuminen sekä jatkuva käyttö, jolloin käyttöönottoa ennen tapahtuvat toiminnot eivät ole niin oleellisia tutkimuksen kannalta. Tutkimusongelmana on miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön, joten Rogersin innovaation diffuusioteoria soveltuu tähän tutkimukseen parhaiten, koska se pyrkii selittämään tarkemmin itse innovaation ominaisuuksia, ei niinkään yksilön ominaisuuksia.

3.2 Innovaation diffuusioteoria

Innovaation diffuusioteoria on esitetty ensimmäisen kerran vuonna 1963, jolloin Rogers julkaisi ensimmäisen painoksensa kirjasta Diffusion of Innovations. Ensimmäisen painoksen jälkeen Rogers päivitti teoriaa aina vuoteen 2003 saakka vastaamaan paremmin kehittyvän maailman tarpeita. Tätä teoriaa on käytetty viitekehyksenä paljon tutkimuksissa, jotka käsittelevät teknologisten innovaatioiden leviämistä ja omaksumista.

Diffuusio on prosessi, joka määrittelee miten ja missä ajassa tieto innovaatiosta leviää tiettyjen kanavien läpi sosiaalisessa verkostossa. Innovaation diffuusioteoriassa neljä keskeistä elementtiä ovat innovaatio, viestintäkanavat, käytetty aika ja sosiaalinen verkosto. (Rogers 2003, 35-36) Innovaatio on idea, toimintakäytäntö tai esine, joka on käyttäjälle uusi. Innovaation omaksumisprosessin nopeuteen vaikuttaa miten sosiaalisen verkoston yksilöt kokevat sen ominaisuudet. Viestintä tässä yhteydessä tarkoittaa prosessia jossa ihmiset luovat ja jakavat tietoa päästäkseen yhteisymmärrykseen. Viestintäkanaviin luetaan joukkoviestimet sekä henkilöiden välinen viestintä, joista joukkoviestimet ovat nopein ja vaikuttavin tapa jakaa tietoa. (Rogers 2003, 18)

3.2.1 Omaksumisprosessi

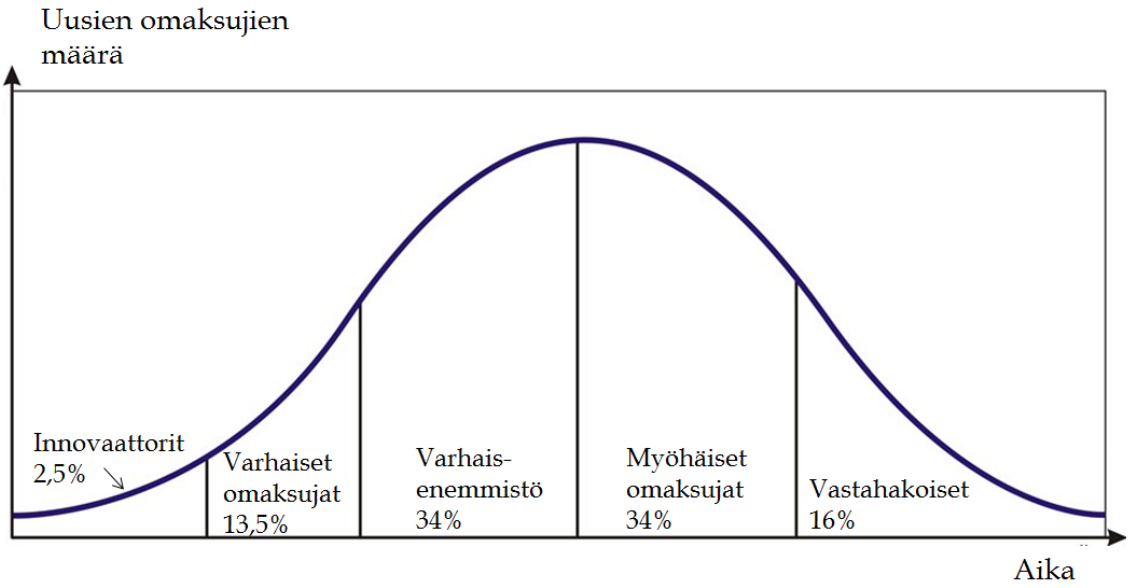
Innovaation diffuusioteoria käsittelee innovaation leviämistä suuren yleisön tietoon. Yhtenä osana leviämiseen vaikuttaa yksilön omaksumisprosessi, eli se miten henkilö omaksuu uuden teknologiaratkaisun käyttöönsä (kuvio 6). Yksilön omaksumisprosessi alkaa tiedon saamisesta ja päättyy siihen kun hän käyttöönottaa tai hylkää innovaation ja hakee tälle päätökselleen vahvistusta. Innovaation omaksumista mitataan ajallisesti; kuinka kauan henkilöllä menee innovaation omaksumiseen tai hylkäämiseen, mitattuna siitä hetkestä kun hän on saanut tiedon innovaatiosta. Omaksumisprosessin ensimmäinen vaihe on tietovaihe, jossa yksilö saa tiedon innovaatiosta ja luo ymmärryksen sen toiminnasta. Toisessa, suostutteluvaiheessa yksilö muodostaa innovaatiota kohtaan myönteisen tai hylkäävän asenteen innovaation viiden ominaisuuden pohjalta. Kolmas vaihe on päätösvaihe, jossa yksilö toteuttaa toimenpiteet innovaation hyväksymiseen tai hylkäämiseen. Neljäs vaihe on toteutusvaihe, jossa yksilö käyttöönottaa ja kokeilee innovaatiota ja viidennessä vaiheessa hän vakiinnuttaa päätöksen hankkimalla innovaatiosta lisätietoa.

Rogers (2003) määrittelee, että diffuusiota tarkastellaan aina tietyssä sosiaalisessa verkostossa (engl. social system), jossa sen jäsenet keskustelevat saadakseen informaatiota uusista innovaatioista tai niiden olemassaolosta. Rogersin (2003) mukaan omaksumiseen liittyy riski, jota omaksujat pyrkivät minimoimaan seuraamalla vertaiskäyttäjien kokemuksia. Innovaation omaksuminen kulkee tartuntamaisesti, mitä enemmän vertaisomaksujia on, sen suuremmaksi paine muita kohtaan kasvaa.

Rogersin (2003) innovaation diffuusio–teoriassa innovaation omaksujat voidaan jakaa viiteen segmenttiin (kuvio 7):

- innovaattorit (engl. innovators) 2,5 % (kaikista omaksujista): elämäntapana teknologiauutuuksien etsiminen, testaaminen ja tutkiminen.
- varhaiset omaksujat (engl. early adopters) 13,5 %: kuuntelevat innovaattoreita ja omaksuvat innovaation heti käyttöönsä, kun saavat positiivisen tuen päätökselleen innovaattoreilta.

- varhaisenemmistö (engl. early majority) 34 %: harkitsevat päätöksiä jokseenkin tarkkaan, mutta haluavat kuitenkin saavuttaa innovaatiosta saadun hyödyn ennen valtaväestön viimeisiä pohdiskelijoita. Kuuntelee varhaisia omaksujia. Innovaation uutuus ei ole tärkein tekijä, vaan sen hyödyllisyys.
- myöhäiset omaksujat (engl. late majority) 34 %: kun enimmät epävarmuustekijät ovat kumottu, myöhäiset omaksujat ovat valmiita omaksumaan innovaation käyttöönsä. Asennoituvat skeptisesti ja epäluuloisesti uusiin innovaatioihin ja kuuntelevat aikaisempien ryhmien kokemuksia tarkkaan.
- vastahakoiset (engl. laggards) 16 %: viivyttelevät päätöksenteon kanssa, perustavat päätöksiään perinteisiin ja aikaisempiin tapahtumiin. Tämä ryhmä kommunikoi lähinnä vertaistensa kanssa ja ovat epäileviä uutuuksien suhteen.



KUVIO 7 Innovaation omaksujaryhmät (Rogers, 2003)

Oleellista on, että diffuusio tapahtuu aina aikajärjestyksessä, jolloin innovaattorit tulevat ensin ja sen jälkeen loput. Jos innovaattorit eivät koskaan omaksu innovaatiota, Rogersin (2003) mukaan se tuskin tulee leviämään muille käyttäjille. Kaikkien omaksujaryhmien välissä voidaan nähdä olevan kuilu, joka pitää ylittää, jotta ketju ei katkea ennen kuin massamarkkinat on tavoitettu. Moore (1999) on käytännön kokemuksensa pohjalta määritellyt että kaikkein vaikeimmin ylitettävä kuilu on varhaisten omaksujien ja varhaisenemmistön välillä, koska näillä ryhmillä on hyvin erilaiset odotukset omaksuttavaa asiaa kohtaan. Kalliokulju ja Palviainen (2006) tiivistävät artikkelissaan, että varhaiset omaksujat ovat visionäärejä ja haluavat olla muutosagentteja kun varhaisenemmistön jäsenet taas ovat käytännöllisiä ja odottavat innovaatiolta tuottavuutta ja tehokkuutta.

Omaksumiseen vaikuttaa innovaation viisi ominaisuutta, jotka voidaan jakaa viiteen osa-alueeseen: suhteellinen hyöty, yhteensopivuus, monimutkaisuus, kokeiltavuus ja havaittavuus (Rogers 2003, 36). Innovaation ominaisuudet käsitellään tarkemmin alaluvussa 3.2.2 Innovaation viisi ominaisuutta.

3.2.2 Innovaation viisi ominaisuutta

Rogers (2003) määrittelee innovaation omaksumisprosessiin vaikuttavan innovaation viisi ominaisuutta: suhteellinen hyöty, yhteensopivuus, monimutkaisuus, kokeiltavuus ja havaittavuus.

Suhteellinen hyöty (engl. relative advantage) on ominaisuus, joka kertoo missä määrin käyttäjät kokevat innovaation paremmaksi ja hyödyllisemmäksi kuin sitä edeltäneen ratkaisun. Omaksumisprosessissa olennaista on, että käyttäjän tulee kokea innovaation olevan joltain osin hyödyllinen, jotta hän voi omaksua sen käyttöönsä. Jos käyttäjä kokee innovaation aiempia ratkaisuja hyödyllisempänä, hän on näin ollen valmis korvaamaan vanhan ratkaisun uudella. Suhteellinen hyöty mittaa myös missä määrin hinta vaikuttaa omaksumisprosessiin. Tuotteen ensimmäinen hinta voi vaikuttaa paljon omaksumisprosessiin. Esimerkiksi jos kuluttajat kokevat hinnan olevan kohtuullinen tuotteen hyötyihin nähden, hän todennäköisesti suosittelee sitä myös muille, jonka nähdään lisäävän innovaation yleistä omaksumismäärää. (Rogers, 2003, 229-240)

Yhteensopivuus (engl. combatibility) kertoo missä määrin innovaatio on yhdenmukainen henkilön arvojen, aiempien kokemusten ja tarpeiden kanssa. Rogers (2003) nostaa esimerkiksi kulttuurilliset vaikutukset. Jotkin innovaatiot eivät ole yhteensopivia kaikkien kulttuurien kanssa. Omaksumista ei myöskään tapahdu, jos innovaatio on ristiriidassa omaksujan uskonnon tai muun vakaumuksen kanssa. (Rogers, 2003, 240-257)

Monimutkaisuus (engl. complexity) kertoo missä määrin on tarvetta muutokseen ja kuinka paljon käyttäjän tulisi mukauttaa toimintaansa käyttäessään uutta innovaatiota. On tärkeää, että innovaatio on helppo ottaa käyttöön ja toimintaperiaatteen ymmärtäminen ei vaadi liikaa vaivaa. Rogersin (2003) mukaan innovaation monimutkaisuudella on kielteinen vaikutus omaksumisprosessiin, toisin kuin muilla ominaisuuksilla. Esimerkkinä Rogers (2003) mainitsee tietokoneiden yleistymisen olleen hankalaa kotitalouksissa, koska ensimmäiset kotikoneet koettiin monimutkaisiksi käyttää. (Rogers, 2003, 257-258)

Kokeiltavuus (engl. trialability) kertoo missä määrin innovaatiota on mahdollisuus kokeilla ennen omaksumista. Useimmiten käyttäjät haluavat testata uutta innovaatiota ennen omaksumispäätöstä. Yleisesti voidaan olettaa, että innovaatiot, joiden kokeileminen etukäteen on mahdollista, omaksutaan nopeammin. Kokeiltavuus on yhteydessä epävarmuuden poistamiseen, jolloin omaksuminen on nopeampaa. Rogers (2003) mainitsee kirjassaan, että epävarmuustekijän poistamiseksi kokeiltavuuden tarjoaminen innovaattoreille ja varhaisille omaksujille on tärkeää, jotta heidän olisi helppo välittää sanaa innovaatiosta eteenpäin. (Rogers, 2003, 258)

Havaittavuus (engl. observability) kertoo missä määrin innovaation vaikutukset ovat näkyvissä yhteisön muille jäsenille. Kun innovaation ominaisuudet on selkeästi havaittavissa, on potentiaalisen omaksujan helpompaa tutustua innovaatioon ja näin poistaa epävarmuutta sitä kohtaan. Innovaation tulisi olla mahdollisimman näkyvä joka suuntaan, jotta se olisi nopeammin omaksuttavissa ja kommunikoitavissa. (Rogers, 2003, 258-259)

3.2.3 Innovaation diffuusioteoriaan kohdistettua kritiikkiä

Innovaation diffuusioteoriaa on kritisoitu ajan kuluessa ja siihen on tehty muutoksia joiltain osin, jotta se vastaisi paremmin nykypäivän tarpeita. Teoria ei vieläkään ole kaikenkattava ja se on saanut kritiikkiä monelta tiedeyhteisön taholta. Kalliokulju ja Palviainen (2006) listaavat esimerkiksi, että teoria esittää liian yksinkertaistetun kuvan todellisuudesta.

Kalliokulju ja Palviainen (2006) sekä Rogers (2003) itse määrittelee diffuusioteorian ongelmakohdiksi esimerkiksi ns. pro-innovaatio harhan (engl. pro-innovation bias), joka tarkoittaa että innovaatioiden pitäisi aina levitä ja mielellään nopeasti. Rogers (2003) esittää diffuusioteorian myös sisältävän yksilöitä syyttävän harhan (engl. individual-blame), joka syyttää yksilöitä omaksumisprosessin epäonnistumisesta sen sijaan, että mietittäisiin sosiaalisen verkoston kannalta miksei innovaatiota omaksuta. Kritiikin kohteena voidaan nähdä myös tiedon palauttamisen ongelman (engl. recall problem), mikä tarkoittaa, että tutkimukseen saattaa tulla vääristymiä, kun tutkittavia pyydetään muistelemaan, milloin he ovat omaksuneet tietyn innovaation (Rogers, 2003).

Lyytinen ja Damsgaard (2001) listaavat artikkelissaan innovaation diffuusioteorian puutteiksi muun muassa seuraavia:

- Teknologiat nähdään muuttumattomina yksiköinä.
- Teknologian leviämisympäristö nähdään homogeenisenä ja muuttumattomana.
- Diffuusion nopeus määritellään pelkästään vetävien ja työntävien voimien funktioina, kuten teknologian ominaisuudet ja kommunikaatiokanavat.
- Omaksujien valinnat nähdään olevan riippuvaisia pelkästään saatavilla olevasta informaatiosta, omaksujien ominaisuuksista tai mieltymyksistä.
- Diffuusio kulkee eri vaiheiden läpi, mutta esimerkiksi monimutkaisen innovaation diffuusiossa niitä on hyvin vaikea erottaa toisistaan.
- Diffuusion aikajänteet nähdään lyhyinä ja omaksumisprosessi ei ota huomioon palautetta.
- Aiempien innovaatioiden omaksumishistoriaa ei nähdä tärkeänä.

Conway ja Steward (2009) kritisoivat kirjassaan sitä, ettei innovaation diffuusioteoria ota omaksumisprosessin jatkuessa riittävästi huomioon innovaation parannuksia, toimivuutta ja hintaa.

4 KVALITATIIVINEN TUTKIMUS

Tässä luvussa käsitellään tarkemmin tutkimusongelma ja –kysymykset, tutkimuksen lähtökohdat, yhteistyötahot ja tutkimuksessa käytettävät tutkimusmenetelmät. Tutkimus on luonteeltaan kvalitatiivinen eli laadullinen tutkimus, jossa tutkittiin Freedomen mobiilisovelluksen käyttäjiä. Hirsjärvi, Remes ja Sajavaara (2003) määrittelevät, että kvalitatiivisen tutkimuksen voidaan yleisesti todeta pyrkivän löytämään tai paljastamaan tosiasioita kuin todentaa jo olemassa olevia (totuus)väittämiä. Tämän tutkimuksen avulla pyrittiin ymmärtämään syvällisesti sovelluksen laatua, ominaisuuksia ja merkityksiä tutkittavien omasta näkökulmasta, jolloin tutkimusotteeksi valikoitui kvalitatiivinen tutkimus.

Tutkimusmenetelmänä käytettiin haastattelua, jonka perusjoukkoon kuuluivat henkilöt, jotka eivät olleet aiemmin käyttäneet mitään VPN-salauspalvelua ja tietosuojapalvelua yhdistävää sovellusta mobiililaitteessaan. Aineiston analysoinnin ja haastattelukysymysten suunnittelun apuna käytettiin CIT-menetelmää, joka keskittyy tutkittavan asian kannalta esiintyviin kriittisiin kokemuksiin.

Tämä tutkimus on toteutettu osana Tekesin rahoittamaa nelivuotista Digilen Need for Speed-ohjelmaa (myöhemmin N4S-ohjelma), jossa F-Secure on osallistujayrityksenä. N4S-ohjelmassa on mukana monia suomalaisia yrityksiä, tutkimusinstituutteja ja yliopistoja.

4.1 Yhteistyötahot: N4S-ohjelma ja F-Secure

Internetin vaikutus koko maailman talouteen on ollut valtava ja se jatkaa kasvuaan koko ajan. Yrityksille ja valtioille on ollut vaikeaa luoda positiivista kehitystä ja kasvua globaalin talouden myllerryksessä. Valmistautuessaan näihin muuttuviin oloihin monet yritykset ovat aloittamassa laajan muutoksen, jolla on tarkoitus määritellä uudestaan kilpailustrategia, uusi tapa johtaa ja yrityksen toimintaprosessit. N4S-ohjelman mukaan avainkysymykseksi tässä tilanteessa

nousee, miten yritykset pystyvät mukautumaan täysin uuteen liiketoimintaympäristöön ja sen mahdollisuuksiin reaaliajassa tai etukäteen. (N4S, 2014)

N4S-ohjelma on perustettu tukemaan suomalaisten ohjelmistoyritysten menestystä uudessa digitaalisessa taloudessa. Projektissa on mukana 11 laajaa teollisuusyritystä, 15 pientä ja keskisuurta yritystä sekä yhteensä 10 tutkimusinstituuttia ja yliopistoa. Ohjelman on tarkoitus kestää neljä vuotta (2014-2017) ja sen yhtenä suurimmista rahoittajista toimii Tekes.

F-Secure on vuonna 1988 perustettu suomalaisyritys, joka työllistää nykyään 940 henkilöä 20 toimipisteessä maailmanlaajuisesti. Alun perin F-Secure oli nimeltään Data Fellows. Data Fellows perustettiin tuottamaan räätälöityjä tietokantaratkaisuja teollisuuden asiakkaille ja pitämään koulutuksia tietokoneenkäyttäjille. 1990-luvulla yritys keskittyi virustorjuntaohjelmistojen tuottamiseen ja 1999 Data Fellows muutti nimensä F-Secureksi sekä listautui Helsingin pörssiin. (F-Secure, 2014)

2000-luvun alussa F-Secure alkoi laajentaa toimintaansa mobiililaitteiden tietoturvamarkkinoille ja muutti myös liiketoimintastrategiansa keskittymään virustentorjuntaan. Vuonna 2005 F-Securesta tuli nopeimmin kasvava virustentorjunta-alan pörssiyhtiö. Samana vuonna ensimmäinen mobiililaitteille suunnattu virustentorjuntaratkaisu julkaistiin Nokialle jakeluun ja ensimmäistä virustentorjuntapalvelua mobiililaitteille alettiin jakaa matkapuhelinoperaattori Elisan kautta. 2000-luvun puolen välin jälkeen F-Secure laajeni Aasian markkinoille, sekä sopi sadannen palveluntarjoajasopimuksensa taiwanilaisen verkkopeliyhtiön kanssa. 2007 F-Secure julkaisi tietoturva palveluna –konseptin yritys- ja kuluttaja-asiakkaille ja kasvatti kokonaistuottoaan 20 prosenttia. (F-Secure, 2014)

2010-luvulla F-Securen kasvun edistäjänä toimi Saas-liiketoimintamalli (engl. software as a service = ohjelmistoja palveluna -liiketoimintamalli), joka mahdollisti liiketoiminnan vahvan kasvun jatkumisen. Vuonna 2013 yritys julkaisi Freedomen, Younited-pilvitallennuspalvelun ja Keyn. (F-Secure, 2014) Younited myytiin vuoden 2015 alussa Synchronosille F-Securen keskittyessä tieto- ja yksityisyydensuojaratkaisuihin.

Freedome on yksityisyydensuojasovellus, joka mahdollistaa turvallisen ja anonyymin tavan selata internetiä sekä virtuaalisijainnin asettamisen. Se suojaa käyttäjän internetyhteyden VPN:llä, jolloin esimerkiksi julkisten langattomien verkkojen käyttö turvallisesti on mahdollista, kun laitteen tiedot pysyvät salassa. Virtuaalisijainti mahdollistaa esimerkiksi käyttäjän ulkomailla oleskellessa käyttävän suomalaisia internetsivustoja, jotka ovat estäneet käytön ulkomaalaisista IP-osoitteista. Freedomen mobiilisovelluksen mukana tulee myös App Security, virusskanneri, joka suojaa laitetta haitallisilta sovelluksilta, viruksilta ja vakoiluohjelmilta. (F-Secure, 2014)

Key on salasanageneraattori, joka muistaa tunnukset ja salasanat käyttäjän puolesta. Key-sovelluksessa on yksi pääsalasana, jonka taakse voi tallentaa eri palveluiden salasanoja, tunnuksia ja muita kirjautumistietoja, jolloin eri palveluissa käytettyjä tietoja ei tarvitse aina tallentaa selaimen muistiin. Key täyttää käyttäjän puolesta salasanat automaattisesti eri palveluiden kirjautumissivuilla,

jolloin käyttäjän ei itse tarvitse tietää generoituja salasanoja. Key toimii Android-laitteilla sekä PC- ja Mac-koneilla. (F-Secure, 2014)

Keyn ja Freedomen lisäksi F-Secure tarjoaa tietoturvaratkaisuja niin yrityksille kuin yksityisille käyttäjille. Yksityisasiakkaille on tarjolla F-Secure SAFE, joka on kaikki käyttäjän laitteet suojaava tietoturvaratkaisu. SAFE:n avulla käyttäjä pystyy suojaamaan kaikki älylaitteet haittaohjelmilta, hakkereilta, tietomurroilta ja muilta verkon vaaroilta, päättää mitä sisältöjä lapset näkevät ja milloin heillä verkon käyttö on sallittua. SAFE mahdollistaa myös kadonneen tabletin tai älypuhelimen jäljittämisen. SAFE:n lisäksi F-Secure tarjoaa Internet Securityn, joka mahdollistaa tietokoneella turvallisen internetselailun. Internet Security suojaa haittaohjelmilta, hakkereilta ja identiteettivarkauksilta, sekä auttaa suojaamaan lapsia verkon haitallisilta sisällöiltä. (F-Secure, 2014)

Perinteisen ohjelmistoalan ollessa murroksessa F-Secure on päivittänyt strategiansa tavoitteet vastaamaan nykypäivän tarpeisiin sopivammiksi. Yhtiö on määritellyt nykystrategian perustuen kolmeen tietoturvamarkkinoita ohjaavaan trendiin, joita ovat:

> ”Uudet laitteet ja käyttötapojen muutos. Uusien laitteiden käyttäjämäärien nopea kasvu muuttaa internetin käyttötapoja. Jatkossa henkilökohtaisen sisällön, digitaalisten muistojen ja maineen suojaaminen ja siihen käytetty aika on tärkeämpää kuin fyysisen laitteen turvaaminen.
>
> Pilviteknologia. Tulevaisuudessa suurin osa tiedosta ja palveluista sijaitsee yhdessä tai useammassa pilvessä. Kuluttajilla ja yrityksillä on käytössä useita pilvipalveluita, minkä johdosta yhä käyttäjäystävällisempiä ja turvallisempia pilvipalveluita tullaan tarvitsemaan. Myös tietoturva siirtyy pilveen.
>
> Kuluttajat ja omat laitteet. Sovellukset, joista kuluttajat pitävät, päätyvät jatkossa yhä useammin myös yrityskäyttöön. Tämä tulee asettamaan erilaisen vaatimustason käyttäjäystävällisyydessä myös yrityskäyttöön suunnitelluille sovelluksille. Sekä ohjelmistoille että laitteille asetetaan samat vaatimukset huolimatta siitä, ovatko ne yksityisessä vai ammatillisessa käytössä.” (F-Secure 2014)

Nykyään yhtiö keskittyy suojaamaan enemmän ihmisten identiteettiä, tietoa ja laitteita mobiililaitemaailmassa, koska valtaosa laitemyynnistä tulee mobiililaitteista.

4.2 Tutkimusongelma ja tutkimuskysymykset

Tutkimusongelma muodostettiin empiiristä tutkimusosaa tukemaan. Tutkimuskysymykset määriteltiin tutkimusongelman ratkaisemisen avuksi.

Tutkimusongelma:

- Miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön?

Tutkimusongelmaa tukevat tutkimuskysymykset:

1. Mitä on mobiililaitteiden kyberturvallisuus ja miten sitä voidaan hallita?

2. Minkälaisia kriittisiä käyttökokemuksia esiintyy Freedomen käytössä ja miten ne vaikuttavat sovelluksen omaksumiseen ja jatkuvaan käyttöön?

Tutkimusongelmaan pyrittiin vastaamaan tutkimuskysymysten avulla. Ensimmäinen tutkimuskysymys valittiin, jotta ymmärretään tutkittavan kohteen taustaa. Freedome on mobiililaitteiden kyberturvallisuuden hallintaan kehitetty ratkaisu, joten yhtenä suurena osa-alueena oli ymmärtää mitä mobiililaitteiden kyberturvallisuus on ja miten sitä voidaan hallita. Toisen tutkimuskysymyksen tarkoituksena oli selvittää, minkälaisia kriittisiä käyttökokemuksia Freedomen käytössä esiintyy. Kysymys laadittiin, jotta voitiin pyrkiä vastaamaan kysymykseen, miten kriittiset käyttökokemukset vaikuttavat sovelluksen omaksumiseen ja jatkuvaan käyttöön.

4.3 Tutkimus- ja tiedonkeruumenetelmät

Toimeksiannon vuoksi tutkimus oli rajattu koskemaan ainoastaan Freedomea ja sen käytössä ilmenneitä merkittäviä käyttökokemuksia. Tutkimusmenetelmäksi valikoitui luonnollisesti tapaustutkimus, koska haluttiin saada tietoa ainoastaan Freedomesta, eikä pyritty luomaan yleistettäviä johtopäätöksiä. Hirsjärven ym. (2003) mukaan tapaustutkimuksesta saadaan yksityiskohtaista ja intensiivistä tietoa yksittäisestä tapauksesta.

Järvinen & Järvinen (1995) kirjoittavat kirjassaan case-tutkimuksen (tapaustutkimuksen) saaneen kritiikkiä muun muassa siksi, että (1) siitä puuttuu tieteellinen kurinalaisuus, (2) yhden tapaustutkimuksen perusteella ei voi yleistää, (3) se vaatii paljon resursseja sekä (4) hyviä tapaustutkijoita on vaikea löytää. Tässä tutkimuksessa pyrittiin nimenomaan tietynlaiseen kurittomuuteen, jotta tutkittavilta saatiin mahdollisimman vapaamuotoisesti ilmaistuja tietoja. Tutkimus ei pyrkinyt yleistettävyyteen ja tutkimus pidettiin yhdessä tapauksessa, jolloin se ei vaatinut liian paljon resursseja. Tutkimusaiheeseen, tiedonkeruutapaan sekä viitekehyksenä toimivaan teoriaan pyrittiin tutustumaan mahdollisimman tarkasti, jotta tutkijalla oli hyvä taustatietämys datan keräämisen ja analysoinnin suhteen.

Järvisen ja Järvisen (1995) mukaan kvalitatiivisessa tutkimuksessa haastattelua pidetään usein tiedonkeruun päämenetelmänä. Myös tässä tutkimuksessa tiedonkeruun päämenetelmänä käytettiin haastattelua ja sen apumetodina käytettiin CIT-menetelmää. Hirsjärvi ym. (2003) määrittelevät haastattelun suurimmaksi eduksi sen joustavuuden aineiston keruussa ja että haastattelu toimii hyvin, kun vastaaja halutaan nähdä tutkimustilanteessa subjektina ja kun ihminen on tutkimuksessa merkityksiä luova ja aktiivinen osapuoli. Tähän tutki-

mukseen tiedonkeruumenetelmäksi valittiin haastattelu, koska tutkittavalle haluttiin antaa mahdollisimman vapaa tapa ilmaista vastauksia. Tiedonkeruumenetelmäksi olisi soveltunut myös kyselytutkimus, mutta siinä olisi ollut rajoitteena saada liian suppeita vastauksia. Haastattelussa tutkittava voi kertoa itsestään ja aiheestaan laajemmin, kuin mitä tutkija pystyy ennakoimaan (Hirsjärvi ym., 2003). Kyselyssä ei myöskään ole mahdollisuutta varmistua miten vakavasti vastaajat ovat suhtautuneet tutkimukseen ja aineisto voi olla hyvin pinnallista (Hirsjärvi ym., 2003). Haastattelun heikoiksi kohdiksi Hirsjärvi ym. (2003) sekä Järvinen ja Järvinen (1995) listaavat, että haastattelujen toteutus ja suunnittelu vaatii paljon aikaa ja se on hyvin herkkä menetelmä, jolloin vastaaja voi kokea sen tungetteluna tai toisaalta pyrkii vastaamaan sosiaalisesti suotavalla tavalla. Nämä heikkoudet pyrittiin huomioimaan jo haastattelurunkoa suunnitellessa ja koehaastatteluissa.

Tutkimushaastattelut voidaan jakaa avoimiin, puolistrukturoituihin ja strukturoituihin sen mukaan, kuinka strukturoitu ja muodollinen (tarkasti säädelty) haastattelutilanne on. Hirsjärven ym. (2003) mukaan täysin strukturoidussa haastattelussa ennalta laaditut kysymyssarjat esitetään tietyssä järjestyksessä, kun taas strukturoimattomassa haastattelussa haastattelijalla on mielessään vain aihe tai alue ja keskustelu etenee vapaasti rönsyillen aihepiirin sisällä. Puolistrukturoidussa- eli teemahaastattelussa Hirsjärven ym. (2003) mukaan on tyypillistä, että haastattelun aihepiirit ja teema-alueet ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat. Hirsjärvi ja Hurme (2011) sekä Rautio (2007) kirjoittavat, että teemahaastattelussa haastateltaville on yhteistä, että he ovat kaikki kokeneet saman tietynlaisen tilanteen, eli se sopii erittäin hyvin tapaustutkimukseen.

Tämän tutkimushaastattelun toteutukseen sopi kaikista parhaiten puolistrukturoitu- eli teemahaastattelu, jossa käytettiin haastattelurunkoa, mutta jätettiin tilaa myös lisäkysymyksille ja -tarkennuksille. Haastattelut toteutettiin yksilöhaastatteluna puhelimitse, jotta haastateltavan maantieteellinen sijainti ei vaikuttanut haastatteluihin. Freedomea käytetään myös paljon suomen rajojen ulkopuolella, joten puhelinhaastattelulla haluttiin sulkea pois este, että ulkomailla asuvan haastattelua ei voida toteuttaa. Haastattelupuhelut tallennettiin, jonka jälkeen ne litteroitiin ja tulokset analysoitiin.

Haastattelun apuna käytetty CIT-menetelmä on alun perin John C. Flanaganin (1954) kehittelemä metodi tutkia kriittisiä kokemuksia, tapahtumia ja tilanteita. CIT-menetelmä voidaan suomentaa esimerkiksi kriittisen tapauksen tekniikaksi, tai merkityksellisen tapahtuman menetelmäksi, mutta tässä tutkimuksessa käytetään termiä CIT-menetelmä. Se on tiedonkeruu-, analysointi- ja havaintojen luokittelumetodi, jossa keskitytään ainoastaan tutkittavan asian kannalta kriittisten tapahtumien tutkimiseen.

Salon (2014) mukaan CIT-menetelmää on aiemmissa tutkimuksissa käytetty tutkimaan itsepalveluteknologioita, internetsivustoja, verkkokauppoja, verkkoasioimista, matkailupalveluja internetissä, sähköpostia ja tietokoneen yrityskäyttöä, mutta vain muutama tutkimus käsittelee mobiililaitteiden käyttöä. Gremler (2004) on toteuttanut palvelututkimuksen CIT-menetelmää käyttäen.

Hän esittelee artikkelissaan CIT-menetelmän hyviä puolia ja siihen kohdistettua kritiikkiä, sekä käy läpi palvelututkimuksen ja sen tulokset.

Hyvänä puolena Gremler (2004) mainitsee tiedon olevan johdattelematonta, koska CIT-menetelmä antaa vastaajan vastata omasta näkökulmastaan. Tieto on myös näin ollen rikasta, koska vastaaja saa itse määritellä mitkä tapahtumat ovat hänen mielestään kriittisiä tutkittavan tapauksen kannalta. CIT-menetelmällä tutkittaessa vastaajaa ei pakoteta mihinkään kehykseen tai kaavaan, vaan tieto tulee kokonaan vastaajan näkökulmasta. CIT-menetelmä soveltuu hyvin tutkimukseen, jossa (1) tutkittava aihe on niukasti dokumentoitu, (2) halutaan tuottaa tarkkoja ja syvällisiä merkintöjä tapahtumista, (3) halutaan tutkia tarkemmin jotain vähemmän tutkittua ilmiötä, (4) halutaan perusteellista ymmärrystä selittämään tai kuvaamaan ilmiötä ja (5) kun halutaan tutkimuksen tuottavan rikasta ja monipuolista tietoa menetelmällä, joka ei ole kulttuurisidonnainen. (Gremler, 2004)

Gremler (2004) listaa artikkelissaan CIT-menetelmän huonoiksi puoliksi muun muassa sen luotettavuuden ja pätevyyden, koska kerätyt tarinat ovat tutkijan tulkittavissa, jolloin väärintulkinnan mahdollisuus on olemassa. Tutkija voi esimerkiksi tulkita sanojen merkityksiä toisin kuin tutkittava on ne tarkoittanut. Usein CIT-menetelmää käytetään takautuvasti, jolloin tilanteet ovat tutkittavan oman muistin varassa, jolloin niissä saattaa ilmetä epäjohdonmukaisuutta ja unohtamista. Gremler (2004) mainitsee artikkelissaan huonoksi puoleksi myös CIT-menetelmän vaativuuden, se vaatii vastaajalta aikaa ja sitoutumista, joten se saattaa vaikuttaa alhaisesti vastausprosenttiin. Kuitenkin lopuksi Gremler (2004) toteaa CIT-menetelmän olevan kannattava tutkimusmenetelmä, koska siihen on ehdotettu suhteellisen vähän muutoksia 50 vuodessa.

4.4 Haastattelurungon laatiminen

Haastattelun tavoitteena oli saada tietoa, jonka pohjalta voidaan selvittää miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön. Tutkimusmateriaali kerättiin puhelinhaastatteluilla käyttäen puolistrukturoitua haastatteluasetelmaa. Haastattelun perusjoukko oli kaikki Freedomen käyttäjät, jotka eivät olleet aiemmin käyttäneet mitään VPN-salauspalvelua ja tietosuojapalvelua yhdistävää sovellusta mobiililaitteessaan. Perusjoukosta valittiin otokseksi 9 henkilöä haastatteluihin. Haastateltavat etsittiin internetin keskustelupalstojen ja sosiaalisen median kautta. Keskustelupalstoille ja sosiaaliseen mediaan välitetty viesti on liitteessä 1. Viestistä ilmeni tutkimuksen tarkoitus, sekä haastatteluun osallistumisesta kiinnostuneita pyydettiin ottamaan tutkijaan yhteyttä.

Hirsjärven ym. (2003) mukaan teemahaastattelussa ei yleensä käytetä tarkkaa kysymyslistaa, eikä tarkkaan rajattua suunnitelmaa miten kysymykset esitetään. Hirsjärvi ja Hurme (2011) mainitsevat kirjassaan, että suunnitteluvaiheessa tutkijan tulee tietää millaisia päätelmiä hän aikoo aineiston pohjalta tehdä, joten teemahaastattelun suunnitteluvaiheen tärkein osa on haastattelutee-

mojen suunnittelu. Tähän tutkimukseen koostettiin haastattelurunko ja kysymyslista, koska haluttiin varmistua, että tietoa saadaan riittävästi ja että kerätty tieto antaa mahdollisimman hyvin vastauksia (kriittisiä käyttökokemuksia) tutkimusongelman ratkaisuun.

CIT-menetelmällä tutkittaessa on erittäin tärkeää perehtyä kysymysten muotoiluun ja sanamuotoihin. Ojasalo, Moilanen ja Ritalahti (2009) ovat määritelleet, että CIT-menetelmällä tutkittaessa oleellista on selvittää (1) toiminta (mitä tapahtui), (2) henkilöt (kuka teki ja mitä), (3) paikka (missä tapahtui), (4) aika (milloin tapahtui), (5) oma arvio (kuinka haastateltava itse arvioi tapahtuman, (6) arvion perusteet (mikä haastateltavan mielestä teki tilanteesta onnistuneen tai epäonnistuneen) ja (6) seuraukset (kuinka haastateltava reagoi tilanteeseen). Salo (2014) on tehnyt monien aiemmin tehtyjen tutkimusten pohjalta havainnon, että CIT-tekniikalla tutkittaessa on hyvä pohjustaa kysymys niin, että vastaajaa kehotetaan miettimään rauhassa ja palauttamaan mieleen erityisen hyvä tai erityisen huono kokemus liittyen tutkittavaan aiheeseen. Salon (2014) ja Gremlerin (2004) tekemien tutkimusten, Ojasalon ym. (2009) ohjeiden sekä tässä tutkimuksessa käytetyn viitekehyksen ja tutkimustehtävien pohjalta muodostettiin haastattelurunko. Liitteessä 2 on haastattelurunko, johon on kirjattu tutkimuksen tarkoitus ja taustatiedot sekä listattu haastattelukysymykset.

Kysymykset muotoiltiin seuraavanlaisesti:

1. Demografiset tekijät: sukupuoli, ikä, päätoiminen asema (opiskelija, töissä, työtön, eläkeläinen jne.)?
2. Kuinka kauan olet käyttänyt Freedomea?
3. Missä laitteissa (merkki ja malli) käytät Freedomea?
4. Mieti rauhassa yksittäinen tilanne, jolloin sinulla on ollut mielestäsi merkittävän positiivinen tai negatiivinen käyttökokemus Freedomen käytössä. Käytä muisteluun kunnolla aikaa.
    a. Oliko kokemus negatiivinen vai positiivinen?
    b. Minkä laitteen käytössä se on tapahtunut?
    c. Missä havaitsit tapahtuman (esimerkiksi töissä, matkoilla tai kotona)?
    d. Milloin havaitsit tapahtuman?
    e. Kuvaile tapahtumaa omin sanoin.
    f. Mikä tarkalleen ottaen aiheutti kokemuksen positiivisuuden / negatiivisuuden?
    g. Millaisia seurauksia tapahtumalla oli käytön kannalta?
    h. Kuinka merkittävä kokemus oli käytön jatkumisen kannalta?
5. Tuleeko sinulle mieleen toista merkittävää kokemusta? (Toistetaan tarvittaessa kysymys numero 4:n alakysymykset.)
6. Jos olet käyttämässä 2 viikon kokeilujaksoa nyt, aiotko jatkaa käyttöä vielä ilmaisen jakson päätyttyä? Miksi?

Rautio (2005) mukaan haastattelutilanteessa aluksi on hyvä kertoa haastattelun tarkoitus, mihin tuloksia käytetään ja että haastattelu mahdollisesti nauhoi-

tetaan. Haastattelutilanne alkoi aina haastateltavan informoinnilla että haastattelu tallennetaan. Sen jälkeen esiteltiin hieman tutkimusta ja edettiin haastattelukysymyksiin.

Haastatteluosuus alkoi selvittämällä demografiset tekijät (kysymys 1). Kysymyksellä numero 2 pyrittiin saamaan taustatietoa, jotta voidaan määritellä missä vaiheessa omaksumisprosessia käyttäjä ajallisesti on. Kysymyksellä numero 3 pyrittiin saadaan tietoa eroavatko eri laitteissa ilmenneet kriittiset käyttökokemukset toisistaan, ja onko käyttäjällä kokemusta Freedomen käytöstä monessa eri laitteessa. Kysymys 4 on pääkysymys, jolla pyrittiin selvittämään kriittisiä käyttökokemuksia. Tässä kysymyksessä oli tärkeää noudattaa samaa kysymyksen johdantoa kaikilla haastateltavilla, antaa vastaajalle aikaa miettiä vastaustaan rauhassa sekä pitää huoli, että kaikkiin alakysymyksiin saadaan vastaus. Kolmas kysymys toistettiin tarvittaessa, jos haastateltavalla oli enemmän kuin yksi merkittävä kokemus liittyen Freedomen käyttöön (kysymys numero 5). Kysymys numero 6:llä selvitettiin miten tutkittava suhtautuu Freedomen käytön jatkamiseen.

4.5 Tutkimushaastattelun toteutus

Tutkimushaastattelun toteutuksessa otettiin huomioon haastatteluista sopiminen sekä haastateltavalle haastattelun keston arvioiminen etukäteen. Jotta haastattelun kestoa voitiin arvioida, tehtiin ensin kaksi koehaastattelua. Koehaastatteluista saatua tietoa käytettiin tutkimusmateriaalin tavoin. Hirsjärven ym. (2003) mukaan haastattelijan on varauduttava puheliaisiin sekä niukkasanaisiin vastaajiin, jolloin on hyvä tehdä joitain koehaastatteluja ennen varsinaista haastattelua. Hirsjärvi ym. (2003) mainitsevat koehaastattelujen myös antavan myös mahdollisuuden kontrolloida haastatteluteemojen toimivuutta.

Koehaastatteluilla pyrittiin saamaan arvio haastattelun kestosta sekä tietoa, olivatko kysymykset oikeanlaiset tukemaan tutkimusongelmaan vastaamista. Myöhemmin haastattelutilanteissa seurattiin (koehaastatteluiden avulla muokattua) haastattelurunkoa, ja näin ollen pystyttiin varmistamaan, että saadaan tarpeeksi tutkimuskysymyksiin vastaavaa tietoa. Haastateltavan kanssa sovittiin aika puhelinhaastattelulle ja kerrottiin myös arvio haastattelun kestosta, jotta hän osasi varata riittävästi aikaa puheluun. Haastattelussa kysymyksen 3 esittämisessä tuli olla tarkka, kuten aiemmin CIT-menetelmästä kerrottaessa mainittiin, on tärkeää, että kysymykset ja saatteet ovat tietynlaisia. Vaikka haastattelu olikin puolistrukturoitu, tutkijan tuli pitää huoli, että kysymys 3 esitetään kaikille haastateltaville samalla saatteella. Esittelyjen ja tarkentavien kysymysten suhteen tutkija käytti omaa harkintaansa sanavalinnoissa.

Rautio (2005) ohjeistaa haastattelutilanteeseen, että tutkijan on hyvä välttää torjumasta tutkittavan kertomia sivuseikkoja ja sen sijaan kärsivällisesti odottaa, että puhuja saa kerrottua asiansa loppuun. Rautio (2005) antaa ohjeeksi myös tutkijalle käyttää myönteistä ohjailua, eli kehotteita (engl. probe) kuten että voisitko kertoa tarkemmin tai miksi niin kävi. Haastateltaville annettiin

mahdollisuus kertoa ensin kokemus, jonka jälkeen tarkentavilla kysymyksillä saatiin lisätietoja. Jos haastateltavalle ei tullut mieleen yhtään kokemusta, häntä ohjeistettiin miettimään ensin yleisesti kaikkia Freedomen käytössä ilmenneitä kokemuksia ja sen kautta miettimään niistä merkittäviä. Toinen tekniikka oli kehottaa vastaajaa miettimään aikajanallisesti käyttökokemuksia, esimerkiksi kysyä ilmenikö mitään merkittävää käyttökokemusta heti käyttöönottamisen jälkeen.

5 TUTKIMUKSEN TULOKSET

Luvussa viisi esitellään tutkimuksen tulokset. Ensin käydään läpi haastatteluissa ilmenneet positiivisina ja negatiivisina koetut kriittiset käyttökokemukset. Sen jälkeen verrataan tutkimustuloksia aiemmin tehtyihin tutkimuksiin ja sijoitetaan tutkimustulokset innovaation diffuusioteoriaan. Lopuksi käsitellään tutkimustulosten yhteenveto.

Tutkimushaastatteluun osallistuneet olivat kaikki Freedomen käyttäjiä, joten he olivat jo aloittaneet omaksumisprosessin. Suurin osa vastaajista oli käyttänyt Freedomea 1-3 viikkoa, eli voidaan olettaa, että he olivat vielä omaksumisprosessin alkupäässä. Vastaajista vain yksi käytti maksullista versiota, muut vastaajat käyttivät jotain ilmaista kokeiluversiota.

Tutkimustulokset ovat jaettu positiivisina ja negatiivisina koettuihin käyttökokemuksiin. Positiiviset ja negatiiviset kokemukset ovat jaettu vielä sen mukaan, mihin sovelluksen ominaisuuteen ne liittyvät.

5.1 Positiivisina koetut käyttökokemukset

Positiivisina kokemuksina haastatteluissa toistui käyttökokemukset liittyen virtuaalisijainnin asettamiseen, seurannan estoon sekä yhteyksien suojaamiseen. Seuraavissa alaluvuissa analysoidaan vastauksissa mainittuja kokemuksia ja käydään läpi sovelluksen ominaisuuksia, joihin mainitut kokemukset liittyivät.

5.1.1 Virtuaalisijainnin asettaminen

Virtuaalisijainti mahdollistaa muun muassa maakohtaisesti rajoitettujen internet-palveluiden käytön. Maakohtaisesti rajoitettuja palveluja ovat tv-kanavien omat nettitelevisiot, tai ainakin osittain niiden sisällöt. Suomalaisista tv-kanavista ainakin MTV3, Yle sekä Nelonen tarjoavat videosisältöä omissa nettitelevisiopalveluissaan. Maakohtaisesti rajoitettuja ovat myös maksulliset tilausvideopalvelut, jotka tarjoavat elokuvia, tv-sarjoja ja dokumentteja suoratoistona

asiakkailleen. Suosittuja tilausvideopalveluja ovat muun muassa Netflix, HBO ja Viaplay. Virtuaalisijainnin käyttäminen on kuitenkin kyseenalaista, kun sitä käytetään kiertämään maksullisten palveluiden maakohtaisia rajoituksia, koska oikeudet ohjelmiin myydään markkina-alueittain. Kuningaskuluttaja (2014) kirjoittaa Netflixin asiakaspalvelun kertoneen maakohtaisten estojen kiertämisen olevan vastoin Netflixin käyttöehtoja, joissa mainitaan että käyttäjä sitoutuu siihen, ettei hän kierrä, poista, muuta, deaktivoi, heikennä tai estä Netflix-palvelun sisällön suojauksia. Myös muiden tilausvideopalveluiden käytössä maakohtaisten estojen kiertäminen on vastoin käyttöehtoja. Kuningaskuluttajan (2014) artikkelissa mainitaan myös, että Netflixin Suomen viestintää hoitavan Cocomms-viestintätoimiston mukaan kyseessä ei kuitenkaan ole rangaistava teko, mutta käyttöehdoissa mainitaan, että mikäli käyttäjä ei hyväksy näitä ehtoja, ei hänen tule käyttää Netflix-palvelua. Näistä voidaan tehdä päätelmä, että maakohtaisen suojauksen kiertäminen ei ole laitonta, mutta palveluehtojen vastaista kyllä, joten kiertäminen jää käyttäjän omalle vastuulle. Alkuvuodesta 2015 Torrentfreak (2015) uutisoi, että Netflix pyrkii estämään sijaintipaikan vaihtavien salattujen VPN-yhteyksien käytön, jotta videosisällöt pysyisivät maakohtaisesti rajoitettuina. Vielä esto ei ole tullut käytäntöön, eikä voida olla varmoja saadaanko tällaista estoa edes toteutettua.

Moni vastaaja kertoi käyttävänsä virtuaalisijaintia voidakseen katsoa maakohtaisesti rajoitettuja videosisältöjä. Virtuaalisijainti mainittiin myös lentotarjousten etsimisessä, jolloin eri sijainnilla palveluntarjoajilta saatiin eri hinnat lentolopuille.

> ”Positiivisena mä näen ton lokaatiopalvelun. Koska nythän mä pystyn vaihtaan vaikka Usan sijainniks niin mä pystyn kattoo Netflixiä niinku Usan palvelimen kautta. Ja nehän on erilaiset ne ohjelmat.” H1

> ”Mä en muista mitä mun piti kahtoo, olin Euroopassa, muistaakseni Puolan puolella sillon niin piti kahtoo Yleltä. Halusin kahtoo läppärillä alun perin mutta sitten mulla oli tuo Freedome tuossa puhelimessa ja siinä saa sen virtuaalipaikan sijotettua suomeen nii pääsee käsiks sitte siihen sisältöön. Se oli kanssa sellanen mukava. Elikkä aluerajotukset sai pois tolla.” H4

> ”Kokeilin onko sillä maa-asetuksella vaikutusta noihin lentodiileihin netissä kun olin varaamassa lentoja. Se kokemus siitä oli positiivinen sillon. ” H3

Tapahtumien positiivisuuden aiheutti virtuaalisijainnin asettamisen helppokäyttöisyys sekä ominaisuuden toimivuus. Sovelluksen käyttöön virtuaalisijainnin asettaminen ei juuri vaikuttanut. Vastauksissa mainittiin myös, että virtuaalisijainnin ensimmäisen kokemuksen jälkeen vastaaja alkoi enemmän käyttää ominaisuutta, sekä etsiä sille myös muita käyttötarkoituksia. Tietokoneen virtuaalisijainnin saa muutettua myös internetselaimen avulla, vastauksista kuitenkin ilmeni, että Freedomen mobiiliversio on helpompi ja turvallisempi käyttää, kun selaimen tarjoama virtuaalisijainnin asettaminen.

> ”Ei varsinaisesti mitään seurauksia sinänsä, että edelleenkin käyttelen sovellusta ja etsin sillä erilaisia käyttötarkoituksia semi-aktiivisesti.” H3

> ”No mä rupesin ehkä sen jälkeen hyödyntää sitä enemmän sitä ominaisuutta. Olin mä kokeillu sitä mielenkiinnosta. Esimerkiksi Youtubea kun kahto niin vaihto virtuaalipaikkaa nii sait vaikka japaninkielisiä mainoksia sinne. Ihan kokeilumielessä. Netflixiäkin periaatteessa pystyy kanssa käyttää. Jenkkien Netflixiä sillee vaivattomasti, jos haluaa. -- Ihan kätsy vaikka selaimellekin on saatavissa niitä mutta ne on vähän heikosti toimivia ja sitte se turvallisuuspuoli on sellanen toissijanen aspekti niissä softissa nii mielummin käytän sitte puhelimen kautta Freedomen avulla.” H4

Merkittävät käyttökokemuksen, joissa virtuaalisijainnin asettaminen mainittiin, mainittiin olevan jokseenkin merkittävä tai merkittävä käytön jatkumisen kannalta. Yksi vastaaja mainitsi, ettei kokemus ollut kovinkaan vaikuttava käytön jatkumisen kannalta. Osa vastaajista myös koki ominaisuuden tuovan lisäarvoa sovellukselle.

5.1.2 Seurannanesto

Kuluttajien internetin käyttöä seurataan muun muassa evästeiden avulla. Evästeet sisältävät esimerkiksi käyttäjän IP-osoitteen, kellonajan, käytetyt sivut, selaintyypin, mistä osoitteesta käyttäjä on tullut kyseiselle verkkosivustolle, miltä palvelimelta käyttäjä on tullut sivuille sekä mistä verkkotunnuksesta käyttäjä on tullut verkkosivuille. Koska evästeet ovat täydellisiä paketteja kohdennettua markkinointia ajatellen, näiden tietojen myymistä harjoitetaan paljon. Seurannanesto on ominaisuus, joka piilottaa käyttäjän IP-osoitteen ja estää seurantaevästeet ja vakoiluohjelmat, eli estää kolmannen osapuolen tiedonkeräysyrityksiä. Tämä ominaisuus mainittiin merkittävissä kokemuksissa aina positiivisena.

Vastauksissa mainittiin sovelluksen ilmoittaneen kuinka monta seurantayritystä on estetty ja että on yllättävää miten monta seurantayritystä sovellus on estänyt. Ominaisuuden kuvailtiin herättävän turvallisuudentunnetta ja hyvää oloa siitä, että laitteessa on näkyvä tietosuoja. Vastaajat kuvailivat, että on hyvä nähdä mitä seurannanesto-ominaisuus on tehnyt ja kuinka monta seurantayritystä on estetty.

> ”No ehkä se että ei ollut ajatellut esimerkiksi että kun surffailee netissä, et miten paljon niitä seurantayrityksiä, tai seurantoja tapahtuu. Kun nyt kun se Freedome on ollu käytössä niin se näyttää sen lukumäärän, että montako seurantayritystä on esimerkiks estetty. Niin olen siitä ollut oikeesti todella yllättynyt miten se määrä voi olla viikossakin niin suuri määrä ja se miten mä en oo aikasemmin tajunnu tommosta ylipäätään.” H1

Yleisesti ottaen kokemusten positiivisuuden aiheutti seurannanesto-ominaisuuden olemassa olo ja se että tietoturvallisuus on ajankohtainen aihe, joka tekee ominaisuudesta hyvän ja mielenkiintoisen. Positiivisuutta herättivät sovelluksen ilmoitukset siitä, kuinka monta seurantayritystä sovellus on estänyt.

Vastauksissa mainittiin, että kun laitteesta itsestään puuttuu näkyvä tietosuoja, positiivisuutta herättää selkeästi havaittava seurannanesto.

> ”Mun mielipiteeni ja mielikuvani on se että koska on menossa just tämä netinkäytön suuri turvallisuushypeaalto niin sehän tekee tällasista tuotteista niin hyviä ja kiinnostavia.” H3

> ”No on se kyllä hyvä että se suojaa se suojaa tota laitetta, kun ei tollasessa padissa oikeen oo muuten mitään suojaa niin se on kiva nähdä että sellanen suoja on. -- No kyllä se on merkittävää (seurannanesto käytön jatkumisen kannalta) ja mä nään merkittävänä asiana.” H6

Käytön jatkumisen kannalta kaikki vastaajat kokivat, että seurannanesto-ominaisuuteen liittyvä kokemus oli merkittävää käytön jatkumisen kannalta.

Ei kuitenkaan voida tietää, ovatko vastaajat täysin ymmärtäneet mitä seurannan esto tarkoittaa. Sovellus ilmoittaa seurannan eston kohdalla tiedon: ”tästä näet, miten monta kertaa seurantaa harjoittavat yritykset (kuten mainostajat) ovat yrittäneet kerätä tietoja sinusta.” Ei ole ilmoitettu mitä kaikkea sovelluksen ilmoittama lukumäärä pitää sisällään. Haastattelussa ei kysytty, mitä vastaajat ymmärtävät seurannan eston tarkoittavan, joten ei voida olla varmoja ymmärsivätkö kaikki vastaajat sen toiminnan samalla tavalla.

5.1.3 Yhteyksien suojaus

Yhteyksien suojausominaisuus salaa käyttäjän verkkoliikenteen, jolloin kolmas osapuoli ei pysty vakoilemaan yhteyttä avoimessa verkossa. Freedome muodostaa yhteyden internetiin F-Securen oman pilven kautta, jolloin laitteen tiedot muuttuvat pilvessä kryptatuksi, jos kolmas osapuoli yrittää niitä lukea. Tämä ominaisuus mainittiin kriittisissä käyttökokemuksissa positiivisena.

Kokemuksen positiivisuuden aiheutti F-Securen luotettava maine sekä luottamus yritykseen, jolloin myös sovellus ja sen ominaisuudet koetaan luotettavina. Sovelluksen käytön kannalta kokemus aiheutti huolettomampaa avointen langattomien verkkojen käyttöä, koska käyttäjän ei enää tarvitse miettiä kenen verkkoon hänen laitteensa on kytkettynä.

> ”No ehkä se ku käyttää suojaamatonta julkista langatonta verkkoyhteyttä niin ei tarvii murehtia siitä. Murehtia että näkee joku. Teen kuitenki aika paljon työhommia ja pankkiasioita puhelimen kanssa nii ei tarvii siitä murehtia sitte, kun tietää että se on kryptattu se liikenne kokonaan. -- Yliopiston avoimessa verkossa joku päivä olin ja rupesin siirtää rahaa kaverille, niin siinä sitten tuumailin samalla kun siirsin, että ompas hyvä nii ei tarvii vaihtaa 4g verkkoon. -- (Mikä aiheutti kokemuksen positiivisuuden?) Varmaan hyvin pitkälle se miten paljon luottaa siihen ihan yritykseen, F-Secureen. Itelle ainaki on iskostunu se F-Secure niinku sellasena luotettavana toimijana. Se varmaan oli siinä taustalla että se sai aikaan sen luottamuksen siihen.” H4

Käytön jatkumisen kannalta tapahtuma koettiin hyvin merkittävänä. Vastauksissa mainittiin myös, että jos luottamus jostain syystä horjuisi, myös Freedo-

men käytön arveltiin loppuvan. Tässä tapauksessa palveluntarjoajan sekä sovelluksen ehdottomalla luotettavuudella ja hyvällä maineella on merkittävä rooli käytön jatkumisen kannalta.

5.2 Negatiivisina koetut käyttökokemukset

Negatiivisina koettuja käyttökokemuksia mainittiin enemmän kuin positiivisina koettuja. Negatiivisten kokemusten toistuvuus oli vähäistä, josta johtuen tulokset eivät ole niin yleistettävissä olevia kuin positiivisena mainitut kokemukset. Tapaustutkimuksessa validius voi olla epäselvä, koska voidaan aiheellisesti ajatella, että kaikki ihmistä ja kulttuuria koskevat kuvaukset ovat ainutlaatuisia. Tämän vuoksi perinteiset luotettavuuden ja pätevyyden arvioinnit eivät ole päteviä tapaustutkimusta arvioidessa. (Hirsjärvi ym., 2003) Tässä tutkimuksessa ei myöskään pyritä tekemään yleistettäviä johtopäätöksiä, vaan selvittää merkittäviä käyttökokemuksia Freedomen käytössä.

5.2.1 Sovellus kuluttaa akkua

Negatiivisista kokemuksista eniten mainittiin sovelluksen vievän akkua päällä ollessaan. Sinänsä tämä on hieman erikoista, koska jos laitteeseen on kytketty sovellus, se luonnollisesti kuluttaa toimiakseen hieman laitteen akkua. Oletuksena on ilmeisesti ollut, että sovellus toimisi huomaamattomasti myös akun käytön osalta. Vastauksissa mainittiin, että koska sovellus menee itsekseen päälle, laite kuluttaa enemmän akkua kuin normaalikäytössä. Negatiivisena kokemuksena mainittiin sovelluksen omatoimisesti käynnistyminen, mutta kokemuksen negatiivisuuden aiheutti akun nopea kuluminen.

> ”No akun kuluminen paljon nopeammin. Se että aikaisemmin mulla on nukkumaan käydessä, mä aina yöllä lataan, mulla on yöllä puhelin latauksessa, niin normisti mulla on miltei puolet, ei nyt ehkä ihan, no 35-55 prosentti akkua jälellä kun mä meen nukkumaan. Nyt sitä on paljon vähempi. Nytten oli 25 prosenttia (kello 20:00 illalla).” H1

> ”Ainoo negatiivinen mikä mul on niin on kun mä sammutan sen (Freedomen) niin se menee itestään koko ajan päälle. Välillä tuntuu, että vaikka mä sammutan sen koko ohjelman nii silti se vaan lähtee päälle uudestaan. Ja sitä oon ihmetelly. -- No kyllä se mun mielestä vie enemmän akkua laitteesta kun se on päällä se ohjelma. Että kun on turhaan päällä niin sit se myös syö turhaan sitä akkua.” H6

Kokemuksen negatiivisuuden aiheutti nimenomaan akun nopea kuluminen ja se koettiin käytön kannalta ärsyttävänä. Enemmistö koki akun kulumisen käytön jatkumisen kannalta vain hieman merkittävänä tai ei juurikaan merkittävänä sekä yksi vastasi sen olevan jokseenkin merkittävää. Nämä merkittävät ko-

kemukset eivät kuitenkaan vaikuttaneet merkittävästi sovelluksen jatkuvaan käyttöön.

> ”No en mä nyt sanois, että se kauheen merkittävää on. Kyllä mä aion sitä silti jatkaa.” H1

> ”No ei ehkä tossa nyt ollu niin ongelma, mutta jos olis ollu reissussa nii sillon se olis ollu ongelma ehkä enemmänki. -- Ei se tässä viikon aikana ehkä kun ei oo ollu kun kotosalla nii ei tässä mitää ongelmaa oo ollu.” H9

Akun kestävyys on mainittu vaikuttavan negatiivisesti myös aiemmissa tutkimuksissa. Esimerkiksi Mylonas ym. (2012) epäilevät tutkimustulostensa pohjalta, että yleensä välinpitämätön asenne voi johtua myös laitteen ominaisuuksista viitaten huonoon akunkestävyyteen sekä laitteen yleisen suorituskyvyn heikkenemiseen. Tässä tutkimuksessa akun kestävyyden ei kuitenkaan koettu olevan kovin merkittävää käytön jatkumisen kannalta. Vastauksissa mainittiin myös, että sovelluksesta on enemmän hyötyä kuin haittaa, jolloin käytön jatkaminen on luontevaan.

5.2.2 Sovellus hidastaa internetliikennettä

Freedome on sovellus, joka suojaa internetyhteyksiä, joten sen toiminta voi vaikuttaa yhteyden nopeuteen ja pysyvyyteen. Merkittävissä kokemuksissa mainittiin internetliikenteen hidastuminen ja pätkiminen ohjelman päällä ollessa.

Tapahtumaa kuvailtiin sovelluksen toiminnan käyttökatkona, kun siirrytään langattomasta verkosta matkapuhelinverkkoon, jolloin sovellus käynnistyy automaattisesti uudelleen. Toisena mainittiin internetyhteyden hidastuminen virtuaalisijaintia käytettäessä, jolloin tiedonsiirto kulkee toisen maan pilvipalvelimen kautta. Yhteyden huomattiin olleen hitaampi esimerkiksi silloin, kun virtuaalisijainti on kytketty päälle ja laitteeseen ladataan videota tai tiedostoja ladataan pilvitallennuspalveluun tai sieltä pois. Vastauksissa ei mainittu, oliko internetyhteyden nopeutta testattu jollain nopeustesti-sovelluksella vai oliko kyseessä käyttäjän oma arvio yhteyden hidastumisesta.

> ”Joo elikkä raskaammat sivut latautuu hitaasti ja joskus esimerkiksi -- kun sä oot kotiverkossa ja sä lähet käymään pihalla niin siinä tulee sellanen katkos kun se eka yhistää 4g verkkoon ja sitten se taas kytkee sitä Freedomee päälle automaattisesti niin siinä tulee sellanen katko ja yleisestikin jos yhistät jonnekin toisen maan serverille niin se on hidas se yhteyttä. Esimerkiksi videoiden lataaminen ja tiedostojen lataaminen pilveen ja pilvestä on hitaampaa, kun normaalisti.” H4

Internetliikenteen hidastuminen huomattiin jo käytön alkuviikkoina ja kokemuksen negatiivisuuden aiheutti sovelluksen huono ja hidas käytettävyys. Käytön kannalta kokemus ei kuitenkaan ollut merkittävä ja sen mainittiin olevan sovelluksen käytön kannalta välttämätön paha.

> ”Se on oikeestaan se hinta mikä noista pitää maksaa että tuommosta käyttää, että se ei toimi ihan niin hyvin kun ilman sitä. Se on vaan surullinen fakta.” H4

Käytön jatkumisen kannalta tapahtumaa ei nähty myöskään merkittävänä, eikä tapahtuma aiheuttanut sovelluksen käytön lopettamisen harkitsemista.

5.2.3 Sovelluksen huono toimivuus

Sovelluksen käytön kannalta negatiivisena kokemuksena nousi esiin sovelluksen toimivan jotenkin tahmeasti ja hitaasti. Mainittiin, että kun sovelluksessa siirtyy katselemaan ominaisuuksien tietoja, tiedot eivät lataudu saumattomasti. Sovelluksen visuaalisuuden toimivuuden ja reagointikyvyn kuvailtiin olevan tahmeaa. Tämän kokemuksen kuvailtiin vievän sovelluksen käyttömukavuutta, jonka vastaaja mainitsee olevan kaikkein tärkein piirre sovelluksen käytössä. Käyttäjällä oli vahva mielikuva selkeästi toimivasta sovelluksesta, joten hän koki tapahtuman yllättävänä ja ärtymystä aiheuttavana. Tapahtuman kuvailtiin myös olevan melko merkittävä käytön jatkumisen kannalta.

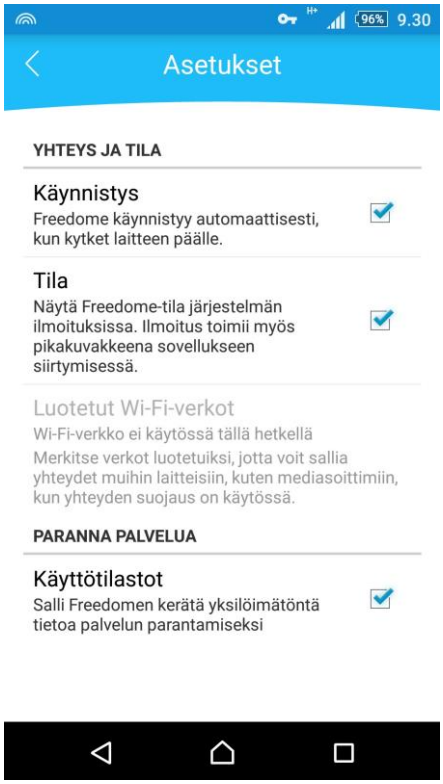
> ”No se on semmonen mikä lähinnä nakertaa sitä mun mielestä kaikkein tärkeintä, eli sitä palvelun käyttömukavuutta.” H3

> ”Mä näen sen melko merkittävänä käytön jatkumisen kannalta, koska mä olin enemmän kun ärsyyntynyt, niin mä olin aika yllättynyt siitä että se ei pyörinytkään niin jouhevasti. Mä oletin, että se olisi ollut selkeästi toimiva. Se oli se mun mielikuva.” H3

Vastauksissa ei käynyt ilmi johtuuko sovelluksen hitaus käyttäjän laitteesta vai itse sovelluksesta. Saman merkkistä laitetta ei ollut muilla vastaajilla käytössä, joten ei myöskään ole verrattavissa onko tämä ominaisuus liitettävissä tiettyyn laitemalliin. Vaikka tämä kokemus aiheutti käyttäjässä ärsytystä ja se koettiin käytön jatkumisen kannalta melko merkittävänä, kokemus ei kuitenkaan johtanut käytön lopettamiseen.

5.2.4 Sovelluksen ikonin näkyminen

Kun Freedome on käynnissä, laitteen yläpalkkiin tulee avaimen kuva näkyviin. Logon näkymistä ei pysty estämään sovelluksen asetuksista, eikä se ole toiminnallinen, jotta sitä voisi käyttää pikakuvakkeena sovellukseen siirtymisessä.



KUVIO 8 Kuvakaappaus: Freedomen asetukset ja ikonit

Freedomessa on myös kaaren näköinen logo valittavissa, jolloin Freedme-tila näkyy yläpalkissa kaarisymbolina ja se toimii myös sovelluksen pikakuvakkeena (kuvio 8). Kaarilogo on toiminnallinen, jonka avulla laitteen yläpalkista pääsee siirtymään suoraan Freedomen sovellusnäkymään, asettamaan virtuaalisijainnin tai sulkemaan ohjelman pois päältä.

Vastauksissa negatiivisena kokemuksena mainittiin sovelluksen ikonin näkyminen laitteen näytön ylälaidassa. Kokemuksen kerrottiin ilmenneen heti, Freedomen käyttöönoton jälkeen. Vastauksessa puhuttiin lukosta, vaikka kyseessä on joko kaarisymboli tai avain.

> ”No tällä hetkellä puhelimella huono kokemus on se, että siellä näkyy se tyhmä lukko kun se on päällä. -- Se kuvake mikä jää sinne ilmotuspalkkiin. Se on vaan ärsyttävä. Ei se käyttökokemusta mitenkään niinku huononna tai paranna vaan se on niinku visuaalisesti ärsyttävä. -- Oon mä sitä vielä käyttänyt mutta kyllä se ärsyttää aina kun se on päällä siellä. No kyllä se on merkittävää (käytön jatkumisen kannalta) minulle. Minun näkökulmasta.” H2

Kokemus nousi merkittäväksi, koska ikoni koettiin niin ärsyttävänä. Tapahtuma nähtiin merkittävänä jatkuvan käytön kannalta, mutta sovelluksen käyttöä jatkettiin silti. Käytön jatkuvuuteen sen kerrottiin myös vaikuttavan merkittävästi.

5.2.5 Sovellus estää muita sovelluksia toimimasta

Freedomen yksi ominaisuus on App Security, joka tarkistaa asennetut sovellukset haittaohjelmien varalta. Se varmistaa, ettei laitteessa ole vahinkoa aiheuttavia tai käyttäjän tietoja kalastelevia sovelluksia ja estää haitalliseksi luokiteltujen sovellusten toiminnan. Negatiivisena käyttökokemuksena mainittiin sovelluksen estävän toisen sovelluksen toimintaa.

Vastauksissa mainittiin, että Freedome oli tulkinnut Snapchat-ohjelman jotenkin haitalliseksi ja näin ollen estänyt sen toiminnan. Snapchat on erityisesti nuorten keskuudessa suosittu valokuvaviestipalvelu, jossa käyttäjä viestittää toisille käyttäjille pelkkiä kuvia ja videoita. Erityisen Snapchatista tekee sen ominaisuus, jossa käyttäjä voi määritellä ajan kuinka kauan vastaanottaja näkee hänen lähettämäänsä kuvaa (1-10 sekuntia), jonka jälkeen tiedot poistuvat vastaanottajan laitteelta ja Snapchatin omilta palvelimilta.

Toisaalta kokemus oli merkittävä, mutta ei kuitenkaan niin merkittävä, että käyttäjä olisi alkanut etsimään ratkaisua ongelmaan. Kokemuksen negatiivisuuden aiheutti huomaaminen, että sovellus ei ole yhteensopiva kaikkien muiden sovellusten kanssa.

> ”No joo, siinä on sellanen huonopuoli –syystä tai toisesta en oo jaksanu F-Securen foorumeilta sitä kahtoo – ihan kaikki softat ja sivustot ei oikeen tykkää siitä. Esimerkiks Snapchat ei toiminu sillon ku oli Freedome päällä. Se tulkitsi sen jotenki haitalliseks. Niin se oli vähän negatiivinen kokemus.” H4

Jatkuvaan käyttöön kokemus ei vaikuttanut muuten kuin, että nyt käyttäjä osaa tunnistaa samantyyppiset ongelmat ja testata ovatko ne Freedomesta johtuvia. Vastauksissa mainittiin, että käyttäjä ei tiedä toimiiko Snapchat nykyään Freedomen kanssa yhdessä, koska Snapchatin käyttöä ei päätetty jatkaa. Käytön jatkumisen kannalta tätä kokemusta ei nähty merkittävänä.

> ”Ehkä enemmän nyt osaa yhistää, että jos joku ei toimi niin tietää että se ehkä johtuu tästä Freedomesta. Mutta ei se muuten oo vaikuttanu. Nyt vaan tietää mistä vikaa lähtee ekana etsimään.” H4

Lopuksi mainittiin, että App Security muuttuu käytön jatkumisen kannalta merkittäväksi, jos se estäisi esimerkiksi pikaviestinpalvelu WhatsAppin tai F-Securen Younited-pilvipalvelun toiminnan laitteessa.

5.3 Tutkimustulokset aiemman tutkimuksen näkökulmasta

Kuten jo edellä on mainittu, aiempien tutkimusten mukaan älypuhelinten käyttäjät sivuuttavat usein sovellusten sopimusehdot sovellusta ladattaessa. (Mylonas ym., 2012, Chin ym., 2013 & Leavitt, 2011) Kun sopimusehtoja ei lueta eikä sovelluksen toimintaan perehdytä, käyttäjä voi huomaamatta ladata laitteeseensa haitallisia sovelluksia, jolloin tietoturvasovelluksen merkitys kasvaa.

Freedomen App Security-ominaisuus vahtii sovellusten luotettavuutta ja tarkistaa, että käyttäjä ei lataa laitteeseensa haitallisia sovelluksia. Haastatteluissa App Security-ominaisuus mainittiin negatiivisessa merkityksessä, jolloin se oli estänyt käyttäjän haluaman sovelluksen käytön. Positiivisena koetuissa kokemuksissa ei App Security-ominaisuutta mainittu kertaakaan.

Mylonaksen ym. (2012) tutkimus osoitti, että suuri osa älypuhelinten käyttäjistä uskoi sovellusten lataamisen virallisesta sovelluskaupasta olevan riskitöntä. Tämän tutkimuksen haastatteluissa mainittiin negatiivisena kokemuksena, että App Security oli estänyt Snapchatin käytön. Haastateltava ei epäröinyt Snapchat-sovelluksen luotettavuutta, vaan koki Freedomen toimivan viallisesti. Tiedossa ei ole miksi App Security on estänyt Snapchatin toiminnan.

> ”No joo, siinä on sellanen huonopuoli – syystä tai toisesta en oo jaksanu F-Securen foorumeilta sitä kahtoo – ihan kaikki softat ja sivustot ei oikeen tykkää siitä. Esimerkiks Snapchat ei toiminu sillon ku oli Freedome päällä. Se tulkitsi sen jotenki haitalliseks. Niin se oli vähän negatiivinen kokemus. -- No Twitshsiä mä oon joskus kokeillu, mutta se on niin buginen että siitä ei uskalla sanoo että on ton Freedomen syytä. En jaksanu enempää lähtee tutkimaan sitä asiaa. Mutta se Snapchat oli sellanen omituinen ja se johtu nimenomaan siitä Freedomesta. -- Ehkä se yhteensopimattomuus (aiheutti kokemuksen negatiivisuuden) tai se että se ei vaan toimi kaikkien kanssa.” H4

Tässä tutkimuksessa havaittiin, että sovellusten luotettavuutta vahtivaa ominaisuutta ei pidetty tarpeellisena. Kuten aiemmat tutkimukset ovat osoittaneet, voidaan myös tämän tutkimuksen tuloksista päätellä, että sovellusten toiminnan luotettavuutta ei epäillä.

Aiempien tutkimusten tulosten pohjalta tutkijat ovat epäilleet, että käyttäjillä on välinpitämätön asenne mobiililaitteiden tietoturvasovelluksia kohtaan. Mylonas ym. (2012) epäilevät, että asenne voi johtua teknisistä ominaisuuksista, kuten muun muassa huonosta akun kestävyydestä ja laitteen yleisen suorituskyvyn heikkenemisestä. Tämän tutkimuksen haastatteluissa suurin osa mainituista negatiivisista käyttökokemuksista johtui siitä, että sovelluksen koettiin kuluttavan laitteen akkua enemmän kuin ilman sovellusta. Vastauksissa mainittiin myös internetyhteyden hidastuminen sekä sovelluksen huono toimivuus, josta vastaaja ei kuitenkaan osannut määritellä johtuuko huono toimivuus sovelluksesta vai hänen laitteestaan.

> ”Palvelun käytön kannalta mä oon kokenut, että miten se toimii ja pyörii silleen visuaalisesti ja miten se reagoi niin se on vähän tahmea. Mut se voi olla että se liittyy kyllä mun puhelimeenkin. En tietenkään voi olla ihan varma mut mä oon kokenut sen silleen että kun menee siihen päänäkymään ja yrittää päästä klikkaamaan johonkin niistä pylpyröistä tai niistä kaarista niin se liikkuu silleen, se ei niinku toimi ihan niin nopsaa kuin mitä olettais. -- Mä näen sen melko merkittävänä käytön jatkumisen kannalta koska mä olin enemmän kun ärsyyntynyt niin mä olin aika yllättynyt siitä että se ei pyörinytkään niin jouhevasti. Mä oletin että se olisi ollut selkeästi toimiva, se oli se mun mielikuva.” H3

> ”Lähinnä se (negatiivinen kokemus) liittyy siihen sovellukseen ja se käyttää akkua aika hurjasti nimittäin. Ainaki ite oon huomannu sellasen. -- En mä silleen tarkemmin ole huomannut. Mut sen vaan huomasin että huomattavasti nopeemmin, kun se oli päällä, niin akku oli huomattavasti tyhjemmäks kun normaalisti. -- No ei ehkä tossa nyt ollu niin ongelma, mutta jos olis ollu reissussa nii sillon se olis ollu ongelma ehkä enemmänki.” H9

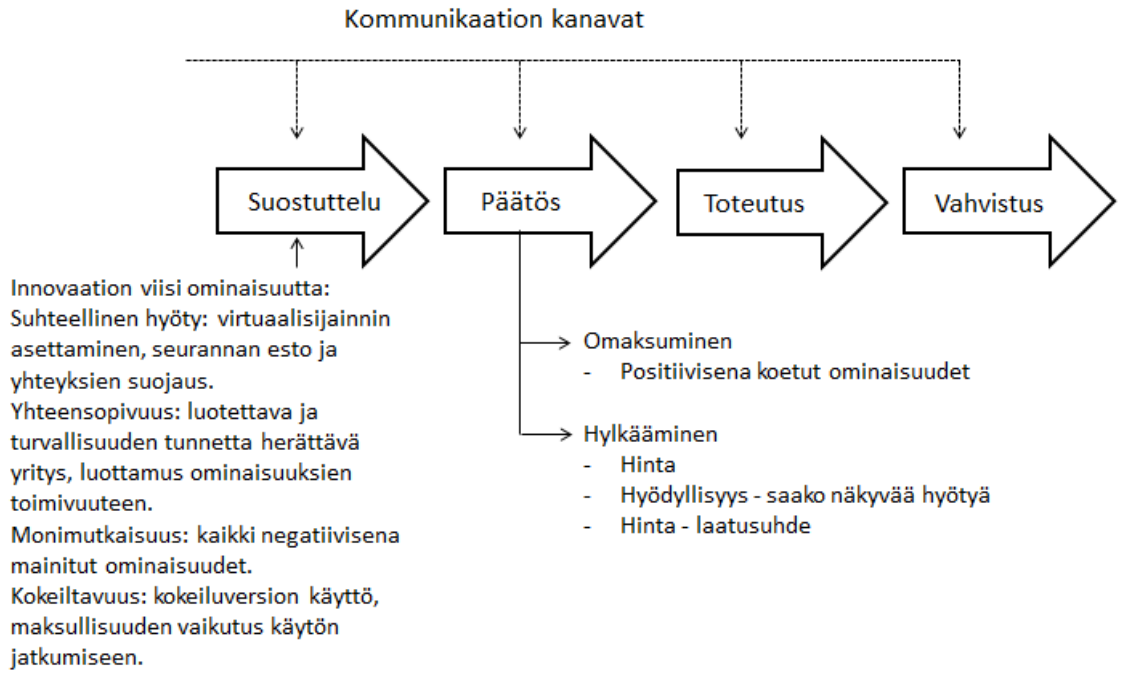
Akun kulumiseen liittyviä kokemuksia ei nähty kovin merkittävinä, mutta sovelluksen huono käytettävyys mainittiin merkittävänä käytön jatkumisen kannalta. Toisaalta mainittiin, että akun kulumisesta olisi voinut muodostua ongelma, jos puhelimen lataukseen ei olisi ollut esimerkiksi matkalla mahdollisuutta.

Mylonaksen ym. (2012) mukaan suurin osa älypuhelinten käyttäjistä ei suojaa laitettaan millään kolmannen osapuolen tarjoamalla tietoturvasovelluksella. Myös tässä tutkimuksessa tuli ilmi, että Freedomen omaksumiseen ei vaikuta pelkästään tietoturvaominaisuudet vaan suurelta osin myös virtuaalisijainnin asettaminen. Tämän tutkimuksen haastatteluista saatujen vastausten mukaan Freedomen ominaisuuksista eniten positiivisina koettuja kriittisiä käyttökokemuksia mainittiin liittyen virtuaalisijaintiin ja toiseksi eniten seurannan esto-ominaisuuten, joka on tietoturvaominaisuus. Kolmanneksi eniten mainittiin yhteyksiensuojaus-ominaisuus. Selvitettäessä miksi käyttäjä aikoo jatkaa Freedomen käyttöä, mainittiin virtuaalisijainnin asettaminen ja turvallisuusominaisuudet.

5.4 Omaksuminen diffuusioteorian mukaan

Rogersin diffuusioteorian mukaa omaksumisprosessin ensimmäisessä vaiheessa (tietovaihe) yksilö saa tiedon innovaatiosta ja luo ymmärryksen sen toiminnasta. Tietovaiheen jälkeen hän muodostaa innovaation ominaisuuksien perusteella sitä kohtaan suosivan tai hylkäävän asenteen. Hyväksyvän tai hylkäävän asenteen muodostamisen jälkeen yksilö siirtyy päätösvaiheeseen, jossa toteutetaan toimenpiteet innovaation hyväksymiseen tai hylkäämiseen. Seuraava vaihe on toteutusvaihe, joka sisältää innovaation käyttöönoton ja kokeilun. Vahvistusvaiheessa päätös vakiinnutetaan hankkimalla innovaatiosta lisää tietoa. Tutkimustulokset sovitettuna Rogersin innovaation diffuusioteoriaan voidaan suurimman osan vastaajista olettaa olevan joko suostuttelu, tai päätösvaiheessa. Pieni osa oli myös toteutus-vahvistuvaiheessa.

Kuviossa 9 on esitetty tutkimuksen tulokset innovaation diffuusioteoriaan sovitettuna. Päätöksentekijän ominaisuudet liittyvät vahvasti tietovaiheeseen, jossa käyttäjä luo ymmärryksen innovaation toiminnasta. Tässä tutkimuksessa ei kuitenkaan nähty oleellisena tutkia päätöksentekijän ominaisuuksia tai tietovaihetta, koska kaikki haastatellut olivat jo Freedomen käyttäjiä ja haluttiin saada tietoa vain siitä miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen.



KUVIO 9 Freedomen omaksuminen innovaation diffuusioteorian mukaan (Rogers, 2003, muokattu.)

Suostutteluvaiheessa käyttäjä muodostaa suosivan tai hylkäävän asenteen innovaatiota kohtaan innovaation ominaisuuksien perusteella. Tässä tutkimuksessa vastaajista suurin osa oli suostutteluvaiheessa, koska moni käytti vielä jotain ilmaista kokeilujaksoa ja vain yksi käyttäjä oli ostanut sovelluksen vuosilisenssin. Rogers (2003) määrittelee innovaatiolle viisi ominaisuutta, jonka perusteella käyttäjä muodostaa asenteensa innovaatiota kohtaan.

Suhteellinen hyöty on innovaation yksi ominaisuus, joka kertoo missä määrin käyttäjä kokee innovaation parempana ja hyödyllisempänä kuin sitä edeltäneen ratkaisun (Rogers, 2003). Oleellista on, että käyttäjän tulee kokea, että innovaatio on hänelle hyödyllinen tai hyödyllisempi kuin aiempi ratkaisu, jotta hän on valmis korvaamaan vanhan ratkaisun uudella. Suhteellinen hyöty käsittelee myös hinnan vaikutusta; kokevatko käyttäjät hinnan olevan kohtuullinen verrattuna innovaatiosta saatuun hyötyyn. Tässä tutkimuksessa haastatteluissa ilmenneissä merkittävissä käyttökokemuksissa verrattiin Freedomen olevan helpompi käyttää, kuin Proxyn virtuaalisijaintia asetettaessa. Näin ollen Free-

domen virtuaalisijainti-ominaisuus nähtiin parempana, kuin sitä edeltänyt ratkaisu. Proxy on välityspalvelin, jonka kautta käyttäjä pystyy salaamaan omat tietonsa välityspalvelimen suojaan, jolloin vieraillun internetsivusto hallinnoijalle näkyy välityspalvelimen tiedot. *Suhteellisena hyötynä* toisaalta voidaan nähdä myös kaikki positiivisena mainitut ominaisuudet, eli virtuaalisijainnin asettaminen, seurannan esto ja yhteyksien suojaus, koska nämä kaikki ominaisuudet koettiin hyödyllisinä. Hinnan vaikutus näkyi selkeästi negatiivisena omaksumisprosessissa; vastauksissa puntaroitiin antaako sovellus tarpeeksi hyötyä hintaan nähden. Sovelluksen hinnan koettiin olevan liian korkea kun sitä verrattiin sovelluksesta saatuun näkyvään hyötyyn.

Innovaation toinen ominaisuus on *yhteensopivuus*, joka kertoo missä määrin innovaatio on yhdenmukainen käyttäjän arvojen, aiempien kokemusten ja tarpeiden kanssa. Rogersin (2003) mukaan omaksumista ei tapahdu, jos innovaatio on ristiriidassa omaksujan uskonnon tai muun vakaumuksen kanssa. *Yhteensopivuus* mainittiin positiivisena koetuissa merkittävissä käyttökokemuksissa. Haastatteluissa nousi esiin, että F-Secure nähdään luotettavana sekä turvallisuuden tunnetta herättävänä toimijana. Luottamus Freedomeen kumpuaa käyttäjän aiemmista kokemuksista ja niiden mukaan rakennetusta mielikuvasta luotettavasta yrityksestä. Käyttäjillä on ollut jo jonkinlainen kokemus F-Securesta, jonka mukaan hänen käsitys yrityksestä vaikuttaa myös tietyn käyttökokemuksen positiivisuuteen. Vastauksissa mainittiin myös, että luottamus ominaisuuden toimivuuteen nähdään hyvin merkittävänä asiana jolloin luottamuksen menetys johtaisi sovelluksen poistamiseen.

Monimutkaisuus on innovaation ominaisuus, joka kertoo missä määrin käyttäjän on tarve muuttua ja mukauttaa toimintaansa käyttäessään uutta innovaatiota. Rogersin (2003) mukaan on tärkeää, että käyttöönotto on helppoa ja toimintaperiaatteen ymmärtäminen ei vaadi liikaa vaivaa. Toisin kuin muilla innovaation ominaisuuksilla, *monimutkaisuudella* on negatiivinen vaikutus omaksumisprosessiin. *Monimutkaisuutena* voidaan nähdä kaikki vastauksissa mainitut negatiivisena koetut ominaisuudet:

- sovellus kuluttaa akkua – pitää sopeutua akun nopeampaan kulumiseen,
- ikoni näkyy näytön ylälaidassa – pitää sopeutua ikonin kuvaan sovelluksen ollessa päällä
- sovelluksen valikoiden huono toimivuus – pitää sopeutua käyttämään sovellusta siitä huolimatta
- hidastaa internetyhteyttä – pitää sopeutua käyttämään hieman hitaampaa yhteyttä sovelluksen ollessa päällä
- ei toimi kaikkien ohjelmien kanssa – täytyy valita kumpaa ohjelmaa tahtoo käyttää tai etsiä tilanteeseen jokin muu ratkaisu
- sovellus menee itsekseen päälle – pitää sopeutua ohjelman koko ajan päällä olemiseen tai etsiä tilanteeseen jokin muu ratkaisu (vastauksissa mainittiin, että tämä ominaisuus on korjaantunut)

Yllämainittuja negatiivisia käyttökokemuksia liittyen sovelluksen *monimutkaisuuteen* ei kuitenkaan nähty kovinkaan merkittävinä, joten tässä tutkimuksessa

sovelluksen *monimutkaisuudella* ei kuitenkaan ollut kovin merkittävää vaikutusta omaksumisprosessiin. Yksi vastaaja mainitsi kokemuksen olleen merkittävä käytön jatkumisen kannalta.

Kokeiltavuus on innovaation ominaisuus, joka määrittää missä määrin innovaatiota on mahdollisuus kokeilla ennen sen omaksumista. F-Secure tarjoaa Freedomen 14 vuorokaudeksi ilmaiseksi kokeilukäyttöön. Freedomen käyttäjät (myös ilmaisversion käyttäjät) pystyvät kutsumaan kavereita 30 päiväksi käyttämään Freedomea ilmaiseksi. Tässä tutkimuksessa haastatelluista vain yksi käytti maksullista versiota ja kaikki muut jotain ilmaista kokeiluversiota. Kokeilujakson käyttäjistä yksi kertoi varmasti jatkavansa käyttöä, kun taas 7/9 vastaajista ei ollut vielä tehnyt lopullista omaksumispäätöstä. Kokeiltavuuden merkitystä ei erikseen haastattelussa kysytty, mutta kokeiltavuus näyttää kuitenkin hyvin vahvasti liittyvän omaksumiseen, koska vastauksissa mainittiin myös sovelluksen maksullisuuden olevan syynä jos sovelluksen käyttöä ei päätetä jatkaa.

Havaittavuus on innovaation ominaisuus, joka määrittää kuinka innovaation vaikutukset ovat näkyvissä yhteisön muille jäsenille. Rogers (2003) määrittelee, että kun innovaation ominaisuudet voidaan selkeästi havaita, on omaksujan helpompi tutustua innovaatioon. Tämän haastattelun vastauksissa ei selkeästi ilmennyt havaittavuuden vaikutusta merkittävissä käyttökokemuksissa. Rogersin (2003) mukaan innovaation tulisi olla näkyvä, jotta se olisi helpommin omaksuttavissa ja kommunikoitavissa. Freedome on ilmaiseksi ladattavissa, eikä sen käyttöön tarvitse esimerkiksi kutsua jo olemassa olevalta käyttäjältä.

Päätösvaiheessa toteutetaan toimenpiteet innovaation hyväksymiseen tai hylkäämiseen. Vastauksissa mainittiin tasaisesti käytön jatkaminen, lopettaminen sekä noin puolet vastasi olevansa vielä epävarmoja jatkosta.

> ”No en aio jatkaa ja se on se hintapolitiikka.” H5

> ”No koska se on hyvä (aikoo jatkaa käyttöä). No kyllä tähän ehkä vähän vaikuttaa myös se että mä sain vuoden ilmasen lisenssin. Jos joutuisi maksamaan niin jatkaisiko? No kyllä mä ehkä. Koska se on vuodessa se 16 euroa niin ei se nyt niin hirveen iso summa oo.” H1

> ”Kyllä ainaki tällä hetkellä aion (jatkaa käyttöä). -- No justii nämä että voi käyttää sitä noissa eri ohjelmissa ja sitte että se suojaa sitä laitetta.” H6

> ”Mikäli mä saan noista maa-asetuksia muuttamalla aikaseks ihan oikeaa rahansäästöä niin on todella todennäköistä et mä jatkan sen käyttöä kyllä.” H3

Myönteiseen omaksumispäätökseen mainittiin vaikuttavan sovelluksen positiivisena koetut ominaisuudet. Ominaisuuksia, jotka mainittiin negatiivisissa käyttökokemuksissa, ei mainittu vaikuttavan käytön jatkumisen, mutta sen sijaan hylkäämispäätökseen mainittiin hinnan vaikutus. Hinnan lisäksi mainittiin yleisesti ominaisuuksista saatu hyöty, moni vastaaja puntaroi, saako hän sovelluksesta tarpeeksi hyötyä, jotta käyttöä kannattaisi jatkaa ilmaisen kokeilujakson päätyttyä.

Toteutusvaihe sisältää innovaation käyttöönoton ja kokeilun. Tämän vaiheen voidaan nähdä olevan Freedomen maksullisen version käyttöönotto ja kokeilu. Tässä tutkimuksessa haastatelluista suurin osa ei ollut vielä toteutusvaiheessa, joten toteutusvaiheen ja omaksumisvaiheen osalta analysointia ei voida tehdä. Innovaation diffuusioteoriassa viimeinen vaihe omaksumisprosessissa on vahvistusvaihe, jossa käyttöönotto- tai hylkäämispäätös vakiinnutetaan hankkimalla innovaatiosta lisää tietoa.

5.5 Tulosten yhteenveto

Tässä alaluvussa käsitellään tutkimuksen tulosten yhteenveto sekä käydään läpi miten tutkimustulokset vastaavat tutkimusongelmaksi muodostettuun kysymykseen.

Tutkimusongelma:

- Miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön?

Tutkimusongelmaa tukevat tutkimuskysymykset:

- Mitä on mobiililaitteiden kyberturvallisuus ja miten sitä voidaan hallita?
- Minkälaisia kriittisiä käyttökokemuksia esiintyy Freedomen käytössä ja miten ne vaikuttavat sovelluksen omaksumiseen ja jatkuvaan käyttöön?

Tutkimuksen toisessa luvussa käsiteltiin mitä on mobiililaitteiden kyberturvallisuus ja viidennen luvun aiemmissa alaluvuissa on käsitelty vastauksia kysymykseen millaisia kriittisiä käyttökokemuksia esiintyy Freedomen käytössä ja miten ne vaikuttavat sovelluksen omaksumiseen ja jatkuvaan käyttöön. Tässä alaluvussa pyritään vastaamaan kysymykseen miten kriittiset kokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön. Jatkuvalla käytöllä tarkoitetaan kokemuksen vaikutusta käytön jatkamiseen ja omaksumisella taas lopullista päätöstä sovelluksen käyttöönotosta.

Positiivisena mainitut kokemukset liittyivät virtuaalisijainnin asettamiseen, seurannan estoon ja yhteyksien suojaamiseen. Nämä kokemukset koettiin kaikki merkittävinä käytön jatkumisen kannalta ja ne vaikuttivat myös sovelluksen omaksumiseen merkittävästi (taulukko 2). Negatiivisina koetuista kokemuksista taas merkittävinä käytön jatkumisen kannalta koettiin vain ikonin näkyminen ja sovelluksen huono toimivuus.

TAULUKKO 2 Merkittävien kokemusten vaikutus Freedomen jatkuvaan käyttöön

Positiivisina koetut kokemukset:	Vaikutus jatkuvaan käyttöön
Virtuaalisijainnin asettaminen	Merkittävä
Seurannan esto	Merkittävä
Yhteyksien suojaus	Merkittävä
Negatiivisina koetut kokemukset:	Vaikutus jatkuvaan käyttöön
Sovellus kuluttaa akkua	Ei juurikaan merkitystä
Sovelluksen ikonin näkyminen	Merkittävä
Sovellus hidastaa internetliikennettä	Ei juurikaan merkitystä
Sovelluksen huono toimivuus	Merkittävä
Sovellus estää muita sovelluksia toimimasta	Ei juurikaan merkitystä

Taulukossa 3 on listattu vastaajittain omaksumispäätökset sekä niihin johtavat syyt. Suurin osa vastaajista ei ollut tehnyt vielä lopullista päätöstä käytön jatkamisen kannalta.

Virtuaalisijainnin asettaminen koettiin positiivisena ja sen mainittiin olevan merkittävää käytön jatkumisen kannalta. Omaksumiseen ja jatkuvaan käyttöön tällä ominaisuudella koettiin olevan eniten vaikutusta. Vastauksissa mainittiin muun muassa, että jos virtuaalisijainnin asettamisen avulla saa rahallista hyötyä, esimerkiksi lentoja ostettaessa, käyttäjä on valmis jatkamaan sovelluksen maksullista käyttöä. Yleisesti vastauksissa mainittiin virtuaalisijainnin asettamisen positiivinen vaikutus käytön jatkumiseen, koska se mahdollistaa maakohtaisesti rajoitettujen internetpalveluiden käytön.

Negatiivisina koettuja kokemuksia mainittiin liittyvän viiteen eri ominaisuuteen, joista kahden sanottiin olleen sillä hetkellä merkittäviä sovelluksen käytön jatkamisen kannalta (ks. taulukko 2). Kun kysyttiin aikooko käyttäjä jatkaa sovelluksen käyttöä vielä maksuttoman kokeiluajan päätyttyä, kukaan ei kuitenkaan maininnut lopettamispäätöksen syyksi negatiivisina koettuja kokemuksia (ks. taulukko 3).

TAULUKKO 3 Freedomen käytön lopulliset omaksumispäätökset

Henkilö	Kuinka kauan käyttänyt	Käytön jatkuminen	Syyt miksi jatkaa / ei jatka Freedomen käyttöä
H1	1 viikon	Ehkä	Yleinen tyytyväisyys sovelluksen toimintaan
H2	2 viikkoa	Ehkä	Jatkaa, jos saa selkeää hyötyä. Vastausajankohtaan mennessä ei ollut kokenut sovellusta tarpeeksi hyödylliseksi.
H3	2 viikkoa	Ehkä	Jatkaa, jos saa selkeää rahallista hyötyä esimerkiksi virtuaalisijainnilla.
H4	1 vuoden	Kyllä	Käyttää jo maksullista versiota ja aikoo jatkaa käyttöä.
H5	2-3 viikkoa	Ei	Ei jatka, koska hinta on liian korkea.
H6	2 viikkoa	Kyllä	Tyytyväisyys sovelluksen ominaisuuksiin sekä suojaukseen.
H7	1 viikon	Ehkä	Jatkamiseen vaikuttaa positiivisesti virtuaalisijainnin asettaminen ja seurantayritysten estäminen, mutta toisaalta korkea hinta vaikutti negatiivisesti omaksumispäätökseen.
H8	2 kuukautta	Ehkä	Ei tiennyt vielä.
H9	1 viikon	Ehkä	Jatkamiseen vaikuttaa positiivisesti virtuaalisijainnin asettaminen, mutta toisaalta korkea hinta vaikutti negatiivisesti omaksumispäätökseen.

Hinnan mainittiin vaikuttavan negatiivisesti Freedomen käytön omaksumiseen. Rogersin (2003) mukaan hinnan vaikutus näkyy positiivisena omaksumisprosessissa, jos käyttäjä kokee hinnan olevan kohtuullinen innovaatiosta saatavaan hyötyyn nähden. Venkatesh ym. (2012) ovat käsitelleet UTAUT2-mallissa hinnan vaikutusta ja todenneet, että hinta on oleellinen tekijä yksilön omaksumisprosessissa. Rogersin (2003) mukaan hinta voidaan nähdä positiivisesti vaikut-

tavana omaksumisprosessissa, jos kuluttaja kokee että hinta on kohtuullinen suhteessa innovaation hyötyihin. Tässä tutkimuksessa hinta nähtiin ainoastaan negatiivisesti vaikuttavana tekijänä, sen ei mainittu vaikuttavan positiivisesti päätöksiin kertaakaan.

Näiden tulosten pohjalta voidaan todeta, että Freedomen omaksumiseen vaikuttavat eniten positiivisena koetut ominaisuudet ja käytön hylkäämiseen vaikutti eniten sovelluksen hinta. Suuri osa haastatelluista ei ollut tehnyt päätöstä jatkaako sovelluksen käyttöä ilmaisen kokeilu jakson jälkeen. Kysyttäessä syitä miksi jatkaisi tai miksi ei jatkaisi käyttöä, esiin nousi yleinen tyytyväisyys sovellukseen, virtuaalisijainnin asettaminen ja tietojensuojauspalvelu. Negatiivisesti omaksumiseen vaikutti hinta ja sovelluksesta saadun näkyvän hyödyn puute.

6 YHTEENVETO

Luku kuusi sisältää tiivistetysti tutkimuksen kulun ja tutkimustulokset, tutkimuksen rajoitteiden ja luotettavuuden arvioinnin sekä jatkotutkimusaiheiden esittelyn.

6.1 Tutkimuksen kulku ja tulokset

Tämän tutkimuksen tarkoituksena oli selvittää mitä on mobiililaitteiden kyberturvallisuus ja miten sitä voidaan hallita, sekä millaisia kriittisiä käyttökokemuksia esiintyy F-Securen Freedomen käytössä ja miten ne vaikuttavat sovelluksen omaksumiseen ja jatkuvaan käyttöön. Tutkimusongelmaksi muodostui: miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön. Tutkimus jaettiin kirjalliseen osaan ja empiiriseen osaan. Kirjallisessa osassa selvitettiin mitä on mobiililaitteiden kyberturvallisuus ja miten sitä voidaan hallita. Empiirinen osa pyrki vastaamaan kysymykseen minkälaisia kriittisiä käyttökokemuksia esiintyy Freedomen käytössä ja miten ne vaikuttavat palvelun omaksumiseen ja jatkuvaan käyttöön.

Kyberturvallisuus on tietoturvallisuutta, verkkoturvallisuutta ja laiteturvallisuutta. Limnellin ym. (2014) mukaan kyberturvallisuus-käsite syntyi, kun tarvittiin käsite, joka kattoi laitteeseen tallennetun tiedon lisäksi myös tiedon liikkeen turvaamisen käyttäjän omissa järjestelmissä ja niiden ulkopuolella. Julkisen hallinnon tietohallinnon neuvottelukunnan (2014) mukaan mobiililaitteet ovat mukana kuljetettaviksi suunniteltuja laitteita, joihin voidaan asentaa sovelluksia, tai joissa on internet selain käytössä. Tiivistetysti mobiililaitteiden kyberturvallisuus on mukana kuljetettavaksi suunniteltujen laitteiden tietojen turvaamista laitteessa itsessään sekä verkossa. Mobiililaitteita uhkaa samat kyberuhkat kuin tietokoneitakin ja koska mobiililaitteiden määrä kasvaa räjähdysmäisesti, myös uhkien määrä kasvaa samaa tahtia.

Mobiililaitteiden kyberturvallisuuden nykytila on aiempien tutkimusten mukaan heikkoa siltä osin, että laitteita suojataan hyvin vähän ulkopuolisilla

tietosuojasovelluksilla, mutta toisaalta taas moni kuitenkin suojaa kaikki laitteensa salasanalla. Turvallisuutta voidaan hallita laitteen turvallisella käytöllä, viruksentorjuntaohjelmilla ja muilla valmiilla ratkaisuilla sekä esimerkiksi työkäytössä VPN-suojauksella. F-Securen Freedome on mobiililaitteiden kyberturvallisuuden hallintaan kehitetty yksityisyydensuojaratkaisu, joka salaa tietoja, suojaa verkkoyhteyden ja torjuu seurantaa, jolloin arkaluontoisia tietoja ei pääse vuotamaan internetiin.

Tutkimuksen viitekehykseksi valikoitiin Everett Rogersin innovaation diffuusioteoria, jota on käytetty tutkimuksissa, joissa käsitellään teknologisten innovaatioiden leviämistä suuren yleisön tietoon ja omaksumista. Innovaation diffuusioteoriassa on viisi keskeistä elementtiä: innovaatio, viestintäkanavat, käytetty aika ja sosiaalinen verkosto. Tämän tutkimuksen analyysiosiossa tuloksia sovitettiin Rogersin teorian omaksumisprosessin vaiheisiin sekä innovaation ominaisuuksiin.

Empiirisen tutkimuksen tutkimusmenetelmäksi valikoitui luonnollisesti tapaustutkimus, koska tutkimuksella ei pyritty luomaan yleistettäviä johtopäätöksiä, vaan saada tietoa ainoastaan Freedomen osalta. Tiedonkeruu toteutettiin puhelinhaastatteluin, käyttäen puolistrukturoitua haastatteluasetelmaa. Haastattelukysymykset muodostettiin viitekehystä ja CIT-menetelmää apuna käyttäen. CIT-menetelmä on metodi, jossa keskitytään ainoastaan tutkittavan asian kannalta kriittisten tapahtumien tutkimiseen. Haastattelun perusjoukkona oli kaikki Freedomen mobiilisovelluksen käyttäjät, jotka eivät olleet aiemmin käyttäneet mitään samanlaista VPN-salauspalvelua ja tietosuojapalvelua yhdistävää sovellusta mobiililaitteessaan. Perusjoukosta otokseen valikoitui 9 henkilöä haastatteluun.

Haastatteluissa positiivisina kokemuksina mainittiin virtuaalisijainnin asettaminen, seurannanesto ja yhteyksien suojaus. Virtuaalisijainnin asettaminen on ominaisuus, joka mahdollistaa maakohtaisesti rajoitettujen palveluiden käytön muuttamalla käyttäjän IP-osoitteen osoittamaan käyttäjän valitsemaan maahan. Seurannanesto on ominaisuus, joka IP-osoitteen piilottamalla estää seurantaevästeet ja vakoiluohjelmat, eli estää kolmannen osapuolen tiedonkeräysyritykset. Yhteyksien suojaus salaa käyttäjän yhteyden langattomassa verkossa, jolloin kolmas osapuoli ei pääse laitteeseen tallennettuihin tietoihin käsiksi. Nämä positiivisina mainitut käyttökokemukset koettiin kaikki merkittävinä ja ne vaikuttivat merkittävästi käytön jatkumiseen.

Negatiivisina kokemuksina haastatteluissa mainittiin sovelluksen kuluttavan akkua, sovelluksen ikonin näkyminen laitteen näytön ylälaidassa, internetliikenteen hidastuminen sovelluksen ollessa päällä, sovelluksen huono toimivuus ja se että sovellus oli estänyt toista sovellusta toimimasta. Näistä kokemuksista merkittävänä käytön jatkumisen kannalta mainittiin ikonin näkyminen ja sovelluksen huono toimivuus. Toisaalta, kun haastattelun lopuksi kysyttiin aikooko Freedomen käyttöä jatkaa ilmaisversion päätyttyä, ei negatiivisina koettuja käyttökokemuksia mainittu kertaakaan.

Aiempien tutkimusten mukaan sovelluskaupoista ladattuja sovelluksia ei epäillä, vaan niiden arvioidaan olevan luotettavia ja myös tässä tutkimuksessa

vastaaja epäili enemmän tietoturvasovelluksen toimintaa, kuin lataamansa sovelluksen luotettavuutta. Mylonas ym. (2012) osoittivat tutkimuksessaan, että suurin osa älypuhelinten käyttäjistä ei suojaa laitettaan millään tietoturvasovelluksella. Myös tämän tutkimusaineiston pohjalta voidaan todeta, että käyttäjät eivät omaksu Freedomea käyttöön pelkästään sen tietoturvaominaisuuksien vuoksi.

Tutkimuksessa havaittiin, että Freedomen omaksumiseen ja jatkuvaan käyttöön vaikuttivat eniten positiivisina koetut käyttökokemukset ja käytön lopettamiseen vaikutti eniten sovelluksen hinta. Tutkimustulokset myös osoittivat samankaltaisuutta aiemmin tehtyjen tutkimusten tulosten kanssa.

Tutkimusongelmana oli; miten kriittiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön. Tutkimusongelmaan voidaan vastata, että positiivisina koetut käyttökokemukset vaikuttivat Freedomen lopulliseen omaksumiseen kaikista vahvimmin, kun taas negatiivisina koettuja kokemuksia ei pidetty niin merkittävinä.

6.2 Tutkimuksen luotettavuus

Tutkimustuloksissa ilmenneet luotettavuuden arvioinnit ovat esitelty luvussa viisi ja tässä alaluvussa tarkastellaan koko tutkimuksen luotettavuutta. Hirsjärvi ym. (2003) mainitsevat, että kaiken tutkimuksen luotettavuutta tulee jollain tavoin arvioida, vaikka ei haluttaisikaan suoraan mitata validiteettia ja reliabiliteettia. Tässä tutkimuksessa luotettavuus on pyritty varmistamaan jokaisessa tutkimusvaiheessa hyvin, jotta lopputulos olisi mahdollisimman luotettava.

Kirjallisuuden luotettavuus pyrittiin varmistamaan etsimällä tutkimuksen taustatietoja mahdollisimman tuoreista lähteistä ja huolehtimalla, että ne käsittelevät läheisesti tutkimuksessa käsiteltäviä teemoja. Viitekehystä valittaessa pyrittiin kuitenkin perehtymään ennemmin alkuperäisiin ja näin ollen myös hieman vanhempiin teoksiin. Viitekehystä valittaessa tutustuttiin myös moneen muuhun teknologian omaksumista selittävään teoriaan ja niistä valittiin kehys, joka tuki parhaiten tutkimusongelman ratkaisua.

Haastattelukysymykset tehtiin kirjallisuuskatsauksen jälkeen, jotta tutkittava aihe olisi mahdollisimman tuttu tutkijalle ennen haastattelun kehittämistä. Ennen haastatteluja keskusteltiin myös muiden CIT-menetelmällä tutkimusta tehneiden henkilöiden kanssa, jotta saatiin mahdollisimman hyvin tietoa ja erilaisia näkökulmia tutkittavaan asiaan. Haastattelukysymyksiä laadittaessa huomattiin, että tähän tutkimukseen parhaiten soveltui puolistrukturoituhaastattelu, jossa jäi tilaa lisäkysymyksille ja tarkennuksille. Tuloksia analysoitaessa kuitenkin nousi esiin kohtia, joissa olisi tarvinnut lisätietoa. Lisätietoa olisi voinut kysyä esimerkiksi siitä miten vastaajat käsittävät mainitsemansa ominaisuudet; käsittävätkö kaikki vastaajat samalla tavalla esimerkiksi mitä seurannanesto-ominaisuus tarkoittaa.

Haastatteluihin haettiin vastaajia sosiaalisen median, internetin keskustelupalstojen ja puskaradion kautta. Otoksessa oli laaja ikähaarukka, mutta suku-

puolijakauma oli hyvin yksipuolinen, kun vastaajista suurin osa oli miehiä. Tasaisempi sukupuolijakauma olisi tuonut yleistettävämpää tietoa, mutta koska tässä tutkimuksessa ei tarkoituksella pyritty yleistettävyyteen, vastaajien sukupuolen ei annettu vaikuttaa otokseen. Ei myöskään tiedetä onko käyttäjäkunta suurimmaksi osaksi miehiä vai ei, koska F-Secure ei tallenna sovellusten käyttäjistä yksilöllisiä tietoja.

Tuloksia analysoitaessa huomattiin, että hinnan vaikutus näkyi selkeästi omaksumisprosessissa. Hinnan vaikutuksesta etsittiin lisätietoa, jotta voidaan ottaa se paremmin huomioon tulosten analysoinnissa ja analyysi olisi luotettavampi. Analysoinnissa pyrittiin käyttämään paljon suoria lainauksia haastatteluista, jotta tutkijan havainnot ja päätelmät olisivat mahdollisimman hyvin tuettuja.

6.3 Jatkotutkimusaiheita

Yleisesti ottaen mobiililaitteiden tietoturvasovellusten tutkiminen on hyvin ajankohtaista ja tärkeää, koska internetiin kytkettyjen ja näin ollen tietomurroille alttiiden mobiililaitteiden määrä kasvaa räjähdysmäisesti. Ensimmäisenä jatkotutkimusaiheena nousi esiin yleistettävä tutkimus mobiililaitteiden tietoturvasovellusten omaksumisesta. Mobiililaitteiden tietoturvapalveluiden omaksumista ja kuluttajakäyttäytymistä on tutkittu vähän, joten olisi tärkeää pyrkiä luomaan laaja tutkimus, malli tai teoria miten käyttäjät yleisesti ottaen omaksuvat mobiililaitteiden tietoturvasovellukset.

Markkinoilla on olemassa hyvin monenlaisia tieto- ja yksityisyydensuojasovelluksia mobiililaitteille. Toinen jatkotutkimusaihe liittyy eri sovellusten omaksumisen tutkimiseen; miten eri sovellusten omaksuminen eroaa. Esimerkiksi maksuttomien ja maksullisten sovellusten tutkimus, jolloin voitaisiin tutkia ja verrata tarkemmin hinnan vaikutusta omaksumisprosessiin. Myös ominaisuuksiltaan eroavien sovellusten vertaileva tutkimus voisi tuoda arvokasta lisätietoa omaksumisprosessin näkökulmasta; miten käyttäjät kokevat eri ominaisuudet ja miten se vaikuttaa omaksumiseen.

Kolmantena esiin nousi se, että hinnan vaikutus omaksumiseen näkyi selkeästi negatiivisena, jolloin Freedomen hinnan vaikutuksen tarkempi tutkimus voisi tuoda F-Securelle arvokasta lisätietoa kuluttajista. Tutkimuksella voitaisiin esimerkiksi selvittää kuinka paljon käyttäjät olisivat valmiita maksamaan sovelluksen käytöstä ja mistä ominaisuuksista käyttäjät olisivat valmiita maksamaan, sekä millainen hinnoitteluperiaate olisi sopivin (esimerkiksi kertamaksu, vuosimaksu tai joku muu).

LÄHTEET

Ajzen I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes* 50, 179-211.

Ajzen I., Fishbein M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall.

Bogel, N., Davis, A., Rafaeli, E. (2003). Diary Methods: Capturing Life as it is Lived. *Annual Review of Psychology; 2003; 54, ProQuest Central* 579-616.

Chang, J., Ho, P. & Chang, T. (2014). *Securing BYOD*. IEEE Computer Society, Securing IT 1520-9202/14, pp. 9-11.

Chin, E., Porter Felt, A., Sekar, V. & Wagner, D. (2012). Measuring User Confidence in Smartphone Security and Privacy. *SOUPS '12 Proceedings of the Eighth Symposium on Usable Privacy and Security Article No. 1.*

Consumer Reports. (2014). Smart phone thefts rose to 3.1 million last year, Consumer Reports finds. Industry solution falls short, while legislative efforts to curb theft continue. Haettu 10.2.2015 osoitteesta: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

Conway, S. & Steward, F. (2009). *Managing and Shaping innovation.* Oxford: University press.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Aceptance of Information Technology. *MIS Quarterly*, 13 (3,) 319-340.

Egenfeldt-Nielsen, S. (2010). The Challenges to Diffusion of Educational Computer Games. *4th European Conference on Games Based Learning 2010, ECGBL 2010.* Denmark : Copenhagen.

F-Secure. (2015a). F-Secure Freedome. Haettu 3.2.2015 osoitteesta https://www.f-secure.com/fi_FI/web/home_fi/freedome.

F-Secure. (2015b). Lehdistötiedotteet: F-Secure estää verkkoseurannan yhdellä napin painalluksella. Haettu 3.2.2015 osoitteesta https://www.f-secure.com/fi_FI/web/press_fi/news-clippings/-/journal_content/56/1082194/1171226?p_p_auth=iN80IyBM&refererPlid=910425.

F-Secure. (2015c). Classification. How F-Secure classifies threats. Haettu 11.2.2015 osoitteesta: https://www.f-secure.com/en/web/labs_global/classification.

F-Secure. (2015d) Google Play: F-Secure Freedome VPN. Haettu 12.2.2015 osoitteesta: https://play.google.com/store/apps/details?id=com.fsecure.freedome.vpn.security.privacy.android&referrer=utm_source%3Dweb_product_page%26utm_campaign%3DFI&hl=fi.

F-Secure. (2013). Lehdistötiedotteet: F-Securen Younited haastaa amerikkalaiset pilvipalvelut. Haettu 4.11.2014 osoitteesta http://www2.f-secure.com/fi/web/corporation_fi/news-info/product-news-offers/view/story/1185238/F-Securen%20younited%20haastaa%20amerikkalaiset%20pilvipalvelut.

F-Secure. (2014). Tietoa F-Securesta. Haettu 28.10.2014 osoitteesta http://www2.f-secure.com/fi/web/corporation_fi/company/about-f-secure.

Fishbein, M., Ajzen, I. (1975). *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research.* Reading, MS: Addison-Wesley.

Flanagan, J.C. (1954). The critical incident technique. *Psychological Bulletin, 51(4),* 327-358.

Gilbert, J. (2012). *Tech Trends Bring Your Own Device to Work.* IT Insight, august 2012, pp. 38-40.

Gremler, D. (2004). The Critical Incident Technique in Service Research. *Journal of Service Research 2004*.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2003). *Tutki ja kirjoita.* Helsinki: Kustannusosakeyhtiö Tammi.

Hirsjärvi, S. & Hurme, H. (2011). *Tutkimushaastattelu, teemahaastattlun teoria ja käytäntö.* Helsinki: Gaudeamus.

IT-Viikko. (2013). Tutkimus: Virussuoja puuttuu monesta mobiililaitteesta. Hettu 19.3.2015 osoitteesta http://www.itviikko.fi/tietoturva/2013/02/13/tutkimus-virussuoja-puuttuu-monesta-mobiililaitteesta/20132394/7.

Kalliokulju, S., Palviainen, J. (2006). Miten massamarkkina syntyy? Keskeisiä teorioita vuosien varrelta. Haettu 2.12.2014 osoitteesta http://www.cs.tut.fi/~ihtesem/s2006/teoriat/esitykset/IHTESEM06_Kalliokulju_Palviainen_diffuusio_311006.pdf

Kuningaskuluttaja. (2014). Vinkkejä Netflixin käyttöön – tee kokemuksesta parempi. Haettu 29.3.2015 osoitteesta http://yle.fi/aihe/artikkeli/2014/05/17/vinkkeja-netflixin-kayttoon-tee-kokemuksesta-parempi.

Järvinen, P., Järvinen, A. (1995). *Tutkimustyön metodeista.* Tampere: Opinpaja Oy.

JUHTA – julkisen hallinnon tietohallinnon neuvottelukunta. (2014). JHS-suositukset: JHS 190 julkisten verkkopalvelujen suunnittelu ja kehittäminen. Haettu 6.2.2015 osoitteesta http://docs.jhs-suositukset.fi/jhs-suositukset/JHS190/JHS190.pdf.

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? *IEEE Computer Society June 2011 Volume: 44.* Pp. 11-14.

Limnell, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*. Jyväskylä: Docendo.

Lin, A., Nan-Chou C. (2012). Cloud computing as an innovation: Percepetion, attitude, and adoption. *International Journal of Information Management 32 (2012)*.

Lyytinen, K., Damsgaard, J. (2001). What's wrong with the Diffusion of Innovation Theory. The case of a complex and networked technology. *Teoksessa Proceedings of the IFIP 8.6. Conference, Canada.*

Miller, K., Voas, J. & Hurlburt, G. (2012). BYOD: Security and Privacy Considerations. *IT Professional Issue No.05 - Sept.-Oct. (2012 vol.14)* pp: 53-55.

Moore, G.A. (1999). *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers.* New York: Harper Business Essentials.

Mylonas, A., Kastania, A. & Gritzalis, D. (2013). Delegate the Smartphone User? Security Awarness in Smartphone platforms. *Computers & Security Volume 34, May 2013.* Pp. 47–66.

Need for Speed N4S. (2014). Haettu 30.10.2014 osoitteesta http://www.n4s.fi/fi/

Ojasalo, K., Moilanen, T. & Ritalahti, J. (2009). *Kehittämistyön menetelmät – Uudenlaista osaamista liiketoimintaan*. WSOYpro: Helsinki.

Routio, P. (2005). Kyselevät tutkimustavat. Haettu 16.02.2015 osoitteesta http://www2.uiah.fi/projects/metodi/064.htm.

Robson, C. (1995). *Real world research: a resource for social scientists and practitioner-researchers* (5. painos). Oxford: Blackwell.

Rogers, E. M. (2003). *Diffusion of Innovations* (5. painos). New York: Free Press..

Salo, M. (2014). Explaining Extreme Mobile Experiences. *Intl. Journal of Human–Computer Interaction, 30*. Pp. 164–176.

Sanastokeskus TSK ry. (2014). Haettu 29.10.2014 osoitteesta http://www.tsk.fi/tepa/netmot.exe?UI=figr&height=161

Tilastokeskus. (2014). Väestön tieto- ja viestintätekniikan käyttö 2014. Puolet suomalaista mukana yhteisöpalveluissa. Haettu 11.2.2015 osoitteesta: http://www.tilastokeskus.fi/til/sutivi/2014/sutivi_2014_2014-11-06_fi.pdf.

Torrentfreak. (2015). Netflix cracks down on VPN and proxy "pirates". Haettu 29.3.2015 osoitteesta https://torrentfreak.com/netflix-cracks-down-on-vpn-and-proxy-pirates-150103/.

Tricks Window. (2012). How to stay Secure on public wifi spot by using VPN. Haettu 12.2.2015 osoitteesta http://www.trickswindow.com/networking/using-vpn-on-public-wifi/.

TNS Gallup digital / NetTrack 2014 (2014). Suomalaiset verkossa – NetTrack 2014 IAB:n kooste. Haettu 3.2.2015 osoitteesta http://www.iab.fi/media/pdf-tiedostot/verkkomainonnan-abc/nettrack-2014_iab.pdf.

Tuomi, J. & Sarajärvi, A. (2004). *Laadullinen tutkimus ja sisällönanalyysi.* Helsinki: Kustannusosakeyhtiö Tammi.

Venkatesh V. & Davis F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, informs,* 46 (2), 186-204.

Venkatesh V., Morris M. G., Davis G. B., Davis F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly 27* (3), 425-478.

Venkatesh, V., Thong, J. Y. L & Xu, X. (2012). Consumer acceptance and use of information technology: Extending The Unified Theory of Acceptance and Use of Technology. *MIS Quarterly, 36(1),* 157-178.

Viestintävirasto. (2014). Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön. Haettu 12.2.2015 osoitteesta https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf.

Viestintävirasto. (2014b). Evästeet. Haettu 26.3.2015 osoitteesta https://www.viestintavirasto.fi/tietoturva/palveluidenturvallinenkaytto/evasteet.html.

LIITE 1

Viesti haastateltavien hakemiseksi.

Hei!

Haen haastateltavia pro gradu-tutkimukseeni, jossa tavoitteena on tutkia miten kriittiset käyttökokemukset vaikuttavat F-Securen Freedomen omaksumiseen ja jatkuvaan käyttöön.

Jos olet Freedome-mobiilisovelluksen käyttäjä, ja sinulla ei ole aikaisempaa kokemusta samantyyppisestä tietosuojapalvelusta, niin haluaisin haastatella sinua sovelluksen käyttöön liittyen.

Jos pystyt osallistumaan lyhyeen puhelinhaastatteluun, niin ota minuun sähköpostitse yhteyttä, kerron mielelläni lisätietoja.

Terveisin,
Anna Nemtsinkoff-Rajala
anna.nemtsinkoff@gmail.com

LIITE 2

Haastattelurunko.

Esittely:
Ensimmäisenä haluan mainita, että tämä haastattelu tallennetaan, ja kirjoitetaan myöhemmin luottamuksellisesti puhtaaksi. Saanko suostumuksesi tallentaa tämän puhelun?

Opiskelen tietojärjestelmätiedettä Jyväskylän yliopistossa; suuntautumisenani tietoyhteiskunta, viestintä ja liiketoiminta. Pro graduni käsittelee mobiililaitteiden kyberturvallisuutta ja tämän haastattelun tavoitteena on selvittää miten erilaiset käyttökokemukset vaikuttavat Freedomen omaksumiseen ja jatkuvaan käyttöön. Tutkimus toteutetaan osana Digilen Need for Speed –projektia.

Toivon sinun vastaavan kysymyksiin rehellisesti, jotta vastaukset olisivat mahdollisimman aitoja. Pro gradussani ei tule näkymään arkaluontoisia tietoja ja tutkimusaineisto käsitellään luottamuksellisesti. (Onko tässä vaiheessa kysyttävää?)

Kysymykset:

1. Demografiset tekijät: sukupuoli, ikä, päätoiminen asema (opiskelija, töissä, työtön, eläkeläinen jne.)?
2. Kuinka kauan olet käyttänyt Freedomea?
3. Missä laitteissa (merkki ja malli) käytät Freedomea?
4. Mieti rauhassa yksittäinen tilanne, jolloin sinulla on ollut mielestäsi merkittävän positiivinen tai negatiivinen käyttökokemus Freedomen käytössä. Käytä muisteluun kunnolla aikaa.
    a. Oliko kokemus negatiivinen vai positiivinen?
    b. Minkä laitteen käytössä se on tapahtunut?
    c. Missä havaitsit tapahtuman (esimerkiksi töissä, matkoilla tai kotona)?
    d. Milloin havaitsit tapahtuman?
    e. Kuvaile tapahtumaa omin sanoin.
    f. Mikä tarkalleen ottaen aiheutti kokemuksen positiivisuuden / negatiivisuuden?
    g. Millaisia seurauksia tapahtumalla oli käytön kannalta?
    h. Kuinka merkittävä kokemus oli käytön jatkumisen kannalta?
5. Tuleeko sinulle mieleen toista merkittävää kokemusta? (Toistetaan tarvittaessa kysymys numero 4:n alakysymykset.)
6. Jos olet käyttämässä 2 viikon kokeilujaksoa nyt, aiotko jatkaa käyttöä vielä ilmaisen jakson päätyttyä? Miksi?