JYVÄSKYLÄ STUDIES IN COMPUTING
234

Minna Alasuutari

Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 234

Minna Alasuutari

Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella julkisesti tarkastettavaksi yliopiston Mattilanniemen A-rakennuksen salissa MaA103 huhtikuun 23. päivänä 2016 kello 12.

Academic dissertation to be publicly discussed, by permission of the Faculty of Information Technology of the University of Jyväskylä, in Mattilanniemi, auditorium MaA103, on April 23, 2016 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2016

Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta

JYVÄSKYLÄ STUDIES IN COMPUTING 234

Minna Alasuutari

Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2016

Editors
Marja-Leena Rantalainen
Department of Mathematical Information Technology, University of Jyväskylä
Pekka Olsbo, Ville Korkiakangas
Publishing Unit, University Library of Jyväskylä

URN:ISBN:978-951-39-6609-6
ISBN 978-951-39-6609-6 (PDF)

ISBN 978-951-39-6608-9 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2016

ABSTRACT

Alasuutari, Minna
The process theory approach that explains the change of IS security behavior related to personal computer use
Jyväskylä: University of Jyväskylä, 2016, 229 p.
(Jyväskylä Studies in Computing
ISSN 1456-5390; 234)
ISBN 978-951-39-6608-9 (nid.)
ISBN 978-951-39-6609-6 (PDF)

IS security behavior has become a mainstream topic in information systems. Extent research is dominated with the viewpoint for discovery of generic and stable predictors. The viewpoint rests on the implicit assumption that information security behavior can be explained by discovering these factors. The best know examples are IS security behavior models grounded upon Protection Motivation Theory (PMT) and the Deterrence Theory (DT). The success of this perspective hinges on the question as to what extend the IS security behavior and the reasons for it, are constant from time to time and from one specific security situation to another. The viewpoint is successful if computer users have built in predictors – such as fear of sanctions, which are stable across security situations and time. But if these build-in predictors change during the time or from one situation to another, this viewpoint encounters problems, because of the investment in stability and context-independence, while nothing on change and context dependence. Based on Searle's theoretical ideas regarding subjective construction of reality and intentionality, I make the case that computer users construct their social reality through interacting with different events, things and situations. I maintain that computer users change their behavior, because certain experiences of events related to information security causes the change in their perceived reality and underlying beliefs, thoughts and judgments. This is an approach, which prior research has not considered, because it has explained IS security behavior as a stable and unchangeable phenomenon. By interviewing computer users, in my doctoral dissertation, I demonstrate how the users create social reality in the interaction with the different combinations of elements of social reality that they experience (for example threats, information sources, harmful consequences). I also show how motivational aspects (needs and emotions) relate to information security behavior. Through accomplishing these objectives, the dissertation illustrates the sources of the change of IS security behavior, the reasons for change, and why it is not static; unlike prior research that applies, for example, PMT and DT theories, assumes.

Keywords: IS security, IS security behavior, motives, IS security practices, subjective construction of reality

Author Minna Alasuutari
Department of Computer Science and Information Systems
University of Jyväskylä

Supervisors Professor Mikko Siponen
Department of Computer Science and Information Systems
University of Jyväskylä

Doctor Mari Karjalainen
Department of Information Processing Science
University of Oulu

Reviewers Prof. Rauno Kuusisto
Finnish Defence Research Agency

Docent Jyri Rajamäki
Laurea University of Applied Sciences

Opponent Docent Tuija Kuusisto
Ministry of Finance

ESIPUHE

Kiinnostukseni tietoturva-asioihin heräsi vuonna 2005, jolloin Oulun yliopistossa aloitettiin tietojenkäsittelytieteen laitoksen organisoima tietoturvan maisteriohjelma. Tähän koulutusohjelmaan pääseminen aloitti uuden, mielenkiintoisen jakson elämässäni. Tämä väitöskirja on 10-vuotisen tietoturva-alan opiskelujeni huipentuma.

Tähän tavoitteeseen pääsemisestä kuuluu kiitokset ohjaajilleni, professori Mikko Siposelle ja tohtori Mari Karjalaiselle. Asiantunteva ja kannustava palautteenne on ollut merkittävää, erityisesti työn ollessa ajoittain vastatuulessa. Olen kokenut olevani etuoikeutetussa asemassa saadessani työskennellä kaltaistenne lahjakkaiden tutkijoiden kanssa. Kiitos myös Jyväskylän yliopistolle tutkimuksen taloudellisesta tukemisesta sekä työn esitarkastajille professori Rauno Kuusistolle ja dosentti Jyri Rajamäelle valaisevista kommenteista ja korjausehdotuksista.

Tutkimusryhmän tuki matkan varrella on ollut tärkeää. Xiuyan Shao, Ying Li, Hemin Jiang, tohtori Nan Zhang, tohtori Yixin Zhang, Hadi Ghanbari, Tiina Koskelainen ja Alain Tambe Ebot: kiitos työstäni antamastanne palautteesta, rohkaisusta ja positiivisen sosiaalisen ilmapiirin luomisesta laitoksella. On ollut tärkeää kuulua ryhmään, jossa muut ovat samassa tilanteessa, jakavat samantyyppisiä onnistumisen ja epäonnistumisen hetkiä sekä unelman väitöskirjan valmistumisesta. Erityiskiitokset Naomi Woodsille tutkimuksen teoreettisen viitekehyksen kommentoinnista psykologian näkökulmasta sekä englanninkielisen abstraktin oikolukemisesta.

35 tietokoneenkäyttäjää tarjosi korvauksetta aikaansa osallistuessaan haastateltavaksi tutkimukseen. Tuhannet kiitokset teille! Olette olleet oppainani tällä matkalla ja jokainen teistä on ollut tärkeä. Kiitos myös Tutkimustie Oy:lle ja Spoken Oy:lle haastattelujen litteroinnista.

Tämän työn valmistumiseen on olennaisesti vaikuttanut myös perheeni, ystävieni ja lasteni tuki. Kiitos teille! Omistan väitöskirjan Ellalle, Jaakolle ja Leolle. Kiitos rakkaudestanne, kannustuksestanne ja ymmärryksestä äidin tutkimustyötä kohtaan ☺

Oulussa 24.3. 2016
Minna Alasuutari

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Internetin käyttö on lisääntynyt nopeasti viimeisten vuosikymmenten aikana ja ihmiset ovat tulleet koko ajan enemmän riippuvaiseksi informaatioteknologiasta. Internet on monipuolinen tietoresurssi ja tarjoaa monenlaisia palveluja mutta toisaalta, ollessaan yhteydessä tietoverkkoon käyttäjät ovat haavoittuvaisia sen tuomille uhkille. Esimerkiksi tietokonevirukset, vakoiluohjelmat ja madot, tietojen kalastelu ja erilaiset huijausviestit uhkaavat tietokoneen käyttäjiä, kun he ovat yhteydessä Internetiin (Kumar et al., 2008; Furnell et al., 2007).

Jos tietokonetta ei ole suojattu, hyökkääjät voivat mm. hyödyntää sitä osana ns. botnetiä ja käyttää resursseja palvelunestohyökkäykseen tai levittää roskapostia ja kalasteluviestejä botnetin avulla (Furnell et al., 2007). Tällaisten tietoturvarikosten haitallisia seuraamuksia ovat mm. identiteettivarkaus, tiedon varastaminen, kiusanteko tai petos (NCSA & McAfee, 2011). Laaja kansainvälinen tutkimus osoitti, että noin 556 miljoonaa aikuista oli kokenut jonkinlaisen tietoturvarikoksen ja enemmän kuin 232.4 miljoonaa identiteettiä varastettiin vuoden 2011 aikana (Symantec, 2011). Tietoturvakäyttäytyminen on tärkeä ja ajankohtainen tutkimusaihe, ja tietojärjestelmätieteilijät ovat viime aikoina käyttäneet paljon resursseja sen selittämiseen (Johnston et al. 2015; Karjalainen & Siponen 2011).

Aiempi tutkimus selittää tietoturvakäyttäytymistä teorioilla, jotka on lainattu muilta tieteenaloilta, kuten esimerkiksi Protection motivation theory (PMT), Theory of reasoned action (TRA) and Deterrence theory (DT). Näistä suosituimmat ovat DT ja PMT (Siponen & Vance, 2014). Tutkimukset, jotka pohjautuvat em. teorioihin, pyrkivät verifioimaan yleisiä ja pysyviä ennustavia tekijöitä (riippumattomia muuttujia) tietoturvakäyttäytymiselle. Tutkimukset tarkastelevat tietoturvakäyttäytymistä vakaana ja muuttumattomana ilmiönä. Tutkimukset olettavat, että ennustavat tekijät – kuten perheen ja vertaisjoukon vaikutus – ovat pysyviä tilanteesta ja ajankohdasta toiseen. Vaikka tämänhetkinen tutkimus auttaa ymmärtämään tietoturvakäyttäytymisen taustalla olevia syitä, se ei ota huomioon että käyttäytyminen voi olla kontekstisidonnaista ja muuttuvaa. Tutkimuksessa on selvitetty ennustavia tekijöitä käyttäytymiselle mutta jätetty huomiotta se, missä tilanteissa nämä ennustavat asiat - kuten esi-

merkiksi perheen ja vertaisten vaikutus tai pelko – selittävät käyttäytymistä ja kuinka tietoturvakäyttäytyminen muuttuu.

Tämän tutkimuksen tarkoitus on ymmärtää ja selittää henkilökohtaisen tietokoneen käyttäjien tietoturvakäyttäytymistä osoittamalla, kuinka tietokoneen käyttäjät luovat subjektiivista todellisuutta itse ja muuttavat käyttäytymistä kokemuksen pohjalta, olemalla yhteydessä erilaisiin tietoturvaan liittyviin asioihin, tilanteisiin, ihmisiin ja tapahtumiin. Muutos ajattelussa aiheuttaa tietoturvakäyttäytymisen muutoksen. Teoreettinen lähtökohta tutkimukselle on John Searlen ajatuksissa todellisuuden luomisesta ja kokemuksen tarkoituksellisuudesta sekä motivaatiopsykologiassa.

Haastattelimme tutkimukseen 35 henkilökohtaisen tietokoneen käyttäjää, jotka edustivat eri kansallisuuksia ja koulutus- ja ammattiryhmiä. Haastattelujen pohjalta tutkimuksessa otettiin tarkempaan tarkasteluun 6 suojaustoimenpidettä:

- varmuuskopiointi
- virustorjunta
- vahvan salasanan laatiminen
- Internet-profiilin hallinta
- varovaisuus verkkokaupassa
- sensitiivisen aineiston prosessointi

Varmuuskopiointi ja virustorjunta valikoituivat mukaan sillä perusteella, että niitä toteutettaessa tietokoneen käyttäjä on tekemisissä erilaisten tietoturvaohjelmistojen tai tallennusvälineiden kanssa (tietoturvaohjelmistot, USB-tikut, pilvipalvelut). Salasanakäyttäytyminen on käyttäytymistyyppinä erilainen kuin edelliset, koska siinä tietokoneen käyttäjän on muistettava ulkoa tietty merkkijono. Internet-profiilin hallinta ja sensitiivisen aineiston prosessointi liittyvät tietojen käsittelyyn ja suojaamiseen Internetissä (sähköposti, sosiaalinen media). Verkkokauppakäyttäytyminen oli tärkeä ottaa mukaan, koska siinä ollaan selkeimmin tekemisissä rahan kanssa: tietoverkon välityksellä liikkuu verkkokaupan maksutietoja kuten esimerkiksi luottokorttinumeroita.

Edellä mainittujen suojaustoimenpiteiden kohdalla käyttäytyminen selkeästi muuttui. Muutosta oli lisäksi kuvattu monipuolisesti, minkä pohjalta käyttäytymisen muutosprosesseja oli hyvä lähteä mallintamaan. Haastattelut havainnollistavat, kuinka tietoturvakäyttäytymisen muutos ja muutoksen syyt voidaan selittää Searlen ajatusten ja motivaatiopsykologian pohjalta.

Tietoturvan ammatinharjoittajille tutkimus tarjoaa välineitä tietoturvakäyttäytymisen parantamiseen, sillä tietoturvakäyttäytymistä on helpompi kehittää, jos sitä voidaan ensin ymmärtää. Tietoturvatutkimukselle tämä työ tarjoaa useita tutkimussuuntia.

Tutkimus on jaoteltu seuraavasti: luku 2 määrittelee tutkimuksen teoreettisen viitekehyksen. Luvussa 3 perustellaan, miksi prosessiteoria-näkökulma on valittu tähän tutkimukseen. Neljäs luku sisältää katsauksen olemassa olevaan

tutkimukseen kotikäyttäjien tietoturvakäyttäytymisestä ja työsidonnaisesta tietoturvakäyttäytymisestä.

Tutkimusmenetelmät ja aineiston hankinta on esitetty luvussa 5. Tutkimustulokset sisältyvät lukuun 6. Vertailu aiempaan tietoturvakäyttäytymiskirjallisuuteen sisältyy lukuun 7. Yhteenveto-luku tiivistää tutkimuksen keskeiset tulokset.

2 TEOREETTINEN VIITEKEHYS

Käyttäytyminen on luonteeltaan muuttuvaa. (Bridle et al., 2005; Weinstein et al. 1998.) Tämän vuoksi näkökulma, jonka tavoitteena on selittää käyttäytymistä ennustavilla ja muuttumattomilla seikoilla (kuten esimerkiksi asenne, sosiaalinen normi tai tietoisuus seuraamusten vakavuudesta) on riittämätön, sillä käyttäytymiseen vaikuttavat seikat muuttuvat (Abbot, 1990; Weinstein et al,. 1998). Esimerkiksi ihmisillä, jotka omaksuvat jonkin tietyn terveyskäyttäytymisen, voi olla monia eri reittejä ja polkuja, jotka johtavat käyttäytymisen muutokseen (Weinstein et al.,1998).

John Searle (1995 & 1983) tarjoaa teoreettisen selityksen käyttäytymisen muutokselle ajatuksillaan todellisuuden luomisesta ja kokemuksen tarkoituksellisuudesta. Keskeisimmät, tähän tutkimukseen soveltuvat ajatukset on esitelty luvussa 2.1. Searlen ideoita käyttäytymisen tarkoituksellisuudesta on sovellettu aiemmin mm. kognitiivisen neurotieteen alalla, tutkittaessa kokeellisesti tarkoituksellista toimintaa (mm. Haggard & Clark, 2003; Becchio et al, 2006).

Tarve/ motiivipsykologia täydentää tutkimuksen teoreettista viitekehystä. Maslow (1954 & 2007), Alderfer ja McClelland (Robbins, 1993) ja Reiss (2004) ehdottavat, että ihmisellä on tarpeita, jotka motivoivat häntä toimimaan tietyllä tavalla. Tässä tutkimuksessa hyödynnettyjä motiiviteorioita on esitelty luvussa 2.2. Tarpeiden tapaan myös tunteet motivoivat käyttäytymistä ja vaikuttavat ajatteluumme (Ellsworth & Schrerer, 2003). Tässä tutkimuksessa tunteiden merkitystä käyttäytymiseen on tarkasteltu erityisesti appraisal-teorian näkökulmasta (luku 2.3.)

2.1 Todellisuuden subjektiivinen muodostaminen

Searle (1995) esittää, että ihmiset luovat todellisuutta itse, omiin tarkoituksiinsa. Siksi todellisuutemme on ihmisen luomaa ja ihmisen ajatuksista riippuvaista. Pohjautuen Searlen (1995) teoreettisiin ideoihin todellisuuden subjektiivisesta muodostamisesta ja kokemuksen tarkoituksellisuudesta (1983) voidaan olettaa

että ihmisten kokemukset, interaktio ympäröivässä maailmassa olevien asioiden, ihmisten, tapahtumien ja tilanteiden kanssa ja kokemuksen tarkoituksellisuuden pohtiminen aiheuttavat käyttäytymisen muutoksen (ks. myös kaavio 1).

Kokemus

Todellisuuden muodostamisessa subjektiiviset kokemukset ovat tärkeässä asemassa, koska ne muuttavat ihmisen ajattelua (Searle, 1990; Searle, 2013). Ihmiset kokevat uusia asioita, tapahtumia ja tilanteita koko ajan ja ovat yhteydessä muihin ihmisiin. Searlen mukaan kokemukset ovat tietoisia tapahtumia, ja niihin sisältyy tarkoituksellisuus (intentionality). Tämä tarkoittaa Searlea tulkiten sitä, että pohdimme kokemiemme asioiden ja tapahtumien merkitystä itsellemme. Tarkoituksellisuuden ja merkityksen pohtiminen sisältyy kaikkiin kokemuksiin. Kokemuksia voidaan verrata käsityksiin, tunteisiin (esim. pelkoihin) ja toivomuksiin, sillä myös niihin sisältyy asioiden merkityksen ja tarkoituksellisuuden pohtiminen (Searle, 1983).

Yhteydet ympäröivään maailmaan (interaktio)

Ihmiset ovat yhteydessä ympäröivään maailmaan, mikä vaikuttaa ajatteluun ja käyttäytymiseen. Kommunikoimme päivittäin ihmisten kanssa, koemme erilaisia tapahtumia ja asioita. Searle (1983) käyttää termiä “background”, jonka tulkitsen tarkoittavan ihmisellä olevia olettamuksia, käytäntöjä ja tapoja. Näitä ei voi esiintyä ilman niitä sosiaalisia yhteyksiä, joita ihmiset päivittäin kokevat.

Tarkoituksellisuus

Tarkoituksellisuus tarkoittaa asioiden, tapahtumien ja tilanteiden merkityksen pohtimista omasta näkökulmasta, ja se on tärkeässä asemassa todellisuuden muodostamisessa (Searle, 1995). Muodostamme ympäristössä ilmenevien asioiden tarkoituksen itsellemme. Searle (1995) kutsuu tätä havainnoija-sidonnaisuudeksi (making observer relative features). Hän ehdottaa, että sosiaalinen todellisuus voidaan ymmärtää ainoastaan sen jaottelun valossa, että on olemassa ns. perustavanlaatuisia elementtejä (intrinsic features) ja havainnoija-sidonnaisia elementtejä. Taulukko 1 tarkentaa näiden elementtien välisiä eroja.

TAULUKKO 1 Perustavanlaatuisten elementtien ja havainnoija-sidonnaisten elementtien erot

Perustavanlaatuiset elementit (intrinsic features)	**Havainnoija-sidonnaiset elementit** (observer relative features)
Luonteeltaan objektiivinen	Luonteeltaan subjektiivinen
Ei ole riippuvainen havainnoijan näkökulmasta ja mielipiteistä.	Edellyttää havaintojen tarkoituksellisuuden pohtimisen. Ovat tarkoituksellisia ja merkityksellisiä havainnoijille.
Esimerkki: "Esineellä edessäni on tietty paino ja tietty kemikaalinen koostumus. Se on tehty osittain puusta, selluloosasta ja osittain metallista."	Esimerkki: "Esine edessäni on ruuvimeisseli, koska ihmiset käyttävät sitä ruuvimeisselinä"

Ihmiset muodostavat havainnoija-sidonnaisia elementtejä, kun he pohtivat asioiden esineiden ja tapahtumien merkitystä itselleen. Searle (1995) kutsuu tätä merkityksen muodostamiseksi (assignment (or imposition) of function).

Käyttäytymisen muutos

Edellä mainitut kolme elementtiä (kokemus, interaktio ja tarkoituksellisuuden pohtiminen) aiheuttavat käyttäytymisen muutoksen. Ihmiset kokevat uusia asioita tapahtumia ja tilanteita ja ovat yhteydessä toisiin ihmisiin Nämä kokemukset herättävät tarkoituksellisuuden, sillä ihmiset miettivät kokemuksen merkitystä itselleen. Muutos ajattelussa aiheuttaa muutoksen käyttäytymisessä. Käyttäytymisen muutos edellyttää siis sekä kokemuksen että interaktion ympäröivän maailman kanssa sekä sen että ihmiset miettivät asioiden merkitystä itselleen.

2.2 Tarve/motivaatiopsykologia

Selityksen käyttäytymisen muutokselle tarjoaa Searlen ajatusten lisäksi motivaatiopsykologia, joka pyrkii selittämään miksi ihmiset käyttäytyvät tai ajattelevat tietyllä tavalla. Motivaatioselitys vaatii, että ihmisellä on käytettävissään vaihtoehtoja (Nurmi & Salmela-Aro, 2002.) Motiivilla tarkoitetaan toiminnan psyykkistä syytä, toimintaa ohjaavaa voimaa ja vaikutinta. (Vilkko-Riihelä, 1999). Motiivit ilmenevät haluna, tarpeena, yllykkeenä ja vaikuttimena. Käyttäytymistä ohjaavat siis sekä sisäiset vietit ja tarpeet että ympäristön ärsykkeet. Yksi modernin motivaatiopsykologian keskeisiä tutkimusaloja on ihmisen henkilökohtaisten pyrkimysten, päämäärien ja tavoitteiden tutkiminen toimintaa ohjaavana tekijänä (Vilkko-Riihelä, 1999). Motivaatio voi ilmetä myös tietyssä tilanteessa, jossa ihminen tulkitsee kokemansa ärsykkeen merkittäväksi itsel-

leen, esimerkiksi kun ihminen näkee jonkin myytävänä olevan tuotteen, hän haluaa ostaa sen.

Motiivit voivat olla keskenään ristiriidassa. Esimerkiksi oma sisäinen toive voi olla ristiriidassa ulkoisen paineen kanssa (Vilkko-Riihelä, 1999). Ihmisellä voi olla myös kaksi vastakkaista tavoitetta, esimerkiksi halu suojata omaisuutta ja toisaalta halu toimittaa jokin asia tehokkaasti sähköisesti mikä aiheuttaa ristiriidan. Motiivikonfliktin ratkeaminen riippuu niin tilanteesta, omista pohdinnoista (omista tulkinnoista ja motiiveihin liitetyistä arvoista) kuten myös muiden ihmisten antamasta palautteesta.

Tässä työssä on sovellettu tulkiten Maslow:n (1954 & 2007) motiivihierarkiaa sekä uudemmista teorioista Alderferin ERG – teoriaa, McClellandin tarveteoriaa (Robbins, 1993) sekä Reiss:n (2004) motiiviteoriaa.

Maslow:n motiivihierarkiassa (1954 & 2007) ihmisellä on ns. puutemotiiveja ja kehittymismotiiveja. Puutemotiiveja ovat mm. turvallisuuden, yhteenkuuluvuuden (halu toimia muiden kanssa ja halu tulla hyväksytyksi) ja sosiaalisen arvostuksen tarpeet (halu suoriutua hyvin ja tulla huomioonotetuksi). Kehittymismotiiveja ovat esteettiset, älylliset (tutkimisen, tietämisen ja ymmärtämisen) sekä itsensä toteuttamisen tarpeet (omien taipumustensa kehittäminen ja voimavarojen käyttäminen).

Turvallisuuden tarve on yksi keskeisiä tarpeita tässä tutkimuksessa, sillä uuden suojaustoimenpiteen käyttöönotto pohjautuu aina tälle tarpeelle. Turvallisuuden tarpeella Maslow (2007) tarkoittaa mm. tarvetta vakauteen, suojaan ja järjestykseen. Ihminen haluaa olla vapaa huolesta ja pelosta ja turvata omaisuutensa (esimerkiksi raha, työpaikka, terveys) ja hakee turvaa ja pysyvyyttä maailmaan, mikä on nähtävissä mieltymyksenä mieluummin tuttuihin kuin tuntemattomiin asioihin. Turvallisuuden tarve voi korostua, jos sosiaalisessa ympäristössä on uhkia laille ja järjestykselle. Turvallisuuden tarve ilmenee myös vaikeissa tilanteissa ja hätätilanteissa.

Alderferin ERG – teoria on tarkistettu versio Maslow:n tarveteoriasta. Alderferin mukaan ihmisellä on kolmenlaisia perustarpeita 1) toimeentulotarpeet (existence), liittymistarpeet (relatedness) ja kasvutarpeet (growth) (Robbins, 1993; Peltonen & Ruohotie, 1987). Toimeentulotarpeet ovat materiaalisia ja sisältävät Maslowin hierarkiassa fyysiset ja turvallisuuden tarpeet. Henkilö kokee tarvetta suojautua fyysiseltä ja emotionaaliselta vahingolta. Liittymistarpeilla Alderfer tarkoittaa halua ylläpitää tärkeitä ihmissuhteita. Ne sisältävät Maslow:n hierarkian yhteenkuuluvuuden motiivit ja osittain myös sosiaalisen arvostuksen motiivit. Kasvutarpeet taas tarkoittavat henkilön luontaista halua henkilökohtaiseen kehittymiseen ja pohjautuvat Maslow:n hierarkiassa kehittymismotiiveihin sekä osittain sosiaalisen arvostuksen motiiviin.

Maslow:n tarvehierarkiaa on aiemmin sovellettu mm. taloustieteissä. Sen avulla on kuvattu ja vertailtu elämänlaadun kehittymistä eri valtioiden välillä (mm. Hagerty, 1999; Sirgy, 1986; Diener, 1997; Veenhoven & Erhardt, 1995; Mazumdar, 1995). On myös selvitetty kuluttajien ostokäyttäytymistä ja päätöksentekoa (Asamoah et al, 2011) sekä verkkokauppakäyttäytymistä (Valacich, 2007) sekä tekijöitä jotka motivoivat työntekijöitä työskentelemään ei-valtiollisella

(non-governmental) sektorilla (Pulasinghage, 2010). Malsow:n teoriaa on sovellettu myös johtamisen tutkimiseen ja johtamistaitojen kehittämiseen (Juliano & Sofield, 2011; Raus, Raita & Lazar, 2012) sekä hoitotieteen puolella hyvinvoinnin, elämänlaadun ja työympäristön- ja hyvinvoinnin tutkimiseen (Ruchiwit, 2013; Cassar & Baldacchino, 2012; Paris & Terhaar, 2011). Myös lääketieteen opiskelijoiden oppimistarpeita ja -haasteita on pyritty ymmärtämään Maslow:n tarvehierarkian avulla (Sockalingam, 2014).

Alderferin ERG-teoriaa on sovellettu sosiologiassa, psykologiassa ja taloustieteessä. Sitä on hyödynnetty mm. tutkittaessa työpaikan motivaatiotekijöitä (mm. Wiley, 1997; Islam & Ismail, 2008; Kaliprasad, 2006 ja Ramprasad, 2013), selvitettäessä kuluttajien tarpeita mobiilipalveluita valittaessa (Yang et al. 2011) ja asiakkaiden interaktiota ja tarpeita web-pohjaisessa projektissa (Chang & Yuan, 2008). Song, Wang & Wei (2007) ovat tutkineet kulttuuristen tekijöiden vaikutusta motivaatioon ja Alderfer & Guzzo (1975) ovat selvittäneet ERG:n soveltuvuutta kestävien toiveiden (enduring desire) mittaamiseen.

McClellandin tarveteoriaan kuuluvat 1) halu saavuttaa ja menestyä (need for achievement) 2) vallanhalu (need for power) ja 3) halu kuulua johonkin (need for affiliation), joka tarkoittaa pyrkimystä ystävällisiin ja läheisiin ihmissuhteisiin. Tätä tarveteoriaa on sovellettu organisaatioissa työntekijöiden motivaation ja käyttäytymisen ymmärtämiseen (mm. Harrel & Stahl, 1984; McClelland & Burnham, 1995; Duffy & Lilly, 2013). Sosiaalipsykologiassa teoriaa on sovellettu vallanhalun ja poliittisten taitojen välisen yhteyden selvittämiseen (Randall, 2011) ja työetiikkaan, jossa motiiveista on tarkastelun kohteen ollut menestymisen halu (Niles, 1994). Psykologian kirjallisuudessa puolestaan on tutkittu mm. yksilön vallanhalun vaikutusta päätöksentekoon (Magee & Langner, 2008) ja McClellandin motiivien suhdetta ihmisten hyvinvointiin ja elämän sujuvuuteen (Schüler et al., 2013).

Yhtä uusimmista motiiviteorioista edustaa Reiss:n (2004) motiiviteoria ”The theory of 16 basic desires”, joka on muodostettu empiirisen tutkimuksen tuloksena. Motiivit perustuvat 2554 ihmisen käsityksiin siitä, mitkä asiat heitä motivoivat. Mielestäni tietoturvakontekstiin liittyviä käyttäytymiseen vaikuttavia tekijöitä olivat uteliaisuus, säästäminen /keräily, sosiaaliset kontaktit, hyväksyntä ja rauhallisuus (tranquility). Reiss:n motiiviteoriaa on sovellettu psykologiassa selvitettäessä TV:n katsomistottumuksia (Reiss & Wiltz, 2004), urheiluun motivoivia tekijöitä (Reiss et al, 2001) sekä heikkoon koulumenestykseen vaikuttavia tekijöitä (Reiss, 2009) Taloustieteen puolella sitä on hyödynnetty yrityksen wiki:n käyttöön liittyvien tunteiden ja motiivien kartoittamisessa (Gears, 2012).

Tarveteorioita on sovellettu tässä tutkimuksessa teknologian ja tietoturvan näkökulmasta. Edellä mainitut tarveteoriat eivät ota teknologiaa huomioon. Esimerkiksi Alderferin ERG – teorian mukaan (Robbins, 1993; Peltonen & Ruohotie, 1987) toimeentulotarve korostaa henkilön tarvetta suojautua fyysiseltä ja emotionaaliselta vahingolta mutta se ei ota tarkemmin kantaa mahdollisuuteen, että fyysinen vahinko voi kohdistua omistettavaan teknologiaan tai tietoomaisuuteen eikä toisaalta turvallisuus viittaa tietoturvallisuuteen. Liittymis-

tarpeista puhuessaan Alderfer tarkoittaa halua ylläpitää tärkeitä ihmissuhteita, mutta tämä ei käsitä tietoverkon kautta tapahtuvan kommunikoinnin tarvetta.

Tarpeiden ohella tunteet ovat käyttäytymiseen olennaisesti vaikuttava tekijä (Bedford, 1988; Fredrickson, 1998; Helkama et al, 1998; Vilkko-Riihelä, 1999). Motiivit liittyvät tunteisiin, koska tiettyyn toimintaan ja tekemiseen voi liittyä monenlaisia tunteita kuten iloa tai epävarmuutta. Toisaalta tunne itsessään voi toimia käyttäytymisen motiivina (Vilkko-Riihelä, 1999).

Tunteen käsite on koettu hankalaksi määritellä, ja sitä onkin ajan saatossa määritelty eri tavoin, eri näkökulmista, ja eri tieteenaloista käsin (mm. biologia, fysiologia ja sosiologia). Tunne-käsitettä ei voida määritellä yhdestä tietystä viitekehyksestä käsin (Sturdy, 2003). Niinpä tutkimuksessa valitaan yleensä jokin tietty näkökulma, jossa keskitytään johonkin tunne-käsitteen eri ulottuvuuksista. Tunne-käsitteeseen voidaan ottaa esimerkiksi psykologinen, historiallinen, kielitieteellinen tai biologinen lähestymistapa.

Tässä tutkimuksessa tunne-käsitteen määrittelyssä on käytetty perinteisen tunneteorian määrittelyä, jonka mukaan tunne voidaan ajatella erilaisiksi tuntemuksiksi, tunne-elämyksiksi ja tunnesanat nimetään uusien tuntemusten mukaan (Bedford, 1988). Olemme vihaisia, ylpeitä tai surullisia jostakin (Harre, 1988). Jokaista tunnetta oletetaan vastaavan kokemus (experience) joka ilmenee ulkoisessa käyttäytymisessä (expression) (Bedford, 1988; Harre, 1988).

Tunne-elämykset ovat yleensä lyhytkestoisia kun taas pitkäkestoisemmat tunnetilat (surumielisyys, ärtyneisyys, huolestuneisuus jne.) ovat mielialoja (Helkama et al, 1998). Emootioista tunne-elämykset erottaa se, että tunne voidaan ajatella emootion yhdeksi komponentiksi. Emootiot tarkoittavat kokonaisuutta, johon sisältyvät lisäksi myös mm. neurofysiologisen muutokset, erityinen käyttäytymisvalmius ja kognitiiviset arvioinnit (Helkama et al, 1998).

Tunteet ovat yksilön sisäisiä voimia, jotka vaikuttavat siihen, kuinka käyttäydymme ja toimimme (Bedford, 1988). Tunteen viriäminen hallitsee tietoisuutta ja tunteen kautta virinnyt toimintamotiivi kohoaa muiden pyrkimysten edelle (Helkama et al, 1998). Tunnesanat antavat perustelut tai ainakin osittaisen perustelun tietylle toiminnalle, esimerkiksi "Hän oli töykeä koska hän oli kateellinen". Tunnesanoja käyttämällä voimme ymmärtää paremmin ihmisen toimintaa. (Bedford, 1988).

2.3 Appraisal-teoria

Appraisal-teoria korostaa tunteiden ja ympäristön välistä yhteyttä (Ellsworth & Schrerer, 2003; Lazarus 1988; Schrerer, 1999). Appraisal-teorian peruslähtökohtana on, että ihmisten arvioinnilla ympäristön olosuhteista on merkittävä rooli tunteiden ilmenemisessä. Tunteet ovat sopeutumisreaktioita ympäröivään maailmaan, eli ihmiset jatkuvasti arvioivat ympäristössä tapahtuvien muutosten merkitystä omalle hyvinvoinnilleen. (Ellsworth & Schrerer, 2003).

Appraisal-teoriassa arviointi (appraisal) käsitetään tunteiden edeltäjäksi: ihmiset ensin arvioivat ympäristönsä minkä jälkeen he muodostavat tilantee-

seen soveltuvan tunteen (Ellsworth & Schrerer, 2003). Appraisal-prosessi, jonka seurauksena tunne muodostuu, on 2-osainen: alkuarvioinnissa (primary appraisal) arvioidaan tapahtuman positiivinen tai negatiivinen vaikutus henkilön hyvinvoinnille. Toinen arviointi (secondary appraisal) tarkoittaa kykyä selviytyä tapahtuman seurauksista. (Schrerer, 1999).

Tunteen kokemus on jatkuva prosessi, ja tunnekokemuksen luonne muuttuu aina uuden arvioinnin (appraisal) myötä (Ellsworth & Schrerer, 2003). Termi uudelleenarviointi (re-appraisal) viittaa siihen, että henkilön arviointi ympäristön tapahtumista on jatkuvaa ja siihen, että henkilö aktiivisesti reagoi palautteeseen. (Lazarus, 1988).

Lazarus korostaa, että kutakin tunnetta tai tunneperhettä määrittelee tietty teema (a core relational theme) joka tarkoittaa tunteen taustalla olevaa keskeistä harmia tai hyötyä (Lazarus, 1988). Taulukossa 2 on esimerkkejä teemoista, jotka johtavat negatiiviseen tunteeseen ja joiden oletetaan ilmenevän tässä tutkimuksessa:

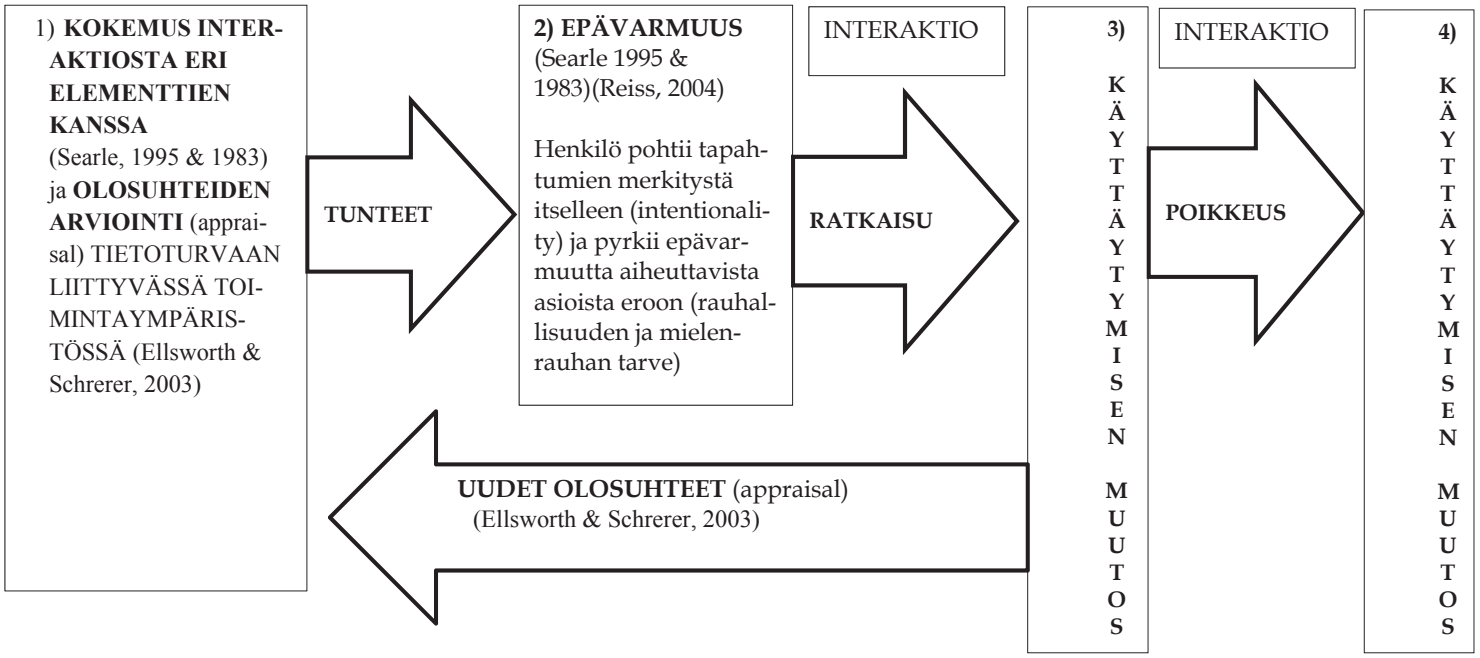
TAULUKKO 2 Negatiivisia tunteita määrittelevät teemat (Lazarus, 1988)

tunne	**teema (a core relational theme)**
viha	rikkomus itseä ja omaa omaisuutta kohtaan
huoli	tuntemattoman uhan kohtaaminen
pelko	konkreettisen ja välittömän fyysisen vaaran kohtaaminen
syyllisyys	moraalisten ohjeiden rikkominen
häpeä	epäonnistuminen ihanne-elämässä
suru	peruuttamattoman menetyksen kokeminen
inho	oleminen liian lähellä vaikeasti hyväksyttävää asiaa tai ideaa

Tässä tutkimuksessa keskitytään negatiivisiin tunteisiin ja niihin liittyviin teemoihin sillä perusteella, että tietoturvaan liittyvät kokemukset herättävät käyttäjissä usein negatiivisia tunteita kuten pelkoa tai häpeää, joista henkilö pyrkii eroon, mikä taas vaikuttaa käyttäytymisen muutokseen. Esimerkiksi tiedostojen häviäminen tietokoneelta aiheuttaa pelkoa ja sensitiivisen aineiston vuotaminen julkisuuteen häpeää. Edellä mainittujen Lazaruksen esittämien tunteiden lisäksi aineistosta nousi sille muitakin tunteita kuten epäluulo, epävarmuus, välinpitämättömyys ja hämmennys. Esimerkiksi sosiaalisen median käytön aloitus aiheuttaa epäluuloa siitä, ketkä kaikki näkevät sinne lisättyjä tietoja. Sähköpostin hakkerointi voi aiheuttaa henkilössä välinpitämättömyyttä siinä tapauksessa, että hän ei pidä hakkerointi suurena ongelmana. Toisaalta taas jos jokin tieto sosiaalisesta mediasta vuotaa ulkopuolisille, tämä aiheuttaa tietokoneen käyttäjässä hämmennystä. Keskustelu ystävien kanssa sosiaalisen median yksityisyydestä aiheuttaa tietokoneen käyttäjässä epävarmuutta siitä, kuka oikeastaan hänen tietojaan pääsee näkemään.

Kuviossa 1 on tiivistetty tutkimuksen teoreettinen viitekehys:

KUVIO 1 Tutkimuksen teoreettinen viitekehys



VAIHEESSA 1 kokemus interaktiosta eri elementtien kanssa herättää henkilössä erilaisia tunteita. VAIHEITA 2, 3 ja 4 MOTIVOIVAT ERILAISET TARPEET (pohjautuvat Maslow:n tarveteoriaan (1954 & 2007), Alderferin ERG – teoriaan ja McClellandin tarveteoriaan (Robbins, 1993) sekä Reiss:n (2004) motiiviteoriaan). RATKAISU-interaktiossa henkilö pohtii konkreettisia ratkaisukeinoja epävarmuutta aiheuttaviin asioihin. UUDET OLOSUHTEET-vaiheessa henkilö palaa uuteen interaktioon ja tekee uuden olosuhteiden arvioinnin. POIKKEUS-interaktiossa henkilö kokee asioita, jotka johtavat poikkemaan omaksutusta käyttäytymisestä

Searlen ajatukset todellisuuden muodostamisesta ja tarkoituksellisuuden pohtimisesta tarjoavat mielestäni uuden näkökulman tietoturvakäyttäytymiseen: tietokoneen käyttäjät luovat itse omaa todellisuuttaan, omiin tarkoituksiinsa. Esitän, että tietoturvakäyttäytyminen voi muuttua mm. eri elementtien välisen interaktion seurauksena sen sijaan, että käyttäytymistä selitettäisiin yksittäisillä tekijöillä, jotka ovat voimassa kaikissa tilanteissa ja kaikkina aikoina. Tietokoneen käyttäjät kokevat tietoturvaan liittyviä asioita (experience) ja ovat yhteydessä muihin ihmisiin ja asioihin (interaction). He pohtivat, mitä nämä kokemukset merkitsevät heidän omalla kohdallaan ja oman tietoturvansa kannalta (intentionality). He esimerkiksi huomaavat, että omat tietokoneelle talletetut valokuvat tai tiedot ovat vaarassa ja pitää toimia niiden suojaamiseksi. Muutos käyttäytymisen taustalla olevissa uskomuksissa ja ajatuksissa voi aiheuttaa käyttäytymisen muutoksen ja tietokoneen käyttäjä esimerkiksi ottaa varmuuskopioinnnin käyttöön.

Uudet kokemukset ja interaktiot voivat edelleen muuttaa henkilön uskomuksia ja ajatuksia, mikä voi taas saada uuden käyttäytymisen muutoksen aikaan. Henkilö esimerkiksi tiukentaa sosiaalisen median tietoturva-asetuksia. Aiempi tutkimus ei ota huomioon tätä käyttäytymisen jatkuvaa muutosta.

Motivaatioteoriat tuovat tarkempaa selitystä sille, mihin tarpeeseen/motiiviin tietokoneen käyttö perustuu, mitkä tarpeet motivoivat omaksumaan tietoturvasuojaustoimenpiteen ja missä määrin tarpeet ovat erilaisia käyttäytymisen muutosta kuvaavan prosessin eri tasoilla (ks. kuvio3). Esimerkiksi tasolla 2 henkilö voi kokea epävarmuutta, josta hän pyrkii eroon. Tätä tasoa määrittää siis rauhallisuuden ja mielenrauhan tarve, Reissiä tulkiten (Reiss, 2004). Ratkaisuinteraktiossa tason 3 jälkeen henkilö esimerkiksi voi pohtia konkreettisia ratkaisukeinoja epävarmuutta aiheuttaviin asioihin ja tasolla 3 henkilö tekee konkreettisia toimenpiteitä epävarmuuden poistamiseksi. Tällöin käyttäytymistä motivoi turvallisuuden tarve: henkilö haluaa suojata omaisuuttaan.

Motiivipsykologiasta pyritään löytämään selitystä myös sille, miksi tietokoneen käyttäjät poikkeavat omaksutusta suojaustoimenpiteestä joko väliaikaisesti tai pysyvästi. Toisin sanoen: millaisia tarpeita ja tarpeiden välisiä ristiriitoja sisältyy poikkeusinteraktioon tasojen 3 ja 4 välissä.

Appraisal-teoria täydentää Searlen ajatuksia subjektiivisesta todellisuuden muodostamisesta ja motivaatiopsykologian ajatuksia tarpeiden vaikutuksesta käyttäytymiseen. Appraisal-teoria korostaa tunteen kokemuksen prosessiluonteisuutta. Tässä tutkimuksessa selvitetään, millaisia tunteita tietoturvaan liittyvät kokemukset tietokoneen käyttäjissä herättävät ja millä tavalla ne vaikuttavat ajatteluun ja käyttäytymisen muutokseen.

Teoreettistä viitekehystä esittävässä mallissa (kaavio 1) tasolla 1 henkilö tekee olosuhteiden arviointia (appraisal) tietoturvaan liittyvässä toimintaympäristössä, mikä herättää erilaisia tunteita, jotka saavat henkilön epävarmuuden tilaan ja pohtimaan ratkaisukeinoja siihen kuinka epävarmuudesta voisi päästä eroon. Käyttäytymisen muutoksen jälkeen (taso 3) henkilö tekee uuden arvioinnin tietoturvaan liittyvässä toimintaympäristössä, mikä taas johtaa uusien

tunteiden heräämiseen. Käyttäytymisen muutoksen jälkeen henkilö kokee poikkeukseen johtavan interaktion. Tämä herättää hänessä erilaisia tunteita. jotka motivoivat häntä poikkeamaan joko väliaikaisesti tai pysyvästi jo omaksutun suojaustoimenpiteen käytöstä.

Tunteiden prosessiluonteisuus korostuu tässä työssä, sillä tietoturvakäyttäytyminen on luonteeltaan koko ajan muuttuvaa. Suojaustoimenpiteen käyttöönoton jälkeen tietokoneen käyttäjä jatkaa tietoturvaan liittyvän toimintaympäristön arviointia, mikä taas johtaa erilaisten tunteiden heräämiseen ja ajattelun ja tietoturvakäyttäytymisen muutokseen.

3 PROSESSITEOREETTINEN NÄKÖKULMA

Tässä tutkimuksessa sovelletaan prosessiteoreettista näkökulmaa. Prosessiteoreettisen näkökulman tarkoitus on kertoa kuvaus siitä, kuinka jotain tapahtuu (Mohr, 1982). Prosessitutkimus selvittää, kuinka asiat kehittyvät ja muuttuvat ajan kuluessa ja miksi ne kehittyvät tällä tavalla (Van de Ven & Huber, 1990; Van de ven, 1992). Prosessiteoreettisen näkökulman avulla voidaan esimerkiksi esittää, minkälaisia muutoksia ihmisen ajattelussa voidaan hahmottaa hänen prosessoidessaan tiettyä asiaa (Van de ven, 1992).

Prosessiteoreettinen tutkimus on kiinnostunut tapahtumista, aktiviteeteista ja valinnoista, jotka tapahtuvat ajan kuluessa. Prosessin ”data” koostuu yleensä tarinoista ja kuvauksista, jotka kertovat mitä tapahtui, kuka teki mitä ja milloin. Prosessimallin tavoite on selittää, miksi prosessin lopputulos tapahtuu. (Van de Ven & Huber, 1990; Langley, 1999; Robey & Newman, 1996).

Tietojärjestelmätieteessä DT- ja PMT teorioita on tyypillisesti tutkittu kyselytutkimuksella, joka on usein kerätty yhtenä tiettynä aikana (Siponen & Vance, 2014). Tässä työssä sovelletaan prosessiteoreettista näkökulmaa, koska tarkoituksena on selittää ja ymmärtää tietoturvakäyttäytymistä laajemmin kuin yhtenä tiettynä hetkenä (Markus & Robey, 1988.) Tärkeä kysymys on, miten ja miksi tietokoneen käyttäjä päätyy tiettyyn suojaustoimenpiteeseen. Prosessiteoreettisen näkökulman avulla on mahdollista kuvata aikajärjestyksessä se, mikä kuvataan käyttäytymisen muutosta kuvaavassa mallissa (luku 6.2.) elementtien ja niiden välisten interaktioiden avulla. Prosessiteoria mahdollistaa käyttäytymisen muutosta selittävien tekijöiden tarkastelemisen ja ilmiön dynaamisuuden kuvaamisen. Prosessiteorian avulla on myös mahdollista vertailla eri käyttäytymistyyppien välisiä eroja, eli miten käyttäytymisen muutos tapahtuu eri käyttäytymistyypeissä.

Teoreettisen mekanismin käyttäytymisen muutosta kuvaavan prosessin ymmärtämiseksi tarjoavat 4 prosessiteorian paradigmaa, life cycle, teleologinen, dialektinen ja evolutionaarinen (Van de ven, 1992). Luvussa 6.3.8. esitetään, kuinka teleologinen paradigma selittää käyttäytymisen muutosprosessin tässä tutkimuksessa. Muutosta tai prosessia voidaan myös kuvata stage theory -lähestymistavalla (Weinstein et al., 1998).

Stage-teoria koostuu kahdesta tai useammasta tasosta. (Schwarzer, 2008b; Schwarzer, 2008a). Stage-teorian avulla on mahdollista esittää ilmiön ajallinen ulottuvuus, sillä tasot esiintyvät prosessissa aikajärjestyksessä (Weinstein et al., 1998). Tärkeää tasojen valinnassa on, että ne ovat tutkimuksen kannalta hyödyllisiä, niiden ei siis tarvitse perustua todellisuuteen (Shwarzer, 2008 b). Käyttäytymisen muutoksen prosessia tutkitaan ja mallinnetaan tässä työssä tarkemmin stage theory-lähestymistapaa hyödyntämällä.

Stage – teoria soveltuu käyttäytymisen mallintamiseen, koska luonteenomaista käyttäytymiselle on, että se muuttuu ja muuttuessaan käy läpi erilaisia tasoja. (Weinstein et al., 1998). Tutkimuksessa laadittu prosessi on stage-teoria koska se noudattelee Weinstein et al (1998) esittämiä vaatimuksia stage-teorialle (ks. myös liite 2):

1. Tasot on määriteltävä ja luokiteltava. Jokaiselle tasolle on oltava omat vaatimukset
2. Tasoilla täytyy olla järjestys.
3. Kullakin tasolla on oltava yleiset faktorit/attribuutit, jotka ihmiset tällä tasolla kohtaavat
4. Eri tasoilla on oltava erilaiset faktorit ja attribuutit, jotka ihmiset tällä tasolla kohtaavat

Prosessin tasot siis eroavat laadullisesti toisistaan, eli ihmiset, jotka ovat eri tasoilla ilmentävät erilaista käyttäytymistä (Weinstein & Sandman, 1992). Toisaalta stage-teoriaa hahmoteltaessa on tunnistettava aineiston pohjalta ne tekijät, jotka mahdollistavat henkilön siirtymisen tasolta toiselle. (Schwarzer, 2008a; Velicer & Prochaska, 2008).

Ihmisillä voi eri tasoilla olla eri tarpeita. (Weinstein et al. 1998). Tässä tutkimuksessa tavoitteena on ollut selvittää mitkä tarpeet prosessin tasoja määrittelevät. Jokaiselle tasolle voidaan määritellä sille ominaiset tarpeet ja siten erottaa tasot selkeästi toisistaan. Ominaisuus, joka toistuu tässä tutkimuksessa teorian kaikilla tasoilla, on kokemus. Eli kun tietokoneen käyttäjä käy läpi tietyt prosessin tasot, hänen kokemuksensa muuttuu.

Stage-teoriassa tasolta toiselle siirtymiseen kuluva aika voi vaihdella suuresti. Henkilö voi käydä tasot läpi nopeasti tai toisaalta taas jäädä nykyiselle tasolleen pääsemättä koskaan siirtymään seuraavalle. Tässä tutkimuksessa kuitenkin suurin osa ihmisistä seuraa määriteltyä prosessia, joten teoriaa voidaan pitää tarkkana ja hyödyllisenä, vaikka muitakin polkuja käyttäytymisen muutokseen olisi aineiston perusteella löydettävissä. (Weinstein et al. 1998.)

4 AIKAISEMPI TUTKIMUS LIITTYEN TIETOKONEEN KOTIKÄYTTÖÖN JA TYÖKÄYTTÖÖN

Tätä tutkimusta varten käytiin läpi 46 kansainvälisissä tieteellisissä lehdissä tai konferensseissa ilmestynyttä tutkimusta, jotka ovat selvittäneet empiirisesti tietoturvakäyttäytymistä ja siihen vaikuttavia tekijöitä. Koska tietokoneen henkilökohtaista käyttöä ja työkäyttöä on joskus vaikea erottaa toisistaan, kirjallisuuskatsaukseen on otettu mukaan sekä tietokoneen työkäyttöä että henkilökohtaista käyttöä käsittelevät tutkimukset.

Aiempi kirjallisuus on ryhmitelty 5 ryhmään erilaisten tutkimusmenetelmien perusteella: 1) kyselytutkimus, 2) kokeellinen tutkimus, 3) haastattelu, 4) seurantatutkimus ja 5) toimintatutkimus.

Ryhmä 1: kysely

Suurin osa aiemmasta tutkimuksesta on ns. survey-tyyppisiä (35 kpl). Seuraavissa kappaleissa on esimerkkejä survey-tutkimuksista.

Henkilökohtaisen tietokoneenkäyttäjän tietoturvakäyttäytymiseen vaikuttavia tekijöitä ovat tutkineet kyselytutkimuksessaan mm. Anderson ja Agarwal (2010). Taustateoriana on käytetty protection motivation – teoriaa sekä goal-framing ja self-view - kirjallisuutta. Kyselyn tulokset osoittivat, että tietokoneenkäyttäjän aikomukseen käyttäytyä tietoturvallisesti vaikuttavat huoli tietoturvauhista, luottamus omiin kykyihin, tietoisuus tehokkuudesta sekä lisäksi sosiaalinen paine ja tietoisuus muiden käytöksestä. Tutkimus myös osoitti, että mitä voimakkaammin henkilö kokee psykologista omistajuutta tietokonetta tai Internetiä kohtaan, sitä todennäköisemmin hän niitä suojaa.

Tutkiessaan tekijöitä, jotka vaikuttavat henkilökohtaisen palomuurin käyttöönottoon, Kumar et al. (2008) ovat soveltaneet technology acceptance -mallia. Tutkimuksessa havaittiin, että huoli tietokoneesta (computer anxiety), tietoisuus suojaustoimenpiteistä (awareness of security measures) ja huoli tiedon yksityisyydestä (concern for information privacy) ovat olennaisia asioista, jotka vaikuttavat aikomukseen ottaa palomuuri käyttöön. Dinev & Hu (2007) ovat puolestaan hyödyntäneet kyselyssään theory of planned behavior - teoriaa tar-

koituksenaan selvittää, mitkä seikat vaikuttavat tietokoneenkäyttäjän aikomukseen käyttää suojaavia teknologioita esimerkiksi vakoiluohjelmia vastaan. Kyselyn tulokset osoittivat, että aikomukseen käyttää suojaavia teknologioita vaikuttaa tietoisuus niistä uhkista, joita negatiiviset teknologiat, kuten vakoiluohjelmat tuovat mukanaan.

Liang & Xue (2010) ovat tutkineet, kuinka henkilökohtaisen tietokoneen käyttäjät välttävät tietoverkon uhkia. Taustateoriana tutkimuksessa on TTAT (technology threat avoidance theory). Tutkimus osoittaa, että tietokoneen käyttäjät ovat motivoituneita toimimaan tietoturvallisesti, jos heistä tuntuu, että uhka on ajankohtainen ja vältettävissä. Lisäksi tietoisuus alttiudesta haitallisille seuraamuksille (perveived susceptibility) ja tietoisuus haitallisten seuraamusten vakavuudesta (perceived severity) motivoivat tietokoneenkäyttäjiä välttämään tietoverkon uhkia.

Pyrkimyksenään selvittää tekijöitä, jotka edistävät tietoturvakäyttäytymistä organisaatioissa Herath & Rao (2009b) ovat hyödyntäneet principal agent – teoriaa. Myös socio-economic theory of compliance ja general Deterrence (GT) ovat toimineet tutkimuksen taustateorioina. Tuloksena oli, että tietoturvakäyttäytymiseen vaikuttavat sisäiset ja ulkoiset motivaatiotekijät. Sisäisiä tekijöitä ovat työntekijän tietoisuus heidän toimintansa tehokkuudesta tietoturvaasioissa. Ulkoisia käyttäytymiseen vaikuttavia motivaattoreita olivat sosiaalinen paine ja työtovereiden käytös.

Chan, Woon et al. (2005) ovat hyödyntäneet kyselyssään taustateoriana safety climate – kirjallisuutta. Tutkimuksessa selvitetään sosiaalisten tilannesidonnaisten tekijöiden vaikutusta työntekijöiden tietoturvaohjeiden noudattamiseen. Kyselyn tulokset osoittivat, että tietoturvaohjeiden noudattamista voidaan edistää lisäämällä työntekijöiden luottamusta omiin kykyihin havaita tietoturvauhka ja toimia uhkaavissa tilanteissa sekä parantamalla tietoisuutta tietoturvailmapiiristä. Ohjeiden noudattaminen riippuu sekä yksilöllisistä että organisaatioon liittyvistä tekijöistä.

Guo et al. (2011) ovat tutkineet tekijöitä, jotka vaikuttava tietokoneenkäyttäjien asenteisiin organisaation tietoturvaa kohtaan sekä tietoturvakäyttäytymisen. Taustateorioina ovat olleet theory of reasoned action (TRA) ja theory of planned behavior (TPB) sekä the composite behavior model. Tulokset osoittivat, että työntekijän aikomukseen rikkoa organisaation tieturvaohjeita ilman aikomusta vahingontekoon vaikuttavat keskeisesti tietoturvarikkomuksesta saatu hyöty työn kannalta (relative advantage for job performance), tietoisuus tietoturvariskistä, joka tietoturvaohjeiden rikkomiseen liittyy (perceived security risk), työyhteisön normit (workgroup norm) ja tietoisuus tietoturvapolitiikkojen sopivuudesta ammatilliseen imagoon (perceived identity match).

Eettisten sääntöjen vaikutusta tietoturvakäyttäytymiseen on tutkinut Harrington (1996). Hän on selvittänyt, estävätkö eettiset ohjeet tietojärjestelmien parissa työskentelevien epäeettistä käytöstä. Ohjeet käsittivät yleiset organisaation ohjeet sekä ne ohjeet, jotka koskivat tietojärjestelmiä. Taustateoriana kyselyssä oli Deterrence theory. Tutkimuksen tuloksena oli, että organisaation eettiset ohjeet voivat vaikuttaa epäeettistä käytöstä vähentävästi niihin työntekijöi-

hin, jotka kieltävät oman vastuunsa käyttäytymisestään. Tietojärjestelmiä koskevilla ohjeilla oli suora vaikutus tietoturvarikkomusten harkintaan ja aikomukseen tehdä rikkomus tasaisesti kaikkien työntekijöiden kohdalla.

Tietoturvapolitiikkojen rikkomisen selittämistä kriminologian teorioiden avulla on tutkinut Hu, Xu, Dinev & Ling (2011). Tutkimuksessa on kehitetty malli Rational choice, Self-control, Deterrence, Shame, Moral beliefs – teorioiden pohjalta ja mallia on testattu käytännössä. Tutkimuksen tuloksena esitetään, että pelotteet eivät yksistään vähennä työntekijöiden tietoturvarikkomuksia, sillä tietoturvakäyttäytymiseen vaikuttaa pelotteita enemmän itsekontrolli ja moraaliset uskomukset siitä, kuinka oikein tai väärin aiottu käyttäytyminen on.

Ryhmä 2: kokeellinen tutkimus

Kokeellista tutkimusasetelmaa ovat hyödyntäneet tutkimuksessaan mm. Anderson & Agarwal (2010) ja Harrington, Anderson & Agarwal (2006). He ovat selvittäneet, kuinka tietoturvakäyttäytymiseen vaikuttaviin muuttujiin voidaan vaikuttaa tarkoituksenmukaisilla viesteillä, jotka pohjautuivat markkinoinnin ja psykologian teorioihin.

Shaw et al. (2009) ovat tutkineet kokeellisesti, kuinka median monipuolisuus lisää tietoturvatietoisuutta 3 tietoisuuden tasolla. Mediatyypit, joita kokeessa sovellettiin, olivat hypermedia, multimedia ja hyperteksti. Koehenkilöt osallistuivat koulutusinterventioon, joka pohjautui johonkin näistä kolmesta mediasta.

Tietoturvaan liittyvää henkilökohtaista vastuuntunnetta ovat tutkineet La Rose et al (2008). He jakoivat kokeessaan koehenkilöt satunnaisesti 1) henkilökohtaisen vastuun käsittelyyn (personal responsibility treatment condition) ja 2) vastuuttomuuden käsittelyyn (irresponsibility treatment).

Johnston & Warkentin (2010) ovat tutkineet kokeellisesti kuinka pelkoa sisältävät elementit (fear appeals) vaikuttavat tietokoneen käyttäjän aikomukseen noudattaa suositeltuja tietoturvaohjeita. Pelkoa sisältävät elementit ovat viestejä, jotka ovat suunniteltu pelottamaan ihmisiä kuvaamalla haitallisia seuraamuksia, joita he kohtaavat, elleivät toimi niin kuin heitä suositellaan (esimerkiksi sähköpostiviestissä).

Tietoturvakäyttäytymiseen vaikuttavia tekijöitä on kokeellisesti tutkinut myös Möller et al (2011). Kokeessa manipuloituja käyttäytymiseen vaikuttavia tekijöitä olivat hyökkäyksen todennäköisyys, tietoturvauhkan vakavuus, käytettävyyskustannukset ja hälytysjärjestelmän sensitiivisyys.

Kaiken kaikkiaan aiemman tutkimuksen joukossa oli 6 kokeellista tutkimusta.

Ryhmä 3: haastattelu

Aiemman kirjallisuuden joukossa oli yksi tutkimus, joka hyödynsi haastattelua tärkeimpänä tutkimusmenetelmänä (Furnell, Tsaganidi & Phippen, 2008). Tutkimuksessa selvitettiin tietokoneen käyttäjien ajatuksia ja kokemuksia Interne-

tin turvallisuuteen liittyen. Tutkimuksessa haastateltiin 20 tietokoneenkäyttäjää Iso-Britanniasta.

Ryhmä 4: seurantatutkimus

Aiemman tutkimuksen joukossa oli lisäksi yksi seurantatutkimus (Wang et al. 2010), jossa seurattiin 658000 henkilökohtaisen tietokoneen käyttäjän hakukoneen (AOL) käyttöä 3 kuukauden ajan. Seurantatutkimus mahdollisti sen selvittämisen, kuinka verkkohyökkäysten yleisyys ja voimakkuus ovat yhteydessä tietoturvaan liittyvän tiedon etsimiseen Internetistä.

Ryhmä 5: toimintatutkimus

Puhakainen & Siponen (2010) ovat toimintatutkimuksessaan kehittäneet teoriapohjaisen tietoturvakoulutusohjelman, jonka toimivuutta käytännössä he testaavat toimintatutkimuksella: missä määrin se parantaa tietoturvaohjeiden noudattamista organisaatiossa.

Taulukkoon 3 on kirjattu seuraavat tiedot kustakin tutkimuksesta:

- Onko tutkimuksessa tarkasteltu eri käyttäytymistyyppejä ja niiden välisiä eroja (esim. varmuuskopiointi, vahva salasana) (K/E)
- Tarkastellaanko tutkimuksessa käyttäytymisen muutosta (K/E)
- Onko tutkimuksessa huomioitu käyttäytymisen tilannesidonnaisuus (K/E)

Liite 3 sisältää tarkennusta taulukkoon. Siihen on merkitty kunkin tutkimuksen osalta

- Onko kyseessä koti/työkonteksti (K/T)
- Ryhmä, johon tutkimus kuuluu tutkimusmenetelmän perusteella
- Tutkimuksen taustateoriat, muuttujat ja päätulokset

TAULUKKO 3 Aiempi tutkimuskirjallisuus, osa 1

Tekijä	**Käyttäytymistyyppien vertailu (K/E)**	**Tarkastellaanko käyttäytymisen muutosta (K/E)**	**Huomioidaanko käyttäytymisen tilannesidonnaisuus (K/E)**
Anderson & Agarwal (2010)	K Sosiaalinen paine (subjective norm) ennustaa merkittävästi aikomusta suojata omaa tietokonetta, mutta ei vaikuta merkittävästi aikomukseen suojata Internetiä. Tietoisuus toisten käytöksestä (descriptive norm) vaikuttaa merkittävästi aikomukseen suojata Internetiä, mutta ei aikomukseen suojata omaa tietokonetta.	K Aikomukseen käyttäytyä tietoturvallisesti voidaan vaikuttaa suojaustoimenpiteen positiivisia vaikutuksia korostavilla viesteillä (promotion-focused goal frame).	E
Boss & Kirsch et al. (2009)	E	E	E
Bryant & Campbell (2006)	E	E	E
Bulgurcu, Cavusoglu, & Benbasat (2010)	E	E	E
Bunnel et al. (1997)	E	E	E
Caldwell & McGarvey (2013)	E	E	E
Chan, Woon et al. (2005)	E	E	E
D'Arcy, Hovav, & Galletta (2009)	E	E	E
Dinev et al. (2009)	E	E	E
Dinev & Hu (2007)	E	E	E
Dodge et al. (2007)	E	E	E
Furnell, Tsaganidi & Phippen (2008)	E	E	E

Furnell et al. (2007)	E	E	E
Furnell, Jusoh & Katsabas (2006)	E	E	E
Furnell (2005)	E	E	E
Guo et al. (2011)	E	E	E
Harrington, Anderson & Agarwal (2006)	E	E	E
Harrington, S. J. (1996)	E	E	E
Herath et al. (2014)	E	E	E
Herath & Rao (2009a)	E	E	E
Herath & Rao (2009b)	E	E	E
Hsu, Shih, Hung & Lowry (2015)	E	E	E
Hu, Xu, Dinev & Ling (2011)	E	E	E
Johnston & Warkentin (2010)	E	K Pelkoa sisältävät argumentit, joissa varoitetaan tietoturvauhasta ja joissa neuvotaan, kuinka uhkaa voidaan torjua, voivat saada jotkut käyttäjät hyväksymään viestin ja tekemään toimenpiteitä uhan vähentämiseksi. Jotkut taas voivat reagoida argumentteihin siten, että he hylkäävät viestin ja tekevät toimenpiteitä pelontunteen vähentämiseksi.	E
Kritzinger & von Solms (2010)	E	E	E
Kumar et al. (2008)	E	E	E
La Rose et al. (2008)	E	E	E
Lee & Kozar (2005)	E	E	E

Lee & Kozar (2008)	E	E	E
Lee, Lee & Yoo (2004)	E	E	E
Liang & Xue (2010)	E	E	E
Lowry, Posey, Bennett & Roberts (2014)	E	E	E
Limayem & Hirt (2003)	E	E	E
Myyry, Siponen, Pahnila, Vartiainen & Vance (2009)	E	E	E
Möller et al. (2011)	E	K Henkilöt, jotka kohtaavat tietoturvauhan usein, omaksuvat varovaisemman tietojärjestelmän käyttötavan. Lisäksi suhteellisen luotettava varoittava järjestelmä tekee heistä riippuvaisempia sen antamista merkeistä.	E
Ng, Kankahalli & Xu, (2009)	E	E	E
Ng & Rahim (2005)	K Asenne (attitude) ja sosiaalinen paine (subjective norm) selittävät aikomuksia virustorjuntaohjelman päivittämiseen, varmuuskopiointiin ja palomuurin käyttöön. Lisäksi tietoisuus hyödyllisyydestä selitti asennetta kaikkia käyttäytymistyyppejä kohtaan. Tietoisuus käytön helppoudesta tai vaikeudesta (Perceived behavioral control) selittää ainoastaan aikomusta palomuurin käyttöön.	E	E
Puhakainen & Siponen	E	K	E

(2010)		Teoriapohjainen koulutus tuotti positiivisia tuloksia: se lisäsi sähköpostiviestien salaamista työntekijöiden keskuudessa ja muutti tietokoneenkäyttäjien asennetta tietoturvaa kohtaan positiivisemmaksi sekä lisäsi kryptausratkaisujen lukumäärää.	
Shaw, R.S. et al. (2009)	E	E	E
Siponen & Vance (2010)	E	E	E
Son, J. (2011)	E	E	E
Stanton, Stam, Mastrangelo & Jolton (2005)	E	E	E
Straub, D.W. (1990)	E	E	E
Wang et al. (2010)	E	K Omakohtaisten verkkohyökkäysten yleisyys ja voimakkuus ovat positiivisesti yhteydessä tietoturvaan liittyvän tiedon etsimiseen Internetistä.	E
Woon, Tan, & Low, R. (2005)	E	E	E

Mitä uutta tämä työ tuo tutkimukselle

Selittäessään tietoturvakäyttäytymistä teorioilla kuten Protection motivation theory (PMT), Theory of reasoned action (TRA), Theory of planned behavior (TPB), Deterrence theory (DT) aiempi survey-tyyppinen tutkimus selittää tietoturvakäyttäytymistä staattisilla syillä (riippumattomia muuttujia). Esimerkiksi TPB – teoriaa soveltavassa tutkimuksessa tarkastellaan sitä, selittävätkö konstruktiot kuten asenne (attitude), subjektiivinen normi (subjective norm) ja kontrolli (perceived behavioral control) aikomusta käyttää tietoturvasuojauksia (Ng & Rahim, 2005). Survey-tyyppinen tutkimus ei kuitenkaan tarkastele tietoturvakäyttäytymisen muutosta.

Kolmessa kokeellisessa tutkimuksessa ja yhdessä seurantatutkimuksessa tuotiin esille muutoksen vaikuttavia tekijöitä, jotka ikään kuin havainnollistavat sen, että tietoturvakäyttäytyminen muuttuu. Tutkiessaan tietoturvakäyttäytymisen muutosta kokeelliset tutkimukset ovat todenneet että henkilöt, jotka kohtaavat tietoturvauhan useammin, omaksuvat varovaisemman tietojärjestelmän käyttötavan (Möller et al., 2011). Lisäksi tietokoneenkäyttäjän halukkuus ottaa riskejä, hänen taipumuksena kieltää riskejä tai hänen kokemuksensa suojaustoimenpiteistä vaikuttavat merkittävästi käyttäytymiseen. Kokeellinen tutkimus on myös selvittänyt, millainen viesti vaikuttaa tehokkaimmin tietokoneen käyttäjien asenteeseen tietoturvaan liittyvää käyttäytymistä kohtaan, sosiaaliseen paineeseen (subjective norm) ja tietoisuuteen muiden käytöksestä (descriptive norm) (Anderson & Agarwal, 2010). Tulokset osoittivat, että jos käyttäytymisen muutosta tavoittelevassa viestissä korostetaan suojaustoimenpiteen positiivisia vaikutuksia, sillä voidaan vaikuttaa aikomukseen käyttäytyä tietoturvallisesti. Lisäksi viestin tehokkuutta lisää se, jos viesti vetoaa henkilön omakuvaan itsenäisenä toimijana vs. Internet-yhteisöstä riippuvana toimijana. Johnston & Warkentin (2010) ja Johnston, Warketing & Siponen (2015) ovat havainneet, että koehenkilöt reagoivat pelkoa sisältäviin argumentteihin eri tavoin. Uhasta varoittavat viestit, jotka neuvovat, kuinka uhkaa voidaan torjua, voivat saada jotkut käyttäjät hyväksymään viestin ja tekemään toimenpiteitä uhan vähentämiseksi. Toisaalta viesti voi herättää emotionaalisen reaktion ja henkilö hylkää viestin. Kokeellisten tutkimusten lisäksi tietoturvakäyttäytymisen muutosta on tutkinut seurantatutkimuksessaan myös Wang et al. (2010). Tutkimuksessa seurattiin Internetin hakukoneen käytön muutosta 3 kuukauden ajan. Tietoturvahyökkäykset vaikuttivat tietokoneen käyttäjiin siten, että he alkoivat etsimään aktiivisemmin tietoa Internetistä.

Vaikka em. tutkimukset käsittelevät tietoturvakäyttäytymisen muutokseen vaikuttavia tekijöitä, ne mallintavat muutosta tai päätöksentekoprosessia aina samalla invariantilla tekijällä. Oletetaan, että vaikutus on stabiili eli että jokaisessa tilanteessa samat asiat vaikuttavat muutokseen. Esim. Johnston et al. (2010) tutkimuksessa pelko aiheuttaa muutoksen (eikä joku muu), eikä esimerkiksi pelko vaihdu joksikin muuksi. Samoin, survey-tyyppinen tietoturvakäyttäytymistutkimus selittää käyttäytymistä muuttujilla, jotka ovat pysyviä tilanteesta toiseen. Aiemman tutkimuksen joukoista tosin löytyi joitakin tutkimuksia liittyen moderaattorien vaikutukseen. Esimerkiksi Dinev et al. (2009) on tutki-

nut kulttuurierojen (Etelä-Korea vs. USA) vaikutusta yhteyteen sosiaalisen paineen ja aikomuksen välillä ja Harrington (1996) on selvittänyt, kuinka aikomukseen väärinkäyttää tietokonetta moderoi vastuun kieltäminen (denial of responsibility). Nämä tutkimukset eivät kuitenkaan huomioi tilannesidonnaisuutta siitä näkökulmasta kuin se on ymmärretty tässä tutkimuksessa.

Tämä tutkimus pyrkii ymmärtämään käyttäytymisen muutosta tarkemmin selvittämällä syitä sille, kuinka käyttäytyminen muuttuu. Esimerkiksi tietoturvaan liittyvä kokemus eli tietoturvaongelma, tietoturvatietoisuuden lisääntyminen tai muutos tietokoneen käytössä herättävät voimakkaita tunteita (epävarmuus, viha, häpeä, pelko). Henkilö pohtii kokemansa merkitystä omasta näkökulmastaan ja oman tietoturvansa kannalta. Hän pyrkii poistamaan negatiivisia tunteita aiheuttavat asiat (oman tieto-omaisuuden tai IT teknologian haavoittuvuus) ottamalla käyttöön suojaustoimenpiteen.

Edelleen, tietokoneen käyttäjä voi luopua suojaustoimesta väliaikaisesti tai pysyvästi tilannekohtaisen tarpeiden priorisoinnin tuloksena. Eli tietyssä tilanteessa ja tietyissä olosuhteissa tietokoneen käyttötarpeet ja turvallisuuden tarpeet (tarve suojata omaisuuttaan) voivat olla ristiriidassa, ja kun tietokoneen käyttäjä priorisoi tarpeita keskenään, hänen tietoturvakäyttäytymisensä muuttuu.

Tilannetta voidaan kuvata siten, että henkilö on jonkin uuden edessä, ja hänen tulee tehdä valintoja. Uusi tilanne voi olla esimerkiksi se, että joku ulkopuolinen taho, esimerkiksi pankki tai virasto pyytää tietokoneen käyttäjää lähettämään sensitiivistä tietoa sähköpostissa. Tarpeiden priorisointiin johtava tilanne voi olla myös uuden Internet-palvelun käyttö, esimerkiksi kirjautuminen keskustelupalstalle.

Tietoturvasuojauksen omaksumisen jälkeen tietokoneenkäyttäjä voi vahvistaa sitä. Hän esimerkiksi kokee uuden tietoturvaongelman, vaikkapa tiedon vuotamisen sosiaalisessa mediassa tai kuulee ystävältä suosituksia virustorjuntaan liittyen ja vahvistaa omaksumaansa suojaustoimenpidettä (yksityisyysasetukset, virustorjunta) edelleen.

Prosessiteoria mahdollistaa käyttäytymisen muutosta selittävien tekijöiden tarkastelemisen ja ilmiön dynaamisuuden kuvaamisen. Käyttäytymisen muutos voi tapahtua vaiheittain vaikkapa niin että henkilö tulee vähitellen varovaisemmaksi verkkokaupan käytössä tai että hän pikkuhiljaa vahvistaa salasanan tai sosiaalisen median yksityisyysasetuksia. Käyttäytymisen muutosprosessi voi päättyä kesken, ilman että käyttäytyminen muuttuu.

Yksi rajoite tai puute aiemmassa tietoturvakäyttäytymistutkimuksessa on, että se ei vertaile eri käyttäytymistyyppien välisiä eroja (esim. salasanan vaihtaminen, varmuuskopiointi, virustorjunta jne.). Ainoastaan Anderson & Agarwal (2010) sekä Ng & Rahim (2005) ovat jossain määrin huomioineet eri käyttäytymistyyppejä. Ng & Rahim tutkivat tietokoneenkäyttäjien aikomusta seuraavien käyttäytymistyyppien osalta:

- virustorjuntaohjelman säännöllinen päivittäminen
- tärkeiden tietojen varmuuskopiointi
- henkilökohtaisen palomuurin käyttö

Tutkimus osoitti, että näiden käyttäytymistyyppien kohdalla löytyi niin samankaltaisuuksia kuin erojakin. Kaikkien käyttäytymistyyppien kohdalla asenteella (attitude) ja sosiaalisella paineella (subjective norm) on merkitsevä yhteys aikomukseen käyttää suojaustoimenpiteitä. Lisäksi, kaikissa em. käyttäytymistyypeissä tietoisuus hyödyllisyydestä oli merkittävä ennustaja asenteelle suojaustoimenpiteitä kohtaan. Ainoastaan palomuurin käytössä tietoisuudella suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (Perceived behavioral control) on merkittävä yhteys aikomukseen käyttää suojaustoimenpiteitä.

Anderson & Agarwal (2010) vertailivat omassa tutkimuksessaan, missä määrin aikomukseen suojata omaa tietokonetta liittyvä muuttujat eroavat aikomukseen suojata Internetiä liittyvistä muuttujista. Samoin kuin Ng & Rahim (2005), myös Anderson & Agarwal (2010) havaitsivat sosiaalisen paineen (subjective norm) merkittäväksi ennustajaksi aikomukselle suojata omaa tietokonetta, mutta toisaalta, sen yhteys aikomukseen suojata Internetiä ei ole merkittävä. Tietoisuudella toisten käytöksestä (descriptive norm) ja aikomuksella suojata Internetiä on merkittävä yhteys, sen sijaan em. muuttujan yhteys aikomukseen suojata omaa tietokonetta ei ole merkittävä. Lisäksi, molempien käyttäytymistyyppien osalta havaittiin, että mitä korkeammalla tasolla psykologinen omistajuus on suhteessa tietokoneeseen tai Internetiin, sitä todennäköisemmin henkilö niitä suojaa.

Tietoturvakäyttäytymisen muutoksen selittämisen ja tilannesidonnaisuuden ohella tämän työn kontribuutio on, että siinä tarkastellaan kuutta eri käyttäytymistyyppiä ja niiden välisiä eroja. Tutkimuksen tuloksena esitetään sekä oma prosessimalli jokaisesta käyttäytymistyypistä että yksittäiset mallit yhdistävä prosessimalli, joka kokoaa yhteen yksittäisten mallien erityispiirteet.

5 TUTKIMUSMENETELMÄT, AINEISTON HANKINTA JA -ANALYYSI

5.1 Kohderyhmä

Tutkimuksen kohderyhmänä ovat tietokoneen käyttäjät. Haastateltavia hankittaessa vaatimuksena on ollut että haastateltavalla on käytössään henkilökohtainen tietokone. Haastateltaviin kuului ensimmäisessä vaiheessa haastattelijoiden ystäviä, sukulaisia ja kollegoita. Toisessa ja kolmannessa vaiheessa haastateltavien joukko koostui satunnaisesti valituista henkilöistä. Heidät rekrytoitiin kaupungilta, puistosta, kirjastolta, yliopistokampukselta ja kauppatorilta. Vaiheiden 1 ja 2 jälkeen aineiston mallintamisessa käytettiin viitekehyksenä John Searlen ideoita todellisuuden subjektiivisesta muodostamisesta ja kokemuksen tarkoituksellisuudesta. Vaiheen 3 haastatteluiden tarkoitus oli tehdä kysymyksiä, jotka painottuivat erityisesti motiivi- ja tarveteorioihin. Kolmas vaihe haastatteluille oli tarpeen toteuttaa myös alustavasti laaditun prosessiteorian vahvistamiseksi ja saturaation saavuttamiseksi.

Haastateltavien ikä vaihteli 19 ja 69 välillä. Haastateltavat edustivat 4 kansallisuutta. Suurin osa haastateltavista oli suomalaisia (80 %). Haastattelimme 21 miestä ja 14 naista. Suomalaisten henkilöiden oli mahdollisuus vastata kysymyksiin omalla kielellään. Tämä on yksi keino välttää ns. “elite bias” (Myers & Newman, 2007).

5.2 Puolistrukturoitu haastattelu

Haastatteluissa sovellettiin puoli-strukturoitua haastattelua. Jotkut kysymyksistä valmisteltiin etukäteen, mutta myös uusia kysymyksiä tehtiin haastattelun aikana. (Myers & Newman, 2007). Valmisteltaessa haastatteluita meillä ei ollut tarkkaa listaa kysymyksistä vaan haastattelurunko, joka sisälsi haastattelun pääteemat. Haastattelukysymykset ovat liitteessä 1.

Koska tämän tutkimuksen tarkoitus on ymmärtää prosessia, joka edeltää tietoturvakäyttäytymisen muutosta (van de Ven 1992; Weinstein 1998), haastat-

teluissa pyrittiin saamaan selville haastateltavien henkilökohtaisia rakenteita, jotka sisältävät elementtejä, konstruktioita ja linkkejä "personal constructs, which comprise elements, constructs and links" (Schulze & Avital, 2011). Haastateltavien tietoturvasuojaustoimenpiteet käsitettiin elementeiksi ja konstruktioiksi miellettiin syyt näiden käytäntöjen taustalla. Kiinnitin huomiota 3 aikaulottuvuuteen (taulukko 4):

TAULUKKO 4 Haastattelukysymysten 3 aikaulottuvuutta

Nykyhetki	▪ Syyt, jotka selittävät tietoturvatoimenpiteiden käyttöä tällä hetkellä ▪ Syyt sille, että henkilö ei käytä tiettyjä tietoturvatoimenpiteitä tällä hetkellä
Tulevaisuus	▪ Syyt, jotka voisivat tulevaisuudessa saada henkilön käyttämään tiettyä tietoturvatoimenpidettä ▪ Syyt, jotka voisivat tulevaisuudessa saada henkilön lopettamaan tilapäisesti tai lopullisesti jonkin tietoturvatoimenpiteen käytön
Mennyt aika	▪ Syyt, jotka vaikuttivat henkilön päätökseen alkaa käyttämään tiettyä tietoturvatoimenpidettä menneisyydessä ▪ Syyt, jotka estivät henkilön käyttämästä tiettyä tietoturvatoimenpidettä menneisyydessä

Haastattelujen myöhemmässä vaiheessa, kun alustavat prosessit oli jo muotoiltu ja tarvittiin lisää teoriaa tukevaa aineistoa, kiinnitettiin enemmän huomiota siihen, millaisia tunteita ja tarpeita käyttäytymisen muutokseen liittyy (esimerkiksi millaisia tunteita tietoturvaongelmat haastateltavissa herättävät) ja siihen, miten tarkalleen ottaen käyttäytyminen muuttuu. Aikaisempaa aineistoa käytettiin tässä hyödyksi esimerkiksi siten, että vastaajilta tiedusteltiin syitä poikkeamiselle omaksutuista suojaustoimenpiteistä. Jos haastateltavan oli hankala muistaa poikkeuksia, mainittiin sitten aikaisemmista haastatteluista ilmenneitä löydöksiä tähän liittyen, ja kysyttiin, olivatko vastaajat kokeneet vastaavaa. Tämän lisäksi haastatteluissa painotettiin suoraan tutkimuksen löydöksiä käsitteleviä kohtia esimerkiksi keskittymällä tähän mennessä tarkasteltuihin tietoturvakäytäntöihin (varmuuskopiointi, virustorjunta jne.). Muut suojaustoimenpiteet, kuten esimerkiksi koneelta uloskirjautuminen, jätettiin tässä vaiheessa käsittelemättä.

Toisaalta taas haastateltavilta kysyttiin syitä siihen, mihin tarpeisiin tietokoneen käyttö pohjautuu, koska aiemmat tietokoneenkäyttötarpeet (proses-

sin taso 1) eivät pohjautuneet haastateltavien omiin kokemuksiin vaan haastatteluista tehtyihin oletuksiin ja tulkintoihin. Siksi pyrittiin saamaan haastateltavien oma näkökulman siihen, mikä heitä motivoi esimerkiksi pelaamiseen, verkkokaupan käyttöön tai yhteydenpitoon Internetissä.

5.3 Laddering-menetelmä

Haastatteluissa sovellettiin ns. "laddering"-menetelmää. Laddering auttaa haastateltavia pääsemään sisälle sisäiseen ajatusmaailmaansa ja siinä oleviin kerroksiin. Haastattelun tarkoitus on ymmärtää, millä tavalla vastaajat näkevät ja ymmärtävät maailman. (Schultze & Avital, 2011).

Sovellettaessa laddering -menetelmää tavoitteena on saada selville henkilöillä olevien, maailman toimintaa selittävien ideoiden tai teorioiden sisältö ja rakenne (constructs) (Schulze & Avital, 2011.) Laddering–tekniikka suosii miten ja miksi-kysymyksiä, joilla rohkaistaan haastateltavia kehittämään linkkejä konstruktioiden välille (Schultze & Avital, 2011).

Laddering-tekniikka tarkoittaa ominaisuuksien, seurauksien ja arvojen "portaistamista" (Reynolds & Gutman, 1988; Shultze & Avital, 2011). Kysymykset kuten "Miksi se on sinulle tärkeää?" tähtäävät keskeisten elementtien, eli ominaisuuksien (A) seurauksien (C) ja arvojen (V) välisten linkkien määrittämiseen. Tuloksena on ns. assosiaatioverkko "association networks", jota kutsutaan myös portaikoksi. (Reynolds & Gutman, 1988.)

Haastattelijan rooli on auttaa haastateltavia tutkimaan kriittisesti niitä oletuksia, jotka vaikuttavat heidän jokapäiväiseen toimintaansa. (Reynolds & Gutman, 1988).

Laddering – tekniikka edellyttää pitkiä haastatteluita, jotta haastatteluissa päästäisiin arvojen keskustelemaan arvoista (portaikon korkein taso) (Schultze & Avital, 2011) Tässä tutkimuksessa haastattelut kestivät arviolta 1 – 2 tuntia.

Haastatteluissa käytettiin useita vastauksen antamista helpottavia tekniikoita siinä tapauksessa, että henkilö koki vaikeaksi selittää käyttäytymisen taustalla olevia syitä ja sitä, miksi ne ovat heille tärkeitä (taulukko 5) (Reynolds & Gutman, 1988):

TAULUKKO 5 Haastattelutekniikat (Reynolds & Gutman, 1988)

Tekniikka	Esimerkki
1) Konstruktion tilannesidonnaisuuden herättäminen	Yritä muistaa milloin viimeksi teit asian, mikä oli taustalla oleva syy?
2) Oletetaan, että asiaa tai tunnetta ei ole olemassa. Haastattelija pyytää haastateltavaa ajattelemaan, millaista olisi, jos tiettyä asiaa tai tunnetta ei olisi olemassa.	Mitä tekisit jos et voisi tehdä sitä?
3) Negative laddering = pyydetään haastateltavaa kuvittelemaan päinvastainen asiantila. Näin voidaan löytää tiedostamattomia syitä käyttäytymiselle.	Miksi et tee päinvastoin? Mitä tapahtuisi jos ominaisuutta tai seurausta ei olisi olemassa?
4) Vastaajan siirtäminen menneisyyteen = "Age regression contrast probe"	Käyttäydyitkö eri tavalla menneisyydessä?
5) Kysytään, kuinka vastaajan lähipiiriin kuuluvat henkilöt tuntisivat tässä tilanteessa = Third person probe	Miksi ystäväsi, perheesi tai työtoverisi kokevat tämän tärkeäksi?
6) Redirecting -tekniikat eli ajattelun suuntaaminen: a) hiljaisuus: Hiljaisuus haastattelun keskellä voi auttaa rohkaisemaan vastaajaa ajattelemaan soveltuvampaa tai tarkempaa vastausta b) Tarkennuksen pyytäminen (communication check). Haastateltava pyytää vastaajaa antamaan tarkemman selvityksen asiasta	Odotapa niin katson, olenko ymmärtänyt oikein
1) Paluu ongelmalliseen asiaan Haastateltava merkitsee ongelmallisen asian ja palaa aiheeseen myöhemmin kun muita siihen liittyvää tulee haastattelussa esille.	Aiemmin sanoit että…

5.4 Peilaus ”Mirroring”

Haastateltaessa tietokoneen käyttäjiä sovellettiin myös “mirroring” – tekniikkaa, mikä tarkoittaa haastateltavan kommenttien toistamista. Ideana on, että haastateltava kuvailee ja selittää maailmaansa käyttäen omia persoonallisia sanavalintojaan. Kun haastattelija esittää kysymyksen tai kommentin, hän käyttää niitä sanoja ja ilmauksia, joita haastateltavakin käyttää. Haastateltavan kielen käyttäminen auttaa tutkijaa keskittymään haastateltavan maailmaan. (Myers & Newman, 2007.)

5.5 Aineiston analyysi

Kun haastattelujen pohjalta on lähdetty laatimaan malleja käyttäytymisen muutoksesta, haastatteluja on ensin vertailtu. Tavoitteena on ollut löytää tekstikatkelmia, jotka kuvaavat käyttäytymisen muutosta johonkin tiettyyn tietoturvasuojaustoimenpiteeseen liittyen.

Tämän jälkeen tekstikatkelmista on hahmoteltu elementit (ks. elementit luvussa 6.1.) kuten esimerkiksi uhka, tietokone, tietoverkko, tietojärjestelmä jne., joiden kanssa tietokoneen käyttäjä toimii interaktiossa ennen kuin käyttäytyminen muuttuu. Kukin elementti on sijoitettu malliin omaksi laatikokseen. Tämän jälkeen näiden laatikoiden välille on hahmoteltu yhteydet. Lähtökohtana yhteyksien tekemisessä elementtien välille on ollut tietokoneen käyttäjän kokemus. Tietokoneen käyttäjän kokemus on ikään kuin teorian kokoava, kognitiivinen elementti, johon muut elementit liittyvät.

Yhteyksien hahmottelemisen jälkeen yhteydet on nimetty eli on pohdittu, mitä yhteydet tarkoittavat ja miksi tietyt elementit ovat yhteydessä keskenään. Esimerkiksi tietokoneen käyttäjä on yhteydessä tietokoneeseen, koska hän käyttää sitä johonkin tarkoitukseen (liiketoiminta, yhteydenpito ystävien kanssa jne.) Tietokoneen käyttäjä on yhteydessä myös tietolähteeseen, koska hän kuulee esimerkiksi ystäviltään, tuttaviltaan ja mediasta tietoturvaan liittyviä uutisia. Mallissa on lisäksi huomioitu tutkimuksen teoreettinen viitekehys, eli mallissa on 3 osaa: kokemus, tarkoituksellisuus, ja käyttäytymisen muutos. Mallien laatimisen apuna on ollut käyttäytymisen muutosta yleisemmällä tasolla kuvaava malli (luku 2.2. kaavio 1) joka muodostaa tutkimuksen teoreettisen viitekehyksen.

Tämän tutkimuksen teoreettinen ymmärrys perustuu ihmisten tietoturvaan liittyviin kokemuksiin ja niihin merkityksiin, jotka he antavat näille kokemuksille (ks. myös Sarker et al, 2001). Prosessiteorian laatiminen on aloitettu siten, että ensin on hahmoteltu tarina eli tapahtumasarja, joka edeltää lopputulosta (suojaustoimen käyttönotto). Tarinat auttavat yhteyksien löytämistä ja määrittelemistä tapahtumien välille (van de Ven & Huber, 1990). Yhteydet täsmentävät sitä, kuinka tarina etenee tasolta toiselle eli tapahtumasta toiseen (Abbott, 1990).

Whettenin (1989) mukaan teorian tulee sisältää 4 oleellista elementtiä: mikä (what), miten (how), miksi (why) and kuka/missä, milloin (who/ where, when). Teorian ydin muodostuu mikä - ja miten -elementeistä. Voidaan sanoa, että mikä - ja miten – elementit kuvailevat, kun taas miksi - elementti selittää. (Whetten, 1989).

Haastattelujen analysoinnissa on hyödynnetty Whettenin (2002) ehdottamaa teoriankehitysprosessia, jossa selvitetään 1) MITKÄ muuttujat/konstruktiot ovat tärkeitä ja miksi? 2) MITEN konstruktiot ovat yhteydessä toisiinsa ja 3) MIKSI konstruktiot ovat yhteydessä toisiinsa.

Haastatteluja on analysoitu seuraavasti tarkoituksena löytää teorian keskeiset konstruktiot ja elementit:

'Mikä'-konstruktiot

Tässä tutkimuksessa prosessiteoriaa muodostettaessa teorianmuodostuksen lähtökohta ja tärkein konstruktio on käyttäytymisen muutos, jota uudella teorialla pyritään selittämään. (Whetten, 2002). Mikä -konstruktiot hahmotettiin tapahtumasarjojen perusteella. Kun kustakin 6 käyttäytymistyypistä oli muodostettu käyttäytymisen muutosta selittävä malli, joka sisältää käyttäytymisen muutokseen liittyvät elementit ja interaktion elementtien välillä (ks. luku 6. 2. ja teet 4 - 9), tämän jälkeen alettiin hahmotella käyttäytymisen muutokseen liittyvät tärkeimmät vaikuttimet ja pohtimaan, miten käyttäytymisen muutos etenee prosessina. Lähtökohtana oli tietokoneenkäyttäjän kokemus, eli teoriaa lähdettiin kehittelemään sen pohjalta, mitä henkilö kokee, tuntee ja ajattelee ennen käyttäytymisen muutosta. Lisäksi pyrittiin selvittämään, omaksuuko tietokoneen käyttäjä tietyn suojaustoimenpiteen pysyvästi vai poikkeaako hän siitä joissakin tilanteissa.

Mikä-konstruktioiden hahmottamisessa apuna toimi tutkimuksen teoreettinen viitekehys. Käyttäytymisen muutosta analysoitiin siitä näkökulmasta, missä määrin muutos toteutuu 3 vaiheessa siten kuin tutkimuksen teoreettinen viitekehys olettaa (eli kokemus, tarkoituksellisuus ja käyttäytymisen muutos). Kun analyysi eteni, tälle oletukselle saatiin tukea, ja alettiin lisäämään yksityiskotia näiden pääkohtien alle: esimerkiksi mistä tietoturvaan liittyvä kokemus muodostuu, mitä tarkoituksellisuus-vaiheessa tapahtuu, mitä henkilö silloin pohtii jne. Oli myös tärkeää lisätä mukaan konteksti, eli mihin tietokoneenkäyttötarkoitukseen käyttäytymisen muutos liittyy. Tämä lisättiin prosessin alkuun 1. mikä-konstruktioksi. Kun aineisto osoitti, että suojaustoimenpiteestä saatetaan luopua joissakin tilanteessa, mukaan otettiin vielä toinen konstruktio käyttäytymisen muutos- vaiheeseen selventämään poikkeustilanteita.

Teoriaan muotoutui 4 mikä – konstruktioita: kokemus (tietokoneenkäyttö normaalitilassa), tarkoituksellisuus (epävarmuus) ja käyttäytymisen muutos, joka muodostui 2 osasta (suojaustoimenpiteen käyttöönotto sekä poikkeaminen suojaustoimenpiteen käytöstä).

Whetten (1989) kehottaa ottamaan huomioon kattavuuden ("comprehensiveness") ja "nuukuuden" ("parsimony") muodostettaessa uutta teoriaa. Tässä

tutkimuksessa mikä-elementtien valinnassa on otettu huomioon, että enempää elementtejä ei olisi ollut järkevää lisätä (comprehensiveness), ja toisaalta mukana ei ole elementtejä, joilla ei ole teoriassa lisäarvoa (parsimony). Esimerkiksi tietoturvaan liittyvä tapahtuma oli aluksi prosessissa omana tasonaan (taso 2) mutta se päätettiin muuttaa yhteydeksi tasojen 1 ja 2 välille koska sen lisääminen omaksi tasokseen ei olisi tuonut teoriaan lisäarvoa.

'Miten' –suhteet

Miten –elementit (yhteydet mikä-elementtien välillä) osoittavat sen, kuinka mikä-elementit (kokemus, tarkoituksellisuus ja 2 käyttäytymisen muutos-konstruktiota) ovat yhteydessä keskenään (Whetten, 1989) eli eteneekö prosessi suoraviivaisesti alusta loppuun vai voiko prosessissa palata taaksepäin tai voiko prosessi kenties loppua kesken. Whettenin (2002) mukaan mikä - ja miten - elementit esittävät teorian ytimen ja perus-tapahtumasarjan.

Tässä tutkimuksessa miten – elementtejä hahmoteltaessa on otettu huomioon mikä-elementtien välinen aikaulottuvuus (eli tapahtuma B seuraa tapahtumaa A). Kokemus, tarkoituksellisuus ja käyttäytymisen muutos –konstruktiot sijaitsevat prosessissa tässä järjestyksessä, mutta näiden välillä voi olla monenlaisia yhteyksiä. Analyysin edetessä huomattiin, että prosessi ei etene yksiselitteisesti tasolta 1 tasolle 4, ja esimerkiksi paluu prosessissa voi olla mahdollista. Tämän vuoksi lisää miten-suhteita mikä-konstruktioiden välille lisättiin analyysin edetessä selventämään muutosprosessia.

'Miksi' -teoreettiset oletukset

Miksi-elementit selventävät, mitä yhteydet miksi-konstruktioiden välillä tarkoittavat. Miksi-elementit muodostavat teorian oletukset ja yhdistävät mallin osat yhteen (Whetten, 1989). Tässä tutkimuksessa miksi-elementit kertovat sen, millä ehdoilla ja millainen interaktio siihen vaaditaan, että henkilön siirtyy tasolta toiselle (Schwarzer, 2008a; Velicer & Prochaska, 2008).

Miksi-elementtien tarkoitus on osoittaa, että mikä - konstruktiot on oikein valittu. Tässä tutkimuksessa pohdittiin, oliko mikä-konstruktioiden välille mahdollista muodostaa mielekäs yhteys? Tavoitteena oli, että prosessi etenee loogisesti ja että miksi-elementit selventävät logiikkaa prosessin tasojen välillä. Tämän vuoksi esimerkiksi mikä-konstruktioista poistettiin tietoturvatapahtuma-konstruktio, sillä sitä ei voitu yhdistää mielekkäällä tavalla muihin konstruktioihin. Oli siis järkevämpää lisätä se omaksi yhteydekseen tasojen 1 ja 2 välille.

6 TULOKSET

Tässä luvussa tutkimuksen tuloksena esitetään 1) malli tietoturvakäyttäytymisen muutoksesta, 2) tietoturvakäyttäytymisen universe of discourse ja 3) prosessiteoria tietoturvakäyttäytymisen muutoksesta.

Luku 6.1. sisältää tietoturvakäyttäytymisen universe of discoursen eli haastatteluiden pohjalta esiin nousevat elementit, joiden kanssa tietokoneen käyttäjät ovat interaktiossa ennen käyttäytymisen muutosta. Universe of discourse muodostaa ikään kuin tietoturvakäyttäytymisen toimintaympäristön.

Luvussa 6.2. esitellään malli siitä, kuinka tietokoneen käyttäjän tietoturvakäyttäytyminen muuttuu interaktiossa eri elementtien kanssa (esimerkiksi tietoturvauhka, tietolähde ja tietoverkko). Luvussa 6.3. on esitelty 6 eri prosessia, jotka johtavat käyttäytymisen muutokseen, eli jokaisesta käyttäytymistyypistä on muodostettu oma prosessi. Yhdistetty prosessi, johon on koottu yksittäisten mallien erityispiirteet esitetään luvussa 6.3.7.

6.1 Tietoturvakäyttäytymisen Universe of discourse

Tietoturvakäyttäytymisen Universe of discoursella tarkoitetaan niitä asioita, joiden kanssa tietokoneenkäyttäjä on yhteydessä kun tietoturvakäyttäytyminen muuttuu. Universe of discoursen määrittely on tärkeää, sillä se helpottaa aihealueen tutkimista. (Bush, 1909). Universe of discourse muodostuu joukosta asioita, joiden puhujat olettavat olevan olemassa ja joista keskustellaan. (Saguillo, 1999). Tässä työssä Universe of discourse muodostuu 10 elementistä, jotka nousivat esille tietokoneen käyttäjiä haastateltaessa. Ne muodostavat tietoturvakäyttäytymisen toimintaympäristön:

- Tietokoneen käyttäjän kokemus = experience of computer user,
- Tietokone = computational devices,
- Suojaustoimi = safeguards,
- Omaisuus = assets,

- Uhka = threats,
- Harmilliset seuraamukset = harmful consequences
- Tietolähde = information source,
- Tietoverkko = computer network,
- Esteet = barrier,
- Edistäjät = driver

Elementit ovat yhteydessä keskenään eri tavoilla. Liitteissä 4-9 on 6 esimerkkiä siitä, millaisia interaktioita elementtien kesken käyttäytymisen muutokseen vaaditaan.

Taulukossa 6 on määrittelty Universe of discoursen elementit

TAULUKKO 6 Universe of discoursen elementtien kuvaus

Elementti	**Kuvaus**
Harmillinen seuraamus	Jos tietoturvauhka realisoituu, siitä seuraa ongelmia tietokoneenkäyttäjälle.
Tietolähde	Tietolähteet kuten media ja ystävät auttavat suojaamaan tietokonetta, koska tietokoneenkäyttäjä saa niiden kautta lisätietoa siitä, kuinka suojata omaisuuttaan ja tietokonelaitteitaan.
Suojatoimi	Tietokoneen käyttäjällä on valittavanaan monenlaisia suojatoimia laitteidensa ja omaisuutensa suojaamiseen kuten virus- ja vakoiluohjelmat, vahvat salasanat ja varmuuskopiointi.
Omaisuus	Tietokoneenkäyttäjällä on runsaasti tietoa, jota täytyy suojata tietoturvauhkilta (valokuvat, liiketoimintaan liittyvät dokumentit, työhakemukset, kopioita passista jne.)
Uhka	Tietokoneenkäyttäjä kohtaa monenlaisia tietoturvauhkia, joita vastaan suojautua (esim. virukset, madot, vakoiluohjelmat, tietojen kalastelu, hujaukset, roskaposti)
Tietoverkko	Tietoverkko on osa informaatioteknologiaa, joka mahdollistaa sähköisen tiedonvälityksen. Toisaalta taas tietoverkossa piilee monia tietoturvauhkia.
Tietokone	Tietokonelaitteet ovat suojattavaa omaisuutta ja alttiita tietoturvauhkille. Toisaalta taas ne ovat osa informaatioteknologiaa, joka mahdollistaa sähköisen tiedonvälityksen.
Tietokoneenkäyttäjän kokemus	Kognitiivinen, tietokoneen käyttäjän ajatteluun liittyvä elementti. Tietokoneen käyttäjät toimivat interaktiossa ympäröivän maailman kanssa,, mikä muuttaa heidän ajatteluaan.

6.1.1 Tietokoneen käyttäjä

Tämä tutkimus selvittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymistä. Määriteltäessä tietokoneen käyttäjää tästä näkökulmasta apuna on käytetty määritelmää kotitietokoneen käyttäjästä (Kritzinger & von Solms, 2010) sillä erotuksella että ei ole rajoituttu yhteen kontekstiin (koti), koska henkilökohtaista tietokonetta käytetään myös kodin ulkopuolella ja erilaisissa verkoissa, esimerkiksi työpaikan verkossa ja julkisissa verkoissa (kirjastot, hotellit, lentoasemat, kahvilat jne.).

Henkilökohtaisen tietokoneen käyttäjät ovat yhteydessä Internetiin omilla laitteillaan. (Kritzinger & von Solms, 2010). Heillä ei ole "valvovaa silmää" antamaan vaatimuksia tietoturvakäyttäytymiselle (Kritzinger & von Solms, 2010). Heillä ei myöskään ole teknistä tukea käytössään, joten he ovat vastuussa itse tietokoneensa suojauksesta viruksia ja haittaohjelmia vastaan (Kritzinger & von Solms, 2010).

Henkilökohtaisen tietokoneen käyttäjät ovat haavoittuvaisia, koska heillä ei välttämättä ole tarpeeksi tietoa tietoverkojen tietoturvasta ja tietotekniikasta sekä taitoja suojata tietokonettaan (Kritzinger & von Solms, 2010; Furnell et al, 2010). Kaikilla tietokoneen käyttäjillä ei välttämättä myöskään ole mahdollisuutta osallistua tietoturvakoulutukseen (Kritzinger & von Solms, 2010).

6.1.2 Tietokone

Perinteisen PC:n lisäksi tietokoneenkäyttäjillä on nykyään käytössään monenlaisia laitteita, joiden välityksellä he ovat yhteydessä Internetiin (kannettava tietokone, tablettitietokone, älypuhelin jne.). Myös pelaamiseen käytettävät laitteet ja kotiteatterisovellukset ovat tulossa yleisiksi tietokoneen käyttäjien keskuudessa.

Tietokonelaitteet ovat haavoittuvaisia, koska ne sisältävät sensitiivistä tietoa kuten kuvia viestejä, yhteystietoja ja dokumentteja (työhakemuksia, matkavakuutuksia, verokortteja, kopioita passista jne.) ja ovat yhteydessä Internetiin.

Kun tietokoneen käyttäjä hankkii uuden laitteen, hän on itse vastuussa soveltuvan suojauksen hankkimisesta sille. Haastateltaessa tietokoneen käyttäjiä tuli ilmi, että käyttäjät suojaavat PC:tä ja kannettavia tietokoneita tarkemmin mutta esimerkiksi tablettien ja älypuhelinten suojaus on vähäisempää. Toisaalta taas, monet uudet älypuhelinmallit sisältävät mobiiliturvan.

6.1.3 Suojaustoimi

Tietokonelaitteiden ja sensitiivisen tiedon suojaukseen on olemassa useita mahdollisuuksia. Sovelluksia löytyy mm. virusten torjuntaan ja varmuuskopiointiin. Suojaavan teknologian lisäksi tietokoneen käyttäjä voi omaksua erilaisia tietoturvakäytäntöjä kuten uloskirjautumisen laitteelta ja vahvojen salasanojen käytön.

Yleisimpiä suojaustoimenpiteitä ovat seuraavat:

- vahvat salasanat
- turvakoodit kannettaviin laitteisiin
- salasanojen säännöllinen vaihtaminen
- uloskirjautuminen laitteilta
- varmuuskopiointi
- virustorjuntaohjelmistot
- anti-spyware-ohjelmistot
- palomuurit
- epäilyttävien Internet-sivujen välttäminen
- sensitiivisen tiedon käsittelyn välttäminen Internetissä
- sähköpostin tai tiedostojen kryptaaminen
- ohjelmistopäivitysten tekeminen

Kun kyseessä on henkilökohtaisen tietokoneen ja henkilökohtaisen tietojen suojaus, tietokoneen käyttäjä käyttää omaa harkintaansa siihen, missä määrin hän ottaa suojaustoimenpiteitä käyttöön.

6.1.4 Omaisuus

Tietokonelaitteisiin tallennetaan monenlaista aineistoa. Tämän tutkimuksen haastattelut osoittivat, että henkilökohtaisiin laitteisiin tallennetaan mm. opiskeluun liittyvää materiaalia, liiketoimintasuunnitelmia, kuvia, musiikkia, elokuvia, työhakemuksia, matkavakuutuksia, pelejä, kopioita passista, verokortteja, kuitteja, chattilogeja, laskuja ja salasanoja.

Kun ihmiset omistavat sensitiivistä materiaalia, heidän tulee myös miettiä, kuinka suojata sitä, jotta se ei päädy vääriin käsiin. Myös tietokonelaitteet edellyttävät huolellista säilytystä. Kannettavat laitteet on helppo hukata, ja jos laite hukkaamisen jälkeen joutuu vääriin käsiin, on vaarana, että sensitiivistä tietoa vuotaa ulkopuolisille. Jos menetettyä tietoa ei ole varmuuskopioitu, sitä ei saa enää takaisin.

Suojaamalla henkilökohtaisia tietojaan tietokoneen käyttäjät suojaavat yksityisyyttään. Yksityisyys on siis myös omaisuutta, ja sitä halutaan varjella esimerkiksi käyttämällä sosiaalisen median tietoturva-asetuksia.

6.1.5 Uhka

Internetin käyttö tuo mukanaan useita tietoturvauhkia. Tunnetuimmat tietoturvauhkat, jotka koskevat henkilökohtaisen tietokoneen käyttäjiä ovat seuraavat:

- haittaohjelmat, virukset ja madot, joilla tarkoitetaan tietokoneohjelmaa tai komentoa, jotka on tarkoitettu aiheuttamaan epätoivottuja tapahtumia tietojärjestelmissä. Ne voivat levitä sähköpostin, Internetin tai tiedostojen välityksellä
- tietomurto ja varkaus tarkoittaa tietokoneen hakkeroimista ja koneen luvatonta käyttöä, tietokoneella olevan materiaalin varastamista ja sen väärinkäyttöä

- huijaus eli lähestytään tietokoneen käyttäjää esimerkiksi pankin tai puhelinoperaattorin nimissä
- ketjukirje eli luvataan esimerkiksi rahaa jos välittää viestin eteenpäin tarpeeksi monelle
- huijausvaroitukset tarkoittavat esimerkiksi tekaistua varoitusta haittaohjelmasta, jossa pyydetään lähettämään viesti mahdollisimman monelle, ja tämä levittää haittaohjelmia. Sellaisten ohjelmistojen myyminen, joka sisältää haittaohjelmia kuuluu myös tähän kategoriaan.
- roskaposti tarkoittaa ei-toivottua sähköpostia joka ei ole tarkoitettu kenellekään erityisesti, vaan lähetetään massaviestinä
- tietosuojarikkomus tarkoittaa henkilötietojen etsimistä Internetistä. Tietojen käyttötarkoitus on usein epäselvä
- hakkerointi tarkoittaa haavoittuvien osien etsimistä tietojärjestelmästä ja tietokoneesta tarkoituksena vahingoittaa järjestelmää
- tietoturva-aukko tarkoittaa haavoittuvuutta tietojärjestelmässä tai sen suojauksessa mikä tarjoaa mahdollisuuden tunkeutua järjestelmään

  (Lähde: Jyväskylän yliopiston WWW-sivut)

Tietoturvauhkat kehittyvät koko ajan. Hakkerit esimerkiksi keksivät koko ajan uusia tapoja tunkeutua järjestelmiin ja vahingoittaa niitä sekä varastaa tietoja. Voidaan sanoa, että tietoturvauhkien suhteen tulevaisuus on aina jossain määrin tuntematon.

6.1.6 Toteutuneen uhkan haitalliset seuraukset

Mikäli tietotokoneen käyttäjä ei noudata hyviä tietoturvakäytäntöjä kuten vahvoja salasanoja tai virustorjuntaa, tästä voi koitua haitallisia seurauksia. Esimerkiksi erilaiset haittaohjelmat, vakoiluohjelmat ja virukset voivat olla seurausta haitallisten Internet-sivujen käytöstä ja roskapostista. Virukset voivat hidastaa konetta ja saastuttaa tiedostoja. Myös vakoiluohjelmat voivat hidastaa tietokonetta ja varastaa käyttäjätietoja. Uloskirjautuminen laitteelta on nopea mutta tärkeä toimenpide, minkä unohtaminen voi johtaa tietokoneen väärinkäyttöön.

Tietokoneen hakkeroinnilla on monia haitallisia seurauksia, esimerkiksi IP osoitetta voidaan käyttää vahingoittamaan tietoverkkoa. Tietokonetta voidaan myös käyttää ns. ”botnetissä”. Henkilön pankkitunnuksia voidaan hakkeroida, samoin kuin sähköpostia. On myös tapauksia, joissa verkkokaupan käyttäjätunnuksia on väärinkäytetty.

Kannettavien laitteiden hakkerointi voi johtaa kuvien ja henkilötietojen menetykseen. Arkaluonteisen tiedon prosessointi julkisissa langattomissa verkoissa (WIFI) esimerkiksi lentokentillä, kahviloissa jne. voi aiheuttaa tietojen vuotamisen kolmannelle osapuolelle.

Tietoturvauhkien seuraukset toimivat samalla tavalla kuin itse uhkat: varoituksina, jotka motivoivat ihmisiä suojaamaan laitteensa ja tietonsa. Jos esimerkiksi ystävä on kokenut sähköpostin hakkeroinnin, uhka tuntuu läheisem-

mältä ja konkreettisemmalta. Samoin, jos henkilö menettää tietoja varmuuskopioinnin puuttumisen vuoksi, hän huomaa, että varmuuskopiointi todella kannattaa ja ottaa tämän suojaustoimenpiteen käyttöön.

6.1.7 Tietolähde

Tietokoneen käyttäjät saavat tietoturvaan liittyvää tietoa useista lähteistä. Esimerkiksi TV, radio ja lehdet informoivat uusista tietoturvauhkista ja kuinka suojautua niitä vastaan. Internetissä monet yliopistot ja oppilaitokset julkaisevat tietoturvaohjeita.

Lisäksi, esim. European Network and Information Security Agency (2006) on julkaissut hyviä käytäntöjä tietokoneen suojaukseen. Pankeilla on omia ohjeistuksia tietoturvaan liittyen samoin kuin viranomaisilla. Esimerkiksi Viestintävirastolla on WWW-sivuillaan tietoturvaopas suomeksi ja englanniksi.

Internetin erilaisilla keskustelupalstoilla käsitellään tietoturva-asioita. Myös ystävät, työkaverit, opiskelukaverit, sukulaiset ja läheiset ihmiset voivat antaa käytännöllisiä neuvoja suojaustoimenpiteisiin liittyen. Monilla työpaikoilla ja oppilaitoksissa järjestetään tietoturvakoulusta. Se, kuinka tietoisia yksityiset tietokoneen käyttäjät ovat tietoturva-asioista, riippuu paljolti omasta motivaatiosta etsiä aiheeseen liittyvää tietoa.

6.1.8 Tietoverkko

Internetiä voidaan kuvailla joukoksi keskenään yhteydessä olevia verkkoja (Will, 1996). Internetissä satoja tuhansia kaupallisia, akateemisia ja hallinnollisia verkkoja sekä henkilökohtaisia tietokonelaitteita ovat yhteydessä keskenään ja vaihtavat tietoa sähköisesti (Downes, 2007; Sieverding, 2008; *Encyclopædia Britannica Online)*

Internetin alkuaika sijoittuu vuoteen 1969, jolloin se aloitti nimellä Arpanet. Tämän jälkeen Internet-yhteyksien määrä on kasvanut valtavasti (Downes, 2007). Tilastojen mukaan vuonna 2014 noin 40.4 % maailman ihmisistä oli Internet-yhteys ja Internetin käyttäjiä oli n. 3 000 000 000 (Internet live stats).

Verkossa liikkuu paljon tietoturvauhkia. Esimerkiksi haittaohjelmat, virukset, madot, roskaposti ja vakoiluohjelmat välittyvät tietoverkkojen välityksellä. Internetissä liikkuu myös hakkereita, jotka etsivät haavoittuvuuksia järjestelmistä ja tietokoneista ja yrittävät vahingoittaa niitä.

Internet muuttuu jatkuvasti ja nopeasti. Yksi syy tähän on se, että järjestelmät lakkaavat toimimasta tai niitä korvataan ajan kuluessa (Kuhn et al. 2009; Gralla, 1998). Internetin taustalla olevan teknologian kehitys on nopeaa (Gralla, 1998; Elango, 2000).

Lisäksi Internetin tietoturvan taso muuttuu koko ajan. Uusia tietoturvauhkia tulee koko ajan (Ishiguro, 2004). Esimerkiksi pilvipalvelut ovat tuoneet mukanaan uusia tietoturvauhkia (Hwang et al 2009; Sabahi, 2011; Chen et al., 2010). Tärkeimmissä pilvipalveluissa on löydetty tietoturva-aukkoja (Wang et al. 2010). Myös matkapuhelimiin kohdistettuja tietoturvauhkia on havaittu (Wu

et al., 2014). On kehitetty esimerkiksi haittaohjelmia, jotka keräävät yhteystilastoja ja puheluhistoriaa ja tallentavat puheluita. (*Computer Security Update 2012.)*

6.1.9 Esteet suojaustoimen käytölle

Vaikka tietokoneen käyttäjä haluaisi omaksua jonkin tietyn tietoturvatoimintatavan, esimerkiksi teknisen osaamisen puute voi aiheuttaa ongelmia. Esimerkiksi kryptaus ei ole tavalliselle tietokoneenkäyttäjälle helposti omaksuttavissa. Jotkut käyttäjät myös ajattelevat, että kryptaus on hidasta olemassa olevaan riskiin verrattuna, mikä estää ottamasta sitä käyttöön. Antivirus-ohjelmiston käytön voi estää se, että käyttäjä ei tiedä miten se asennetaan.

Tämän tutkimuksen mukaan yksi syy siihen, minkä vuoksi käyttäjät eivät laadi vahvoja salasanoja, on ongelmat monimutkaisten salasanojen muistamisessa ja halu välttää ylimääräistä vaivaa. Taloudelliset syyt voivat myös muodostua esteeksi tietoturvasuojausten omaksumisessa. Jos esimerkiksi antivirusohjelmistosta täytyy maksaa, tämä voi muodostua esteeksi sen hankkimiselle. Esteiden tunnistaminen on tärkeää. Tämä auttaa ymmärtämään tietoturvakäyttäytymistä paremmin, mutta myös kehittämään tietoturvapalveluita. Jos tiedämme, mitkä syyt esimerkiksi estävät asentamasta mobiiliturvaa, se auttaa kehittämään tätä palvelua.

6.1.10 Edistäjät

Tietoturvatoimenpiteen omaksumista edistää mm. se että tietoturvaohjelmisto on helppo asentaa tai että salasana on helppo muistaa. Jotkut järjestelmät ohjaavat vahvan salasanan laatimisessa mikä auttaa tietokoneen käyttäjää, jos hän ei itse osaa laatia vahvaa salasanaa. Salasanan merkitseminen muistikirjaan tai kännykkään helpottaa vaikean salasanan muistamista. Jos tietokoneen käyttäjä haluaa hallita tietoja, jotka hänestä on näkyvillä Internetissä, hakukoneet ja kuvahaku ovat avuksi omien tietojen etsimisessä Internetistä.

Kaiken kaikkiaan tässä luvussa esitelty tietoturvakäyttäytymisen Universe of discourse on tärkeä osa tutkimusta. Elementtien määrittely tutkimuksen alkuvaiheessa auttoi olennaisesti hahmottamaan sitä toimintaympäristöä, jossa tietokoneenkäyttäjät toimivat ja jossa käyttäytyminen muuttuu. Universe of discoursen määrittely helpotti käyttäytymisen muutoksen mallintamista (luku 6.2.). Tietoturvakäyttäytymistä kuvaavassa mallissa universe of discoursen elementit on esitetty graafisesti ja niiden välille on hahmoteltu yhteyksiä. Mukaan on lisätty 1 elementti, joka pohjautuu tutkimuksen teoreettiseen viitekehykseen ja on mallin ns. kognitiivinen elementti (tietokoneenkäyttäjän kokemus). Universe of discourse on täydentänyt myös prosessiteoriaa, sillä prosessiteoriassa kuvataan ne elementit ja interaktio, joka saa käyttäytymisen muutoksen aikaan.

6.2 Malli tietoturvakäyttäytymisen muutoksesta

Malli tietoturvakäyttäytymisen muutoksesta (kaaviossa 2) on yhdistetty malli, joka on muodostettu 6 eri käyttäytymistyyppiä kuvaavan mallin pohjalta (Internet profiilin hallinta, vahvan salasanan laatiminen, varmuuskopiointi, varovaisuus verkkokaupassa, virustorjuntaohjelman käyttöönotto ja sensitiivisen aineiston prosessointi). Yksittäiset mallit (6 kpl) on esitetty liitteissä 4-9.

Malli tietoturvakäyttäytymisen muutoksesta osoittaa sen, että tietokoneen käyttäjien tietoturvakäyttäytyminen muuttuu ajan myötä, kun tietokoneenkäyttäjät ovat yhteydessä ympäröivään maailmaan ja kokevat tietoturvaan liittyviä asioita (Searle, 1995 & 2013 & 1990) (ks. kaavio 1). Kokemukset ovat tietoisia tapahtumia, ja ne herättävät tarkoituksellisuuden: tietokoneenkäyttäjä pohtii kokemusten merkitystä itselleen, oman tietoturvansa kannalta. Muutos ajattelussa aiheuttaa muutoksen tietoturvakäyttäytymisessä.

Mallin sisältämien elementtien välille voidaan hahmotella 8 tyyppisiä yhteyksiä: harmillisten seuraamusten ymmärtäminen, tietoturvallinen toiminta, tietoturvatietoisuuden lisääntyminen, omistaminen, edellytykset, käyttäytymisen muutoksen helpottuminen/nopeutuminen, käyttäytymisen muutoksen hidastuminen sekä tarve tietokoneen käytölle. Tietokoneen käyttäjä on esimerkiksi yhteydessä omaisuus-elementtiin, koska hän omistaa luottokorttinumeron. Tietokoneen käyttäjä on yhteydessä myös suojaustoimenpide-elementtiin, koska hänellä on käytössään virustorjuntaohjelmisto. Taulukossa 7 on esitelty kaikki tietoturvakäyttäytymistä kuvaavissa malleissa esiintyvät yhteystyypit ja niiden variaatiot:

TAULUKKO 7 Tietoturvakäyttäytymistä selittävän mallin yhteystyypit ja niiden variaatiot eri käyttäytymistyypeissä

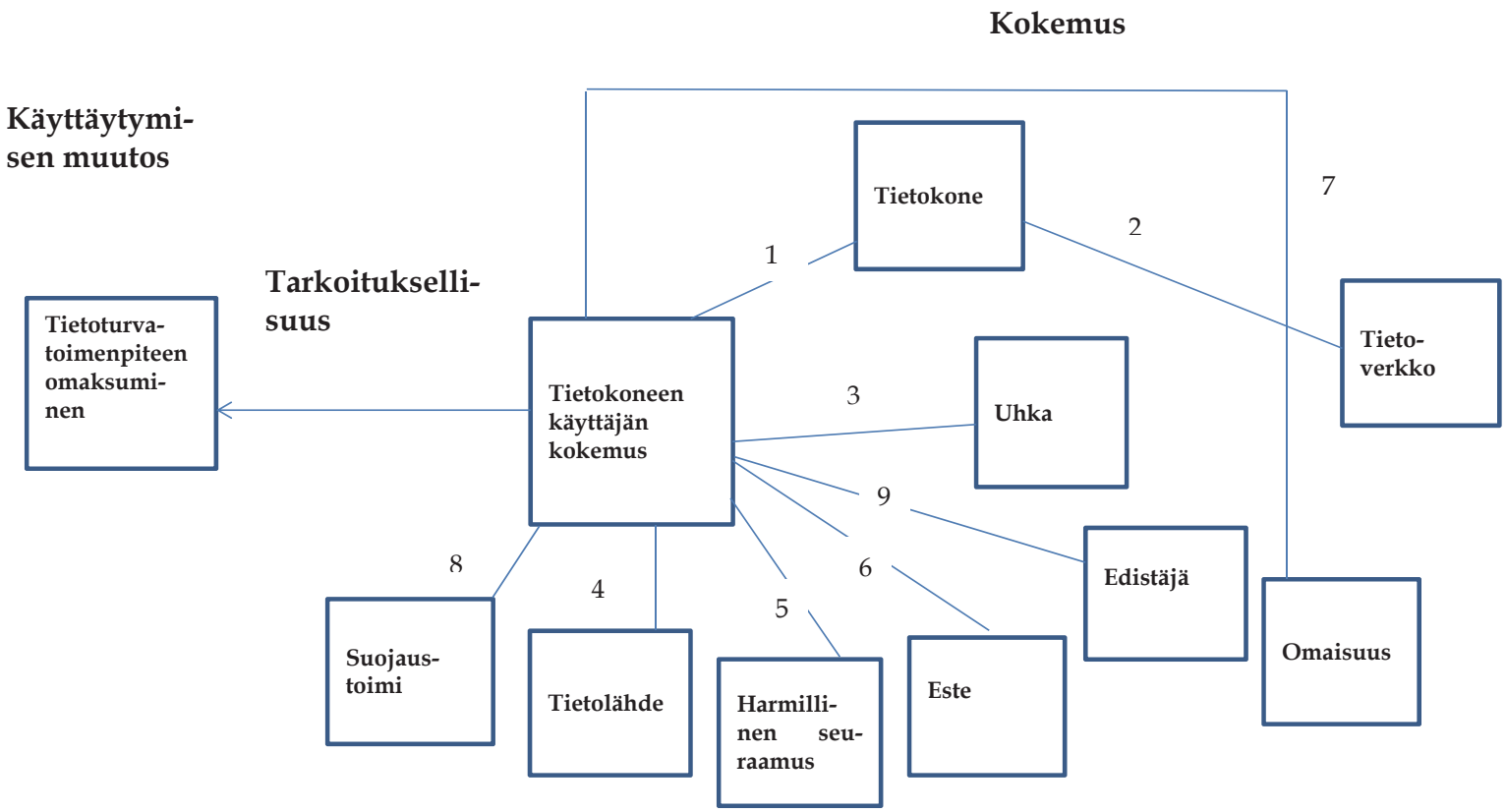
Yhteys #	Yhteyden tyyppi	Yhteyden kuvaus
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta verkkokauppa-asiointiin, yhteydenpitoon, liiketoimintaan, oman työn markkinointiin, harrastuksiin, asiointiin esimerkiksi viranomaisten kanssa tai verkkopankissa, tiedonhakuun, tiedon välittämiseen, pelaamiseen, opiskeluun ja kuvien, muistiinpanojen, erilaisten tekstien, videoiden ja musiikin tallennukseen, musiikin kuunteluun ja videoiden katseluun. Käyttäytymistä motivoivat liittymistarve (need for relatedness) ja toimeentulotarve (Alderfer), kehittymisen tarve (Maslow), itsensä toteuttamisen tarve (Maslow), henkilökohtaisen kasvun tarve (Alderfer), uteliaisuuden ja säästämisen tarve (Reiss),tietämisen ja ymmärtämisen tarve (Maslow), sosiaalisen arvostuksen tarve (Maslow), tarve sosiaalisiin yhteyksiin (Social contact) (Reiss), hyväksynnän tarve (acceptance) (Reiss), esteettisyyden tarve (Maslow, Reiss). Myös asioinnin tarve sekä ajan ja vaivan säästämisen tarve selittävät käyttäytymistä tällä tasolla.
2	Edellytykset	Tietokone on yhteydessä Internetiin, kun sitä käytetään em. käyttötarkoituksissa.
3	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä tulee tietoiseksi sosiaalisen median käyttöön, sensitiivisen tiedon välittämiseen, heikkoihin salasanoihin, verkkokaupan käyttöön, viruksiin sekä varmuuskopioinnin puuttumiseen liittyvistä uhista.
4	Tietoturvatietoisuuden lisääntyminen	Tietoturvatietoisuuden lisääntyminen eri tietolähteiden kautta:

		– ystävät, sukulaiset, perhe ja tuttavat – asiakkaat ja kollegat – työ ja koulu – koulutus työn ja koulun ulkopuolella – palveluntarjoajat: pankki, sosiaalinen media, verkkokauppa, luottokunta – media: TV, Internet, uutiset ja nettifoorumit
5	Harmillisten seuraamusten ymmärtäminen	**Esimerkkejä harmillisista seuraamuksista** **Internet-profiilin hallinta** Tietokoneen käyttäjän kuva päätyy Internetissä julkisesti saatavaksi tai ei-halutuille sivuille. Tietoja häviää sosiaalisen median palvelusta. Tietokoneen käyttäjän sosiaalisen median profiili kopioidaan. Tietokoneen käyttäjä tulee tietoiseksi siitä että sosiaalisessa mediassa olevia tietoja voi vuotaa ulkopuolisille ja että käyttäjistä voidaan levittää väärää tietoa sosiaalisen median profiilin kaappauksen myötä. Kuvanjakopalveluun talletettuja kuvia päätyy julkiseksi. **Sensitiivisen tiedon prosessointi** Tietokoneen käyttäjän ystävän sähköpostiviesti päätyy ulkopuolisille. Tietokoneen käyttäjä kuulee tv:stä, Internetistä, työpaikalla tai koulussa, että sensitiivistä tietoa ei saa lähettää sähköpostissa ja että ne voidaan varastaa. Tietokoneen käyttäjä kuulee, että tietoja saattaa kadota sosiaalisesta mediasta.

		Vahva salasana Tietokoneen käyttäjän sähköpostitili kaapataan ja sähköpostitiliä väärinkäytetään. Ystävä kokee tiedonmenetyksen sähköpostin hakkeroinnin seurauksena. **Varmuuskopiointi** Tietokoneen käyttäjä kokee tiedon menetyksen koneen rikkoutumisen/viruksen seurauksena. Ystävä kokee tiedon menetyksen, koska tietokone saastuu viruksesta. **Varovaisuus verkkokaupassa** Tietokoneen käyttäjä kokee rahanmenetyksen verkkokauppa-asioinnin seurauksena. Ystävän luottokortti hakkeroidaan, mistä seuraa rahanmenetys ja tilin käyttö estyy. Tietokoneen käyttäjän luottokorttitietoja vuotaa verkkokaupasta julkisuuteen. **Virustorjuntaohjelmiston käyttöönotto** Tietokoneenkäyttäjän tietoturvaohjelmisto ei suojaa kaikilta haittaohjelmilta, mistä seuraa ongelmia kuten koneen hidastuminen, aloitussivun vaihtuminen selaimessa, käynnistysongelmia ja popup-ikkunoita.
6	Käyttäytymisen muutoksen hidastuminen	Erilaiset tietokoneenkäyttäjän kohtaamat esteet hidastavat tietoturvasuojauksen käyttöönottoa. Esimerkkejä: Tietokoneenkäyttäjä ei hallitse kuvanjakopalvelun yksityisyysasetusten käyttöä, minkä vuoksi kuvia päätyy julkisesti saataville. Virustorjuntaohjelma on vaikea asentaa. Vahvoja salasanoja on vaikea muistaa.

7	Omistaminen	Käyttäessään tietokonetta verkkokauppa-asiointiin, yhteydenpitoon, yhdistystoimintaan, liiketoimintaan, verkkopankkiasiointiin, tiedonhakuun, pelaamiseen, opiskeluun ja tallennukseen tietokoneen käyttäjä prosessoi mm. seuraavia asioita: luottokorttinumero, raha, kuvat, sähköpostitiedot, sosiaalisen median päivitykset, identiteetti, tilinumero, sähköpostiviesti, henkilökohtaiset viestit, ostokuitit, potilastiedot, henkilötunnus,verkkokauppaan liittyvät tiedot, luottokorttitiedot, puhelinnumero, osoite, liiketoiminta-asiakirjat, työhön liittyvät tiedot, opiskeluun liittyvät asiakirjat, kuvat, tietokone, salasanat, pankkitunnukset, työnantajaan liittyvät tiedot
8	Tietoturvallinen toiminta	Ennen uuden suojaustoimen hankkimista tietokoneen käyttäjällä voi olla käytössään jokin suojaustoimenpide, jota pitää myöhemmin täydentää /vahvistaa. Tietokoneen käyttäjä esimerkiksi suojaa tietokoneensa tietoturvaohjelmistolla, jonka hän luulee suojaavan tietojen häviämiseltä.
9	Käyttäytymisen muutoksen helpottuminen / nopeutuminen	Tietoturvasuojauksen käyttöönottoa edistää mm., se, että hakukoneiden avulla käyttäjä pystyy etsimään itseään koskevaa tietoa Internetistä, että varmuuskopiointi on helppoa ja että tietojärjestelmä (esim. pankin) ohjaa vahvan salasanan laatimisessa. Koska virustorjuntaohjelmisto on helppo asentaa ja ilmainen, tämä nopeuttaa sen käyttöönottoa.

KUVIO 2 Yhdistetty malli käyttäytymisen muutoksesta (pohjautuu: Searle (1995 &1983), ks. luku 2.2. kuvio1



TAULUKKO 7 Käyttäytymistä kuvaavan mallin elementtien variaatiot

Elementti	**Elementin variaatiot eri käyttäytymistyypeissä**
tietokone	tietokone jota käytetään asioinnissa, esimerkiksi verkkokauppa-asioinnissa, verkkopankkiasioinnissa, yhteydenpidossa esimerkiksi ystäviin ja työnantajiin, yhdistystoiminnassa, pelaamisessa, opiskelussa, liiketoiminnan edistämisessä, oman työn markkinoinnissa, kuvien, videoiden, musiikin ja muistiinpanojen yms. tallennuksessa ja Internet-sivujen selaamisessa
tietoverkko	Internet
omaisuus	luottokorttinumero, raha, sosiaalisen median tiedot ja päivitykset, yksityisyys, identiteetti, tilinumero, sähköpostiviestit ja sähköpostitiedot, potilastiedot, henkilötunnus, verkkokauppaan liittyvät tiedot, oma nimi, puhelinnumero, osoite, kriittinen informaatio sähköpostissa kuten esimerkiksi henkilökohtaiset viestit, ihmissuhteisiin liittyvät tiedot ja ostokuitit, liiketoiminta-asiakirjat, työhön ja työnhakuun liittyvät dokumentit ja tiedot, artikkelipohjat, opiskeluun liittyvät asiakirjat, kuvat, tietokone ja sinne talletetut tiedot, kuten salasanat ja pankkitunnukset, tiedostomateriaali, lopputyöhön liittyvään yritykseen ja tuotteeseen liittyvät tiedot, oma henkilöhistoria, pankkitiedot, käyttäjätunnus ja salasana
este	ongelmat verkkokaupan englanninkielisten ohjeiden ymmärtämisessä, tietokoneen käyttäjä ei osaa käyttää kuvanjakopalvelua niin että kuvat eivät leviäisi julkisesti saataville, tietokoneen käyttäjä ei hallitse yksityisyysasetusten laittamista sosiaalisessa mediassa, vahvan salasanan muistaminen hankalaa, tietokoneen ikä (ei mahdollista uuden virustorjuntaohjelman asentamista), laiskuus ja välinpitämättömyys liittyen vahvan salasanan laatimiseen, välinpitämättömyys varmuuskopiointia kohtaan, salasanoja on vaikea muistaa, tietokoneenkäyttäjä epäilee virustorjunnan tehokkuutta, puutteelliset taidot virustorjuntaan liittyvän tiedon etsimiseen netistä ja ohjeiden ymmärtämiseen
edistäjä	hakukoneen avulla voi etsiä itseään koskevaa tietoa Internetistä; pankin järjestelmä ohjaa vahvan salasanan laatimisessa; tietoturvaohjelmisto, esimerkiksi virustorjunta-

	ohjelmisto, on helppo asentaa ja helppo käyttää; verkkopalvelu pakottaa laatimaan vahvan salasanan jotta palvelua pääsee käyttämään, Internetistä löytyy ohjeita vahvan salasanan laatimiseen, palvelu pyytää vahvistamaan salasanaa, varmuuskopiointi on helppo tehdä, tietoturvaohjelmisto on ilmainen, selain tallettaa salasanat joten niitä ei tarvitse muistaa
harmillinen seuraamus	rahan menetys verkkokaupassa, tilin käytön estyminen, pitkät selvittelyajat, ylimääräiset lisät verkkokauppaostoksiin, luottokorttitietojen vuotaminen julkisuuteen, tietojen vuotaminen esimerkiksi sosiaalisesta mediasta ulkopuolisille, tietojen katoaminen sosiaalisesta mediasta, väärän tiedon levittäminen identiteettivarkauden seurauksena, oman kuvan päätyminen ei-halutuille sivuille, kuvien vuotaminen kuvanjakopalvelusta julkisesti saataville, omien tietojen, esimerkiksi pankkitietojen, väärinkäyttö, liiketoiminta-asiakirjojen / kuvien/opiskeluun liittyvien dokumenttien menetys, koneen saastuminen, koneen hidastuminen, pop-up ikkunat, selaimen aloitussivun vaihtuminen, sähköpostitunnusten kaappaaminen, sähköpostin tietojen menetys, erikoiset kaveripyynnöt sosiaalisessa mediassa, tuntemattomien ihmisten päivitysten näkeminen, vääristyneen kuvan muodostuminen itsestä Internetissä olevien tietojen perusteella, eitoivotut yhteydenotot, tavaroiden tilaaminen toisen nimellä, chat-keskustelun kaappaus, nettikiusaaminen, koneen hallinnan menettäminen, tiedostomateriaalin päätyminen vääriin käsiin, salasanojen vuotaminen ja varastaminen, sähköpostin käyttäminen ja lähettäminen toisen nimissä, koneen hallinnan menettäminen
tietolähde	ystävät, sukulaiset ja muu lähipiiri, firman asiakkaat, verkkokauppa, luottokunta, nettifoorumi, LinkedIn – koulutus, perhe, TV, Internet, koulu, koulupoliisi, palveluntarjoaja (esim. sosiaalinen media), pankki, työ, tietokonealan lehdet, kollegat sekä uutiset, palveluiden foorumit
uhka	huijaus verkkokaupassa, verkkokaupan toimintaongelmat, verkkokaupan tietokannan hakkerointi, luottokortin hakkerointi, roskaposti, käyttäjätunnusten, esimerkiksi sosiaalisen median tunnusten väärinkäyttö, sosiaalisen median profiilin kopiointi, iden-

	titeettivarkaus, sähköpostiviestien levittäminen/varastaminen, haittaohjelmat ja virukset, jotka tuhoavat tiedostoja, tietokoneen rikkoutuminen, varmuuskopioinnin unohtaminen, tietojen varastaminen, salasanojen (esimerkiksi sähköposti) hakkerointi, haittaohjelma kaappaa tietokoneen, ”olan yli katseleminen” ja salasanan selville saaminen, tietokoneen kuluminen, verkkokauppatunnusten tai luottokorttinumeroiden vuotaminen
tietokoneenkäyttäjän kokemus	tietokoneenkäyttäjän kokemus liittyen Internet-profiilin hallintaan, sensitiivisen aineiston prosessointiin, vahvan salasanan laatimiseen, varmuuskopiointiin, verkkokauppa-asiointiin ja virustorjuntaan
suojaustoimi	käytössä oleva suojatoimi (antivirusohjelmisto, tietoturvaohjelmisto)

Taulukkoon 8 on esitetty tiivistetysti miten malli (kuviossa 1) selittää tietoturvakäyttäytymistä:

TAULUKKO 8 Miten tutkimuksessa kehitetty malli selittää tietoturvakäyttäytymistä

Kokemus (Experience)	Käyttäytyminen muuttuu kokemuksen kautta henkilön toimiessa interaktiossa useiden ulkoisten elementtien kanssa (uhka, tietoverkko, tietolähde jne.) Kun elementit ovat interaktiossa keskenään muodostuu prosesseja, jotka saavat käyttäytymisen muutoksen aikaan
Interaktio	Malli osoittaa mitkä elementit ovat yhteydessä toisiinsa ja ovat muodostamassa tietokoneen käyttäjän kokemusta Malli esittää, mitkä elementit ja millainen interaktio vaaditaan siihen että käyttäytyminen muuttuu
Tarkoituksellisuus (Intentionality)	Kokemukseen liittyy aina tarkoituksellisuus Henkilö pohtii, mitä kokemus tarkoittaa hänen omasta näkökulmastaan ja oman itsensä kannalta Merkityksen löytäminen kokemukselle Ihminen ymmärtää/ ajattelee/ huomaa miten pitää toimia Kokemus, interaktio ja tarkoituksellisuus (intentionality) yhdessä aiheuttavat ajattelun muutoksen, mikä johtaa käyttäytymisen muutokseen

Tietokoneen käyttäjä on yhteydessä useisiin elementteihin ennen kuin käyttäytyminen muuttuu. Malli havainnollistaa nämä elementit sekä sen, millainen interaktio vaaditaan siihen, että elementit aiheuttavat muutosta. Mallissa myös määritellään yhteydet elementtien välillä: miksi elementit ovat yhteydessä keskenään.

Malli, joka kuvaa käyttäytymisen muutosta, pystyy kuvaamaan, kuinka tietoturvaan liittyvä kokemus aiheuttaa käyttäytymisen muutoksen. Kokemus koostuu elementeistä (esimerkiksi uhka, omaisuus, tietoverkko) ja interaktiosta elementtien välillä (esimerkiksi omistaminen, tietoturva-asioista tiedottaminen tai neuvominen, tietoturvauhkan kokeminen jne). Teoreettinen ymmärrys tässä tutkimuksessa perustuu siis henkilöiden kokemukseen ja merkityksiin, jotka he antavat näille kokemuksille (ks. myös Sarker et al, 2001). Kokemus aiheuttaa käyttäytymisen taustalla olevien uskomusten ja ajatusten muutoksen. Ihmisen kokemus ja kognitio muodostavat tietoturvakäyttäytymistä kuvaavan mallin ytimen, eli kokemus on tavallaan mallin kokoava elementti, johon muut elementit yhdistyvät. Myös käyttäytymisen muutosta kuvaavassa prosessiteoriassa (luku 6.3.) kokemus on yhdistävä ominaisuus, joka toistuu teorian kaikilla tasoilla. Eli tietokoneen käyttäjän kokemus muuttuu kun hän käy läpi tietyt prosessin tasot.

Yksi tässä tutkimuksessa kehitettyjen mallien hyöty on se, että ne kuvaavat myös käyttötarkoituksen eli kontekstin, johon tietoturvasuojaustoimenpide liittyy ja jossa käyttäytyminen muuttuu: käytetäänkö tietokonetta esimerkiksi liiketoiminnan edistämiseen, kommunikointiin, tiedon etsimiseen vai dokumenttien tallentamiseen. Näin tutkimuksessa kehitetyt mallit ja teoria sidotaan kontekstiin.

Seuraavassa luvussa esitetään 6 erilaista prosessia siitä, kuinka tietoturvakäyttäytyminen muuttuu. Jokaisesta tutkimuksessa käsitellystä käyttäytymistyypistä on laadittu oma prosessi. Yhdistetty prosessi luvussa 6.3.8. kokoaa yksittäisten mallien erityspiirteet yhteen.

6.3 Prosessiteoria tietoturvakäyttäytymisen muutoksesta

Tässä luvussa esitetään 6 vaihtoehtoista prosessia, jotka johtavat tietoturvakäyttäytymisen muutokseen (ks. myös liitteet 10 - 15). Tutkimuksen tarkoitus on esittää useita vaihtoehtoisia tapahtumakulkuja ja osoittaa, että ihmisten käyttäytyminen muuttuu erilaisten interaktioiden ja prosessien seurauksena. Kaikki yksittäiset prosessit muistuttavat toisiaan siinä mielessä, että kaikista prosesseista on löydettävissä tietokoneenkäyttö normaalitilassa-taso, epävarmuuden taso ja suojaustoimenpiteen käyttöönoton taso. Poikkeaminen omaksutusta tietoturvatoimenpiteestä löytyy kaikista muista prosesseista paitsi Internet-profiilin hallinta-prosessissa. Luvut 6.3.1. – 6.3.6. täsmentävät kunkin yksittäisen prosessin erityspiirteet.

Yhdistetty prosessi (luku 6.3.7.) kuvaa tietoturvakäyttäytymisen muutosta yleisemmällä tasolla ja kertoo käyttäytymisen muutoksesta siten vähän enem-

män kuin yksittäiset prosessit. Siihen on yhdistetty 6 alatason prosessia. Yhdistettyyn prosessiin on lisätty mukaan tarve/motiivipsykologia eli ne motiivit (tarpeet ja tunteet) jotka ohjaavat tietokoneen käyttäjien käyttäytymistä kullakin tasolla. Prosessiteoriaa on kehitetty vaiheittain: yksittäiset mallit on laadittu hahmottamaan pelkistetysti sen, kuinka yksittäiset prosessit etenevät. Yhdistettyyn malliin on pyritty lisäämään selittäviä elementtejä, jotka mahdollistavat prosessin nostamisen korkeammalle tasolle.

6.3.1 Internet-profiiilin hallinta

Internet-profiilin hallinta tarkoittaa niitä keinoja, joilla tietokoneenkäyttäjä pyrkii hallinnoimaan sitä, mitä hänestä on näkyvillä Internetissä. Hän harkitsee, mitä Internetissä julkaisee ja tarkistaa hakukoneiden avulla, onko tietoja päätynyt julkisesti saataville tai ei-toivotuille sivuille. Tässä käyttäytymistyypissä tietokoneen käyttäjä käyttää tietokonetta kommunikointiin esimerkiksi ystäviensä, opiskelukavereidensa ja liiketuttaviensa kanssa, oman työn markkinointiin, uusien asioiden opetteluun ja viihtymiseen. Tietokoneen käyttötarve on liittymistarve ja toimeentulon tarve (Alderfer), Maslowin hierarkiassa yhteenkuuluvuuden tarve ja tietämisen ja itsensä toteuttamisen tarve. Myös uteliaisuuden tarve (Reiss) selittää käyttäytymistä esimerkiksi siinä tapauksessa, että henkilö seuraa twitterissä mielenkiintoisia hahmoja.

Turvallisuuden tarve tarkoittaa tässä esimerkissä tarvetta yksityisyyden suojaamiseen Internetissä, eli omaisuus, jota suojataan, ovat yksityiset tiedot. Henkilö ei halua jakaa yksityiselämäänsä liittyviä tietoja Internetissä julkisesti:

> *K: No kun sää aloit miettimään näitä asioita näitä tietoturva-asioita niin oliko sualla joitakin ystäviä tai luitko jostain tai millä perusteilla sää lähit näitä edistämään, vai oliko se vaan sun omaa päättelyä sitten?*
> *V: No ehkä just siitä lähtökohdasta että kun aikasemmin ei oo sillä lailla mitään jakanu, ei oo ollu mitenkään julkisesti tai puolijulkisesti esillä niin en mä ainakaan halunnu sitten millään tapaa levittää ihan kaiken kansan luettavaksi ainakaan.*

Prosessissa korostuu se, että tietoturvakäyttäytymisen muutos on jatkuvaa, eli tietokoneen käyttäjä tarkistaa ajoittain hakukoneiden avulla, mitä hänestä on näkyvillä Internetissä ja tiukentaa sosiaalisen median asetuksia näiden tarkistusten pohjalta:

> *K: Voitko kuvata jonku tilanteen, kun sää oot sitte vielä tiukentanu entisestään? Mikä tilanne on saanu?*
> *V: Varmaan se, ku kerran tarkastin siinä ne omat tiedot ja sit huomasin, et mul on kaikki... Saa sen avattua sen mun palkin, kaikis luki julkinen. Sit mää sillon muun muassa kans googletin itteni, katoin, nii jumaliste, kaikkihan täällä näkyy.*

Tämä prosessi osoittaa, että käyttäytymisen muutoksen liikkeellepanija ei tarvitse olla tietoturvaongelma, vaan prosessin voi saada liikkeelle myös se että

ottaessaan uuden palvelun (esim. sosiaalinen media) käyttöön tietokoneen käyttäjä alkaa pohtia, mitä tämän palvelun käyttö merkitsee hänen yksityisyytensä kannalta.

Tässä prosessissa korostuu suojaustoimenpiteen eli oman profiilin hallinnan haasteellisuus. Ongelmat yksityisyysasetusten käyttöönotossa sosiaalisessa mediassa tai kuvanjakopalvelussa koetaan hidastavaksi tekijäksi, ja siinä tapauksessa että asetuksia ei osata laittaa kuntoon, sensitiivistä aineistoa voi päätyä julkisesti saataville. Henkilö voi epähuomiossa esimerkiksi laittaa sosiaaliseen mediaan liian laajan kaveripiirin. Toisaalta oman profiilin hallintaa helpottaa se, että henkilö oppii käyttämään kuvahakua omien tietojen etsimiseen Internetissä.

Prosessin erityispiirre on, että oman profiilin hallintaa toteutetaan selkeästi 2 vaiheessa. Aluksi määritellään sosiaalisen median yksityisyysasetukset ja pohditaan yleisesti mitä Internetiin kannattaa/ ei kannata laittaa (tasot 2 ja 3). Toiseen vaiheen muodostaa se, kun henkilö kokee tärkeäksi olla selvillä siitä, mitä hänestä on näkyvillä Internetissä ja omia tietoja aletaan etsiä Internetissä hakukoneiden avulla (tasot 4 ja 5).

6.3.2 Sensitiivisen aineiston prosessointi Internetissä

Tietokoneen käyttäjä käyttää sosiaalista mediaa, sähköpostia ja pikaviestipalveluita kommunikointiin ystäviensä kanssa, sähköpostia myös asiointiin esimerkiksi koulun, virastojen tai työnantajien kanssa. Hänellä on liittymistarve (Alderfer), Maslow:n hierarkiassa yhteenkuuluvuuden tarve. Sähköpostin käyttöä motivoi myös tietämisen tarve (Maslow) esimerkiksi siinä tapauksessa, että henkilö saa tietoa harrastuksiin liittyvistä asioista sähköpostin välityksellä sekä itsensä toteuttamisen tarve, koska ystävien kanssa viestittely on hauskaa ajanvietettä. Sähköpostitse hoidetaan esimerkiksi pankkiasioita, joten sen käyttöä motivoi asioinnin tarve. Ajan ja vaivan säästäminen selittää myös käyttäytymistä sillä sähköposti ja some-palvelut ovat nopeita ja käteviä käyttää

Tietoturvaongelma, tietoisuuden lisääntyminen tai sosiaalisen median käytön aloitus ja siihen liittyvä tiedon lisääntyminen aiheuttavat sen, että henkilö alkaa kyseenalaistaa sensitiivisen aineiston lähettämisen sähköpostissa ja sosiaalisessa mediassa.

Turvallisuuden tarve tarkoittaa tässä esimerkissä sitä, että henkilöllä on tarve suojata omaisuuttaan kuten esimerkiksi tilinumeroa, rahaa, identiteettiä, ihmissuhteisiin liittyvää tietoa, potilastietoja, henkilötunnuksia, verkkokauppaan liittyviä tietoja, yhteystietoja kuten puhelinnumero tai osoite:

> *I: When we are talking about email, do you think about the security issues when you send email? How do.. you take into account the security, when you are sending mails?*
> *R: I rarely, don't send my.. henkilötunnus?*
> *I: Personal ID or.. ID number..*
> *R: ID number.. in email and.. if I.. have bought something online, it has to be so that it's trustable, when I'm sending email about my.. orders and stuff.*

I: How have you come this kind of behavior that you don't send sensitive via email+
R: I have heard that they could be stolen.
I: How have you heard?
R: I've read from the internet and.. we have this.. security lectures at school, that you can never use any patient information in your personal email and..

Tietokoneen käyttäjä voi suojaustoimenpiteen omaksuttuaan luopua siitä kokonaan. Alussa kun sosiaalisen median käyttö on uutta, tietokoneen käyttäjä miettii, mitä sinne kirjoittaa mutta ajan kuluessa tämä pohdinta vähenee. Tämän pysyvän muutoksen lisäksi käyttäytyminen voi poiketa myös väliaikaisesti eli henkilö esimerkiksi vahingossa lähettää arkaluontoisen viestin sähköpostilla.

Poikkeamista omaksutusta tietoturvatoimenpiteestä selittää liittymistarve (Alderfer), Maslowilla yhteenkuuluvuuden tarve ja ajan ja vaivan säästämisen tarve sekä asioinnin tarve. Kun henkilö väliaikaisesti lähettää sensitiivistä tietoa sähköpostissa, tämä perustuu asioinnin tarpeeseen: henkilön täytyy saada toimitettua jokin asia esimerkiksi verkkokaupan kanssa eikä hän löydä vaihtoehtoista tapaa toimittaa tätä asiaa. Se miksi tietokoneen käyttäjä ei mieti enää minkälaista tietoa välittää sähköpostissa / sosiaalisessa mediassa selittyy liittymisen tarpeella (Alderfer) ja sillä, että kokemus uhkasta vähenee ajan kuluessa. Henkilö kokee tärkeäksi olla yhteydessä ystäviin, mutta ei halua rajoittaa kommunikointia miettimällä tietoturva-asioita.

Riippumattomuuden tarve (Reiss) selittää poikkeamista siinä tapauksessa, että henkilö ajattelee, ettei voi koskaan miellyttää kaikkia, joten ei myöskään pohdi enää niin paljon mitä julkaisee Internetissä.

Tämän prosessin erityispiirre on myös se, että se ei sisällä esteitä eikä hidasteita tietoturvasuojauksen käyttöönotolle. Muissa prosesseissa esiintyy joko esteitä, edistäjiä tai molempia.

6.3.3 Vahvan salasanan laatiminen

Tietokoneen käyttäjä käyttää tietokonetta kommunikointiin ystäviensä ja sukulaistensa kanssa esimerkiksi sähköpostin tai sosiaalisen median kautta sekä verkkopankkiasiointiin ja asioiden hoitamiseen esimerkiksi työnantajien kanssa. Tietokoneen käyttötarpeet ovat asioinnin tarve, liittymisen tarve (Alderfer), Maslow:lla yhteenkuuluvuuden tarve. Tutkimisen, tietämisen ja ymmärtämisen tarve korostuu silloin jos tietokoneenkäyttäjä on työnantajiin ja kouluun yhteydessä opiskeluun liittyvissä asioissa. Myös esteettisyyden tarve korostuu jos sähköpostin välityksellä jaetaan kuvia, esimerkiksi puutarhavinkkejä. Sosiaalisessa mediassa on erilaisia harrastuksiin liittyviä ryhmiä, joten sosiaalisen median käyttöä selittää myös itsensä toteuttamisen tarve.

K: Tota, sitte jos mietitään sitä tarvetta, mikä näitten käyttötarkotusten taustalla on, niin ku sää oot siellä sosiaalisessa mediassa, nii mihinkähän tarpeeseen tai mikä motiivi siinä taustalla on, että miksi sää käytät näitä palveluita?

V: No periaatteessa en käytä mitään muuta ku Facebookia, että ei oo mitään Instagramia eikä mitää muuta, Twitteriä tai semmosta. Että käytän siihen, että pidän – no, ku on kaukasia sukulaisia, heihin yhteyttä.
K: Yhteydenpito.
V: Joo, yhteydenpito. Ja onhan siellä paljo myös semmosia erilaisia ryhmiä, joissa on mukava myös keskustella ihmisten kanssa eri aiheista, asioista ja harrastuksista. Nii seki on tosi mukavaa.

--

K: Joo, mutta voiskohan siinä tulla kysymykseen tämmönen tiedonhankkimisen tarve sitte?
V: Joo, kyllä seki, että sieltä löytää ja oppii uusia juttuja.

Tässä prosessissa henkilöllä voi jo prosessin alussa olla käytössään vahva salasana mutta sitä tulee tarve vahvistaa ajan kuluessa. Salasanan vahvistaminen voi tapahtua vähitellen.

Turvallisuuden tarve tarkoittaa tässä esimerkissä sitä, että tietokoneen käyttäjä haluaa suojata omaisuuttaan kuten rahaa verkkopankissa ja kriittistä informaatiota sähköpostissa, esimerkiksi henkilökohtaisia viestejä ja ostokuitteja ja henkilöhistoriaa käyttämällä vahvaa salasanaa:

K: Mikä sai sut sitte laatimaan tämän tosi vahvan salasanan siihen (-) [0:09:44 pp]?
V: Ihan vaan se että ku mä en halusin et se yhen tietyn paikan salasana on mahdollisimman vahva että sitä ei pystyis ainakaan brute forcella breikkaamaan ja et se ei olis sama ku missään muualla. Et se on kuitenkin sen semmonen sähköposti on semmonen mihin tulee kaikki mun ostokuitit, paljon sellasta henkilökohtasta sähköpostia niin se on ehkä semmonen minkä mä haluan pitää mahdollisimman vahvana.
K: No saitko sä jostain tietoa tähän vai päättelitkö sinä vaan ite että ku tämä on niin arkaluontosta tietoa niin mä haluan suojata tämän vai..
V: No varmaan..
K: ..luitko jostain tai?
V: Mie luulen et se on ehkä tässä viimesen kymmenen vuo-, koko ajanhan siitä on ollu puhetta siitä että piä salasanasi mahdollisimman hyvänä ja näin. Et ehkä se on vaan silleen et okei no tää on semmonen minkä mä haluan pitää mahdollisimman hyvänä. Ei se silleen myötäsyntysesti oo tullu. Kyllä mä muistan et jossakin varmaan joskus 2000-luvun alkupuolella oon siirtyny siihen että okei että tää on nyt semmonen. Varmaan sillon kun mä aloin Google mailia käyttään että sitte okei haluan tänne kaikki mun tärkeet sähköpostit niin sillon mä aloin käyttään siinä tosi tiukkaa salasanaa.

Tasolta 3 on mahdollista palata takaisinpäin, jos henkilö kokee, että salasanaa on aihetta vahvistaa vielä entisestään. Tasolta 4 paluu mahdollistuu esimerkiksi silloin, kun on kirjauduttu johonkin palveluun heikolla salasanalla ja palataan takaisin käyttämään vahvaa salasanaa esimerkiksi sähköpostiin, jossa on työhön liittyvää tärkeää tietoa.

Prosessissa korostuu ulkopuolisten edistäjien merkitys: esimerkiksi pankin järjestelmä ohjaa vahvan salasanan laatimisessa ja erilaiset verkkopalvelut muistuttavat vahvoista salasanoista, jotkut jopa pakottavat laatimaan vahvan salasanan jotta palvelua pääsee käyttämään, Internetistä löytyy myös ohjeita vahvan salasanan laatimiseen.

Tämän prosessin erottaa muista prosesseista se, että siinä on suora yhteys tasolta 1 tasolle 3, eli siinä tapauksessa, että järjestelmä edellyttää vahvan salasanan laatimista, jotta sitä pystyy käyttämään, tietokoneen käyttäjä laatii vahvan salasanan. Hän ei siis päädy epävarmuuden tasolle (taso 2) pohtimaan kokemuksen merkitystä oman tietoturvansa näkökulmasta. Vaihtaessaan salasanan hän ei välttämättä pohdi tietoturva-asioita lainkaan vaan ainoastaan sitä, että pääsee jatkossakin käyttämään järjestelmää.

Vahvan salasanan laatiminen edellyttää tietokoneen käyttäjältä enemmän muistamista kuin muut suojaustoimenpiteet, joita tässä tutkimuksessa tarkastellaan. Tämä on nähtävissä myös prosessissa: esteeksi suojaustoimenpiteen käyttöönotolle muodostuu se että vahvoja salasanoja on hankala muistaa. Vahvan salasanan laatiminen edellyttää tiettyä vaivannäköä, ja oma saamattomuus aiheuttaa sen, että vahvaa salasanan laatiminen lykkääntyy. Toisaalta, jotkut käyttäjät antavat selaimen tallettaa salasanansa, joten niitä ei tarvitse käyttäjän itse muistaa.

Poikkeamista omaksutusta tietoturvakäyttäytymisestä selittää liittymisen tarve (Alderfer), Maslowilla yhteenkuuluvuuden tarve sekä ajan ja vaivan säästämisen tarve. Henkilö esimerkiksi kokee tärkeäksi kommunikoida netissä ystävien kanssa mutta ei koe tarpeelliseksi laatia vahvaa salasanaa kaikkiin netin palveluihin. Tämä helpottaa ja nopeuttaa kirjautumista:

> *K: Mutta tarkennan, että ei oo mitään väliä, niin millä tavalla? Että mikä sua motivoi käyttäytymään sillä tavalla?*
>
> *V: No esimerkiks sitte, jos se on vaikka helppo muistaa tai jotaki tai että jos on joku semmonen, et jonne pitää vaikka vaan rekisteröityä ja sitten jos sitä käyttää vaan yhesti, niin se on tavallaan vaan semmonen ns. kertakäyttöinen profiili. Ehkä.*
>
> *K: Joo elikkä haluaks sää säästää siinä aikaa ja vaivaa?*
>
> *V: Joo.*

6.3.4 Varmuuskopiointi

Tässä prosessissa tietokoneen käyttäjä käyttää tietokonetta liiketoiminnan kehittämiseen, työntekoon (freelancer) opiskeluun ja kuvien, kaunokirjallisten tekstien, muistiinpanojen ja musiikin tallentamiseen sekä yhdistystoimintaan. Tietoja tallennetaan myös silloin, jos löydetään jokin idea tms. myöhemmin hyödynnettäväksi. Liiketoiminnan kehittämistä selittää toimeentulon tarve (Alderfer). Kuvien, musiikin ja videoiden tallentamista selittää esteettisyyden tarve (Maslow; Reiss). Henkilö esimerkiksi haluaa käydä läpi tunteita, muistoja ja

kokemuksia. Tietokoneen käyttö opiskelutarkoituksessa, sukuhistorian tallentamisessa sekä ideoiden tallettaminen pohjautuu tietämisen ja ymmärtämisen tarpeeseen (Maslow, 1954), ja yhdistystoiminta ja valokuvien sekä musiikin tallentaminen itsensä toteuttamisen tarpeelle. Muistiinpanojen tallentamista selittää ajan ja vaivan säästämisen tarve, samoin kuin opiskeludokumenttien tallentamista pilveen (tällöin useat opiskelijat voivat muokata dokumenttia samanaikaisesti ja usealta laitteelta). Työhön liittyvien dokumenttien tallentamista selittää toimeentulon tarve (Alderfer) ja valokuvien tallentamista myös liittymisen tarve koska valokuvia halutaan jakaa ja näyttää lähipiirille.

Turvallisuuden tarve tarkoittaa tässä käyttäytymistyypissä tarvetta suojata omaisuutta kuten liiketoiminta-asiakirjoja, opiskeluun ja työhön liittyviä asiakirjoja ja kuvia tuhoutumiselta tai häviämiseltä ottamalla niistä varmuuskopioita:

> *I: So you started to take backups, after you had this kind of.. crash?*
> *R: Yes.*
> *I: You didn't take backups at all before that?*
> *R: No. But hopefully I had a friend who's, I don't know, (he do) many things with this kind, also have been study here in, maybe on this tietotekniikka I don't know, so he had some kind of program, what could find the pictures and put them back, to me. But it was not, it take very long time.*

Poikkeustilanteita selittää esimerkiksi vahinko ja unohdus. Varmuuskopiointi voi epäonnistua vahingossa, ja tietokoneenkäyttäjä voi lisäksi unohtaa varmuuskopioinnin vaikka onkin omaksunut tämän toimintatavan.

Välinpitämättömyys selittää käyttäytymistä poikkeustilanteissa silloin, jos tietokoneenkäyttäjä kokee että tekeillä oleva työ ei ole tärkeä. Samoin, joskus jos työ on keskeneräinen, siitä ei oteta varmuuskopioita.

Jotkut tietokoneenkäyttäjät tekevät varmuuskopioita sähköpostiin. Siinä tapauksessa että he lähettävät dokumentin jollekulle toiselle, jolta on vastaus odotettavissa viestiin, he eivät ota muita varmuuskopioita

Tämän prosessin erityispiirre on se, että se ei sisällä tietoturvasuojauksen omaksumista hidastavia tekijöitä. Haastateltavat kertoivat varmuuskopioinnin ja varmuuskopiointiohjelmistojen (esim. pilvipalvelut) käytön olevan pääasiassa helppoa. Muista prosesseista tämä poikkeaa myös siten, että käyttäytymisen muutoksen eli varmuuskopioinnin käytön saa alkamaan se, että henkilölle tulee enemmän henkilökohtaisempaa suojattavaa, esimerkiksi isompia opiskeludokumentteja. Tämä ei korostunut muissa prosesseissa.

Lisäksi, tämä prosessi on suoraviivaisin kaikista siinä mielessä, että siinä ei ole paluuta tasolta 3 tasolle 2 eli suojaustoimen vahvistaminen esimerkiksi jonkun tietoturvaongelman seurauksena ei korostunut. Tästä voidaan päätellä, että tietokoneen käyttäjät ovat varmuuskopioinnin omaksumisen jälkeen siihen tyytyväisiä, joten sitä ei ole tarvetta vahvistaa. Toisin kuin muissa prosesseissa, tässä prosessissa esiintyy suojaustoimi-elementti tasolla 1 mikä tarkoittaa sitä, että henkilöllä on käytössään virustorjuntaohjelma, jonka hän uskoo estävän

tietojen katoamisen koneelta. Tämän vuoksi hän ei koe tarvitsevansa varmuuskopiointia.

6.3.5 Varovaisuus verkkokaupassa

Verkkokaupan käyttö pohjautuu itsensä toteuttamisen tarpeeseen (Maslow), Alderferin ERG- teoriassa henkilökohtaisen kasvun tarpeeseen. Verkkokaupasta tilataan mm. musiikkia, pelejä, matkoja, vaatteita, elektroniikkaa, ja vuokrataan hotellihuoneita sekä loma-asuntoja. Verkkokaupan käyttöä selittää myös ajan ja vaivan säästämisen tarve. Verkkokauppa on nopea ja helppo tapa hankkia esim. musiikkia puhelimeen. Uteliaisuuden tarve (Reiss) selittää myös käyttäytymistä, sillä tietokoneen käyttäjät seuraavat verkkokaupasta mitä uutuuksia on saatavilla. Laajemmasta valikoimasta voi valita juuri itselle sopivan tuotteen. Pelaamista selittävät myös liittymisen tarve (Alderfer) ja Maslowin luokittelussa sosiaalisen arvostuksen motiivit. Pelaaminen selittyy myös tarpeella sosiaalisiin yhteyksiin (Social contact) ja hyväksyntään (acceptance) (Reiss).

Turvallisuuden tarve tarkoittaa tässä tapauksessa tarvetta suojata omaisuutta kuten rahaa ja luottokorttitietoja noudattamalla varovaisuutta verkkokauppa-asioinnissa esimerkiksi välttämällä epäluotettavia/ pieniä ulkomaisia verkkokauppoja tai luottokortin käyttöä verkkokauppa-asioinnissa:

> *K: No vaikuttiko tämä sitte tämä ongelma että se sun ystävä menetti niitä rahoja niin vaikuttiko se sinun käyttäytymiseen sitte?*
> *V: Joo. Tietenki nyt et en osta ulkomaalaisista sitte, mä oon huomannu kans ite ku jäi se iTunesista se, jäi vahingossa vaan. Tai siis mä olin sulkenu sen, tai siis mä olin..*
> *K: Siis kerropa vielä tarkemmin, siis se iTunesista voi..*
> *V: iTunesista voi..*
> *K: ..ladata musiikkia.*
> *V: Nii musiikkia ja mä olin sitte pannu semmosen, kuukausi, mä olin kyllä sulkenu sen mut sieltä vaan tuli ja sitte mä en ollu muka sulkenu sitä.*
> *K: Elikä sulla oli joku lataus koko ajan siinä päällä?*
> *V: Niin, mulla tuli automaattisesti, luottokortilta vähenty mutta mä en oo nyt tilannu noista ulkomaalaisilta sivustoilta ku joskus matkoja vaan, että mä oon sillä lailla..*

Tämän prosessin erityispiirre on se, että verkkokaupan käytön rajoittaminen on vähittäinen prosessi, eli negatiiviset kokemukset verkkokaupan käytöstä aiheuttavat sen rajoittamista ja tulevaisuudessa verkkokaupan käyttö voidaan jopa kokonaan lopettaa. Tämä on vaihtoehtoisista prosesseista ainoa, jossa tietokoneen käyttö tietyssä käyttötarkoituksessa ollaan valmiita lopettamaan siinä tapauksessa että kohdataan vakavia tietoturvaongelmia.

Toisaalta, luottamus verkkokauppaan voi ajan myötä lisääntyä, ja tietokoneen käyttäjä vähentää verkkokauppaan liittyviä rajoituksia. Kun verkkokauppa yleistyy, luottamus sitä kohtaan lisääntyy pysyvästi, mikä saa tietokoneen käyttäjän vähentämään siihen liittyviä rajoituksia. Jos hän on aiemmin vaatinut

ostoksistaan paperilaskun, hän luopuu tästä kokonaan ja alkaa maksamaan ostokset sähköisesti. Tässä tapauksessa muodostuu ristiriita itsensä toteuttamisen tarpeen ja suojaamistarpeiden välille.

6.3.6 Virustorjunta

Tietokoneen käyttäjä käyttää tietokonetta tiedonhakuun Internetistä. Tiedonhaku perustuu uteliaisuuden tarpeeseen (Reiss), tutkimisen, tietämisen ja ymmärtämisen, itsensä toteuttamisen tarpeeseen (Maslow), henkilökohtaisen kasvun tarpeeseen (Alderfer) liittymisen tarpeeseen (Alderfer) sekä esteettisyyden tarpeeseen (Maslow; Reiss). Internetistä etsitään esimerkiksi tietokoneenkorjausohjeita, taideteoksia tai harrastuksiin liittyvää tietoa, vaikkapa treeni- ja harjoitteluohjeita

> *K. No tota, sitte sää surffaat jonkin verran netissä, nii miks sää käytät tietokonetta tähän tarkotukseen?*
> *V: No just uutisia tulee aina ehkä kerran viikossa katottua, tietää vähäse missä mennään. Mutta ei niinkään paljon. Just se Googlesta se tiedonhankkinnan, jos tulee jotain kysymyksiä, saattaa olla ihan mitä tahansa, että kartasta ettiä mihin mennä, jos pitää löytää reitti johonki, nii se on aika yleinen. Ja säätä joskus katsoo, jopa ku lähtee reissuun, tämmöstä normaalia, pientä selailua.*
> *K: Tiedon hankintaa.*
> *V: Joo tiedon hankintaa.*
> *K: Mää mietin, oisko se semmone uteliaisuuden tarve myös vai onko se iha..?*
> *V: Se on iha uteliaisuus, jos vaikka joku sanoo että "hei ookko kuullu tästä?"*

Turvallisuuden tarve viittaa tässä yhteydessä tarpeeseen suojata omaisuutta kuten tietokonetta ja sinne talletettuja tietoja (salasanat ja pankkitunnukset) sekä omaa yksityisyyttä käyttämällä virustorjuntaohjelmaa:

> *K: Voisitko tarkentaa, että ennen kuin otit spybotin käyttöön, mietitkö sitä että mitä saavutat oman tietoturvasi kannalta kun käytät tätä ohjelmistoa? Miksi se oli tärkeää että virukset ja haittaohjelmat eivät pääse läpi, esimerkiksi millaista vahinkoa ne olisivat voineet aiheuttaa?*
> *V: Kone hidastui, koneen aukaistessani selain aukesi ja siihen tuli ihan outo aloitussivu, jota ei saanut pois edes selainta uudelleen asentamalla, käynnistysongelmia, popup-ikkunoita tuli. Näitä siis ihan käytännössä. Sen lisäksi haittaohjelmat saattaa kopioida salasanoja sähköpostiin ja pankkitunnuksia kaapata, kerran multa gmail varottikin että joku Nigeriasta käyttänyt mun sähköpostitiliä ja lähettäny sähköpostiakin mun nimissä.*

Virustorjunnan käyttöä edistää se, jos ohjelmisto on helppo asentaa ja käyttää. Lisäksi, jos ohjeet ovat suomenkielisiä, niitä on helpompi ymmärtää. Toisaalta, esteeksi tässä prosessissa voi muodostua tietokoneen ikä, joka ei mahdollista modernin virustorjuntaohjelman asentamista. Tietokoneen käyttäjällä voi myös olla puutteelliset taidot virustorjuntaohjelmien etsimiseen Internetistä ja asennusohjeiden ymmärtämiseen, mikä hankaloittaa virustorjuntaohjelmien käyt-

töönottoa. Jos virustorjuntaohjelma on maksullinen, sitä ei oteta käyttöön, koska saatavilla on monia ilmaisiakin ohjelmia. Joskus tietokoneenkäyttäjä voi epäillä virustorjunnan tehokkuutta.

Tässä prosessissa korostuu muita prosesseja enemmän virustorjunnan tiheä muutostahti, jota prosessi pyrkii kuvaamaan. Tasolta 3 palataan siis toistuvasti takaisin tasolle 2, koska uudet tietoturvaongelmat (esimerkiksi virustorjunnan tehottomuus) motivoivat vaihtamaan virustorjuntaohjelmaa. Tietoturvaongelma herättää epävarmuuden tunteen, jonka tietokoneenkäyttäjä haluaa poistaa: esimerkiksi entinen virustorjuntaohjelma ei pysty poistamaan virusta eikä estä kaikkia tietoverkon välityksellä koneelle tulevia haittaohjelmia.

Virustorjunnan vaihtamiseen motivoi myös teknologinen kehitys. Ystävä voi esimerkiksi suositella uutta parempaa virustorjuntaohjelmaa. Jos entisen maksullisen virustorjuntaohjelman tilalle otetaan ilmaisohjelma, käyttäytymistä selittää lisäksi säästämisen tarve samoin kuin silloin jos vapaan version uudelleen lataaminen ei onnistu ja etsitään tilalle toinen vapaa versio. Virustorjuntaohjelma saattaa haitata tietokoneen käyttötarkoitusta eli www-selausta. Se voi blokata liikaa tai sen mainokset/ lisäominaisuudet/ virheilmoitukset alkavat ärsyttää. Tällöin turvallisuuden tarpeen lisäksi käyttäytymistä motivoi tietokoneen käyttötarve (tutkimisen ja tietämisen tarve), mikä aiheuttaa käyttäytymisen muutoksen ja tietokoneenkäyttäjä vaihtaa virustorjuntaohjelman toiseen.

Virustorjuntaa kuvaavassa prosessissa korostui muita prosesseja enemmän se, kuinka vakavasti tietokoneen käyttäjät suhtautuvat virusten aiheuttamaan uhkaan ja koneen ja tietojen suojaaminen viruksilta, haittaohjelmilta jne. Virustorjunnan laiminlyöntiä esiintyi vain hyvin harvoissa tapauksissa. Kun tietokoneen käyttäjä käyttää tietokonetta ohjelmistojen testaamiseen, virustorjunta otetaan sen takia hetkellisesti pois päältä. Tällöin tutkimisen ja tietämisen tarve selittää käyttäytymistä ja muodostuu ristiriita em. tarpeen ja turvallisuuden tarpeen välille. Toisaalta, myös turvallisuuden tarve selittää käyttäytymistä siinä mielessä, että virustorjunta otetaan pois päältä hallitusti ja se on pois päältä minimiajan. Virustorjunnan tärkeänä pitämisestä kertoo myös se, että haastateltavat varoittelivat ottamasta virustorjuntaa pois päältä. Jos näin kuitenkin tehdään, täytyy olla ole varma teknisistä taidoistaan.

Johtopäätöksenä voidaan todeta, että kaikille yksittäisille prosesseille löytyi omat erityispiirteensä, jotka erottavat ne muista prosesseista. Tietoturvakäyttäytymisen muutos näyttäisi siis tulosten mukaan tapahtuvan hieman eri tavalla eri käyttäytymistyypeissää. Eroja prosessien välillä oli esimerkiksi tietoturvasuojaustoimenpien käyttöönottoa estävien/hidastavien ja edistävien asioiden suhteen. Esteet ja hidastajat olivat erilaisia eri käyttäytymistyypeissä. Esimerkiksi virustorjunnan käyttöönottoa edistää sen helppo käyttö ja estää ohjelmiston maksullisuus. Vahva salasana-prosessissa hidastavana tekijänä koetaan laiskuus eli vahvan salasanan koetaan vaativa liikaa vaivannäköä. Edistäväksi tekijäksi koetaan se, että Internetissä on saatavilla ohjeita hyvän salasanan laatimiseen.

Yleensä käyttäytymistyypeissä oli joko esteitä tai hidastajia tai molempia mutta esimerkiksi sensitiivisen aineiston prosessointi-käyttäytymistyyppi ei sisällä esteitä eikä hidastajia.

Prosessit eroavat myös siinä mielessä toisistaan, että suojaustoimenpiteen laiminlyönti voi olla joko väliaikaista tai pysyvää. Esimerkiksi sensitiivisen aineiston prosessointi - käyttäytymistyypissä laiminlyönti voi olla pysyvää, eli henkilö vähitellen lakkaa pohtimasta, mitä Internetiin voi/kannattaa kirjoittaa. Virustorjunnan käytössä laiminlyönti on aina väliaikaista, eli virustorjunta otetaan päältä vain hetkellisesti ja harkitusti. Tämä toisaalta kertoo vakavasta suhtautumisesta virustorjuntaa kohtaan: virustorjuntaohjelman käyttö koetaan tärkeäksi suojaustoimenpiteeksi.

Käyttäytymisen muutosnopeudessa voidaan havaita eroja prosessien välillä. Erityisesti virustorjunnan kohdalla muutostahti on korostetun nopeaa verrattuna muihin. Virustorjuntaa päivitetään/vaihdetaan lyhyelläkin aikavälillä eri syistä: vaihdetaan ilmaisesta toiseen ilmaiseen ohjelmaan, halutaan teknisesti toimivampi ohjelmisto, halutaan tehokkaampi ohjelmisto jne.

Prosessin pituudessa voidaan myös havaita eroja. Erityisesti Internet-profiilin hallinta-prosessi on pidempi kuin muut, sillä se on tavallaan 2-osainen sisältäen sosiaalisen median yksityisyysasetusten määrittämisen ja omien tietojen etsimisen Internetistä.

Kolmessa prosessissa tuli ilmi, että prosessi voi pysähtyä eikä etene kohti lopputulosta eli suojaustoimenpiteen käyttöönottoa. Vahvan salasanan laatiminen, Internet-profiilin hallinta ja verkkokauppa prosessi voivat pysähtyä kesken. Yhteistä etenemisen pysähtymiselle on se, että henkilö ei koe jostain syystä tärkeäksi edistää tietoturvaansa. Vaikka henkilö saa tietoa vahvojen salasanojen merkityksestä, hän ei silti halua vaihtaa salasanaansa vahvemmaksi. Sähköpostin hakkerointia ei pidetä niin vakavana ongelmana, että sen takia kannattaisi vaihtaa salasana. Oma salasana voi olla myös niin hauska, ettei sitä ei haluta muuttaa. Toisaalta ongelmia verkkokaupassa ei ehkä pidetä niin vakavina että niiden takia kannattaisi rajoittaa verkkokaupan käyttöä.

Prosesseja vertailtessa mielenkiintoinen havainto oli myös se, että aina henkilö ei välttämättä päädy epävarmuuden tasolle, sillä esimerkiksi vahva salasana-prosessissa ainoa syy salasanan vaihtamiseen voi olla se, että järjestelmä vaatii vahvaa salasanaa, jotta sitä pääsee käyttämään. Tällöin henkilö siirtyy suoraan tasolta 1 tasolle 3 eikä pohdi välttämättä vahvan salasanan merkitystä oman tietoturvansa kannalta. Henkilön käyttäytymisessä korostuu tietokoneenkäyttötarve turvallisuuden tarpeen sijasta.

Prosessien välillä ilmeni myös eroja turvallisuuden tarpeessa. Turvallisuuden tarve, eli tarve suojata omaisuutta tasolla 3 tarkoittaa eri prosesseissa hieman eri asioita. Esimerkiksi virustorjunnassa korostuu tarve suojata tietokonetta ja sinne talletettuja tietoja kuten salasanoja ja pankkitunnuksia. Varmuuskopioinnissa esille nousivat työhön ja opiskeluun liittyvät asiat eli henkilö haluaa suojata liiketoiminta-asiakirjoja, artikkelipohjia, opiskeluun liittyviä asiakirjoja ja kuvia tuhoutumiselta tai häviämiseltä. Toisaalta Internet-profiilin hal-

linnassa painottuu erityisesti tarve yksityisyyden ja identiteetin suojaamiseen Internetissä.

6.3.7 Yhdistetty prosessi

Yhdistettyyn prosessiin (kuvio 3) on tiivistetty yksittäisten prosessien erityispiirteet. Näin se kertoo vähän enemmän käyttäytymisen muutoksesta kuin yksittäiset mallit. Yhdistetty prosessi kokoaa samaan malliin myös poikkeustilanteet, jolloin suojaustoimenpide jostain syystä laiminlyödään sekä tarpeet ja tunteet, jotka motivoivat tietoturvakäyttäytymistä. Yhdistetty prosessi täsmentää lisäksi sitä, miksi jokin tietty tarve loppuu tasolta toiselle siirryttäessä.

Yhdistetyn prosessin pohjana on kaikkien haastateltavien kokemukset. Tietokoneenkäyttäjät pääosin seuraavat määriteltyä prosessia, joten käyttäytymisen muutoksen voidaan sanoa tapahtuvan prosessissa esitetyllä tavalla. Taulukko 10 kokoaa yhteydet prosessin tasojen välillä eli mikä mahdollistaa henkilön siirtymisen tasolta toiselle.

Yhdistetty prosessi on stage-teoria, sillä se sisältää stage-teorian keskeiset piirteet (Weinstein et al, 1998) ks. myös liite 2. Prosessissa on tasot, jotka poikkeavat toisistaan siten, että tasojen käyttäytymistä motivoivat tarpeet poikkeavat toisistaan. Tasoa 1 määrittelee tietokoneenkäyttötarpeet, tasoa 2 rauhallisuuden/ mielenrauhan tarve ja tasoa 3 turvallisuuden tarve. Edelleen, tasoa 4 määrittää tietokoneenkäyttötarpeet, joita on mainittu tasolla 1 sekä uutena riippumattomuuden tarve. Yhteisenä ominaisuutena kaikilla tasoilla on kokemus, eli tietokoneen käyttäjän kokemus muuttuu hänen käydessään tasot läpi.

Teoreettisen mekanismin käyttäytymisen muutosta kuvaavan prosessin ymmärtämiseksi tarjoaa teleologinen paradigma, joka on yksi neljästä prosessiteorian paradigmoista eli ns. ideaalityypistä, joilla selitetään muutosprosesseja (Van de ven, 1992). Teleologisen paradigman avulla voidaan selittää tätä työtä seuraavalla tavalla:

1) Muutosprosessin etenemisen kuvaus

Teleologinen prosessiteoria kuvailee vaiheittaisen muutosprosessin, joka johtaa lopputulokseen. Kehittyminen on liikkumista kohti tarkoituksen, tavoitteen tai halutun lopputuloksen saavuttamista. Entiteetti kehittyy kun se kasvaa monimuotoisemmaksi tai vastaavasti yhtenäisemmäksi tai se täyttää tietyn toiminnan vaiheet. Käyttäytymisen muutosprosessi esitetään alusta loppuun saakka mukaan lukien poikkeukset.

Teoria tietoturvakäyttäytymisen muutoksesta kuvaa vaiheittaisen muutosprosessin, jossa tietokoneen käyttäjä omaksuu uuden tietoturvasuojaustoimenpiteen. Muutosprosessiin sisältyy erilaisia vaiheita ja yhteyksiä vaiheiden välillä (esimerkiksi tietoturvatapahtumat). Prosessiteoria mahdollistaa sen kuvaamisen, että käyttäytyminen muuttuu useassa kohdassa prosessia sekä sen, millainen elementtien välinen interaktio aiheuttaa käyttäytymisen muutoksen ja missä vaiheissa prosessia käyttäytyminen muuttuu. Prosessiteoria kuvaa myös poikkeukset omaksutusta suojaustoimenpiteestä.

2) Useat tapahtumaketjut (multiple progressions)

Teleologisessa prosessiteoriassa ei ole vaiheittaista tapahtumaketjua vaan lopputulos ja useita tapahtumaketjuja, jotka johtavat samaan lopputulokseen eli tässä tutkimuksessa on useita vaihtoehtoisia polkuja, jotka johtavat tietoturvasuojaustoimenpiteen käyttöönottoon. Lopputulos voidaan saavuttaa useita eri reittejä pitkin.

Tämän tutkimuksen tarkoitus on osoittaa, että ihmisten käyttäytyminen muuttuu erilaisten interaktioiden ja prosessien seurauksena. Esim. Internet-profiilin hallinta ja vahvan salasanan laatiminen ovat prosessina erilaisia, ja käyttäytymisen muutos etenee erilaisten tilanteiden ja tapahtumien kautta. Prosesseissa on erilaisia esteitä ja edistäjiä

3) Ennustettavuus

Teleologinen prosessiteoria on luonteeltaan ennustava, eli kehitysprosessin tavoite on ennakoitavissa. Tässä tutkimuksessa kehitysprosessin tavoite eli omaksuttava tietoturvatoimenpide on ennalta tiedossa ja teoria selittää kehityksen tätä lopputilannetta kohti.

4) Paluu takaisin päin prosessissa on mahdollista (repeating strings of events or activities)

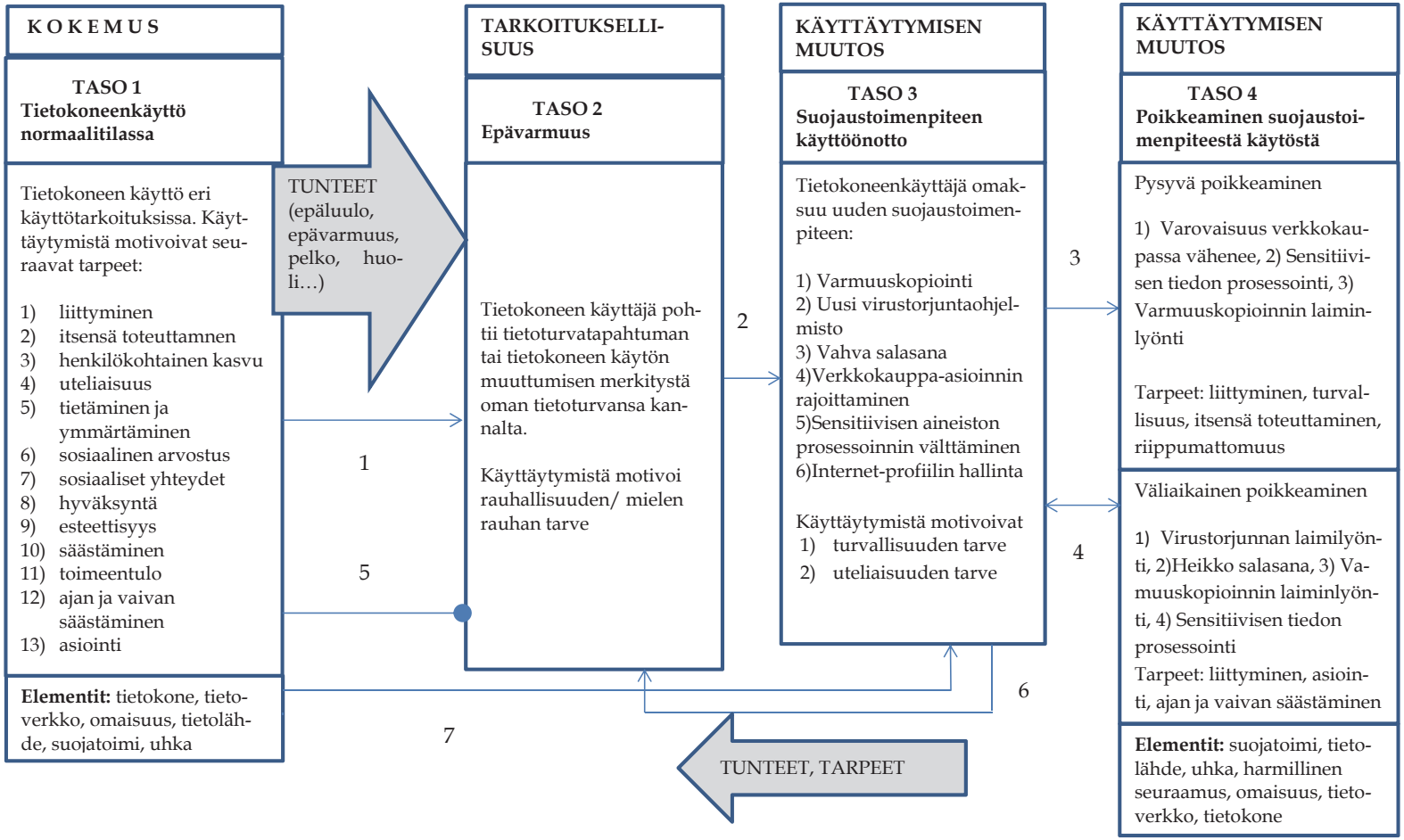
Teleologisessa prosessissa on mahdollista palata edellisille tasoille. Tietoturvatoimenpiteen omaksuttuaan tietokoneen käyttäjä voi palata aiemmalle tasolle esimerkiksi siinä tapauksessa, että hän kokee uuden tietoturvaongelman, joka herättää negatiivisia tunteita ja saa vahvistamaan suojaustoimenpidettä, esimerkiksi salasanaa.

5) Lopullinen tavoite voi olla väliaikainen (process does not stay in permanent equilibrium)

Vaikka teleologinen prosessi päättyy tiettyyn lopputulokseen, voi tämä tila kuitenkin muuttua ajan kuluessa, koska käyttäytyminen on luonteeltaan muuttuvaa (Bridle et al., 2005; Weinstein et al: 1998.). Suojaustoimenpiteen omaksumisen jälkeen alkaa uusi kehityskaari, joka johtaa tietoturvakäyttäytymisen muutokseen. Prosessiteorian avulla on mahdollista kuvata se, että tietoturvakäyttäytymisen muutos on jatkuva (vrt. esimerkki Internet-profiilin hallinnasta) ja että käyttäytyminen voi tulevaisuudessa myös muuttua joko väliaikaisesti tai pysyvästi.

Yhdistetty prosessi on kuvattu kuviossa 3. Taulukko 9 sisältää tarkemmat kuvaukset yhteyksistä prosessin tasojen välillä, yhteyksien variaatiot sekä kuhunkin yhteyteen liittyvät näytteet haastatteluaineistosta.

KUVIO 3 Yhdistetty prosessi



TAULUKKO 9 Yhteydet yhdistetyn mallin tasojen välillä

#	Yhteyden kuvaus	Yhteyksien variaatiot	Näyte aineistosta
1	Tietoturvaan liittyvä kokemus	1) tietoturvaongelma 2) tietoturvatietoisuuden lisääntyminen 3) muutos tietokoneen käytössä 4) muutos elämäntilanteessa 5) suojattavan määrä ja henkilökohtaisuus kasvaa	*1)V: No ehkä siin on et mä en ylipäätään oo tykänny hirveesti kirjotella henkilökohtasia asioitani mihinkään mut silleen tietosesti se käsitys siitä että kuinka julkinen oikeasti tommonen niin sanotusti sulettu ympäristö interne-, sulettu ympäristö Facebookissakin oikeesti on tai sulettu ympäristö IRC:issä oikeesti on niin se on sitte ehkä kehittyny siinä ajan myötä ihan silleen vaan pikkuhiljaa. Että..* *K: Että vaikka et oo sinne mitää arkaluontosta laittanukaan mutta kuitenkin oot sitte alkanu tarkemmin miettiin että..* *V: Kyllä se kun..* *K: ..miten tärkiää.* *V: ..lähinnä kun niitä tapauksia on tullu vastaan missä porukka on laittanu tosi arkaluontosta asiaa ja sitte se ei todellakaan oo pysyny siellä kaverien silmien alla vaan sen lähteny kiertämään. Koko ajahan niit tulee vastaan tälläsii caseja.* *2) I: But in Facebook you mentioned that you have blocked, like what word you used, like you hide something?* *R: Yes.* *I: So where did you learn that?* *R: In Facebook they let us know how to hide. And how to open, in the corner, so.* *I: OK, so Facebook send you some email..* *R: No, no. They, there was some kind of campaign, they released a campaign and they send their customer the message how to manage your security, account security and something, skills. So in the time I checked how to use this tool, security.*

I: Like privacy setting?

R: Yes, privacy setting.

3) *V: Joo kyllä et ainakin Facebookissa oon laittanu ne asetukset silleen että tuota, kaverit vaan näkee eikä ulkopuoliset näe.*

K: Laitoitko sää nämä heti aluksi kun aloit käyttään sitä Facebookia vai tuliko nää..?

V: Joo kyl mä aika lailla.

K: No kun aattelee syitä että miksi niin mikä motivoi sua tekemään näin? Miks tää oli tärkeetä laittaa nää tietoturva-asetukset näin?

V: No ainakin tuota, se on varmaan nyt ollu tässä vähän semmosta myöskin opettelua tähän tämmöseen enemmän julkiseen esillä oloon. Mä ainakin koen sen niin että kun ei ole siihen tavallaan kasvanut, et nyt nää nuoremmat sukupolvethan tulee kasvamaan siihen ihan eri tavalla jo.

4)K: Tuota no muistakko missä vaiheessa se muutos tapahtu, että sää aloit sitte laatimaan niitä vahvempia salasanoja?
V: No se tuli sitte just tuossa yläasteen ja amiksen vaihteella, ku tuli näitä tärkeämpiä asiakirjoja, mitä piti lähettää tai hoitaa sähköpostin kautta esim. nii sitte piti muuttaa niinku kaikki. Ja sitten muutin myös Facebookiin tuli muutettua tunnukset ja kaikki.
5) K: Elikkä sää koet välinpitämättömyyttä. Miks sää kuitenki sitte vaihat (salasanan)? Mikä sut saa…
V: Siis vaikka se on välinpitämättömyyttä, mut sitte se on toisaalta myöski silleen, että ei tästä oo ny mulle varsinaisesti mitään lisähaittaakaan, että sitten samoin vaan semmosiin tärkeisiin juttuihin, nii sitten laittaa sitä turvallisuutta. Mää oon lukenu pari semmosta tarinaa, että jollaki on tyyliin yhessä tapauksessa joku onnistu kräkkäämään niitten Apple ID -salasanan ja sitte sitä kautta ne pysty formatoimaan niitten tietokoneen ja läppärin ja puhelimen ja sitte tyyliin kaikki, mitä niil oli kaheksan vuojen ajalta, valokuvia...

--

V: Käytännössä se on tosiaan se kaks juttua. Tietoisuus siitä, että miten hel-

			posti se (hakkerointi) voi tapahtua periaatteessa, ja sitten kun tuli enemmän ja enemmän henkilökohtasempaa ja tärkeämpää suojattavaa, nii sitten jossain vaiheessa pääsi siitä laiskuudesta yli [?? 01:21:25].
2	Ratkaisuinteraktio	**Internet-profiilin hallinta** Tietokoneenkäyttäjä on tietoinen siitä, että sosiaalisen median tietoturva-asetuksia pystyy muokkaamaan niin ettei kuvat näy julkisesti kaikille. Este: tietokoneenkäyttäjä ei hallitse yksi-tyisyysasetusten määrittelemistä sosiaalisessa mediassa ja kuvanjakopalvelussa **Sensitiivisen aineiston prosessointi Internetissä** Tietokoneenkäyttäjä on tietoinen siitä, että arkaluontoisen tiedon päätymistä ulkopuolisille voi välttää harkitsemalla, mitä netissä julkaisee ja mitä sähköpostiin kirjoittaa ja lisäämällä sinne ainoastaan sellaista materiaalia mistä ei ole haittaa jos se päätyy ulkopuolisille. **Vahva salasana** Tietokoneenkäyttäjä on tietoinen siitä, että salasanojen hakkerointia voi aktiivisesti estää	**Internet-profiilin hallinta** *I: OK, so Facebook send you some email..* *R: No, no. They, there was some kind of campaign, they released a campaign and they send their customer the message how to manage your security, account security and something, skills. So in the time I checked how to use this tool, security.* *I: Like privacy setting?* *R: Yes, privacy setting.* *I: So Facebook told you? What kind of things they told you when they made that campaign?* *R: You can select a person.. the person you don't want to show. And you can make the (-) [1:44:36.5] and.. That kind of things.* *I: OK, so they gave you some instructions what kind of things you can do to hide some things.* *R: Mmm. And to manage it, my information, comments. Comments means the posts, posting.* **Sensitiivisen aineiston prosessointi Internetissä** *I: When we are talking about email, do you think about the security issues when you send email? How do.. you take into account the security, when you are sending mails?* *R: I rarely, don't send my.. henkilötunnus?* *I: Personal ID or.. ID number..* *R: ID number.. in email and.. if I.. have bought something online, it has to be so that it's trustable, when I'm sending email about my.. orders and stuff.* *I: How have you come this kind of behavior that you don't send sensitive via email+* *R: I have heard that they could be stolen.*

	laatimalla palveluihin vahvat salasanat. Käyttäytymisen muutosta edistää se, että pankin järjestelmä ohjaa vahvan salasanan laatimisessa, verkkopalvelu pakottaa laatimaan vahvan salasanan jotta palvelua pääsee käyttämään tai pyytää vahvistamaan salasanaa, Internetistä löytyy ohjeita vahvan salasanan laatimiseen, selain tallettaa salasanat, joten niitä ei tarvitse muistaa. Esteet: välinpitämättömyys sekä se, että vahvan salasanan muistaminen on hankalaa **Varmuuskopiointi** Tietokoneenkäyttäjä on tietoinen siitä että tärkeiden tietojen me-nettämisen voi estää tallentamalla tiedot useampaan paikkaan Siirtymistä tasolle 3 edistää se, että varmuuskopiointiohjelmisto on helppo asentaa ja että varmuuskopiointi yleensäkin on helppoa. **Varovaisuus verkkokaupassa**	*I: How have you heard?* *R: I've read from the internet and.. we have this.. security lectures at school, that you can never use any patient information in your personal email and..* *I: In university studies or?* *R: Yes. And we had in high school if I remember correctly.* *I: Do you follow all of the instructions you have got from the lectures?* *R: Mostly yes. It's just.. I don't want to risk my future because if I send patient information through email..* **Vahva salasana** *I: What kind of consequences of this kind of hacking, what has this caused to your friend?* *R: He lost everything in that email. Whatever was there, he lost it. And then the consequence could be, there could be some critical information which he might have lost. Or it might go to some unwanted people. However, to keep that in mind, I always have a very, I think it is a very strong password, the one which I use. Because it has uppercase, it has low-, a special character and it has numerals. So, I think it is kind of very strong password.* *I: Where have you heard that, how do you know that it is strong? Have you read somewhere, or?* *R: I got that habit when I started accessing my internet banking. And I received suggestions from there, that if you are developing your password, then do it this way. So, then, maybe, I guess my email was hacked, this fake email. So that was also in my mind that I may lose information in my email, in my genuine email. And I learned it from my bank accounts online. So I applied there, when I developed my password for emails, something like that. So then I have very strong passwords there.* **Varmuuskopiointi** *K: Elikkä koulutöitä et oo koskaan menettäny, mutta ootko jottain muuta materiaalia menettäny varmuuskopioinnin puuttumisen takia? Jonku tosi tärkiän?*

	Tietokoneenkäyttäjä on tietoinen siitä, että verkkokaupankäynnin turvallisuutta voi parantaa - välttämällä luottokortin käyttöä verkkokaupassa - lopettamalla epäluotettavan verkkokaupan käytön. - kieltämällä luottokorttinumeroiden säilytyksen verkkokaupassa. - ottamalla käyttöön pay pal: lin verkkokaupassa maksettaessa - tarkistamalla millainen salaus on verkko-kaupassa, eli onko ns. turvallisempi moodi päällä - tarkistamalla maksuvaihtoehdot - ottamalla epävarmuutta aiheuttavissa asioissa yhteyttä suoraan yritykseen Este: Verkkokaupan englanninkielisiä ohjeita on vaikeita ymmärtää, mikä muodostuu esteeksi turvallisen verkkokaupan käytölle	*V: Ei oo tosi tärkeitä. Muutamia kirjotustöitä on joskus saattanu mennä hukkaan, mutta ei semmosta, mikä ois ollu. Kyllä tietysti harmittamaan on jääny, mutta että siis mitään tosi radikaalia, mikä ois ollu taloudellista tai muuten vaikutusta, niin ei.* *K: Miten sun käyttäytyminen muuttu sitte tämmösen kokemuksen jäläkee? Se harmitti, mutta…* *V: Se harmitti, mutta se muistutti siitä, että kun ei oo kysymys oikeesti kun näppäinyhdistelmän painamisesta.* **Varovaisuus verkkokaupassa** *K: Minkälaisia ajatuksia, tunteita? Nyt päästään näihin tunteisiin, nii minkälaisia ajatuksia, tunteita, minkälainen reaktio on ollu, ku nää oot kuullu näistä tämmösistä, mitä ongelmia voi seurata?* *V: Se on se välttämisreaktio.* *--* *K: Ymmärräkkö nää välttämisen sillä tavalla, että lopettanu kokonaan?* *V: En, vaan... No sanotaanko, että ehkä mä sitte vältän semmosia sivustoja, missä mulla tulee semmonen intuitio, missä voi olla, mihin mä en luota.* **Virustorjunta** *K: Minkälaisia ajatuksia ne tietomurrot tai minkälaisia ajatuksia tai tunteita ne tietomurrot sussa herättää?* *V: Se herätti just sitä, että mää otin sitte sieltä Saunalahen kautta sen tietoturvan siihen omaan puhelimeen ja tähän koneeseen. Et mää en voinu olla huolettomana niin, että se huolehtii siitä, että mun ei tartte ite koko ajan päivittää jotaki vaan se tulee sieltä automaattisesti.*

		Virustorjunta Tietokoneenkäyttäjä on tietoinen siitä, että tietokoneen ja siinä olevat tiedot voi suojata viruksilta virustorjuntaohjelmalla. Lisäksi, virustorjuntaohjelmaa vaihtamalla voi saada koneelleen tehokkaamman suojan. Edistäjät: ohjelmisto on helppo asentaa, käyttää ja ymmärtää jos käyttöohjeet ovat suomeksi. Ohjelmiston ilmaisuus edesauttaa sen käyttöönottoa. Este: tietokoneenkäyttäjä epäilee virustorjunnan tehokkuutta	
3	Poikkeusinteraktio	Syyt pysyvään muutokseen: - TARPEIDEN PRIORISOINTI: Uhkan kokemuksen väheneminen - TARPEIDEN PRIORISOINTI: Luottamuksen lisääntyminen - TARPEIDEN PRIORISOINTI: Riippumattomuus	ks. näytteet aineistosta prosessin tasolta 4: Poikkeukset
4	Poikkeusinteraktio	Syyt väliaikaiseen poikkeamiseen - TARPEIDEN PRIORISOINTI: Tietojen/tiedostojen priorisointi	ks. näytteet aineistosta prosessin tasolta 4: Poikkeukset

		- TARPEIDEN PRIORISOINTI: Muistamiseen liittyvät ongelmat - TARPEIDEN PRIORISOINTI: asian toimittaminen - TARPEIDEN PRIORISOINTI: palvelun käytön lyhytkestoisuus - Vahinko - TARPEIDEN PRIORISOINTI: Applikaation asentaminen tai ohjelmiston testaaminen - TARPEIDEN PRIORISOINTI: uhkan kokemuksen väheneminen	
5	Prosessi pysähtyy	Prosessin pysähtymiseen liittyvät tunteet 1) huvittuneisuus 2) välinpitämättömyys 3) luottamus 4) itsevarmuus	*1) I: So your friend knew that it is not good password and told it to you?* *R: She just told me that this is not really a (-) [0:55:45.1]. I think I thought that this is secret, so maybe this idea is good, but she told me that no.* *I: So and you changed it after your friend told it to you?* *R: No, I didn't change. But..* *I: Why? Was it that you didn't believe or you didn't care or what was the reason?* *R: Anyway I thought that my password is funny. So because the password is secret, I thought that. When I was, that time I was in the middle school, I just thought that this password is secret. This is funny, so I used that.* *2) I: OK. So do you remember why you started to use these long passwords?* *R: Why?*

			I: Why, in Yahoo! and in Facebook. Or do you, if you previously maybe had some shorter passwords. So when and why did you find out that you should have longer passwords? *R: I..* *I: Do you remember who told you, or did you read it somewhere, or?* *R: This is not the reason, but the, when I used the Hotmail, MSN, someone hacked my account. And then the person wanted to borrow money by using my account. So my friends called me, I think the person is not you, but why you want? Wanted to borrow the from me, in the MSN chat. But this is not the reason, but anyway I experienced this kind of happening.* *I: So did you change your behaviour somehow after this hacking experience?* *R: Maybe it affected my behaviour but, in the time I didn't think this is serious problem. I don't know the reason why I changed it, my password to complicated password* *3) K: Mitä, jos sun lähipiirissä tapahtus tämmöne iso ongelma, vaikka rahaa menis paljo jotenki vuotas tai siis joku menettäu rahhaa. Niin vaikuttasko se sun käyttäytymisee, että voisikko sää lopettaa vaikka verkkokaupan käytön kokonaan tämmöseen?* *V: Jos puhutaan jostain yksittäisestä verkkokaupasta, mitä itse aktiivisesti käyttäs, niin yksittäisen kaupan kohalla, joka ei välttämättä ei itteä mietitytä tai oikeestaa ees itte omaan elämänpiiriin liittyvä asia, niin jos semmosta tapahtuu, niin kyllä mä nyt edelleen jatkasin normalia verkkokaupankäyntiä.* *4) K: Mitä nä siinä tilanteessa aatelit, että minkälaisia fiiliksiä herätti?(salasanojen hakkerointiyritys)* *V: Lähinnä naurahdin, ku mulla on se kaksvaihe autentifikaatio, siinäpähän yrittävät.* *K: Että ei tullu mitään semmosta huolta, eikä…* *V: Ei, ei todella. Ehkä saattaa olla sillai, että vaihan sillon sen salasanan sinne.*
6	Uusi tietoturvaan liittyvä tapahtuma tai kokemus	1) tietoturvaongelma 2) tietoisuuden lisääntyminen 3) teknologinen kehitys	*1) R: However, I'm quite sensitive, for example, I signed one application with Facebook that's called TripIt or something like that. And what happened, I booked a ticket through Norwegian and it, without knowing me, it updated on Facebook that I'm travelling from here to there. And that was quite scary for*

	4) kokemus tietoturvauhan lisääntymisestä	*me. So I immediately changed my setting in that.* *2) K: Mua kiinnostaa se, miksi ihmiset vaihtaa näitä virustorjuntaohjelmia toisesta toiseen. Miksi sää oot vaihtanu, et oo käyttäny sitä samaa koko ajan?* *V: Koska kaveri sano, että tämmönen uus tai tämä toinen. Se [?? 00:37:43] voi olla vähän parempi, että pannanko tää. Mulle käy kaikki, sää tiiät näistä, mää en tiedä mitään, laita se. Se on hyvä ollu.* *3) K: Joo miks sää oot vaihtanu sitte toiseen, että…?* *V: No jos sitä vapaata versiota ei oo pystyny lataamaan uudelleen, niitäki on tapahtunu. Ja sitte jos on kuullu jostain paremmasta, nii sitte haluaa totta kai sen paremman sitte ku on suositteluja lukenut.* *K:Minkälainen on parempi? Kuvaile vähän minkälainen on parempi ohjelma.* *V: Se on, mitenkäs vertaisin jotain kahta ohjelmaa…* *K: Tai mitä sää oot siinä tilanteessa pohtinu, ku sää oot niinkö alkanu vaihtamaan sitä, nii minkälaisia ajatuksia/tunteita sää oot käyny siinä läpi, että miks sää oot vaihtanu?* *V: Sitä että jos se edellinen ohjelma on tehny niitä tarkistuksia koneella ja on sanonu, että ei mitään niinku viruksia tai mitään. Oon laittanu uuden ohjelman ja se ilmottaa, että on viruksia ja se poistaa ne välittömästi. Mutta sillee voiha seki olla, en tiiä voiko se vaa sanoa, että siellä on jotain ihan pieniä, iha pikkuruisia roskia, mitä se vaa sanoo, että nää on viruksia, ne pitää poistaa.* *K: Tarkotatko, että se on vähä ollu tehottomampi se entinen?* *V: Nii, siihen vertaisin ehkä enemmänki.* 2) *K: Miten sitte jatkossa, pysyykö tämä periaate samana vai meneekö ehkä toiseen suuntaan vai tiukennatko ehkä vielä tästä tietojen suojausta tästä nykysestä tilanteesta?* *V: Joo ei se ainakaan löysätä voi. Että kyllä se koko ajan näyttää menevän siihen suuntaan, että yhä taitavampii on noi hakkerit, että sitä joutuu vielä tästä ryhtyä vieläki tiukentaa ja rajottamaan sitte vieläki nettikäyttöö. Pahaltahan se näyttää.*

7	Pakottaminen	Järjestelmä pakottaa laatimaan vahvan salasanan	*I: OK. So if there would not have been this enforcing in your country, so do you think you still would have short password also in Yahoo! and in Facebook?* *R: I think so.. Yes. Yes I think so, because in that time why I changed my password, because if I didn't change it to a long password, I couldn't use the website anymore. So I didn't have any option.* *I: But still you said that these days you use short password for Gmail for example. So is it because you can do it, it's possible to do it?* *R: Yes.* *I: OK. So you don't have any other reason for selecting long password except that you are kind of, you have to do that, that you can use it?* *R: Yeah.*

6.3.8 Prosessin yhteydet

Tässä luvussa tarkastellaan yksityiskohtaisesti prosessin yhteydet: millaisia tunteita ja tarpeita yhteyksiin liittyy ja missä määrin jotkut tarpeet päättyvät tasolta toiselle siirryttäessä. Luvussa esitetään myös tietoturvaan liittyvät kokemukset, jotka vaikuttavat tietoturvakäyttäytymisen muutokseen sekä millaisten elementtien kanssa tietokoneenkäyttäjä toimii interaktiossa eri yhteyksissä. Luvussa selvennetään lisäksi millaisia esteitä/ edistäjiä ja tarpeiden priorisointia yhteyksiin liittyy. Yhteyden 2 kohdalla kuvataan ratkaisuinteraktioilla sitä, miten tietokoneenkäyttäjä kokee voivansa aktiivisesti poistaa epävarmuutta aiheuttavan asian

Yhteys 1. Tietoturvaan liittyvä kokemus

Yhteys 1 mahdollistaa tietokoneenkäyttäjän siirtymisen tasolle 2 eli tarkoituksellisuuden ja merkityksellisyyden pohtimiseen. Tietoturvaan liittyvä kokemus herättää tietokoneenkäyttäjässä erilaisia tunteita (taulukko 10). Tunteet on eritelty tarkemmin liitteessä 16.

TAULUKKO 10 Tarpeiden, tunteiden ja motiivien määrittely, yhteys 1

Tason 1 tietokoneenkäyttötarpeet säilyvät yhteydessä 1 ennallaan, siirryttäessä prosessissa tasolle 2	1) liittyminen 2) itsensä toteuttaminen 3) henkilökohtainen kasvu 4) uteliaisuus 5) tietäminen ja ymmärtäminen 6) sosiaalinen arvostus 7) sosiaaliset yhteydet 8) hyväksyntä 9) esteettisyys 10) säästäminen 11) toimeentulo 12) ajan ja vaivan säästäminen 13) asiointi
Tietoturvakokemus herättää tietokoneen käyttäjässä erilaisia tunteita	1) epäluulo, epäilys 2) epävarmuus 3) välinpitämättömyys 4) pelko 5) huoli 6) huvittuneisuus 7) hämmennys 8) turhautuminen 9) viha 10) ihmettely, epäuskoisuus 11) pettymys 12) ärtymys 13) hätäännys 14) kauhu/paniikki 15) vähättely 16) harmi 17) surullisuus 18) häpeä 19) raivo 20) myötätunto 21) painostava tunne

Tietoturvaan liittyvä kokemus on esimerkiksi

- arkaluontoisen tiedon vuotaminen ulkopuolisille esim. sosiaalisessa mediassa tai sähköpostissa
- sähköpostin salasanojen hakkerointi
- tietojen menetys tai vaara menetyksestä hakkeroinnin/ tietokoneviruksen/ varmuuskopioinnin puuttumisen /tietokoneen rikkoutumisen seurauksena
- pankkikortin hakkerointi
- rahanmenetys
- huijaus
- virustorjunnan puutteellisuuden huomaaminen

- tietokoneen käyttäjä ottaa käyttöön facebookin
- facebook-profiilin kopiointi
- facebook-tunnusten väärinkäyttö
- tietokoneen käyttäjä lähettää arkaluontoista tietoa sähköpostissa
- tietokoneen käyttäjä alkaa käyttää tietokonetta verkkopankkiasiointiin.
- tietokoneen käyttäjä ottaa käyttöönsä google mailin
- tietokoneen käyttäjä alkaa kirjoittamaan isompia opiskeluun liittyviä dokumentteja tietokoneella
- luottokorttinumeron vuotaminen julkisuuteen
- ylimääräisten kaveripyyntöjen ja julkaisujen saaminen sosiaalisessa mediassa
- tietokoneen käyttäjä alkaa omistamaan henkilökohtaisempaa ja tärkeämpää aineostoa
- elämäntilanteen muutos (lapsen syntymä, koulun vaihto, opiskelujen aloitus, työnhaku)
- sosiaalisessa mediassa ulkoiset palvelut pyytävät saada käyttää tietoja
- chat-keskustelun kaappaus sosiaalisessa mediassa
- salasanan paljastuminen ”olan yli katselemisen” seurauksena
- sähköpostin hakkerointi ja sähköpostin väärinkäyttö
- tietokoneen myynti
- steam-tilin kaappaus (some)
- tietokoneen kuluminen ja hidastuminen
- lomaosakkeen vuokraaminen sivustolta, joka on kopioitu alkuperäisen firman sivustosta
- sähköpostiviestin ja liitetiedoston katoaminen
- tutusta hotelliketjusta varastetaan miljoonien asiakkaitten luottokorttitiedot.
- tiedostomateriaalin päätyminen vääriin käsiin
- salasanojen vuotaminen tai varastaminen
- peli-tilin hakkerointi ja väärinkäyttö
- google playsta tilataan omissa nimissä tavaraa
- tietokoneen käyttäjän ystävä tilaa verkkokaupasta elektroniikkaa jonka takuun kanssa tulee ongelmia

Tietokoneen käyttäjä tai joku hänen lähipiiristään kokee tietoturvaongelman. Tietoturvaongelma voi olla sensitiivisen tiedon vuotaminen ulkopuolisille tai sähköpostin hakkerointi ja tietojen menetys hakkeroinnin seurauksena. Tietokoneen käyttäjä voi menettää tärkeitä tietoja varmuuskopioinnin puuttumisen ja virusten takia. Tietoturvaongelma voi olla myös facebook-profiilin kopiointi, hakkerointi ja siihen liittyvä sosiaalisen median tunnusten väärinkäyttö tai tietojen vuotaminen sosiaalisesta mediasta ulkopuolisille.

Verkkokauppaa käytettäessä tietoturvaongelma voi olla pankkikortin hakkerointi, rahan menetys ja huijaus. Tietokoneen käyttäjä voi kohdata ongelmia myös virustorjuntaan liittyen, hän esimerkiksi huomaa, että virustorjuntaohjelmisto ei torju kaikkia haittaohjelmia.

Yhteys 1 voi sisältää myös tapahtuman, jossa tietoturvatietoisuus lisääntyy, esim. pankki neuvoo vahvojen salasanojan laatimisessa tai tietokoneen käyttäjä osallistuu tietoturvakoulutukseen. Hän voi saada tietoturvaan liittyvää tietoa myös ystäviltä, sukulaisilta, firman asiakkailta, mediasta tai Internetistä. Tietokoneen käyttäjä saa tietoa ja ohjausta vahvan salasanan laatimiseen, varmuuskopiointiin, facebookin tietoturva-asetusten käyttöön ja virustorjuntaohjelmistojen käyttöön. Hän kuulee identiteettivarkauksista ja niiden seurauksista sekä sensitiivisen tiedon suojaamisesta sähköpostissa sekä tietovuodoista. Hän oppii miten omia tietoja voi tarkistaa Internetistä. Tietokoneen käyttäjä kuulee mitä uhkia facebookin käyttöön liittyy (tiedot saattavat esim. hävitä) ja että sähköpostia kirjoitettaessa tiedot eivät tallennu kotikoneelle vaan myös järjestelmään. Tietokoneen käyttäjä kuulee haittaohjelmista ja viruksista ja niiden haitallisista seuraamuksista. Tietokoneen käyttäjä saa muistutusviestin salasanan vahvistamisesta

Tietoturvaan liittyvä tapahtuma voi olla myös se, kun tietokoneen käyttäjä alkaa käyttää tietokonetta uuteen käyttötarkoitukseen (sosiaalinen media, verkkopankki, musiikin lataus) tai laajentaa tietokoneen käyttöä tietyssä käyttötarkoituksessa, esimerkiksi ottaa käyttöönsä uuden sähköpostiohjelmiston. Elämäntilanteen muutos voi olla tietoturvatapahtuma, samoin kuin se että henkilö alkaa omistamaan enemmän tärkeämpää ja henkilökohtaisempaa suojattavaa.

Kun tietokoneenkäyttöä tietyssä käyttötarkoituksessa, esimerkiksi sosiaalisen median käyttö, on jatkunut jonkin aikaa, tietokoneen käyttäjä voi alkaa kyseenalaistamaan tämän palvelun käytön tietoturvasyistä. Tämän voi tulkita myös tietoturvaan liittyväksi tapahtumaksi, joka motivoi käyttäytymisen muutokseen.

Yhteydessä 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa (Taulukko 11):

TAULUKKO 11 Yhteys 1 ja interaktiot

Elementti	**Variaatiot elementeistä eri käyttäytymis-tyypeissä**
tietokone	Tietokonetta käytetään seuraavissa käyttötarkoituksissa: 1) kommunikointi ystävien, tuttujen ja sukulaisten kanssa (sosiaalinen media, sähköposti, pikaviestipalvelu) 2) oman työn markkinointi 3) liiketoiminnan kehittäminen ja työnteko 4) opiskelu 5) yhdistystoiminta 6) verkkopankin käyttö 7) verkkokaupan käyttö 8) tiedonhaku 9) uusien asioiden opettelu 10) ajanviete /viihtyminen (pelaaminen, musiikin kuuntelu, elokuvien katselu) 11) asioiden hoitaminen esimerkiksi liiketuttavien, pankin ja viranomaisten, koulun ja työnantajien kanssa 12) kuvien, muistiinpanojen, videoiden ja musiikin tallentaminen Tietokone toimii myös tietoturvauhkien kohteena (esim. hakkerointi, virusten levittäminen)
tietoverkko	Internet
omaisuus	1) sosiaalisen median tiedot ja päivitykset 2) identiteetti 3) sähköpostiviestit ja sähköpostitiedot 4) kriittinen informaatio sähköpostissa (esimerkiksi henkilökohtaiset viestit, ihmissuhteisiin liittyvät tiedot ja ostokuitit) 5) raha 6) työhön tai työhakuun liittyvät ja liiketoiminta-asiakirjat 7) luottokorttinumero 8) tietokone 9) salasanat 10) pankkitunnukset ja -tiedot 11) yksityisyys 12) kuvat ja musiikkitiedostot 13) opiskeluasiakirjat 14) tilinumero 15) potilastiedot 16) henkilötunnus 17) verkkokauppaan liittyvät tiedot 18) puhelinnumero 19) osoite ja koti 20) lopputyöhön liittyvään yritykseen ja tuotteeseen liittyvät tiedot 21) käyttäjätunnus ja salasana

	22) chattilogit 23) artikkelipohjat 24) muistiinpanot 25) kaunokirjalliset tekstit
tietolähde	1) LinkedIn-koulutus 2) sukulaiset, ystävät ja perhe 3) palveluntarjoaja (esim. sosiaalinen media) 4) media (TV, uutiset) 5) pankki 6) firman asiakkaat 7) Internet 8) koulu 9) verkkokauppa 10) luottokunta 11) työ 12) Internetin keskustelufoorumi 13) kollegat 14) poliisi 15) tietokonealan lehdet
uhka	1) salasanojen (esimerkiksi sähköposti) hakkerointi 2) sähköpostiviestien levittäminen/varastaminen 3) haittaohjelmat ja virukset, jotka tuhoavat tiedostoja 4) huijaus verkkokaupassa 5) luottokortin hakkerointi 6) verkkokaupan toimintaongelmat 7) facebook-profiilin kopiointi 8) facebook-tunnusten väärinkäyttö 9) identiteettivarkaus 10) tietokoneen rikkoutuminen ja kuluminen 11) verkkokaupan tietokannan hakkerointi 12) haittaohjelma kaappaa tietokoneen 13) roskaposti 14) tietojen varastaminen 15) roskaposti 16) ”olan yli katseleminen” ja salasanan selville saaminen. 17) musiikkipalvelun tili jää auki
suojatoimi	1) käytössä oleva suojatoimi - Antivirus-ohjelmisto - Tietoturva-ohjelmisto 2) uusi suojatoimi - vahva salasana - varmuuskopiointi - sosiaalisen median tietoturva-asetukset - virustorjuntaohjelmisto

	- sensitiivisen tiedon suojaaminen sähköpostissa - omien tietojen tarkistaminen Internetistä - varovaisuus verkkokaupassa
harmillinen seuraamus	1) oma kuva päätyy ei-halutulle sivulle 2) omien tietojen, esimerkiksi pankkitietojen, väärinkäyttö 3)sensitiivisen tiedon vuotaminen esimerkiksi sosiaalisesta mediasta ulkopuolisille 4) sähköpostin tietojen menetys 5) liiketoiminta-asiakirjojen/ kuvien/opiskeluun liittyvien dokumenttien menetys 6)rahan menetys verkkokaupassa, tilin käytön estyminen, pitkät selvittelyajat 7) koneen saastuminen, koneen hidastuminen, pop-up ikkunat, selaimen aloitussivun vaihtuminen, sähköpostitunnusten kaappaaminen 8)tietojen häviäminen sosiaalisesta mediasta 9)tietojen vuotaminen sosiaalisen median ulkopuolelle 10)väärän tiedon levittäminen identiteettivarkauden seurauksena 11)luottokorttitietojen vuotaminen julkisuuteen 12)verkkokauppaostoksiin tulee ylimääräisiä lisiä 13)ylimääräisten kaveripyyntöjen ja epäolennaisen tiedon saaminen sosiaalisessa mediassa 14)sosiaalisessa mediassa ulkoiset palvelut pyytävät saada käyttää tietoja 15)facebook-profiilin kopiointi, 16)kuvajakopalvelun kuvia vuotaa julkisuuteen, 17)vääristyneen kuva muodostuminen Internetissä olevien tietojen perusteella 18) tilausten tekeminen toisen nimellä, 19) chat –keskustelun kaappaus, 20) nettikiusaaminen 21) sähköpostin käyttäminen ja lähettäminen omissa nimissä, 22) some-tilin tai peli-tilin kaappaus ja väärinkäyttö, tietokoneella olevien henkilökohtaisten tietojen menetys, 23) tiedostomateriaalin päätyminen vääriin käsiin, 24) salasanojen vuotaminen j varastaminen 25) tietojen muuttuminen käyttökelvottomaksi, 26) verkkopankkitunnuksia vuotaa julkisuuteen, 27) rahan menetys tekaistulta verkkosivulta tehdyn ostoksen seurauksena, 28) verkkokaupasta ostetusta elektroniikkalaitteesta ei mene takuu läpi 29) koneen hallinnan menettäminen

Yhteys 2

Yhteys 2 mahdollistaa tietokoneenkäyttäjän siirtymän tasolle 3 eli uuden suojaustoimenpiteen valintaan.

Tarpeiden ja motiivien määrittely

Edellisen tason eli tason 2 rauhallisuuden ja mielenrauhan tarve päättyy, koska tietokoneen käyttäjä reagoi epävarmuutta aiheuttaneeseen asiaan. Hän tietää kuinka voi aktiivisesti vaikuttaa omaan tietoturvaansa ja aikoo ottaa käyttöön suojaustoimenpiteen, esimerkiksi tietoturva-asetukset sosiaalisessa mediassa, minkä ansiosta tietoturvaan liittyvät asiat lakkaavat vaivaamasta mieltä.

Ajattelun muutos johtaa käyttäytymisen muutokseen. Tietoturvatapahtuma on aiheuttanut negatiivisia tunteita ja epävarmuutta, josta tietokoneen käyttäjä pyrkii eroon. Tässä vaiheessa korostuu tietokoneenkäyttäjän oma aktiivisuus: hän aktiivisesti pyrkii vaikuttamaan tietoturvaan. Taulukossa 12 on esitelty ratkaisuinteraktiot käyttäytymistyypeittäin

TAULUKKO 12 Ratkaisuinteraktiot

Käyttäytymistyyppi	**Ratkaisu epävarmuuden poistamiseen**	**Interaktio**	**Esteet/ edistäjät suojaustoimenpiteen omaksumiselle**
Internet-profiilin hallinta	Sosiaalisen median tietoturva-asetuksia pystyy muokkaamaan niin ettei kuvat näy julkisesti kaikille. Omia tietoja voi tarkistaa Internetistä hakukoneiden avulla.	Ystävät kertovat, kuinka sosiaalisen median tietoturva-asetuksia voidaan määritellä. Facebook järjestää kampanjan, jossa kerrotaan, kuinka facebookin tietoturva-asetuksia voidaan määritellä. LinkedIn koulutuksessa saa tietoa kuvahakujen tekemisestä	Esteet Käyttäytymisen muutoksen esteeksi voi muodostua se, että tietokoneenkäyttäjä ei hallitse yksityisyysasetus-ten määrittelemistä sosiaalisessa mediassa tai kuvanjakopalvelussa
Sensitiivisen tiedon prosessointi	Arkaluontoisen tiedon päätymistä ulkopuolisille voi välttää harkitsemalla mitä netissä julkaisee ja mitä sähköpostiin laittaa ja lisäämällä sinne ainoastaan sellaista materiaalia mistä ei ole haittaa jos se päätyy ulkopuolisille.	Tietokoneen käyttäjä kuulee tv:stä, lähipiiriltä, Internetistä, tietokonealan lehdistä, asiantuntijoilta ja kou-lussa, että sensitiivistä tietoa ei saa lähettää sähköpostissa/ laittaa sosiaaliseen mediaan	-

Vahva salasana	Salasanojen hakkeroin-tia voi aktiivisesti estää laatimalla palveluihin vahvat salasanat.	Tietokoneen käyttäjä saa tietoa vahvoista salasanoista ja kuinka niitä laaditaan mm. pankilta ja uutisista, Internetistä, lähipiiriltä ja työstä, palveluiden foorumeista	Esteet Vahvan salasanan laatimista ehkäisee laiskuus ja välinpitä-mättömyys sekä se, että vahvan salasanan muistaminen on hankalaa Edistäjät Järjestelmät, esimerkiksi pankin järjestelmä ohjaa käyttäjää laatimaan vahvan salasanan. Verkkopalvelu pakottaa laatimaan vahvan salasanan jotta palvelua pääsee käyttämään. Internet-selain tallettaa salasanat, joten niitä ei tarvitse muistaa.
Varmuuskopiointi	Tärkeiden tietojen menettämisen voi estää tallentamalla tiedot useampaan paikkaan	Tietokoneen käyttäjän ystävä neuvoo käyttämään pilvipalveluita varmuuskopiointiin. Myös koulun, työ-paikan ja Internet-keskustelujen kautta tietokoneen käyttäjä kuulee varmuuskopioinnin tärkeydestä.	Edistäjät Varmuuskopiointi on helppoa Varmuuskopiointiohjelmisto on helppo asentaa
Varovaisuus verkkokaupassa	Verkkokaupan-käynnin turvallisuutta voi parantaa - välttämällä luotto-kortin käyttöä verkkokaupassa - lopettamalla tietyn verkkokaupan käytön. - kieltämällä luotto-korttinumeroiden säilytyksen verkkokaupassa. - ottamalla käyttöön pay pal: in - tarkistamalla millainen salaus on verkkokaupassa, eli	Tietokoneenkäyttäjä keskustelee ystävien ja lähipiirin kanssa verk-kokauppaan liittyvistä ongelmista ja seuraa Internetistä asiaan liit-tyvää keskusteluja, esimerkiksi hintavertailuja	Este Verkkokaupan englanninkielisiä ohjeita on vaikeita ymmärtää, mikä muodostuu esteeksi turvallisen verkkokaupan käytölle

	onko ns. turvallisempi moodi päällä - tarkistamalla maksuvaihtoehdot - ottamalla epävarmuutta aiheuttavissa asioissa yhteyttä suoraan yritykseen		
Virustorjunta	Tietokoneen ja siinä olevat tiedot voi suojata viruksilta virustorjuntaohjelmalla.	Tietokoneen käyttäjä saa ystävältä/ sukulaiselta neuvoja virustorjuntaohjelman valintaan. Internetistä ja alan lehdistä löytyy myös tietoa virustorjuntaohjelmista.	Este Tietokoneen ikä ei mahdollista modernin virustorjuntaohjelman asentamista, puutteelliset taidot virustorjuntaohjelmien etsimiseen internetistä ja asennusohjeiden ymmärtämiseen, virustorjuntaohjelman maksullisuus, tietokoneenkäyttäjän epäilevä suhtautuminen virustorjunnan tehokkuuteen Edistäjät tietoturvaohjelmisto, esimerkiksi virustorjuntaohjelmisto, on helppo asentaa ja helppo käyttää, ohjelmisto on ilmainen, ohjeet helposti ymmärrettävissä

Yhteys 3

Yhteys 3 mahdollistaa tietokoneenkäyttäjän siirtymän tasolle 4, jossa henkilö poikkeaa omaksutusta suojaustoimenpiteestä pysyvästi.

Syyt pysyvään muutokseen:

- TARPEIDEN PRIORISOINTI: Uhkan kokemuksen väheneminen
- TARPEIDEN PRIORISOINTI: Luottamuksen lisääntyminen
- TARPEIDEN PRIORISOINTI: Riippumattomuus

Tarpeiden ja motiivien määrittely
Edellistä taso märittänyt turvallisuuden tarve voi tämän yhteyden aikana päättyä siksi, että uhkan kokemus vähenee/laimenee eli henkilö ei enää välitä, mitä kirjoittaa sosiaaliseen mediaan, koska tämän palvelun käyttö on jo niin tuttua. Samoin, tietokoneenkäyttäjä voi ajatella ettei voi aina miellyttää kaikkia kirjoituksillaan joten vähentää tämän takia pohdintoja siitä, mitä esimerkiksi sosiaaliseen mediaan kirjoittaa (riippumattomuus)

Turvallisuuden tarve voi päättyä myös siksi että luottamus verkkokauppaan lisääntyy. Eli henkilö vähentää verkkokaupan rajoituksia koska verkkokauppa yleistyy ja tulee tutummaksi. Myös talletettavien tietojen luokittelu saa aikaan turvallisuuden tarpeen päättymisen eli henkilö luokittelee aineistot tärkeyden perusteella ja jättää varmuuskopioimatta ei-tärkeät
Turvallisuuden tarve voi säilyä siirryttäessä poikkeustilanteeseen. Siinä tapauksessa että henkilö halua vahvistaa virustorjuntaa käyttäytymistä motivoi teknologinen kehitys yhdessä turvallisuuden tarpeen kanssa

Yhteys 4

Yhteys 4 mahdollistaa tietokoneenkäyttäjän siirtymän tasolle 4, jossa henkilö poikkeaa omaksutusta suojaustoimenpiteestä väliaikaisesti

Syyt väliaikaiseen muutokseen:

- TARPEIDEN PRIORISOINTI: Tietojen/tiedostojen priorisointi
- TARPEIDEN PRIORISOINTI: Muistamiseen liittyvät ongelmat
- TARPEIDEN PRIORISOINTI: asian toimittaminen
- TARPEIDEN PRIORISOINTI: palvelun käytön lyhytkestoisuus
- Vahinko
- TARPEIDEN PRIORISOINTI: Applikaation asentaminen tai ohjelmiston testaaminen
- TARPEIDEN PRIORISOINTI: uhkan kokemuksen väheneminen

Tarpeiden ja motiivien määrittely
Turvallisuuden tarve, joka määritti edellistä tasoa eli tasoa 3, voi yhteyden 4 aikana joko säilyä tai päättyä. Tarve säilyy siinä tapauksessa, että henkilö välillä unohtaa varmuuskopioinnin tai lähettää vahingossa sensitiivistä tietoa Internetissä.

Toisaalta turvallisuuden tarve voi päättyä. Henkilö vaikkapa lähettää sensitiivistä tietoa satunnaisesti sähköpostilla tai sosiaalisessa mediassa. Syy miksi turvallisuuden tarve tässä tapauksessa päättyy on, että henkilön pitää saada asia toimitettua. Hän tietää, ettei arkaluotoista viestiä, kuten pankkitietoja, saisi lähettää muttei koe että olisi muutakaan vaihtoehtoa.

Jos henkilö ajattelee, että tulee kirjautumaan johonkin tiettyyn Internet-palveluun vain muutaman kerran, hän laatii heikon salasanan vaikka muuten käyttäisi vahvoja salasanoja. Hänen toimintaansa ei määritä tällöin enää turvallisuuden tarve koska viestintää ei ole tarpeen suojata vahvalla salasanalla, vaan liittymisen tarve ja ajan ja vaivan säästämisen tarve.

Mikäli tietokoneenkäyttäjällä on tarve testata ohjelmistoa, ja hän sen takia ottaa virustorjunnan pois päältä, turvallisuuden tarve jää taka-alalle tai vaihtoehtoisesti se otetaan huomioon yhtä aikaa tutkimisen ja tietämisen tarpeen kanssa
Myös siinä tapauksessa turvallisuuden tarve jää taka-alalle, jos henkilö kokee välinpitämättömyyttä varmuuskopiointia kohtaan: koska mitään onnettomuutta ei ole sattunut hän jättää tiedostoja varmuuskopioimatta

Suojaustoimenpiteestä poikkeamisen syyt esitelty tarkemmin tason 4 kohdalla

Yhteys 5

Yhteys 5 osoittaa että tietokoneenkäyttäjä ei välttämättä etene tasolta 1 tasolle 2

Tietokoneen käyttäjä ei välttämättä ota suojaustoimenpidettä käyttöönsä, vaikka tietoturvatietoisuus lisääntyy tai hän kokee tietoturvaongelman. Ystävän neuvo salasanan vahvistamisesta ei vaikuta, koska tietokoneen käyttäjän oma salasana on hauska, eikä hän sen vuoksi halua vaihtaa sitä. Hakkerointi sähköpostiin ei motivoi vaihtamaan sähköpostin salasanaa vahvemmaksi, koska tietokoneen käyttäjä ei ajattele hakkeroinnin olevan mitenkään suuri ongelma.

Tarpeiden ja motiivien määrittely
Koska prosessi pysähtyy tason 1 jälkeen, tietokoneen käyttäjä ei myöskään päädy tasolle 2 eli epävarmuuden tasolle Tietokoneen käyttäjä jakaa tietokoneen käyttöä normaalitilassa, ja käyttöä motivoi aiemmat tietokoneenkäyttötarpeet

Yhteys 6

Yhteys 6 osoittaa että uusi tietoturvatapahtuma mahdollistaa tietokoneenkäyttäjän siirtymän tasolle 2, eli epävarmuuden tasolle

Vaiheessa 6 tietokoneenkäyttäjä kokee uuden tietoturvatapahtuman, esimerkiksi tietoturvaongelman (tietojen vuotaminen sosiaalisesta mediasta, salasanan hakkerointi tai virushyökkäys). Tietoturvatapahtuma voi olla myös se, että markkinoille tulee uusi ohjelma tai uusi mahdollisuus suojata, minkä johdosta tietokoneen käyttäjä ottaa käyttöönsä uuden tehokkaamman/ palveluita sisältävän/käytettävyydeltään paremman virustorjuntaohjelmiston tai uuden sosiaalisen median tietoturva-asetuksen. Tietoturvatapahtuman voi muodostaa tietoisuuden lisääntyminen: tietokoneenkäyttäjä esimerkiksi kuulee suositteluja uudesta paremmasta virustorjuntaohjelmasta.

Kokemus herättää tunteita esim. pelkoa ja pettymystä. Tietoturvatapahtuma ja siihen liittyvät negatiiviset tunteet vaikuttavat siihen, että tietokoneenkäyttäjä siirtyy takaisin epävarmuuden tasolle.

Tarpeiden ja motiivien määrittely
Turvallisuuden tarve, joka määrittää tasoa 3 säilyy tämän yhteyden aikaan ennallaan mutta sen rinnalle tulee rauhallisuuden ja mielen rauhan tarve. Tietokoneenkäyttäjä huomaa, että vaikka hän on käyttänyt tiettyä suojaustoimenpidettä, tämä ei riitä ja hänen täytyy vahvistaa sitä, esimerkiksi tiukennettava sosiaalisen median yksityisyysasetuksia. Mikäli uusi virustorjuntaohjelma on edullisempi kuin entinen, käyttäytymisen muutosta motivoi turvallisuuden tarpeen lisäksi myös säästämisen tarve. Samoin, jos virustorjuntaohjelman vaihtamista motivoi se että entinen virustorjuntaohjelma haittaa eli www-selausta, käyttäytymisen muutosta motivoi turvallisuuden tarpeen lisäksi tutkimisen ja tietämisen tarve

Yhteys 7

Yhteys 7 osoittaa että siirtyminen tasolta 1 suoraan tasolle 3 eli suojaustoimenpiteen käyttöönottoon on mahdollista

Tietokoneen käyttäjä voi siirtyä suoraan tasolta 1 tasolle 3 siinä tapauksessa, että järjestelmä vaatii laatimaan vahvan salasanan. Tietokoneen käyttäjällä ei ole muuta mahdollisuutta kuin laatia vahva salasana jotta pääsee käyttämään järjestelmää. Hän ei päädy epävarmuuden tasolle, koska hän ei pohdi asiaa tietoturvan kannalta. Sen sijaan hän haluaa jatkaa järjestelmän käyttöä normaalisti

6.3.9 Prosessin tasot

Tässä luvussa esitellään yksityiskohtaisesti tietoturvakäyttäytymisen muutosta selittävän prosessin 4 tasoa: tietokoneenkäyttö normaalitilassa, epävarmuuden taso, suojaustoimenpiteen käyttöönotto sekä poikkeaminen suojaustoimenpiteen käytöstä. Luvussa myös kuvataan tietokoneen käyttötarkoitukset (tasolla 1), käyttäytymistä motivoivat tarpeet ja elementit, joiden kanssa tietokoneen käyttäjä toimii eri tasoilla interaktiossa.

Taso 1. Tietokoneen käyttö normaalitilassa

Tasolla 1 tietokoneen käyttäjä käyttää tietokonetta seuraavissa käyttötarkoituksissa

- kommunikointi ystävien, tuttujen ja sukulaisten kanssa (sosiaalinen media, sähköposti, pikaviestipalvelut)
- oman työn markkinointi
- liiketoiminnan kehittäminen ja työnteko
- opiskelu
- yhdistystoiminta
- verkkopankin käyttö
- verkkokaupan käyttö
- tiedonhaku
- uusien asioiden opettelu
- ajanviete / viihtyminen (pelaaminen, musiikin kuuntelu, elokuvien katselu)
- asioiden hoitaminen esimerkiksi työnantajien, liiketuttavien, pankin ja viranomaisten, koulun ja työnantajien kanssa
- aineiston tallennus (esim. kuvien, muistiinpanojen, kaunokirjallisten tekstien, videoiden ja musiikin)

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko

- omaisuus
- tietolähde
- edistäjä
- suojatoimi
- uhka

Tarpeet, jotka motivoivat käyttäytymistä

- liittymistarve (need for relatedness) (Alderfer)
- itsensä toteuttamisen tarve (Maslow)
- henkilökohtaisen kasvun tarve (Alderfer)
- uteliaisuuden tarve (Reiss)
- tietämisen ja ymmärtämisen tarve (Maslow).
- sosiaalisen arvostuksen tarve (Maslow)
- tarve sosiaalisiin yhteyksiin (Social contact) (Reiss)
- hyväksynnän tarve (acceptance) (Reiss)
- esteettisyyden tarve (Maslow, Reiss).
- säästämisen tarve (Reiss)
- toimeentulotarve (Alderfer)
- ajan ja vaivan säästäminen
- asiointi

Tällä tasolla kuvataan, mihin tarkoitukseen henkilö käyttää tai on aloittamassa käyttämään tietokonetta. Tietokoneen käyttäjä käyttää tietokonetta esimerkiksi yhteydenpitoon ystäviensä kanssa sosiaalisen median tai sähköpostin kautta. Hän käyttää tietokonetta myös liiketoiminnan edistämiseen kuten esimerkiksi liiketoiminta-asiakirjojen talletukseen, sekä lisäksi verkkokauppa-asiointiin, opiskeluun, kuvien tallentamiseen, Internet-sivujen katseluun ja pelaamiseen.

Searlen ajattelussa tietokoneen käyttö normaalitilassa on kokemus-vaihetta eli tietokoneen käyttäjä toimii interaktiossa eri elementtien kanssa mutta ei vielä ajattele kokemuksen tarkoituksellisuutta oman tietoturvansa kannalta.

Yhteydenpito perustuu Alderferin ERG - teoriassa liittymistarpeeseen (need for relatedness), Maslowilla yhteenkuuluvuuden tarpeeseen ja itsensä toteuttamisen tarpeeseen sillä sosiaalisessa mediassa keskustellaan harrastuksiin liittyvistä asioista. Somen avulla voi myös oppia uusia asioita kuten käsitöitä. Twitterin käyttöä määrittelee uteliaisuuden tarve (Reiss) uteliaisuus tätä palvelua kohtaan. Liiketoiminnan edistäminen pohjautuu Maslow: n (1954) jaottelussa kehittymisen tarpeeseen eli henkilöllä on tarve kehittää omia taipumuksiaan ja käyttää omia voimavarojaan (Vuorinen & Tuunala, 1995). Tietokoneen käyttö työntekoon perustuu toimeentulon tarpeeseen (Alderfer) Verkkokauppa-asiointi ja verkkopankkiasiointi perustuvat itsensä toteuttamisen tarpeeseen, Alderferin ERG- teoriassa henkilökohtaisen kasvun tarpeeseen (Maslow, 1954, Robbins, 1993). Verkkokaupasta hankitaan esim. harrastuksiin liittyviä tuotteita. Verkkokauppa on vaivaton ja nopea tapa saada tuotteet itselle.

Esimerkiksi verkkopalvelu auttaa saamaan nopeasti musiikkia puhelimeen (ajan ja vaivan säästämisen tarve). Verkkokaupassa voi myös säästää rahaa, jolloin käyttäytymisen taustalla vaikuttaa säästämisen tarve (Reiss). Tiedonhaku perustuu Reiss:n (2004) motiiviteoriassa uteliaisuuden tarpeeseen (ks. myös Mustonen, 2001). Tiedollisten motiivien perusta on myös itsensä toteuttamisen tarpeessa (Maslow, 1954) ja henkilökohtaisen kasvun tarpeessa (Robbins, 1993). Opiskelun voidaan katsoa pohjautuvan tietämisen ja ymmärtämisen tarpeeseen (Maslow, 1954).

Playstation-pelien pelaaminen ja musiikin kuuntelu pohjautuu itsensä toteuttamisen tarpeeseen (Maslow, 1954) Pelejä tilataan, koska pelaaminen on huvia ja hyvää ajanvietettä. Pelaamista selittävät toisaalta Alderferin luokittelussa liittymisen tarve (Robbins, 1993) ja Maslowin luokittelussa sosiaalisen arvostuksen motiivit. Reiss:n motivaatioluokittelussa (2004) pelaaminen selittyy tarpeella sosiaalisiin yhteyksiin (Social contact) ja hyväksyntään (acceptance). Playstation-pelejä pelataan koska kaveritkin pelaa ja koska halutaan saada arvostusta ja hyväksyntää muiden pelaajien keskuudessa.

Kuvien tallentaminen pohjautuu esteettisyyden eli kauneuden kokemisen tarpeelle (Maslow, 1954, Reiss, 2004). Henkilö tallentaa kuvia tietokoneelleen, koska kokee ne jollain tavalla merkitykselliseksi itselleen. Erilaisia työhön liittyviä aineistoja kuten video- ja äänitiedostoja tallennetaan koska halutaan vakuuttaa omaa työtä. Tässä tarpeen taustalla toimii toimeentulon tarve (Alderfer) Tietoturvakäyttäytyminen voi tällä tasolla olla riskialtista, esimerkiksi siten, että henkilö lähettää arkaluontoista tietoa sähköpostissa tai jättää liiketoimintadokumentit varmuuskopioimatta.

Taso 2: Epävarmuus

Tasolla 2 tietokoneen käyttäjän kokemus (tietoturvaongelma, tietoturvatietoisuuden lisääntyminen, muutos tietokoneen käytössä) aiheuttaa muutoksen ajattelussa ja hän pohtii tapahtuman merkitystä oman tietoturvansa kannalta. Tällä tasolla henkilö huomaa, että omaa tietoturvakäyttäytymistä on aihetta muuttaa.

Tarpeet jotka motivoivat käyttäytymistä
– rauhallisuuden ja mielen rauhan tarve (Reiss)

Samanaikaisesti henkilöllä säilyy tasolla 1 esitellyt tietokoneenkäyttötarpeet eli

- liittyminen
- itsensä toteuttaminen
- henkilökohtainen kasvu
- uteliaisuus
- tietäminen ja ymmärtäminen
- sosiaalinen arvostus
- sosiaaliset yhteydet
- hyväksyntä

- esteettisyys
- säästäminen
- toimeentulo
- ajan ja vaivan säästäminen
- asiointi

Taso vastaa Searlen ajattelussa tarkoituksellisuus-vaihetta eli henkilö pohtiii tietoturvakokemuksen merkitystä oman tietoturvansa kannalta ja mitä hänen kannattaisi tehdä parantaakseen tietoturvaansa.

Tietokoneen käyttö on tuonut esille tietoturvaongelmia tai -haasteita, ja tietokoneenkäyttäjässä herää rauhallisuuden ja mielen rauhan tarve. Henkilö haluaa päästä eroon epävarmuutta aiheuttavista asioista:

> *K: Sää vähän naurahtelit sille, että onko tämä nyt liioteltua, mutta sitte sää kysyit siltä sun siskon pojalta, nii se sit sai vakuutettua, et se on ihan, että kannattaa ottaa.*
> *V: Nii justiin, että ota, jos susta tuntuu siltä. Että ainaki saa semmosen mielenrauhan.*

Facebookin käyttöä aloittaessaan tietokoneen käyttäjä pohtii yksityisyysasioita ja facebookin yksityisyysasetusten määrittämistä. Hän ei halua, että ulkopuoliset näkevät hänen kuviaan ja päivityksiään Facebookissa. Hänellä ei ole kokemusta julkisesti esillä olemisesta, joten hän ei halua myöskään Internetin kautta levittää tietojaan kaikkien luettavaksi ja nähtäväksi.

Kokemus facebook-profiilin kopioinnista vaikuttaa tietokoneen käyttäjään siten, että hän haluaa jatkossa välttää identiteetin kopioimisen ja siitä aiheutuvat seuraukset, roskapostin ja facebook-profiilin kopioimisen. Facebookin yksityisyysasetusten määrittämisen merkitys voidaan hoksata myös Facebookin järjestämän tietoturvakampanjan myötä. Tietokoneen käyttäjä haluaa säännöllisesti käydä tarkistamassa hakukoneella mitä hänestä on näkyvillä Internetissä. Hän haluaa suojata yksityisyyttään ja estää paikkansapitämättömien asioiden esilläolemisen netissä jotta hänestä ei muodostu vääristynyttä kuvaa niiden perusteella. Hän haluaa suojata myös työnantajaansa liittyviä tietoja. Muutos elämäntilanteessa (suuntautuminen työelämään) vaikuttaa tietokoneen käyttäjään siten, että hän kokee tärkeämmäksi kuin ennen tutkia mitä hänestä on näkyvillä Internetissä.

Tietokoneen käyttäjä on kuullut ja kokenut mitä siitä seuraa, jos arkaluontoisia viestejä päätyy ulkopuolisille, joten hän pohtii sähköpostin käytön rajoittamista. Tietokoneen käyttäjä kokee tärkeäksi estää sen, ettei hänen tietojaan vuoda ulkopuolisille. Tietokoneenkäyttäjä lähettää arkaluontoista tietoa sosiaalisessa mediassa / pikaviestipalvelussa. Ystävät varoittelevat tästä, mikä saa pohtimaan sensitiivisen tiedon prosessoinnin rajoittamista netissä. Kuultuaan nettikiusaamisesta tietokoneen käyttäjä kokee tärkeäksi rajoittaa omien tietojen lisäämistä nettiin, ettei joudu nettikiusaamisen uhriksi.

Sosiaalisen median ja sähköpostin käytön aloitus herättää ajatuksia ja pohdintoja siitä, kuka tietoihin pääsee käsiksi. Osallistuminen tietoturvaluennolle saa pohtimaan sitä, kuinka tärkeää on välttää esimerkiksi potilastietojen välittämistä sähköpostissa.

Kun tietokoneen käyttäjä alkaa käyttää verkkopankkia, hän saa tietoa vahvan salasanan merkityksestä pankin nettisivuilta. Hän kokee, että on tärkeää laatia vahva salasana verkkopankkiin, jotta rahat säilyvät tallessa. Tämän lisäksi tietokoneen käyttäjä pohtii myös sitä, että vahva salasana on tärkeää ottaa käyttöön myös henkilökohtaisessa sähköpostissa, jonka kautta välitetään sensitiivistä tietoa. Sähköpostin hakkerointi saa tietokoneen käyttäjän pohtimaan omien salasanojensa vahvuutta ja että on tärkeää vahvistaa salasanoja entisestään. Hän haluaa estää tärkeän tiedon katoamisen ja päätymisen eitoivotuille henkilöille ja www-sivuille sekä sen että joku esiintyy hänen identiteetillään ja esimerkiksi lähettää sähköposteja hänen nimissään. Jos tietokoneen käyttäjä on pitänyt pitkään samaa salasanaa ja kirjautunut julkisille koneille, hän kokee tärkeäksi lisätä salasanaansa ”digitejä” jotta se olisi vahvempi.

> *V: Se hyöty mulle ainaki itelleni on, et mää voin olla rauhallisella mielillä. Jos sattuu niin, että se mun sähköposti menee väärään paikkaan, että sitte ei ainakaan tuu, että joku sais tietää jotaki semmosta arkaluontosta. Saa olla huolettomana siitä.*

Tietojen menettäminen varmuuskopioinnin puuttumisen seurauksena, ystävän kokemus tietojen menetyksestä tai varmuuskopioinnin hyödyistä kuuleminen motivoivat pohtimaan varmuuskopioinnin aloittamista. Tietokoneenkäyttäjä on nähnyt paljon vaivaa esimerkiksi opiskeluun liittyvien dokumenttien ja artikkelipohjien valmisteluun, joten ei halua menettää niitä varmuuskopioinnin puuttumisen takia:

> *K: Että missä määrin nämä sitte tämmösen turvaamiskeinot, sensitiivisen aineiston välttäminen, että sitä ei prosessoi avoimesti ja sitte on nämä virustorjunnat ja varmuuskopioinnit ja nämä, nii missä määrin nämä täyttää semmosen mielenrauhan tavoitteen? Että sää haluat olla rauhassa, ettei tarvi miettiä tämmösiä?*
> *V: Joo, kyllä siis siinä mielenrauhassa nyt varmuuskopioinnin kannalta, että jos kone menee syystä tai toisesta lunastuskuntoon, eikä saa enää mitään tietoja saa takasi, niin ne on jossain muuallaki ne tiedot. Se on mielenrauha on se.*
> *K: Että saa olla huoleti?*
> *V: Niin, saa olla huolehtimatta siitä asiasta.*

Negatiiviset kokemukset verkkokaupassa (esim. kokemus rahanmenetyksestä musiikkipalvelussa, huijaus asunnon vuokraamisessa ja ystävän kokemus (hakkerointi)) tekee varovaisemmaksi verkkokauppojen suhteen. Tietokoneen käyttäjä esimerkiksi haluaa toimia vain luotettavien toimijoiden kanssa. Tietokoneen käyttäjä ei halua tulla huijatuksi eikä menettää rahaa. Hän ei halua myöskään ylimäärästä vaivaa siitä, että rahanmenetystä pitää selvitellä eikä tiliä voi käyttää vähään aikaan. Jos tietyssä verkkokaupassa on ongelmia, tietoko-

neenkäyttäjä harkitsee kyseisen kaupan käytön lopettamista. Tietokoneenkäyttäjä haluaa toimia vain luotettavien toimijoiden kanssa.

Tietokoneen käyttäjä haluaa välttää ongelmat, joita kokenut virusten takia (esimerkiksi koneen saastuminen/ rikkoutuminen) ja torjua koneensa viruksilta tehokkaammin sekä välttää pankkitunnusten kaappaamisen ja salasanojen kopioimisen. Hän on saanut tietoa viruksista ja niiden haitallisista seuraamuksia sekä virustorjuntaohjelmista Internetistä, ystäviltä ja muulta lähipiiriltä. Hän pohtii virustorjuntaohjelman asentamista.

Taso 3: Suojaustoimenpiteen käyttöönotto

Käyttäytyminen muuttuu. Searlen teoreettisiin ideoihin pohjautuen tämä taso kuvastaa käyttäytymisen muutos-vaihetta. Tietokoneen käyttäjä ottaa käyttöön jonkin seuraavista tietoturvasuojaustoimenpiteistä

- Alkaa varmuuskopioida tärkeitä aineistoja
- Vahvistaa virustorjuntaa
- Laatii vahvemman salasanan
- Tarkentaa omaan Internet-profiiliaan
- Tulee varovaisemmaksi verkkokauppa-asioinnissa
- Välttää lähettämästä sensitiivistä aineistoa sähköpostissa /sosiaalisessa mediassa

Tarpeet, jotka motivoivat käyttäytymistä tasolla 3:

Maslow:n (1954 & 2007) tarvehierarkiassa tarve suojata omaisuutta pohjautuu turvallisuuden tarpeeseen: henkilö haluaa tuntea olonsa varmaksi ja turvatuksi. Hän haluaa olla vapaa huolesta ja pelosta ja turvata omaisuutensa (esimerkiksi raha, työpaikka, terveys). Myös uteliaisuuden tarve (Reiss) selittää käyttäytymistä joissakin tapauksissa kun henkilö etsii omia tietoja Internetistä.

Taulukko 13 sisältää koosteen siitä, mitä turvallisuuden tarpeella eri käyttäytymistyypeissä tarkoitetaan.

TAULUKKO 13 Turvallisuuden tarve eri käyttäytymistyypeissä

Käyttäytymistyyppi	**Mitä turvallisuuden tarve tässä käyttäytymistyypissä tarkoittaa**
Internet-profiilin hallinta	Tarve yksityisyyden ja identiteetin suojaamiseen Internetissä. Henkilö ei halua jakaa yksityiselämäänsä liittyviä tietoja Internetissä julkisesti.
Sensitiivisen aineiston prosessointi sähköpostissa /sosiaalisessa mediassa	Tarve suojata sähköpostissa ja sosiaalisessa mediassa ihmissuhteisiin liittyvää tietoa, potilastietoja, henkilötunnuksia, verkkokauppaan liittyviä tietoja, tilinumeroa, ja yhteystietoja kuten puhelinnumero tai osoite sekä lomiin liittyvää tietoa (milloin on poissa kotoa).
Vahvan salasanan laatiminen	Tarve suojata rahaa verkkopankissa ja kriittistä informaatiota sähköpostissa, esimerkiksi henkilökohtaisia viestejä ja ostokuitteja sekä identiteettiä ja omaa henkilöhistoriaa.
Varmuuskopiointi	Tarve suojata omaisuutta kuten liiketoiminta-asiakirjoja, artikkelipohjia, opiskeluun liittyviä asiakirjoja ja kuvia tuhoutumiselta tai häviämiseltä.
Varovaisuus verkkokaupassa	Tarve suojata rahaa ja luottokorttitietoja noudattamalla varovaisuutta verkkokauppa-asioinnissa.
Virustorjuntaohjelman asentaminen	Tarve suojata omaisuutta kuten tietokonetta ja sinne talletettuja tietoja kuten salasanoja ja pankkitunnuksia.

Alderferin ERG-teoriassa turvallisuuden tarve sisältyy toimeentulotarpeeseen (Robbins, 1993).

Näiden lisäksi käyttäytymistä motivoivat tason 1 tarpeet eli

- liittyminen
- itsensä toteuttaminen
- henkilökohtainen kasvu
- uteliaisuus
- tietäminen ja ymmärtäminen
- sosiaalinen arvostus
- sosiaaliset yhteydet
- hyväksyntä
- esteettisyys
- säästäminen
- toimeentulo
- ajan ja vaivan säästäminen
- asiointi

Tietokoneen käyttäjä käyttää tietokonetta esimerkiksi liiketoiminnan edistämiseen, koska hänellä on toimeentulon tarve. Hän kokee tärkeäksi suojata käsittelemänsä liiketoimintadokumentit varmuuskopioinnilla, mikä pohjautuu turvallisuuden tarpeelle, tarpeelle suojata omaisuutta. Tällöin tietokoneen käyttäjä huomioi sekä toimeentulon tarpeen että turvallisuuden tarpeen samanaikaisesti.

Taso 4. Poikkeaminen suojaustoimenpiteen käytöstä
Omaksuttuaan jonkin tietyn tietoturvasuojaustoimenpiteen, tietokoneen käyttäjä voi joko väliaikaisesti tai pysyvästi muuttaa käyttäytymistään:

Pysyvä poikkeaminen
- Varovaisuus verkkokaupassa vähenee
- Sensitiivisen tiedon prosessointi lisääntyy
- Teknologinen vahvistaminen,
- Varmuuskopioinnin laiminlyönti

Käyttäytymistä motivoivat liittyminen, turvallisuus, itsensä toteuttaminen, riippumattomuus
Väliaikainen poikkeaminen

- Virustorjunnan laiminlyönti
- Heikko salasana
- Varmuuskopioinnin laiminlyönti
- Sensitiivisen tiedon prosessointi

Käyttäytymistä motivoivat liittyminen, asiointi, ajan ja vaivan säästäminen. Käyttäytymistä motivoi poikkeustilanteissa myös erilaiset tunteet: pelko, huoli, pettymys, hämmennys, välinpitämättömyys. Tietoturvaongelma sosiaalisessa mediassa aiheuttaa tietokoneen käyttäjässä pelkoa ja sensitiivisen tiedon vuotaminen ulkopuolisille hämmennystä. Myös sensitiivisen tiedon lähettäminen sähköpostissa huolestuttaa, mutta tämä ei vaikuta henkilön käyttäytymiseen eli henkilö tästä huolimatta lähettää tiedot, koska hänellä ei ole muuta vaihtoehtoa ja toisaalta riski sille, että joku väärinkäyttää tietoa (tilinumero) on pieni. Virustorjuntaohjelman tehottomuus aiheuttaa pettymystä

Tasolla 4 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa (taulukko 14):

TAULUKKO 14 Taso 4 ja interaktiot

Elementti	**Variaatiot elementeistä eri käyttäytymis-tyypeissä**
tietokone	tietokone toimii 1) yhteydenpidon 2) verkkokauppa-asioinnin 3) sähköisen tiedonhaun mahdollista-jana sekä 4) virushyökkäyksen kohteena
tietoverkko	1) tietokoneen eri käyttötarkoitusten, 2) tietoturvauhkien ja 3) sähköisen tiedonvälityksen mahdol-listaja
omaisuus	1) tietokone ja sinne talletetut tiedot 2) sensitiivinen tieto sosiaalisessa medi-assa ja sähköpostissa 3) tilitieto 4) raha 5) identiteetti
tietolähde	1) uutiset 2) palveluntarjoaja (sosiaalinen media) 3) ystävä
uhka	pahantahtoinen henkilö, joka varastaa tieto-ja ja linkittää niitä vääriin yhteyksiin
harmillinen seuraamus	1) identiteettivarkaus 2) omien tietojen käyttö väärissä yhteyksissä 3) rahanmenetys verkkokaupassa

Pysyvä käyttäytymisen muutos tapahtuu suojaustoimenpiteen omaksumisen jälkeen seuraavista syistä (kohdat 1-3):

1) TARPEIDEN PRIORISOINTI: Uhkan kokemuksen väheneminen

Internet-pohjaisen palvelun (esimerkiksi sähköposti tai sosiaalinen media) käyttö voi alkaa ajan kuluessa tuntua tietokoneen käyttäjästä niin tutulta, että hän ei enää mieti mitä palveluihin kirjoittaa. Tämän voi tulkita siten, että henkilö kokee uudet asiat uhkaavampina kuin tutut asiat. Aluksi kun palvelun käyttö on uutta, henkilö pohtii sitä, ketkä pääsevät näkemään hänen kirjoittamiaan viestejä. Ajan kuluessa hän lakkaa ajattelemasta, että viestien päätymisessä ulkopuolisille olisi jotain vakavaa haittaa. Tämä pohdinta johtaa suojaustoimenpiteen laiminlyöntiin:

> *K: Sitten ku aattelee tätä tietoturvakäyttäytymistä niin miten kuvailisit sitä ite, miten se on ehkä lisääntyny tai onko lisääntyny vuosien kuluessa? Ootko sä heränny aatteleen enempi näitä asioita vai onko se pysyny samana?*

V: Ehkä toisin päin, musta on ehkä tullu vähän huolettomampi.

K: Ootko sä (-)[00:41:43 pp] miettiny että miksi-

V: Ku mä oon välillä just miettiny sitä että ei mulla siellä nyt mitää niin huippusalaisia juttuja oo että vaikka ne ny jonneki meniskin niin joku mun paskanlätinä kavereitten kanssa [nauraa], nii mitä sitte. Mutta sitä, joo nimenomaan näin.

K: Elikä siit ei ois mittää haittaa vaikka sun viestit päätys jonneki?

V: No oishan se asteen verran epämiellyttävää mutta ei siitä varsinaisesti haittaa ois.

K: Kun vertaa johonkin terveystietoihin tai tämmösiin niin onhan se vähän eri asia sitte. Mitkä muut asiat vaikuttaa tähän että susta on tullu huolettomampi? Jos sä aluks olit tarkempi?

V: Asiat on tullu tutummaksi.

Tässä esimerkissä esiintyy ristiriita poikkeuksellisen käyttäytymisen aiheuttavan tarpeen (liittymistarve) ja suojaustoimenpiteiden käyttöönottoon liittyvän tarpeen välillä eli turvallisuuden tarve, tarve suojata omaisuutta jää taka-alalle, koska henkilö ei koe enää niin tärkeäksi kuin ennen välttää sensitiivisen informaation lähettämistä Internetissä.

2) TARPEIDEN PRIORISOINTI: Luottamuksen lisääntyminen

Verkkokauppakäyttäytymisessä luottamuksen lisääntyminen verkkokauppaa kohtaan selittää käyttäytymisen muutosta. Aluksi tietokoneen käyttäjä pyytää paperilaskun ostoksistaan mutta verkkokauppojen yleistyttyä hän luopuu paperilaskusta. Yleinen suhtautuminen verkkokauppoihin muuttuu myönteisemmäksi:

K: Jos aattelee tota verkkokauppaa, kun nää teet ostoksia niin ootko miettiny näitä tietoturva-asioita siinä ostoksia tehessäsi?
V: Joo, kyllä oon.
K: Millä tavalla oot miettiny tai ottanu ne huomioon?
V:Sillon ihan aluksi tilasin lähinnä semmosista missä tuli lasku mukkaan, ettei tarvinnu antaa mitään tietoja minnekään. Mutta nyt oon, oon kyllä tillaillu aika sujuvasti. Ehkä se että mun mielestä siinä jo ku vähän kattoo sitä putiikkia mistä on tillaamassa niin saa jonku näkösen käsityksen että minkälainen kauppa on. Ja tietenkin se että mä monesti tillaan samoista liikkeistä mistä oon tilannu aikasemminki mitkä oon kokenu hyviksi ja turvallisiksi. Mut PayPal-tiliä mulla ei oo. Sitten jos sitä on joskus tarvinnu, sitte ollaan tehty sillai että, miehen PayPal-tilin kautta.
K: Kun sää muutit sit käyttäytymistä niin muistatko että mikä sai sut muuttamaan siihen ettet sä pyytäny enää sitä laskua? Ku miettii näitä vaiheita tässä käyttäytymisessä, niin miks sä luovuit siitä paperilaskusta?

V: Ehkä ne alko siinä vaiheessa ylipäätänsä yleistymään ja koin sitte sen että jos tilaa jostain tommosesta vähän isommasta lafkasta niin kyllä niillä täytyy olla ne asiat aika lailla kunnossa jos laajalle määrää ihmisiä markkinoi. Sitte taas pienet putiikit mistä oon tilannu, ne on aika pitkälti ollu kotimaisia et jos tullee jotaki ongelmaa niin on sitte helepompi selevittää.

Itsensä toteuttamisen tarve on tässä esimerkissä ristiriidassa suojaustoimenpiteen taustalla olevan tarpeen kanssa, eli kun henkilö aloittelee verkkokaupankäyttöä, hän pyytää ostoksistaan aina paperilaskun, jolloin omien tietojen lähettämistä ei vaadita. Ajan kuluessa henkilö ei koe enää niin tärkeäksi suojata omaisuuttaan (maksamisen yhteydessä vaadittavat tiedot) koska luottamus verkkokaupankäyntiin lisääntyy.

3) TARPEIDEN PRIORISOINTI: Riippumattomuus

Tietokoneen käyttäjä voi aluksi olla tarkempi siitä mitä kirjoittaa sosiaaliseen mediaan, mutta hän voi myöhemmin luopua tästä periaatteesta pysyvästi:

K: Mikä siihen on vaikuttanu?
V: Ihan suurimmassa yksinkertaisuudessaan se, että kun ei voi koskaan miellyttää samanaikasesti kaikkia ihmisiä, nii sitte on vaan hyväksyttävä se, että vaikka kuinka hienotunteisesti ja poliittisesti korrektisti haluaisiki kirjottaa, niin aina, aina on joku, joka saa siitä sitte pahan mielen. Niin koettaa lähinnä tuoda itsensä selväksi, käyttää faktoja ja näin eespäin.

Tätä poikkeusta selittää riippumattomuuden/ itsemääräämisoikeuden tarve (Reiss). Tietokoneen käyttäjä haluaa olla riippumaton muiden ihmisten mielipiteistä, ja riippumattomuuden tarve muodostaa ristiriidan suojaamistarpeiden kanssa.

Seuraavissa tapauksissa henkilö poikkeaa omaksutusta suojaustoimenpiteestä väliaikaisesti (kohdat 4-10).

4) TARPEIDEN PRIORISOINTI: Tietojen/tiedostojen priorisointi

Sensitiivisen aineiston prosessointia ja varmuuskopiointia selittää sama poikkeustilanne: tietokoneenkäyttäjä jaottelee tiedot ja tiedostot tärkeisiin ja eitärkeisiin, ja suojaa tärkeät tiedot tarkemmin. Esimerkiksi jos tietokoneen käyttäjän työstämä dokumentti jää keskeneräiseksi, sitä ei koeta tärkeäksi varmuuskopioida, koska työtä tullaan jatkamaan myöhemmin (esimerkki 3). Vastaavanlaista tietojen jaottelua toteutetaan sosiaalisen median puolella. Jos kyseessä on esimerkiksi Instagram tai LinkedIn, teksti on asiallisempaa, kun taas sellaiseen mediaan, jossa on itselle läheisiä ihmisiä, kirjoitetaan vapautuneemmin (esimerkki 1). Samoin silloin, kun kommunikoidaan Internet-pelissä online-

persoonan nimissä, viestit ovat arkaluontoisempia kuin sosiaalisessa mediassa oikean elämän persoonan nimissä kirjoitetut viestit (esimerkki 4)

Esimerkki 1

K: Sitten noista sisällöistä, mitä nää kirjoittelet somepalveluihin ja sähköposteihin, niin mietikkö sää hirveen tarkasti, että mitä sää sinne laitat vai ooks sää aika huolettomasti laitellu tietoja sinne?
V: Mä oon rajannu aika pitkälti muutamissa sosiaalisen median palaveluissa sen, että minkälaisia juttuja mää laitan. Et sitte semmoset… vapautuneemmin tietysti puhuu semmosissa, missä on lähinnä lähipiiri.
--
Sitten, jos aattelee jotain Twitteriä tai vastaavaa, Instagramia, niin kyllähän se on niin sanotusti painokelpoisempaa se ilmaisu, mitä sinne jakaa, koska ne on niin paljon selkeämmin muitten nähtävillä.

Esimerkki 2

K: Elikkä sulla on semmonen osittainen varmuuskopiointi nyt käytössä. Mitä sää et varmuuskopioi sitte?
V: Vaikka semmosia, jos mää teen jonku jutun ja jos ei se oo tärkee. Semmonen, mikä pitää panna eteenpäin arvioitavaksi. Sit mä lähetän, mä [konsaan? 00:44:35] siitä takas jonku jutun. Mun pitää lähettää joku asia johonki. Jos mä saan siitä vielä takas jonku vastauksen. Niitä mä en yleensä varmuuskopioi.

Esimerkki 3

K: Onko tämä (varmuuskopiointi) ihan systemaattista vai tuleeko semmosia poikkeustilanteita...?
V: Ei tule.
K: Että se on aina?
V: [nauraa] Valokuvien kohalla.
K: Että ei missään nimessä. Entä sitten nämä tekstidokumentit, nii onko sille sama, että aina kahteen paikkaan vai tuleeko siinä [?? 00:47:09] [päällepuhuntaa]?
V: Se on tietysti vähän riippuen, mitenkä on muokattavissa. Valmiita tekstejä tallennan tuplasti, mutta sitten ne, jotka on keskeneräsiä, niitä en välttämättä joka kerta.
K: Mikset sää niitä sitte tallenna?
V: En mää tiiä. Kai se on se keskeneräisyyen ajatus, että sitte vielä jatkaa. Se on ihan hyvä kysymys, miksihän niitä ei sitte.

Esimerkki 4

K: Voiko tästä nyt päätellä, että sää Facebookiin laitat vähempi tietoa ku sinne peliin, ku aattelee asioitten sensitiivisyyttä?
V: Oikeestaan tietyssä mielessä kyllä.

K: Miksi?
V: Siis Facebookiin...
K: Miksi sää laitat sitä arkaluontosempaa sinne peliin?
V: Mutta se on erilaista, koska se on... Tää Facebook ikään ku on tää mun arkipersoona, oikean elämän persoona.

Tämän poikkeustilanteen kohdalla syntyy tarpeiden välinen ristiriita liittymistarpeen ja suojaamistarpeiden kanssa (henkilö lisää sensitiivistä tietoa sosiaaliseen mediaan ja nettipeliin). Toisaalta tietämisen ja ymmärtämisen tarve on ristiriidassa suojaamistarpeiden kanssa eli henkilö ei laadi varmuuskopioita kaikista kirjoittamistaan dokumenteista.

5) TARPEIDEN PRIORISOINTI: Muistamiseen liittyvät ongelmat

Väliaikaista suojaustoimenpiteen laiminlyöntiä voi aiheuttaa unohtaminen, eli henkilö unohtaa esimerkiksi varmuuskopioinnin. Tällöin ei myöskään tarpeiden välistä ristiriitaa ilmene vaan henkilöllä säilyy tarve suojata koneellaan olevia tiedostoja tilapäisestä unohtamisesta huolimatta. Varmuuskopiointi muistuu uudelleen mieleen tietoturvaongelman jälkeen tai jos käyttäjä huomaa, ettei ole ottanut varmuuskopioita pitkään aikaan:

V: Kyllä mä oon jonkin verran tehny sitä (varmuuskopiointi) sillon jo sanotaanko et sillon ku tuli opiskelemaan alko olla sellasia tiedostoja mitä opiskeluasioista halus pitää tallessa. Kyllä niitä sitte on kopioinu johonki CD:lle tyyliin. Ottanu vaan aika silleen ei hirveen miten sen nyt sanois suunnitellusti. Huomannu vaan että jaa mä en oo näitä juttuja laittanu varmaan mihinkään talteen viimeseen puoleentoista vuoteen että laitetaanpa ne nyt. Aina sillon kun jollaki kaverilla hajoaa kovalevy koneesta niin sitte aina hei pitäiskö munki kopioida nämä?

Sen sijaan, jos tietokoneen käyttäjä laatii heikon salasanan sen vuoksi, että hänellä on ongelmia salasanan muistamisessa, käyttäytymistä motivoi liittymisen tarve (kun kyseessä on esimerkiksi salasana sosiaaliseen mediaan) ja tietämisen tarve (kun kyseessä on www-tiedonhaku). Tällöin muodostuu ristiriita suojaamistarpeiden ja poikkeuksen aiheuttavien tarpeiden välille.

K: Ookko nää tavallaan muuttanu sitä salasanaa vuosien kuluessa..
V: No ehkä pari kertaa sitäki että kun en oo ite muistanu nii helpommaks.
K: Onko sieltä tullu jotain muistutuksia sitte?
V: Ei oo tullut mutta ei oo vaan muistanu niin ei saa sähköpostia auki. Siis et se on vaa.. Mutta nythän se tulee älypuhelimeen niin se on siinä hyvä älypuhelimeen, ite asias mä en ees tiiä muistanko mä mun sähköpostin niin se on hyvä ku pystyy aukaseen sen, ja älypuhelimestaha näkee suoraa mutta justiisa ku on monia, on näitä tunnuksia ja, salasanoja nii ei muista kaikkia. Se siinä on kyllä hankalaa.

6) TARPEIDEN PRIORISOINTI: asian toimittaminen

Vaikka henkilö ei yleensä välitä sensitiivistä tietoa sähköpostissa, hän kuitenkin voi lähettää arkaluontoista tietoa sähköpostissa, jos hän kokee, ettei hänellä ole muuta tapaa toimittaa asiaa (ks. esimerkki 1) tai hän kokee että hänen henkilöllisyyttään ei voida muuten todistaa

> *I: Has there been any exceptions sometimes that..?*
> *R: (There) [0:37:41.1] has been. I mistakenly paid my bill to another company's account, and I had to send the payment information through e-mail. So that was pretty much, I thought about it but then I just realised that there's no other way I could send it so..*
> *I: So what kind of worries you had that, what could happen?*
> *R: I had to send my account number. But then again, no one really does anything with just my account number, because, he can't go to the bank and, OK, I have this account number, I wanna take all the money he or she has. But still it's a bit sensitive information.*

Em. esimerkissä poikkeuksen aiheuttava tarve eli asioinnin tarve on ristiriidassa turvallisuuden tarpeen kanssa, eli henkilö välittää pankkitietoja vaikka yleensä suojaa omaisuuttaan eli sensitiivistä tietoa sähköpostissa. Tietojen lähettäminen aiheuttaa huolta, mutta tietokoneen käyttäjä päättelee, ettei kukaan voisi saada vahinkoa aikaan pelkästään hänen tilinumerollaan.

7) **TARPEIDEN PRIORISOINTI: palvelun käytön lyhytkestoisuus**

Jos Internetissä olevan palvelun käyttö on lyhytkestoista (esimerkiksi tietokoneen käyttäjä kirjautuu keskustelupalstalle, jota tietää käyttävänsä vain muutaman kerran kuten Netflix ja suoratoistopalvelut) hän voi laiminlyödä suojaustoimenpiteen eli vahvan salasanan käytön väliaikaisesti. Hän ajattelee, ettei tarvitse olla huolissaan vahvasta salasanasta muutaman kirjautumisen takia. Palveluihin joissa on tärkeää tietoa, esimerkiksi omia tietoja tai työhön liittyvää, tai joita käytetään paljon laaditaan vahvempi salasana (sosiaalinen media, koulun sähköposti, nettipokerisovellus jne.):

> *I: So is there any cases that you use your own judgment?*
> *R: Sometimes. For example, picking up a password for some page that I usually (-) [0:36:28.3]. For example, these forums where you have to sign up to write them, and if I know that I only use it for once or twice, I'm not so concerned about password.*

Tässä poikkeuksen aiheuttava tarve eli liittymistarve on ristiriidassa suojaustoimenpiteiden käyttöönottoon liittyvän tarpeen kanssa. Tietokoneen käyttäjä on ottanut vahvan salasanan käyttöönsä, mikä selittyy turvallisuuden tarpeella. On tärkeää laatia vahva salasana verkkopankkiin, jotta rahat säilyvät tallessa.

Samoin on tärkeää käyttää vahvoja salasanoja sähköpostissa, jotta sen kautta välitetty kriittinen tieto ei häviä ja etteivät tiedot päädy ei-toivotuille henkilöille. Kun henkilöllä on tarve liittyä keskusteluun Internet-foorumissa, jota hän tietää käyttävänsä vain muutaman kerran, tai kun hän haluaa katsoa esimerkiksi elokuvan Netflix-palvelusta, hän laatii heikon salasanan. Tällöin turvallisuuden ja omaisuuden suojaamisen tarve jää taustalle ja liittymistarve korostuu. Toisaalta, haastatteluesimerkistä 1 voidaan päätellä, että henkilö haluaa välttää vaivannäköä laatimalla heikon salasanan, jonka muodostamista ei tarvitse miettiä kauaa. Koska henkilö tietää, että tulee käymään tietyllä keskustelupalstalla vain muutaman kerran, hänellä korostuu liittymistarpeen lisäksi myös ajan ja vaivan säästämisen tarve.

8) Vahinko

Vaikka tietokoneen käyttäjä osaa suojata sensitiivistä tietoaan sosiaalisessa mediassa, hän voi joskus vahingossa määritellä tietoturva-asetukset puutteellisesti. Samoin, joskus varmuuskopioinnin yhteydessä saattaa tulla virhe, jonka vuoksi tiedostoja häviää.

Vahingon seurauksena esim. sosiaalisessa mediassa salatuksi tarkoitettuja ihmissuhteita voi päätyä julkiseksi. Tämä aiheuttaa tietokoneenkäyttäjässä hämmennystä:

> *R: At the time it's quite good example. Even though I hided our relationship with him, I didn't check that some persons in Facebook who should have checked if we want to hide to someone. Like we should have checked which person cannot see the information. But I forgot some people. And the person knows the relationship with him, and then I really embarrassed. But anyway..*
> *I: So it's important for you to hide, because you want to avoid of get embarrassed?*
> *R: Yes. Yes, that's right.*

Koska tietojen salaamatta jättäminen perustuu vahinkoon, se ei aiheuta tarpeiden välistä ristiriitaa, vaan henkilöllä säilyy tarve suojata omaisuuttaan (sosiaalisessa mediassa olevia sensitiivisiä tietoja, tietokoneelle talletettuja tiedostoja).

9) TARPEIDEN PRIORISOINTI: Applikaation asentaminen tai ohjelmiston testaaminen

Tietokoneenkäyttäjä voi laiminlyödä virustorjunnan käytön siinä tapauksessa, että hän haluaa testata jotain ohjelmistoa koneellaan, jolloin virustorjunta muodostuu esteeksi:

> *K: Onko sulla joskus ollu virustorjunta pois päältä?*
> *V: On semmosiaki aikoja, mutta ne on vähäisiä.*
> *K: Mikä syy siinä on ollu sitte, että väliaikasesti...?*

V: Joskus on ollu semmosia applikaatioita, joita pikkuohjelmia, jotka virustorjunta varmaan se heuristiikka väärin tulkitsee viruksiksi. Sitte joskus semmosia, että pystyy semmosia ajamaan, nii sitte väliaikasesti tai kokeilee, että ajaa sitä tai tehä sen jonku tietyn jutun, nii sitte väliaikasesti kytkee sen virustorjunnan pois päältä sitä varten. Mutta tommoset jutut ja yleensä ottaen se, että virustorjunta on pois päältä, nii se on ollu aina hyvin tietonen siitä, että mitä tekee sillon, ku se virustorjunta on pois päältä, ja olla tietonen siitä, mitkä ne riskit on, ettii tietoa siitä, mitä riskejä siinä on, että onko se oikeesti turvallinen, ennen ku tekee sen, ja sitte, että se on pois päältä minimiajan.

Poikkeustilanteessa muodostuu ristiriita suojaamistarpeiden ja käyttötarpeiden (tutkimisen ja tietämisen tarve) välille, jonka käyttäjä ratkaisee siten, että hän huomioi ne yhtä aikaa. Hän ottaa virustorjunnan pois päältä siten, että se ei aiheuta tietoturvan kannalta vahinkoa.

10) TARPEIDEN PRIORISOINTI: uhkan kokemuksen väheneminen

Mikäli tietokoneenkäyttäjä huomaa että varmuuskopioinnin puuttuminen ei lisää tietoturvaongelmia, hän saattaa alkaa suhtautumaan siihen välinpitämättömämmin:

K: Mikä tätä käyttäytymistä selittää, miks se on välillä jääny?
V: Se sitte vaivaa jos mulla on jääny ja kyllä mä yleensä muistan sen, että mä en oo tallentanu sitä ku sinne. Ja nytki mulla on yks, sitä mää aattelin, että mun täytyy se tikulle pistää vielä että.
K: Eli onks se joku tämmönen, että vaan unohtaa?
V:Niin, niin, joo.
K:Että siinä ei kuitenkaan semmonen välinpitämättömyys selitä sitä käyttäytymistä?
V:Ei oo. Kyllä mulla on aika tarkkaan ollu siinä.
K:Että sen vaan epähuomiossa unohtaa sitte?
V: Nii, ja sitte ehkä, sitte nyt huomannu, että ei oo ollu mitään ongelmia, nii ehkä tullee sitte semmonen, siinä mielessä ehkä välinpitämättömyyttä sitte tulee, että ei ookkaan tapahtunu mittään että, ei sillä lailla että…
K: Että uskaltaa tavallaan jättää ne kopioimatta?
V: Niin, niin.

Tässä esimerkissä esiintyy ristiriita poikkeuksellisen käyttäytymisen aiheuttavan tarpeen (tutkimisen ja tietämisen tarve, esteettisyyden tarve, itsensä toteuttamisen tarve, ajan ja vaivan säästämisen tarve sekä toimeentulon tarve) ja suojaustoimenpiteiden käyttöönottoon liittyvän tarpeen välillä eli tietokoneenkäyttäjä ei koe enää niin tärkeäksi kuin ennen ottaa varmuuskopioita, joten turvallisuuden tarve jää taka-alalle ja tietokoneen käyttötarpeet korostuvat.

Yhdistetty prosessi tuo uutta tietoa tietoturvakäyttäytymisen muutoksesta. Tietokoneen käyttäjät toimivat aktiivisesti interaktiossa ympäröivän maailman

kanssa. Tietoturvatapahtuman kokeminen (esimerkiksi tietoturvaongelma) herättää tietokoneen käyttäjässä negatiivisia tunteita, joista henkilö pyrkii eroon ottamalla käyttöönsä suojaustoimenpiteen. Tietoturvakokemukset, joita tässä tutkimuksessa ovat 1) tietoturvaongelma, 2) tietoturvatietoisuuden lisääntyminen, 3) muutos tietokoneen käytössä, 4) muutos elämäntilanteessa, 5) suojattavan määrä ja henkilökohtaisuus kasvaa, käynnistävät ajattelun ja käyttäytymisen muutoksen. Näin malli tukee John Searlen (1983, 1990, 2013) ajatuksia oman subjektiivisen todellisuuden luomisesta. Yhdistetty prosessi esittää tiivistetysti ne kokemukset, elementit ja interaktion, joka saa käyttäytymisen muutoksen aikaan sekä kuvaa ne tarpeet ja tunteet, joita kokemukset herättää ja jotka toimivat motiiveina tietoturvakäyttäytymisen muutokselle.

Esimerkiksi uusien tietoturvatoimenpiteiden omaksuminen pohjautuu aina turvallisuuden tarpeelle ja tietoturvakokemukset aiheuttavat tietokoneen käyttäjissä erilaisia tunteita, kuten harmia, pelkoa ja epäluuloa, jotka vaikuttavat heidän käyttäytymiseensä. Joskus tarpeiden välille muodostuu ristiriita, eli henkilöt asettavat esimerkiksi liittymisen tarpeen turvallisuuden tarpeen edelle ja laativat heikkoja salasanoja palveluihin, joita käyttävät vain muutaman kerran, vaikka tärkeisiin palveluihin käyttäisivätkin vahvoja salasanoja.

Tietoturvaongelma voi olla yksi käyttäytymisen muutoksen käynnistäjä. Tietokoneen käyttö uudessa käyttötarkoituksessa voi saada aikaan ajattelun ja käyttäytymisen muutoksen: henkilö pohtii esimerkiksi mitä sosiaalisen median käyttö merkitsee hänen yksityisyytensä kannalta. Samoin, elämäntilanteen muutos (koulun vaihto, työelämään siirtyminen, lapsen syntymä) tai se, että henkilö alkaa omistaa yhä enemmän tärkeämpää ja henkilökohtaisempaa suojattavaa, voivat käynnistää käyttäytymisen muutoksen.

Käyttäytymisen muutos voi olla myös vähittäinen eli henkilö kokee tietoturvakokemuksen, muuttaa käyttäytymistään ja taas uuden kokemuksen myötä tehostaa omaksuttua suojaustoimea, esimerkiksi rajoittaa verkkokauppakäyttäytymistä, vahvistaa salasanojaan tai tiukentaa virustorjuntaa.

Prosessi voi joskus loppua kesken eli suojaustoimenpidettä ei omaksuta. Henkilö ei tällöin päädy epävarmuuden tasolle eikä hän koe rauhallisuuden ja mielenrauhan tarvetta. Hän ei esimerkiksi koe tärkeäksi salasanan vahvistamista tai luottaa verkkokauppaan niin paljon että tietoturvaongelmat eivät aiheuta epävarmuuden tunteita. Hän voi myös tuntea itsevarmuutta oman suojaustoimenpiteen vahvuuden johdosta (kaksivaiheinen autentikaatio), joten hakkerointiyritys ei aiheuta epävarmuutta ja tietokoneenkäyttö jatkuu entiseen tapaan.

Uutta selitystä tämä tutkimus tuo myös siksi, että se osoittaa kuinka motiivit ja tarpeet vaikuttavat tietoturvakäyttäytymiseen. Esimerkiksi uusien tietoturvatoimenpiteiden omaksuminen pohjautuu aina turvallisuuden tarpeelle. Turvallisuuden tarve eri käyttäytymistyypeissä on esitelty tason 3 esittelyn yhteydessä (taulukko 11) **T**ietoturvakokemukset aiheuttavat tietokoneen käyttäjissä erilaisia tunteita, kuten harmia, pelkoa ja epäluuloa, jotka vaikuttavat heidän käyttäytymiseensä. Lisäksi, joskus tarpeiden välille muodostuu ristiriita, eli henkilöt asettavat esimerkiksi liittymisen tarpeen turvallisuuden tarpeen edelle

ja laativat heikkoja salasanoja palveluihin, joita käyttävät vain muutaman kerran, vaikka tärkeisiin palveluihin käyttäisivätkin vahvoja salasanoja.

Yhdistetyn prosessin etu on, että se pystyy ottamaan huomioon henkilökohtaisen tietokoneen käytön erityispiirteen: tietokoneen käyttäjät luovat itse oman harkintansa pohjalta (kokemusten tarkoituksellisuudet ja merkityksellisyydet) turvallisia käyttäytymistapoja. Työpaikalla voidaan ongelmien ilmaantuessa ottaa suoraan yhteyttä tietokonetukeen, joka myös hoitaa ohjelmistojen asennukset ja varmuuskopioinnin. Tavalliset tietokoneen käyttäjät ovat itse vastuussa tietokonelaitteidensa ja -tietojensa hallinnoinnista. Tämä edellyttää aktiivisuutta ja oman toiminnan arviointia ja pohdintaa. Tietokoneen käyttäjät pohtivat omaa tietoturvaansa kokemuksen kautta. He ovat yhteydessä ympäröivään maailmaan (interaktio) eli esim. kuulevat asioita mediasta, keskustelevat muiden tietokoneenkäyttäjien kanssa, osallistuvat koulutukseen, seuraavat Internetiä, tutkivat tietokoneensa käyttäytymistä, esimerkiksi virustorjuntaohjelman lokeja jne. Tämä interaktio saa aikaan muutoksen ajattelussa ja tietoturvakäyttäytymisessä.

7 POHDINTA

Tässä luvussa esitellään tutkimuksen keskeisimmät uudet löydökset (luku 7.1.) Tutkimuksen rajoitteita ja soveltuvuutta tarkastellaan luvussa 7.2. Tiivistelmät tutkimuksen pohjalta esiin nousseista käytännön suosituksista sisältyvät lukuun 7.3.

7.1 Tutkimuksen keskeisimmät uudet löydökset

Tämän tutkimuksen kontribuutiona esitetään 1) malli tietoturvakäyttäytymisen muutoksesta, 2) tietoturvakäyttäytymisen universe of discourse ja 3) prosessi tietoturvakäyttäytymisen muutoksesta. Malli tietoturvakäyttäytymisen muutoksesta pohjautuu universe of discourseen, jolla tarkoitetaan niitä elementtejä, joiden kanssa tietokoneen käyttäjät ovat interaktiossa ennen käyttäytymisen muutosta (esimerkiksi tietoturvauhka, tietolähde ja tietoverkko). Siihen on koottu 6 eri käyttäytymistyypin (Internet-profiilin hallinta, sensitiivisen aineiston prosessointi, vahvan salasanan laatiminen, varmuuskopiointi, varovaisuus verkkokaupassa sekä virustorjunta) toimintaympäristö eli millaisten elementtien kanssa henkilöt ovat interaktiossa tietoturvakäyttäytymisen muutoksen yhteydessä ja millaisia asioita he pohtivat tietoturvakäyttäytymiseen liittyen. Edelleen, malli tietoturvakäyttäytymisen muutoksesta on ollut apuna laadittaessa prosessia tietoturvakäyttäytymisen muutoksesta.

1. kontribuutio: käyttäytymisen muutoksen selittäminen

Tutkimuksen tärkein kontribuutio on prosessiteoreettinen näkökulma käyttäytymisen muutoksesta. Prosessi osoittaa käyttäytymisen muutoksen syyt, kuinka tietoturvakäyttäytyminen muuttuu ajan kuluessa sekä kuinka motivaatioasiat (tarpeet ja tunteet) vaikuttavat tietoturvakäyttäytymiseen. Tutkimuksen teoreettinen lähtökohta on John Searlen teoreettisissa ideoissa todellisuuden subjektiivisesta luomisesta sekä motivaatiopsykologian teorioissa (erityisesti Maslow, Alderfer, Reiss, Lazarus, Schrerer). Käyttäytymisen muutos selittyy sillä, että

tietokoneenkäyttäjä toimii interaktiossa ympäröivän maailman kanssa ja kokee tietoturvaan liittyviä tapahtumia. Tietoturvaan liittyvät kokemukset herättävät henkilössä erilaisia tunteita ja rauhallisuuden ja mielenrauhan tarpeen: hän pohtii tietoturvakokemuksen merkitystä omasta näkökulmastaan ja oman tietoturvansa kannalta ja pyrkii eroon epävarmuutta aiheuttavista asioista ottamalla käyttöön suojaustoimenpiteen.

Aiempi tietoturvakäyttäytymiseen liittyvä empiirinen tutkimus on hyödyntänyt seurantatutkimusta, kokeellista tutkimusta ja survey-tyyppistä tutkimusta. Survey-tyyppinen tutkimus on selittänyt tietoturvakäyttäytymistä teorioilla kuten esimerkiksi technology acceptance model (TAM) (Kumar et al, 2008; Dinev et al, 2009; Herath et al, 2014), technology threat avoidance theory (TTAT) (Liang & Xue, 2010; Wang et al, 2010; Herath et al, 2014), protection motivation theory (PMT) (Woon et al., 2005; Anderson & Agarwal, 2010; La Rose et al , 2008) ja theory of planned behavior (TPB) (Dinev & Hu, 2007; Lee & Kozar, 2005 & 2008; Ng & Rahim, 2005; Caldwell & McGarvey, 2013). theory of reasoned action (TRA) (Guo et al., 2011), Deterrence theory (Straub, 1990; D'arcy, 2009; Son, 20l1, Lee et al. 2004, Harrington, 1996) ja Neutralization theory (Siponen & Vance, 2010). Edellä mainitut survey-tyyppiset tutkimukset eivät kuitenkaan tarkastele tietoturvakäyttäytymisen muutosta vaan käyttäytymiseen vaikuttavia staattisia tekijöitä. Tutkimuskirjallisuuden joukossa oli 3 kokeellista tutkimusta (Möller et al., 2011; Anderson & Agarwal, 2010; Johnston & Warkentin, 2010) sekä yksi seurantatutkimus (Wang et al., 2010, jotka olivat selvittäneet käyttäytymisen muutosta. Ne kuitenkin yleistävät tutkimustulokset pätemään kaikkiin tapauksiin ja tilanteisiin ja olettavat, että vaikutus on stabiili eli että jokaisessa tilanteessa samat asiat kuin tutkimuksessa esitetyssä tapauksessa vaikuttavat käyttäytymisen muutokseen.

2. kontribuutio: käyttäytymisen tilannesidonnaisuus

Tutkimuksen toisena kontribuutiona esitetään, että tietoturvakäyttäytyminen on tilannesidonnaista sinä mielessä, että suojaustoimenpiteen käyttöönoton jälkeen tietokoneenkäyttäjä voi jossain tilanteessa poiketa siitä. Esimerkkinä tällaisesta tilanteesta on vaikkapa kirjautuminen Internetin keskustelualueelle tai tilanne, jossa tietokoneenkäyttäjän täytyy välittää sähköpostitse tietojaan esimerkiksi johonkin virastoon. Tietokoneenkäyttäjä kokee tarpeiden välisen ristiriidan, ja tarpeiden priorisoinnin seurauksena hän väliaikaisesti tai pysyvästi luopuu suojaustoimen käytöstä (esimerkiksi lähettää sensitiivistä tietoa sähköpostissa tai laatii heikon salasanan). Poikkeustilanteessa voi esimerkiksi liittymisen tarve tai asioinnin tarve korostua turvallisuuden tarpeen jäädessä taka-alalle. Tutkimuksessa osoitetaan, minkätyyppisiä ovat ne tarpeiden väliset ristiriidat, jotka aiheuttavat käyttäytymisen muutoksen poikkeustilanteessa.

Aiempi tutkimuskirjallisuus ei ole huomioinut tietoturvakäyttäytymisen tilannesidonnaisuutta siitä näkökulmasta kuin se on ymmärretty tässä tutkimuksessa. Esimerkiksi survey-tyyppinen tutkimus (mm. Anderson & Agarwal (2010); Kumar et al., 2008; Liang & Xue, 2010; Chan, Woon et al., (2005); Herath & Rao, (2009b) olettaa, että tietoturvakäyttäytyminen ja sen syyt ovat staattisia

ja pätevät ajankohdasta ja tilanteesta toiseen. Muutamissa tutkimuksissa oli selvitetty tilannesidonnaisuutta, joka selittyy moderaattorien vaikutuksella. Esimerkiksi Dinev et al. (2009) on tutkinut kulttuurierojen (Eteläkorea vs. USA) vaikutusta yhteyteen sosiaalisen paineen ja aikomuksen välillä ja Harrington (1996) on selvittänyt, kuinka aikomukseen väärinkäyttää tietokonetta moderoi vastuun kieltäminen (denial of responsibility). Ne eivät kuitenkaan huomioi käyttäytymisen tilannesidonnaisuutta, joka johtuu tarpeiden priorisoinnista.

3. kontribuutio: eri käyttäytymistyyppien vertailu

Tässä tutkimuksessa osoitetaan, että eri käyttäytymistyypeissä (esim. salasanan vaihtaminen, varmuuskopiointi, virustorjunta jne.) käyttäytymisen muutos tapahtuu hieman eri tavalla. Käyttäytymisen muutoksen johtavassa prosessissa on erityyppisiä esteitä ja hidasteita. Eroja on myös siinä, onko poikkeaminen suojaustoimenpiteestä luonteeltaan pysyvä vai väliaikainen. Joissakin käyttäytymistyypeissä prosessi voi loppua kesken ilman että käyttäytyminen muuttuu. Myös prosessien monimutkaisuudessa on eroja käyttäytymistyyppien välillä.

Aiemmassa tietoturvakäyttäytymistutkimuksessa oli ainoastaan kaksi tutkimusta (Anderson & Agarwal (2010) sekä Ng & Rahim (2005) jotka olivat jossain määrin huomioineet eri käyttäytymistyyppejä. Ne ovat kuitenkin selvittäneet aikomusta käyttää suojaustoimenpiteitä (esimerkiksi virustorjuntaohjelma, tietokoneen suojaaminen) eivätkä ole huomioineet käyttäytymisen muutosta ja sitä että muutos tapahtuu eri tavalla eri käyttäytymistyypeissä.

Kaiken kaikkiaan tämä tutkimus tuo uuden lähestymistavan ja näkökulman tietoturvakäyttäytymistutkimukseen. John Searlen esittämiä ideoita todellisuuden subjektiivisesta muodostamisesta ei ole aiemmin hyödynnetty tietoturvatutkimuksessa: eli kuinka tietoturvakäyttäytyminen muuttuu kokemuksen pohjalta, interaktiossa ympäröivän maailman kanssa ja kokemuksen merkityksellisyydeksi kokemisen sekä uskomusten ja ajatusten muutoksen myötä. Erottuakseen tietoturvatutkimuksen valtavirrasta selkeämmin, teoreettista viitekehystä on otettu täydentämään tässä tutkimuksessa motivaatiopsykologia eli Searlen käsitteiden rinnalle on otettu taustateoriaa motivaatio-/tarvepsykologiasta. Näin prosessin tasot on saatu selkeämmin erottumaan toisistaan, sillä jokaiselle tasolle on ollut löydettävissä tarpeet, jotka erottavat sen selkeästi muista tasoista. Tarpeiden välisellä konfliktilla on taas tarkemmin pystytty selittämään poikkeustilanteet eli mistä syystä henkilö poikkeaa omaksutusta suojatoimenpiteestä.

Koska ihmisen käyttäytymiseen vaikuttaa olennaisena motivaattorina tarpeiden lisäksi myös tunteet, myös tämä näkökulma oli järkevää ottaa tutkimukseen mukaan. Tämä valinta osoittautui tutkimuksen kannalta hyödylliseksi, sillä lopulta löydöksenä oli 21 erilaista tunnetta, joilla on vaikutusta tietoturvakäyttäytymiseen. Tunteiden merkitystä käyttäytymisen motivoijana tässä määrin ei ole aiemmassa tutkimuksessa huomioitu. Ainoastaan pelko (mm. Johnston & Warkentin, 2010) ja huoli (mm. Anderson & Agarwal, 2010; Kumar et al. , 2008) on jossain määrin huomioitu tietoturvakäyttäytymiseen vaikuttavina asioina.

7.2. Tutkimuksen rajoitteet ja soveltuvuus

Tutkimuksen validiteettia on tarkasteltu Maxwell (1992) viitekehyksen pohjalta (taulukko 15). Validiteettia tarkasteltaessa on otettu huomioon kuvauksen tarkkuus (descriptive validity), vastaajan näkökulman ja ajatusten tarkkuus (interpretive validity), teoreettinen validiteetti (theoretical validity) ja yleistettävyys (generalizability).

TAULUKKO 15 Tutkimuksen validiteetti (pohjautuu Maxwell, 1992)

Tyyppi	Kuvaus	Soveltaminen tässä tutkimuksessa
Kuvauksen tarkkuus (Descriptive validity)	Laadullisen tutkimuksen tavoitteena on tarjota perusteltu ja pätevä kuvaus objekteista, tapahtumista ja ilmiöön liittyvästä käyttäytymisestä. Kuvauksen tarkkuus viittaa tosiasioiden paikkansapitävyyteen eli että tutkijat ovat rehellisiä sen suhteen, mitä he ovat nähneet ja kuulleet.	Haastatteluissa käytettiin tallenninta, joten haastattelun jälkeen oli mahdollista tarkistaa haastateltavien vastaukset. Tutkimuksessa on käytetty runsaasti tekstiesimerkkejä haastatteluista, jotka auttavat tarkan kuvauksen saamista aineistosta.
Vastaajan näkökulman ja ajatusten tarkkuus (Interpretive validity)	Laadullisen tutkimuksen tekijä ottaa huomioon sen, mitä objektit, tapahtumat ja käyttäytyminen haastateltaville merkitsevät. "Haastateltavan näkökulma" sisältää esimerkiksi haastateltavan intention, ajattelun, tunteen, käsityksen ja arvioinnin. Tulkitsevat kuvaukset tulisi esittää tutkimuksessa niin paljon kuin mahdollista vastaajien omia sanoja ja käsitteitä käyttäen. Tulisi myös ottaa huomioon, että osallistujat eivät välttämättä ole tietoisia omista tunteistaan tai näkemyksistään, eikä ole selvää, että ihmiset muistavat asioita tarkasti. He ovat myös saattaneet unohtaa joitain asioita. Joskus he salaavat tai vääristävät	Koska tutkimusaihe on sensitiivinen, ongelmana voi olla se että haastateltavat eivät aina puhu totta. Tämän vuoksi haastateltaville kerrottiin haastattelun alussa, että haastattelun tarkoitus ei ole arvostella eikä arvioida käyttäytymistä ja että yhtä oikeaa tai väärää vastausta ei ole. Korostettiin myös sitä, että yksittäisiä vastauksia ei kerrota kenellekään ja että olemme kiinnostuneita laajemmista tuloksista, emme yksittäisen henkilön vastauksista. Lisäksi kysyimme luvan nauhoittaa haastattelu. Haastateltavalla oli oikeus kieltäytyä nauhoituksesta jos esimerkiksi asioiden kertominen olisi ollut täten helpompaa. Jos haastateltava ei muistanut haastattelussa jotain asioita, asiaa on jatkettu käsittelemällä sitä toisesta näkökulmasta.

	näkökulmiaan, joko tiedostetusti tai tiedostamattaan.	Uusia kysymyksiä on esitetty selkiyttämään asioita ja estämään vääristymät. Myös siihen on kiinnitetty huomiota, että haastateltavan loukkaamista / mielen pahoittamista on vältetty, koska tämä voi johtaa haastateltavan harhaan (Myers & Nyman (2007). Puolistrukturoitu haastattelu ohjaa haastattelua mutta haastateltavilla on ollut mahdollisuus tuoda omia ideoitaan ja mielipiteitään esille ja toisaalta asioita on käsitelty sitä mukaa, kun ne haastateltavan puheessa on tullut esille. Mirroring-menetelmää on käytetty avuksi pääsemään sisälle haastateltavan kokemusmaailmaan, eli on käytetty haastateltavan käyttämää kieltä ja ilmauksia. On tärkeää, että haastateltavat kertovat omista kokemuksistaan omin sanoin (Myers & Nyman, 2007) Tekstinäytteet haastatteluista on kirjoitettu haastateltavan puhekielellä.
Teoreettinen validiteetti (Theoretical validity)	Kohdistuu teoreettisiin konstruktioihin, jotka tutkimuksessa on kehitetty. Jokaisella teorialla on kaksi komponenttia: 1) käsitteet tai kategoriat, joita teoria käyttää, and 2) oletetut yhteydet käsitteiden välillä. Teoreettinen validiteetti perustuu em. teorian näkökohtiin: ilmiössä käytettyjen käsitteiden ja kategorioiden validiteetti ja niiden yhteyksien validiteetti, joiden oletetaan ilmenevän käsitteiden välillä.	Aineistoa on luettu tarkasti ja kategoriat (tasot) on johdettu aineistosta, samoin yhteydet tasojen välillä. Teorian muodostaminen ja se, miten päätelmät on johdettu aineistosta on esitetty vaihe vaiheelta. Käytetyt tutkimusmenetelmät on kerrottu avoimesti.
Yleistettävyys (generalizability)	Tutkijan tulisi ymmärtää kuinka tutkittavan toiminta ja näkökulmat voivat olla erilaisia toisissa tilanteissa. Koska tutkija yleensä viettää melko lyhyen ajan	Tutkimuksessa on huomioitu sisäinen yleistettävyys seuraavasti: Uusia haastateltavia on rekrytoitu niin paljon kuin on tarvittu uuden tiedon saamisek-

	haastateltavan kanssa, tämä aiheuttaa ongelmia: tiivistelmät siitä, mitä tapahtui haastateltavan elämässä pitää tehdä verrattain lyhyessä ajassa. Yleistäminen laadullisessa tutkimuksessa tarkoittaa sen huomioimista, että kehitetty teoria on ymmärrettävä ja järkevä tietyissä olosuhteissa ja että sama prosessi voi johtaa erilaisiin tuloksiin olosuhteiden ollessa toiset. Laadullisessa tutkimuksessa on 2 näkökantaa: 1) Sisäinen yleistettävyys (internal generalizability). Tämä on näistä kahdesta tärkeämpi. Tämä tarkoittaa yleistämistä tutkitun yhteisön, ryhmän tai instituution sisäpuolella ihmisiin, tapahtumiin ja ympäristöön, jotka eivät olleet suoranaisesti tutkimuksen kohteena 2) Ulkoinen yleistettävyys (external generalizability): yleistetään muihin yhteisöihin, ryhmiin tai organisaatioihin.	si. Saturaatio on määrittänyt haastateltavien lukumäärän. Kuitenkin, haastateltavien määrä (n=35) on verrattain pieni, joten uusia syitä käyttäytymisen muutokselle sekä tarpeita ja tunteita, jotka vaikuttavat käyttäytymisen muutokseen voisi löytyä uusista haastatteluista. Haastateltavat koostuivat pääosin satunnaisotannalla valituista henkilöistä Myers & Newman (2007) suosittelevat ottamaan mukaan erityyppisiä haastateltavia, eli että haastateltavat eivät olisi yksi yhtenäinen joukko. Tämä mahdollistaa useiden äänien esille saamisen. Tässä tutkimuksessa laadittua käyttäytymisenmuutosprosessia ei voida yleistää suoraan muuntyyppiseen käyttäytymiseen. Muunlaisia käyttäytymistyyppejä ei voida kuvata niillä tasoilla ja käyttäytymistä motivoivilla asioilla, jotka on esitetty tässä tutkimuksessa.
Arvioiminen (Evaluative validity)	Arvioiminen tarkoittaa arviointikehyksen soveltamista tutkimuksen objekteihin esimerkiksi pohtimalla onko tietyn ihmisen käyttäytyminen oikein vai väärin.	Tässä tutkimuksessa ei ole arvioitu haastateltavien käyttäytymistä. Pyrkimys on ollut ymmärtää ja selittää tietoturvakäyttäytymistä.

Kuvauksen tarkkuuteen on kiinnitetty huomiota tässä tutkimuksessa siten, että haastattelut on nauhoitettu ja tekstissä on käytetty runsaasti tekstiesimerkkejä haastateltavien vastauksista, mikä mahdollistaa tarkemman kuvauksen saamisen aineistosta.

Vastaajan näkökulman ja ajatusten tarkkuuteen on kiinnitetty huomiota korostamalla haastatteluissa sitä, että vastausten käsittely on luottamuksellista ja että vastauksia ei ole tarkoitus tutkimuksessa arvostella tai arvioida. Haastattelun nauhoituksesta on ollut mahdollista kieltäytyä esimerkiksi siinä tapauksessa, jos haastateltava on kokenut, että hänen olisi helpompi kertoa ajatuksistaan ilman että haastattelu nauhoitetaan. Vääristymiä ja väärinymmärryksiä on pyritty välttämään tekemällä tarkentavia lisäkysymyksiä haastattelun aikana. Tutkimusaihe on sensitiivinen, minkä takia vaarana on, että haastetaltavat eivät välttämättä aina puhu totta. Tämän vuoksi haastattelussa on pyritty ylläpitämään positiivista ilmapiiriä. Vaikka haastattelijalla onkin ollut luetteko käsiteltävistä teemoista, asioita on käsitelty paljolti sitä mukaa kun ne haastattelussa on tullut esille. Mirroring-menetelmä, eli haastateltavan käyttämien termien ja ilmausten toistaminen on auttanut pääsemisessä haastateltavan maailmaan. Tekstinäytteissä on käytetty puhekieltä, mikä antaa tarkemman kuvauksen haastateltavien ajatuksista ja pohdinnoista.

Teoreettinen validiteetti on huomioitu tässä tutkimuksessa siten, että prosessin tasot on johdettu tarkasti aineistoa lukemalla. Teorian muodostamisprosessi ja tutkimusmenetelmät on myös kuvattu avoimesti.

Saturaatio on määritellyt haasteltavien määrän. Kun samat aiheet on alkaneet toistua, uusien haastateltavien rekrytointi on lopetettu. Satunnaisotannalla on pyritty vaikuttamaan monipuolisesti erilaisten äänien ja näkökulmien esille saamiseen. Em. toimenpiteillä on huomioitu tulosten sisäinen yleistettävyys. Tutkimuksessa on pohdittu myös tulosten ulkoista yleistettävyyttä: tutkimuksessa laadittua käyttäytymisen muutosprosessia ei voida yleistää muuntyyppiseen käyttäytymiseen.

Jatkotutkimusaiheet

Tämän tutkimuksen tarkoitus on tarjota esimerkkejä siihen, miten tietoturvakäyttäytymistä voitaisiin lähteä jatkossa tutkimaan: mitä aiemmasta tutkimuksesta puuttuu ja miten tutkimussuuntausta lähdetään viemään eteenpäin. Esimerkiksi seuraavat 5 linjaa voisi olla kiinnostavia jatkotutkimuksen aiheita tämän tutkimuksen tulosten valossa.

Ensimmäinen jatkotutkimusaihe liittyy tietoturvakäyttäytymisen tilannesidonnaisuuteen. Tietoturvakäyttäytymisen tilannesidonnaisuutta voisi tarkastella laajemmin. Tässä tutkimuksessa tilannesidonnaisuus on määritelty uudeksi tilanteeksi, jossa henkilö priorisoi ristiriitaisia tarpeita. Tilannesidonnaisuudelle voitaisiin etsiä ja laatia myös muita määritelmiä ja tutkia laadullisesti, esimerkiksi haastattelututkimuksella, tietoturvakäyttäytymistä laajemmin tilannesidonnaisuuden näkökulmasta.

Toisena jatkotutkimusalana esitän tuloksieni tilastollisen yleistettävyyden testaamista. Tämä tarkoittaa sitä, että tämän tutkimuksen tuloksista muodostetaan hypoteeseja, joita tutkitaan riittävän isolla otoskoolla, joka mahdollistaa tilastollisen yleistettävyyden testaamisen.

Kolmanneksi, aiheesta voisi laatia uuden teorian grounded theory -menetelmällä. Teoria kuvaisi ihmisen tietokäyttäytymistä, jossa tietoturva muodostaisi yhden osan. Näin saisimme kokonaiskuvan siitä, kuinka tietoturvakäyttäytyminen nivoutuu osaksi tietokäyttäytymistä.

Neljäs esitykseni jatkotutkimukseksi liittyy tietoturvakäyttäytymistyyppeihin. Tähän tutkimukseen valittiin mukaan 6 käyttäytymistyyppiä. Jatkossa voisi laajentaa käyttäytymistyyppien vertailua ja ottaa mukaan uusia (esimerkiksi tietokonelaitteilta uloskirjautuminen, salasanan säännöllinen vaihtaminen, salasanan jakaminen) ja tutkia, löytyisikö näin uusia syitä käyttäytymisen muutokselle.

Viimeinen esitys jatkotutkimukseksi liittyy tutkimuksen tekemiseen organisaatiokontekstissa. Tässä tutkimuksessa haastateltavat on rekrytoitu pääasiassa satunnaisotannalla kaupungilta, kauppatorilta, kirjastolta ja yliopistolta ja kohderyhmänä ovat olleet henkilökohtaisen tietokoneen käyttäjät. Jatkossa laadullista tutkimusta voitaisiin laajentaa myös organisaatiokontekstiin ja haastatella, mitkä syyt selittävät työntekijöiden käyttäytymisen muutosta ja miten työntekijöiden tietoturvakäyttäytyminen muuttuu ajan kuluessa.

7.3. Tiivistelmät käytännön suosituksista

Aikaisemmat alan tutkimukset, jotka perustuvat teorioille kuten PMT ja DT, tarjoavat tietokoneenkäyttäjille pelkoa uhasta (PMT) tai rangaistuksista (DT). Aikaisempi tutkimus ei oleta, että käyttäytymisen syyt ja motivaattorit vaihtuvat: esimerkiksi PMT-teoriassa käyttäytymisen motivaattori on aina uhan pelko ja DT-teoriassa aina rangaistuksen saamisen pelko tai kiinnijäämisen riski seurauksena omasta tietoturvakäyttäytymisestä. Tämä tutkimus haastaa nämä näkemykset ja esittää, että käyttäytymisen syyt ja motivaatio vaihtelevat. Jos tämä löydös pitää paikkaansa, niin tietoturvakäyttäytymisen muuttaminen on paljon haastavampaa kuin aikaisempi tutkimus antaa ymmärtää. Lisäksi hyvätkin tietoturvakäyttäytymisen tulokset, esimerkiksi koulutusintervention tai tietoturvakampanjan kautta saatuna, voivat muuttua käyttäjien uusien kokemuksien pohjalta. Tämä tarkoittaa sitä, että tietoturvakäyttäytymisen muutokseen pyrkivän toiminnan tulee olla paljon käyttäjätilanneriippuvaisempaa kuin aikaisempi (esim. PMT ja DT) tutkimus esittää. Samalla rangaistuksella tai uhkalla pelottelu ei aina riitä, vaan tietoturvakäyttäytymisen muutos vaatii tarkempaa ymmärrystä kunkin käyttäjän tilanteesta. Samalla on huomioitava, että tietyllä hetkellä vallitseva käsitys käyttäjän tietoturvakäyttäytymisen syistä voi myöhemmin muuttua, jopa tavoilla, joita on vaikea etukäteen tarkasti ennustaa.

Yllä mainitun lisäksi käyn läpi myös muita näkökulmia, jotka nousivat esiin empiiristen tulosteni pohjalta.

Tietoturvasuojaustoimenpiteiden käyttöönoton edistämistä ajatellen tiedotus tietoturva-asioista eri kanavia pitkin on tärkeää, joka tosin jo mainittu aikaisemmassa tutkimuksessa (esim. Siponen, Mahmood & Pahnila, 2009; Vance & Siponen, 2012). Koska henkilökohtaisen tietokoneen käyttäjä on itse vastuussa tietoturvasta, oma harkinta, ajattelu ja päättely sekä tietoturvan suunnittelu korostuu eri tavalla kuin organisaatiossa, jossa tekninen tuki huolehtii työntekijöiden tietokoneiden ja tietojen suojauksesta.

Haastatteluissa tuli ilmi myös se, että suojaustoimenpiteiden käytön neuvontaa tarvitaan, jotta niiden omaksuminen tulisi helpommaksi. Tämä tosin on myös mainittu aikaisemmassa tutkimuksessa (Puhakainen & Siponen 2010; Siponen, Mahmood & Pahnila, 2009; Vance & Siponen, 2012). Esimerkiksi sosiaalisen median käyttö ja yksityisyysasetukset, sähköpostin ja sähköpostin salausohjelmien sekä virustorjuntaohjelmien käyttö aiheuttavat päänvaivaa. Yksi mahdollisuus helpottaa tietokoneenkäyttäjien arkea olisi integroida tietokonelaitteisiin tietoturva jo laitteen valmistusvaiheessa.. Näin on jo tehtykin ainakin joidenkin älynpuhelinmallien kohdalla.

Ohjelmistokehittäjille tutkimus tarjoaa haasteen kehittää vaihtoehtoisia sovelluksia sosiaaliseen mediaan. Tyytymättömyys nykyisiin some-palveluihin mm. niiden tietoturvaan aiheuttaa niiden käytön rajoittamista. Verkkokaupoille tutkimus taas osoittaa haasteen kehittää verkkokauppaa turvallisemmaksi. Johtuen huonoista kokemuksista verkkokaupassa sen käyttöä rajoitetaan/vähennetään. Kaupankäynti verkossa voisi saavuttaa huomattavasti suuremman volyymin, kun turvallisuusasioihin kiinnitettäisiin enemmän huomiota.

Haastattelut osoittivat, että tietoturvakoulutusta tarvitaan liittyen henkilökohtaisen tietokoneen käyttöön, joka tosin ei ole uusi suositus (ks. Esim Puhakainen & Siponen 2010). Monet haastateltavat olivat kokeneet tietoturvaongelmia. Osasta voitaisiin välttyä tietoturvatietoisuutta lisäämällä. Jokaiselle saatavilla oleva www-pohjainen koulutus liittyen omien laitteiden ja tietojen suojaamiseen Internetissä olisi hyvä vaihtoehto. Koulutuksen voisi Suomessa esimerkiksi Viestintäviraston Kyberturvallisuuskeskus järjestää. Tietokoneen ja Internetin turvallinen käyttö tulisi olla yksi kansalaistaitoja ja turvallista tietokoneen käyttöä tulisi opettaa kattavasti myös koulussa, aina esikoulusta lähtien.

YHTEENVETO (SUMMARY)

Tämän tutkimuksen aiheena on tietokoneenkäyttäjien tietoturvakäyttäytymisen muutos. Vaikka tietototurvakäyttäytymistä ja siihen vaikuttavia tekijöitä on tutkittu laajasti, tietoturvakäyttäytymisen muutoksesta, ja siitä, kuinka se tarkalleen ottaen tapahtuu, ei ole aiempaa tutkimustietoa. Aiempi tutkimus selittää tietoturvakäyttäytymistä staattisilla vaikuttimilla, jotka pysyviä tilanteesta ja ajankohdasta toiseen (esim. TTAT:n vaikuttimet uhka (perceived threat), suojaustoimen tehokkuus (safeguard effectiveness), suojaustoimen hinta (safeguard cost) ja omat kyvyt (self-efficacy). Se on jättänyt huomiotta tietoturvakäyttäytymisen tilannesidonnaisuuden, mikä tässä tutkimuksessa tarkoittaa sitä, että ristiriitaiset tarpeet saavat tietokoneen käyttäjä jossain tilanteessa luopumaan omaksumastaan suojaustoimenpiteen käytöstä. Tutkimustietoa puuttuu myös siitä, kuinka käyttäytymisen muutos tapahtuu eri käyttäytymistyypeissä (esimerkiksi varmuuskopiointi, vahvan salasanan laatiminen, virustorjunnan käyttöönotto jne.)

Kirjallisuuskatsaus, johon kuului 46 tietokoneen kotikäyttöön ja työkäyttöön liittyvää empiiristä tutkimusta osoitti, että tietoturvakäyttäytymisen muutosta oli tutkittu vain muutamissa kokeellisissa tutkimuksissa ja seurantatutkimuksessa. Näitä tuloksia ei kuitenkaan voida yleistää muihin tapauksiin ja tilanteisiin kuin siihen, jossa tämä nimenomainen tutkimus on toteutettu.

Täydentääkseen aiempaa tutkimusta tässä tutkimuksessa on selvitetty, miten tietoturvakäyttäytymisen muutos tapahtuu ja kuinka motivaatiotekijät kuten tarpeet ja tunteet vaikuttavat tietoturvakäyttäytymisen muutokseen. Teoreettisen viitekehyksen tutkimukselle muodostavat John Searlen ajatukset todellisuuden subjektiivisesta muodostamisesta ja kokemuksen tarkoituksellisuudesta sekä motivaatiopsykologia.

Tutkimuksessa haastateltiin 35 eri-ikäistä henkilökohtaisen tietokoneen käyttäjää. Haastatteluihin pohjautuen on laadittu tietoturvakäyttäytymisen Universe of discourse, millä tarkoitetaan niitä elementtejä, joiden kanssa tietokoneenkäyttäjä toimii interaktiossa käyttäytymisen muutoksen yhteydessä (esimerkiksi omaisuus, uhka, tietoverkko). Universe of discoursen pohjalta on laadittu malli käyttäytymisen muutoksesta, joka osoittaa tietoturvakäyttäytymisen toimintaympäristön ja sen, miten eri elementit ovat yhteydessä toisiinsa.

Työn tärkeimpänä kontribuutiona esitetään prosessiteoreettinen näkökulma tietoturvakäyttäytymisen muutoksesta. Prosessiteoreettinen näkökulma esittää käyttäytymisen muutoksen aikajärjestyksessä. Prosessiteoreettinen näkökulma esittää myös syyt käyttäytymisen muutokselle sekä sen, kuinka tietoturvakäyttäytyminen muuttuu ajan kuluessa. Prosessiteoreettinen näkökulma kuvaa myös, millaisten elementtien kanssa tietokoneenkäyttäjä toimii interaktiossa ja mitkä tarpeet ja tunteet vaikuttavat tietoturvakäyttäytymiseen prosessin eri vaiheissa. Yhden yhdistetyn prosessiteoreettisen näkökulman lisäksi tutkimuksessa on laadittu oman malli jokaisesta tutkitusta käyttäytymistyypistä (oman Internet-profiilin hallinta, sensitiivisen aineiston prosessointi, vahvan salasanan laatiminen, varmuuskopiointi, varovaisuus verkkokaupassa ja virus-

torjunta). Erittelemällä kunkin yksittäisen mallin erityspiirteet tutkimus osoittaa, että käyttäytymisen muutos tapahtuu eri tavalla eri käyttäytymistyypeissä.

Tulokset tukevat John Searlen ideoita todellisuuden subjektiivisesta muodostamisesta sekä motiivipsykologian ajatuksia tunteiden ja tarpeiden vaikutuksesta käyttäytymiseen. Tietokoneenkäyttäjä muodostaa todellisuuttaan itse kokemuksena pohjalta olemalla yhteydessä ympäristössä oleviin elementteihin. Tietoturvaan liittyvä kokemuksen seurauksena henkilö pohtii kokemuksen merkitystä oman tietoturvansa kannalta. Kokemus herättää negatiivisia tunteita, joista tietokoneen käyttäjä pyrkii eroon ottamalla käyttöön suojaustoimenpiteen. Käyttäytyminen muuttuu, kun käyttäytymisen taustalla olevat ajatukset ja uskomukset muuttuvat. Edelleen, uudet tietoturvaongelmat herättävät tietokoneenkäyttäjässä tunteita, jotka saavat hänet vahvistamaan tietoturvaansa edelleen.

Tutkimus osoittaa, että tietoturvakäyttäytymisen muutos on tilannesidonnainen prosessi. Suojaustoimenpiteen omaksuttuaan tietokoneenkäyttäjä voi poiketa siitä joko väliaikaisesti tai pysyvästi, mikä selittyy tarpeiden välisellä ristiriidalla. Henkilö priorisoi ristiriitaisia käyttötarpeita ja suojaustarpeita, minkä seurauksena hän joko väliaikaisesti tai pysyvästi laiminlyö suojaustoimenpiteen käytön. Aiempi tutkimus ei ole tutkinut käyttäytymisen muutosta tästä näkökulmasta, koska se on selittänyt tietoturvakäyttäytymistä staattisena ja muuttumattomana ilmiönä. Samoin, tunteiden ja tarpeiden merkitys käyttäytymisen muutoksen liikkeellepanevana voimana on aiemmassa tutkimuksessa jätetty huomioimatta.

Tietojärjestelmätiede on perinteisesti nähty soveltavana tieteenalana, joka viittaa muihin tieteenaloihin (Baskerville & Myers, 2002). Tietojärjestelmien tutkijat ovat olettaneet, että tietojärjestelmätutkimuksen laatu ja kypsyys tulisi mitata suhteessa teorioihin ja metodeihin, jotka pohjautuvat muihin tieteenaloihin kuten taloustiede, kognitiivinen psykologia ja matematiikka. Tämä tutkimus vastaa em. haasteeseen kehittämällä teorian, jonka lähtökohta on omassa tieteenalassa. Lisäksi, tutkimuksessa sovellettu tulkitseva tutkimussuuntaus (interpretive research tradition) auttaa ymmärtämään ihmisen ajattelua ja käyttäytymistä ja tuottamaan tietojärjestelmätieteeseen uusia näkökulmia ja avauksia. (Klein & Myers, 1999; Orligowski & Baroudi, 1991). Tutkimuksen pohdintaosuudessa esitetään tietoturvakäyttäytymistutkimukselle joitakin uusia tutkimussuuntia.

LÄHTEET

Abbott, A. (1990). A primer on sequence methods. Organizational science 1(4).

Alderfer, C., & Guzzo, R. 1979. Life experiences and adults' enduring strength of desires in organizations. Administrative Science Quarterly, 24(3), 347-361.

Anderson, C. L. & Agarwal, R. 2010. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral inten tions. MIS Quarterly 34 (3), 613-643.

Asamoah, E. S., Chovancová, M., De Alwis, A. C., Ajantha Kumara, S. M., & Guo, Y. 2011. MOTIVATION FOR BUYING BRANDED ITEMS: A CROSS COUNTRY APPLICATION OF MASLOWS HIERARCHY OF NEEDS IN CONSUMER DECISION MAKING. Scientific Papers Of The University Of Pardubice. Series D, Faculty Of Economics & Administration, 16(21), 6-18.

Bedford, E. 1988. Emotions and statements about them. In R. Harre (Eds) The social construction of emotions. Oxford: Basil Blackwell.

Becchio, C, et al. 2006. How the brain understands intention: Different neural circuits identify the componential features of motor and prior intentions. Consciousness and cognition 15, 64-74.

Boss, S., Kirsch, L. et al. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European journal of in formation systems 18 (2), 151-164.

Bridle, C. C., Riemsma, R. P., Pattenden, J. J., Sowden, A. J., Mather, L. L., Watt, S., & Walker, A. A. 2005. Systematic review of the effectiveness of health behavior interventions based on the transtheoretical model. Psychology & Health, 20(3), 283-301.

Bryant, K. & Campbell, J. 2006. User Behaviours Associated with Password Security and Management. Australasian Journal of Information Systems 14 (1).

Bulgurcu B., Cavusoglu, H. & Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3), 523–548.

Bunnel, J., Podd, J., Henderson, R., Napier, R., & Kennedy-Moffat, J. 1997. Cognitive, associative and conventional passwords: Recall and guessing rates. Computers & Security, 16 (7), 629-641.

Bush, W.T. 1909. The Existential Universe of Discourse. The Journal of Philos ophy, psychology and Scientific Methods, 6 (7), 175-182.

Caldwell, A. & McGarvey, J. 2013. Modeling user behaviour in response to cyberthreats. Signals and Systems Conference (ISSC 2013), 24th IET Irish, 1 (7), 20-21.

Cassar, S., & Baldacchino, D. R. 2012. Quality of life after percutaneous coronary intervention: part 1. *British Journal Of Nursing*, *21*(16), 965-971.

Chan, M., Woon, I. et al. 2005. "Perceptions of information security at the workplace: linking information security climate to compliant behavior." Journal of Information Privacy and Security 1(3): 18–41.

Chang, W., & Yuan, S. 2008. A synthesized model of Markov chain and ERG theory for behavior forecast in collaborative prototyping. *Journal of Information Technology Theory and Application*, *9*(2), 45-63.

Chen, Y., Paxson, V., & Katz, R. H. 2010. What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.

Computer network. [online]. [viitattu 10.4.2014]. *Encyclopædia Britannica Online.* Saatavana www-muodossa: <URLhttp://www.britannica.com.ezproxy.jyu.fi/EBchecked/topic/130637/computer-network >

Computer Security Update, 13(2). AhnLab announces mobile security threat trends for 2012. [online]. [viitattu 14.4.2014]. Saatavana www-muodossa: <URL http://search.proquest.com/docview/918655181?accountid=11774 >

D'Arcy J., Hovav, A. & Galletta, D. 2009. User awareness of security counter measures and its impact on information systems misuse: a deterrence approach. Information Systems Research 20(1), 79–98.

Dinev et al. 2009. User behavior towards protective information technologies: (19), 391-412.

Dinev, T. & Hu, Q. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the association for information systems 8(7) 386-408.

Dodge, R.C. et al. 2007. Phishing for user security awareness. Computers & Security (26) 73-80.

Downes, P. K. 2007. An introduction to the Internet. British Dental Journal, 202(5), 255-8.

Elango, B. 2000. Do you have an internet strategy?. Information Strategy: The Executive's Journal, 17(1), 32-38.

Ellsworth, P. C. & Schrerer, K. R. 2003. Appraisal processes in emotion. In R.J. Davidson, K.R. Screrer & H. Hill Goldsmith (Eds) Handbook of affective sciences. Oxford; New York: Oxford University Press.

European Network and Information Security AgencY. 2006. A users' guide: how to raise information security awareness. [online]. [viitattu 6.8.2013]. Saatavana www-muodossa: <URL: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/A%20Users%20Guide%20How%20to%20Raise%20Information%20Security%20Awareness.pdf>

Diener, E. 1995. A value based index for measuring national quality of life. Social indicators research 36, 107-127.

Duffy, J. A., & Lilly, J. 2013. Do Individual Needs Moderate the Relationships between Organizational Citizenship Behavior, Organizational Trust and Perceived Organizational Support? Journal Of Behavioral & Applied Management, 14(3), 185-197.

Furnell, S., Tsaganidi, V. & Phippen, A. 2008. Security beliefs and barriers for novice Internet users. Computers & security (27), 235-240.

Furnell, S. et al. 2007. Assessing the security perceptions of personal Internet users. Computers & Security (26) 410-417.

Furnell, S., Jusoh, A. & Katsabas, D. 2006. The challenges of understanding and using security: a survey of end-users. Computers and security (25) 27-35.

Furnell, S. 2005. Why users cannot use security. Computers & security (24), 274-279.

Gears, D.A. 2012. Corporate wiki conduct: A study of organizational influ ences, emotion, and motivation. Journal of leadership, Accountability and ethics 9 (3), 75-85.

Gralla, P. 2004. How the Internet works. Indianapolis, IN: Que, cop.

Guo, K. et al. 2011. Understanding nonmalicious security violations in the workplace: a composite behavior model. Journal of Management Information Systems 28(2), 203–236.

Hagerty, M. R. 1999. Testing Maslow's hierarchy of needs: National quality-of-life across time. Social Indicators Research, 46(3), 249.

Haggard, P. & Clark, S. 2003. Intentional action: Conscious experience and neural prediction. Consciousness and cognition 12, 695-707.

Harre, R. 1988. An outline of the social constuctionist viewpoint. In R. Harre (Eds) The social construction of emotions. Oxford: Basil Blackwell.

Harrel, A.M. & Stahl, M.J. 1984. McClelland's trichotomy of needs theory and the job satisfaction and work performance of CPA firm professionals. Accounting, organizations and society 9 (3), 241-252.

Harrington, S., Anderson, C. L. & Agarwal, R. 2006. Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. ICIS 2006 Proceedings. Paper 93.

Harrington, S. J. 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Quarterly 20(3), 257–278.

Helkama, K., Myllyniemi, R. & Liebkind, K. 1998. Johdatus sosiaalipsykologiaan. Helsinki. Edita.

Herath, T. et al. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Information systems journal 24 (1), 61-84.

Herath,T. & Rao, H.R. 2009a. Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems 18(2), 106–125.

Herath, T. & Rao, H.R. 2009b. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems 47(2), 54–165.

Hsu, J., Shih, S., Hung,Y. & Lowry, P. 2015. How extra-role behaviors can improve information security policy effectiveness. Information Systems Research (forthcoming; accepted 19-Jan-2015).

Hu, Q., Xu Z., Dinev, T. and Ling, H. (2011). Does deterrence really work in reducing information security policy violations by employees? Communications of the ACM 54(6), 54–60.

Humphreys, E. (2010). Information security risk management. British Standards Institution, 54, 56-61.

Hwang, K., Sameer ,K. & Yue, H. 2009. Cloud security with virtualized defense and reputation-based trust mangement. Dependable, Autonomic and Secure Computing. DASC'09. Eighth IEEE International Conference on. IEEE, 2009.

Internet users in the world. Internet live stats. [online]. [viitattu 31.7.2015]. Saatavana www-muodossa: URL< http://www.internetlivestats.com/internet-users/>

Ishiguro, M., Suzuki, H., Murase, I., & Ohno, H. 2004. Internet threat detection system using bayesian estimation. In Proceedings of The 16th Annual Computer Security Incident Handling Conference.

Islam, R. & Ismail, A. Z. 2008. Employee motivation: A Malaysian perspective. International Journal of Commerce & Management, 18(4), 344-362.

Johnston, A.C., Warkentin, M. & Siponen, M. 2015.An Enhanced Fear Appeal Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric, *MIS Quarterly*, Vol. 39, No. 1, 2015, pp. 113-134.

Johnston, A. & Warkentin, M. 2010a. Fear appeals and information security behaviors: an empirical study. MIS Quarterly 34(3), 549–566.

Juliano, S. C., & Sofield, B. L. 2011. Principled Leadership: Think needs. *Human Development*, *32*(3), 37-39.

Kaliprasad, M. 2006. The human factor I: Attracting, retaining, and motivating capable people: A publication of the American Association of Cost Engineers. Cost Engineering, 48(6), 20-26.

Karjalainen, M. & Siponen, M. 2011. Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. Journal of the Association for Information Systems 12 (8), 518-555.

Klein, H.K. & Myers, M.D. 1999. A set of principles for conducting and evaluat ing interpretive field studies in information systems. MIS Quarterly 23 (1), 67-94.

Kritzinger, E. & von Solms, S.H. 2010. Cyber security for home users: A new way of protection through awareness enforcement. Computers & security (29) 840-847.

Kuhn, R., Liu, S., & Rossman, H. 2009. Practical interdomain routing security. IT Professional Magazine, 11(6), 54-56.

Kumar, N. et al. 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. Decision support systems (46), 254-264.

La Rose et al. 2008. Promoting personal responsibility for internet safety. Communications of the ACM. (51) 3.

Langley, A. 1999. Strategies for theorizing from process data. The academy of management review 24 (4), 691-710.

Lazarus, R.S. (1988). Emotion and adaptation. In J.M. Jenkins, K. Oatley & N.L. Stein (eds.) Human emotions: a reader. Malden (Mass.): Blackwell.

Lee, A. S. & Baskerville, R. L. 2003. Generalizing generalizability in infor mation systems research. Information systems research 14 (3), 221-243.

Lee, Y. & Kozar, A. 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. Information & Management 45, 109-119.

Lee, Y. & Kozar, K.A. 2005. Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM. 48 (8), 72-77.

Lee, S. M, Lee, S. G. and Yoo, S. 2004. An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 41(6), 707–718.

Liang, H. & Xue, Y. 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. Journal of the association for information systems 11(7), 394-413.

Lowry, P., Posey, C, Bennett, R and Roberts, T. 2014. Leveraging fairness and rectance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. Information Systems Journal 25 (3). 193-230.

Limayem, M., & Hirt, S. 2003. Force of Habit and Information Systems Usage: Theory and Initial Validation. Journal Of The Association For Information Systems 4 (1), 465-95.

Magee, J. C., & Langner, C. A. 2008. How personalized and socialized power motivation facilitate antisocial and prosocial decision-making. Journal Of Research In Personality, 42(6), 1547-1559.

Markus, M. L. & Robey, D. 1988. Information technology and organizational change: causal structure in theory and research. Management science 34(5), 583-598.

Maslow, A.H. 1954. Motivation and personality. New York. Harper & Brothers.

Maslow, A.H. 2007. Motivation and personality. New Delhi. Pearson.

Maxwell, J. A. 1992. Understanding and validity in qualitative research. Harvard educational review 62 (3), 279-301.

Mazumdar, K. 1995. Classification of countries: A socio-economic approach, Social Indicators Research 34 (2), 261–273.

McClelland, D.C. & Burnham, D.H. 1995. Power is the great motivator. Harward business review 73 (1) , pp. 126-139.

Mohr, L.B. 1982. Explaining organizational behavior. San Francisco: Jossey-Bass.

Mustonen, A. 2001. Mediapsykologia. Helsinki. WSOY.

Myers, M. D. & Newman, M. 2007. The qualitative interview in IS research: Examining the craft. Information and organization, 17(1), 2-26.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. 2009. What levels of moral reasoning and values explain adherence to information security policies? An empirical study. European Journal of Information Systems 18(2), 126–139.

Möller, S. et al. 2011. Modeling the behavior of users who are confronted with security mechanismis. Computers & security 30 (4), 242-256.
Ng, B-Y, Kankahalli, A & Xu, Y. 2009. Studying users' computer security behavior using the health belief model. Decision Support Systems 46(4), 815–825.
Ng, B.-Y. & Rahim, M. 2005. A socio-behavioral study of home computer users' intention to practice security. PACIS 2005 Proceedings. Paper 20.
Niles, F. S. 1994. The Work Ethic in Australia and Sri Lanka. Journal Of Social Psychology, 134(1), 55-59.
Nurmi, J.E. & Salmela-Aro, K. (2002). Modernin motivaatiopsykologian perusta ja käsitteet. Jyväskylä. PS-kustannus.
Orligowski, W.J. & Baroudi, J.J. 1991. Studying information technology in organizations: research approaches and assumptions. Information systems research 2 (1).
Paris, L. G., & Terhaar, M. 2011. Using Maslow's Pyramid and the National Database of Nursing Quality Indicators™ to Attain a Healthier Work Environment. Online Journal Of Issues In Nursing, 16(1).
Peltonen & Ruohotie 1987. Motivaatio. Menetelmiä työhalun parantamiseksi. Helsinki. Otava.
Pentland, B.T. 1999. Building process theory with narrative: from description to explanation. Academy of management review 24(4), 711-724.
Puhakainen, P. & Siponen, M. 2010. Improving employees' compliance through information systems security training: an action research study. MIS Quarterly 34(4), 757–778.
Pulasinghage, C. 2010. Employee Motivation: What Factors Motivate Employees to Work in Nongovernmental Organizations (NGO) in Sri Lanka: A Study According to Maslow's Hierarchy of Needs Model. International Journal Of Interdisciplinary Social Sciences, 5(4), 197-211.
Ramprasad, K. 2013. Motivation and workforce performance in Indian industries. Research journal of management sciences vol 2(4), 25-29.
Randel, A. E., & Wu, A. 2011. Need for Power, Collective Identity, and Political Skill: An Investigation in Taiwan. Journal Of Social Psychology, 151(4), 395-398.
Raus, A., Haita, M., & Lazâr, L. 2012. Hierarchy of needs, perception and preference for leadership styles within a police educational institution. Transylvanian Review Of Administrative Sciences, (36), 238-255.
Reiss, S. 2009. Six Motivational Reasons for Low School Achievement. Child & Youth Care Forum 38(4), 219-225.
Reiss, S. 2004. Multifaceted nature of intrinsic motivation: the theory of 16 basic desires. Review of general psychology 8 (3), 179-193.
Reiss, S., & Wiltz, J. 2004. Why people watch reality TV? Media Psychology 6 (4), 363–378.
Reiss, S., Wiltz, J., & Sherman, M. 2001. Trait motivational correlates of athleticism. Journal of Personality and Individual Differences 30 (7), 1139–1145.

Reynolds, T.J. & Gutman, J. 1988. Laddering theory, method, analysis and interpretation. Journal of advertising research 28(1), 11-21.

Robey, D. & Newman, M. 1996. Sequential patterns in information systems development: an application of a social process model. CAN Transactions on information systems 14(1), 30-63.

Robbins, S.P. 1993. Organizational behavior: concepts, controversies and applications. Englewood Cliffs (N. J.): Prentice Hall, cop.

Ruchiwit, M. 2013. Determinants affecting the well-being of people in the Greater Mekong Subregion countries. Nursing & Health Sciences, 15(1), 94-100.

Sabahi, F. 2011. Cloud computing security threats and responses. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (pp. 245-249). IEEE.

Saguillo, J.M. 1999. Domains of sciences, universe of discourse, and omega arguments, History and philosophy of logic 20 (3-4), 267–280.

Sarker, S., Lau, F & Sahay, S. 2000. Using an adapted grounded theory approach for inductive theory building about virtual team development. ACM SIGMIS Database 32(1), 38-56.

Searle, J. 2013. Theory of mind and Darwin's legacy. Proceedings Of The National Academy Of Sciences, 110 (Supplement 2), 10343-10348.

Searle, J. 1995. The construction of social reality. New York. Free press.

Searle, J. 1990. Collective intentions and actions. Intentions in communication 401, 401.

Searle, J. 1983. Intentionality. An essay in the philosophy of mind. Cambridge: Cambridge University Press.

Schneider, K.J , Bugental J. F. T & Pierson J. F. 2001. The handbook of humanistic psychology. Thousand oaks (Calif.). Sage publications, cop.

Schrerer, K. R. 1999. Appraisal theory. In T. Dalgleish & M.J. Power (Eds) Handbook of cognition and emotion. Chichester: John Wiley & Sons, cop.

Schüler, J., Brandstätter, V., & Sheldon, K. 2013. Do implicit motives and basic psychological needs interact to predict well-being and flow? Testing a universal hypothesis and a matching hypothesis. Motivation & Emotion, 37(3), 480-495.

Schultze, U. & Avital, M. 2011. Designing interviews to generate rich data for information systems research. Information and organization 21 (1), 1-16.

Shaw, R.S. et al. 2009. The impact of information security awareness training effectiveness. Computers & Education 52 (1), 92-100.

Sieverding, M. 2008. Choice in government software procurement: a winning strategy. Journal of Public Procurement 8(1), 70-97.

Siponen, M. & Vance, A. 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly 34(3), 487–502.

Siponen, M., Mahmood, M.A. & Pahnila, S. 2009. Are employees putting your company at risk by not following information security policies? Communications of the ACM 52 (12), 145-147.

Siponen, M & Vance, A. 2014. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. European Journal of Information Systems 23 (3), 289-305.
Sirgy, M.J. 1986. A quality-of-life theory derived from Maslow's developmental perspective. American journal of economics and sociology 45 (3), 329-342.
Sockalingam, S., Khan, A., Tan, A., Hawa, R., Abbey, S., Jackson, T., & Okrainec, A. 2014. A Framework for Understanding International Medical Graduate Challenges During Transition Into Fellowship Programs. Teaching & Learning In Medicine, 26(4), 401-408.
Son, J. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management 48(7), 296–302.
Song, L., Wang, Y., & Wei, J. 2007. Revisiting motivation preference within the Chinese context: An empirical study. Chinese Management Studies, 1(1), 25-41.
Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. 2005. Analysis of end user security behaviors. Computers and security 24(2), 124-133.
Straub, D.W. 1990. Effective IS security: an empirical study. Information Systems Research 1(3), 255–276.
Sturdy, A. J. 2003. Knowing the Unknowable? A Discussion of Methodological and Theoretical Issues in Emotion Research and Organisational Studies, Organisation 10(1), 81–105.
Trauth, E.M. 1997. Achieving the research goal with qualitative methods: Lessons Learned along the way. Information systems and qualitative research. Springer US, 225-245.
Valacich, J. S., Parboteeah, D. V., & Wells, J. D. 2007. The online consumer's hierarchy of needs. Communications Of The ACM, 50(9), 84-90.
Van de ven, H. & Huber, G.P. 1990. Longitudinal field research methods for studying processes of organizational change. Organizational science 1(3), 213-219.
Van de ven, H. 1992. Suggestions for studying strategy process: a research note. Strategic management journal 13, 169-188.
Vance, A. & Siponen, M.T. 2012. IS security policy violations: a rational choice perspective. Journal of Organizational and End User Computing (JOEUC) 24 (1), 21-41.
Vasconcellos, J. 2001. Foreword. In K.J. Schneider, J.F.T. Bugental & J.F Pierson (Eds) The handbook of humanistic psychology. Leading edges in theory, research and practice. Thousand oaks (Calif.) Sage publications, cop.
Veenhoven, R. & Erhardt, J. 1995. The cross-national pattern of happiness. Test of predictions implied in three theories of happiness.Social Indicators Research 34 (1), 33–68.
Vuorinen, R. & Tuunala, E. 1995. Psykologian perusteet. Aivot ja psyyke. Keuruu. Otava.

Wang, J. et al. 2010. Drivers of information security search behavior: an investigation of network attacks and vulnerable disclosures. ACM Transactions on management Information systems 1(1).

Wang, Cong, et al. 2010. Privacy-preserving public auditing for data storage security in cloud computing. INFOCOM, 2010 Proceedings IEEE. Ieee, 1-9.

Weick, K.E. & Sutcliffe, K.M. 2005. Organizing and the process of sensemaking. Organization science 16 (4), 409-421.

Weinstein, N.D., Rothman, A.J., & Sutton, S.R. 1998. Stage theories of health behavior: conceptual and methodogical issues. Health psychology 17 (3), 290-299.

Wertz, F.J. 2001. Humanistic psychology and the qualitative research tradition. In K.J. Schneider, J.F.T. Bugental & J.F. Pierson (Eds) The handbook of humanistic psychology. Leading edges in theory, research and practice. Thousand oaks (Calif.) Sage publications, cop.

Whetten, D. A. (2002). Modelling-as-Theorizing: A systematic methodology for theory development. London. SAGE publications Ltd. London..

Whetten, D.A. (1989). What constitutes a theoretical contribution? Academy of management review 14 (4).

Wiley, C. (1997). What motivates employees according to over 40 years of motivation surveys? International Journal of Manpower, 18(3), 263-280.

Vilkko-Riihelä, A. 1999. Psyyke: psykologian käsikirja. Porvoo. WSOY.

Will, L. 1996. How to connect. The Lancet, 348 (9020), 10.

Willison, R. & Warkenting, M. 2013. Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly 37(1), 1-20.

Woon, I., Tan, G. W. & Low, R. 2005. A protection motivation theory approach to home wireless security. ICIS 2005 Proceedings, 31.

Wu, L., Du, X. & Fu, X. 2014. Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. Communications Magazine, IEEE 52 (3), 80-87.

Yang, C. et al. 2011. An empirical study of the existence, relatedness, and growth (ERG) theory in consumer's selection of mobile value-added services. African Journal of Business Management 5 (19), 7885-7898.

LIITTEET

LIITE 1. HAASTATTELUKYSYMYKSET

Interview questions: Development of computer users' IS security behavior

The purpose of this study is to understand the process of computer users' IS security behavior (van de Ven 1992; Weinstein 1998). The study explores personal computer use and the change of computer use in the course of time. Especially the study is interested in exploring how the IS security practices, securing the data and the devices (for example constructing strong passwords and back-up copying) has changed with time and how and why behavior changes in relation to varying elements (threats, safaguards, networks, etc).

The purpose of the study is not to evaluate behavior but understand behavior and the change of behavior and how the behavior changes due to own experiences. The study underscore that there is no right or wrong way to act.

Interview answers of the study will be processed with confidence.

The study explores participants "personal constructs, which comprise elements, constructs, and links" (Schulze & Avital, 2011; see also Marsden & Littler 1998)

a. Participants' IS security practices (= elements),
b. Reasons behind these practices (= constructs),
    - Present:
        - Reasons for using IS security practices currently
        - Reasons for not using certain IS security practices currently
    - Future:
        - Reasons that would make a person use certain IS security practices in the future
        - Reasons that would make a person abandon certain IS security practices occasionally or permanently in the future?
    - Past:
        - Reasons that influenced a person's decisions to use certain IS security practices in the past?
        - Reasons that prevented a person in using certain IS security practices in the past?

In the interviews it will be used laddering – technique for laddering attributes, consequences, and values (Reynolds & Gutman1988; Shultze & Avital 2011)

The question group	Purpose of questions
1. Background questions a. Age b. Gender (mark down) c. Education d. Occupation and work experience e. Nature and amount of personal computer use	Mapping personal and contextual aspects → Create a list of interviewees' computer use practices, which are reflected from the security point of view beginning from the question group 2 When interviewee mentions purpose for computer use, interviewee tries to find out

I. How do you use computer and Internet, for what purpose? II. What kind of needs do you have for computer use? III. What kind of computer you have? IV. How much you use computer and how long you have used it? V. Has there emerged change in these practices	what is a need behind that purpose
2. Conceptualizing current IS security behavior (using different IS security practices) a. Describe (as many ways as possible of) how do you take IS security into account in your personal computer use (go through <u>all areas</u> of computer use listed in question 1e)	Element selection (Marsden & Litter 2000): Understanding how interviewees consider IS security and is security behavior → Create a list of IS security practices that interviewees use and the descriptions of these practices → rest of the interview is concentrated on understanding reasons for using these practices, and processes of development of using these practices
3. Issues that have influenced on the development of current IS security behavior in the past → use laddering - Reacting possible answers through asking why these issues brought up are important to the person → go through all practices a listed in the previous question 2a using laddering technique (Reynolds & Gutman 1988) - when interviewee mentions reasons for behavior, for example certain events, time ordering of them will be amplified and did the computer user think about the purpose of the events for their IS security behavior - Describe accurately what you mean by reasons: are there differences between IS security practices (has the same reason different meaning in some other behavior type) b. What you think you gain by applying this IS security practice or lose if you do not apply it c. Could you do something more in addition to this IS security practice d. Has your behavior (or attitudes) changed somehow since you first time	Construct elicitation (Marsden & Litter 2000): Finding out reasons for current IS security behavior • reasons for behavior • barriers of change • a possibility of multiple ways of adopting IS security practices • a possible existence of multiple phases before current situation • a possibility for relapses If necessary, the interviewee will be told different situations when it is possile to completely/ occasionally avoid certain practices COMPLETELY: - increase of trust - security problem - technological development - experience of the threat decreases OCCASIONALLY: - forgetting - mistake - need for doing certain task - using time of the service will be short

started to conduct "the security practice X" until now? Why or why not? - use laddering - on the grounds of results of previous interviews interviewer can suggest how the behavior may have changed and what reasons may have affected to change e. How did you learn these practices? f. Were there some kind of obstacles in the way that prevented you from adopting IS security practices? g. If learning was not easy, what would have been making it easier for you to adopt these practices? h. What kind of emotions did you meet before you started to conduct these IS security practices? i. Would it be possible to you to give up completely/ occasionally avoid certain IS security practices? In what circumstances? Why? If you have given up certain IS sec practices what kind of <u>needs</u> for computer use did you have then? → use laddering j. What do you think you would lose/gain if you give up completely or occasionally avoid using the practice? → use laddering	
4. Issues influencing on the development of current IS security behavior in the future a. Are you satisfied with the IS security of your personal computer use? Why? → use laddering technique b. Have you experienced any IS security problems? What kind of? What does these problems mean to you? What kind of emotions these experiences aroused? → use laddering technique c. Do you think you should change your current IS security behavior? How, why? Is this important to you? Why or why not? → use laddering technique d. What it would require to make you use those IS security practices that you are not using at the moment? e. What prevents you from making changes you consider could be useful? → use laddering technique	Construct elicitation (Marsden & Litter 2000): Finding out the reasons for development of current IS security behavior - barriers of change

LIITE 2. STAGE-TEORIAN OMINAISUUDET (WEINSTEIN ET AL., 1998)

1)	Luokittelyjärjestelmä tasojen määrittelyyn	Tasot ovat teoreettisia konstruktioita. Jokaisella stage-teorialla on vaatimuksia, jotka määrittävät mihin kategoriaan henkilö kuuluu. Henkilöt kullakin tasolla jakavat ominaisuudet, jotka määrittävät tason mutta samalla tasolla olevien henkilöiden kesken voi olla pientä vaihtelua ja eroja. Kuitenkin tasojen väliset erot ovat suurempia kuin tason sisällä olevat erot.
2)	Tasojen järjestys	Stage-teoriassa tasojen järjestys täytyy täsmentää. Tasojen läpi voi kulkea yksi tärkein polku, mutta tämän lisäksi stage-teoriassa voi olla muita toiminnan polkuja. Suurimman osan ihmisistä tulisi seurata tärkeintä polkua, sillä muutoin teoriaa ei voida pitää tarkkana ja käytännöllisenä.
3)	Yleiset tekijät/ attribuutit samalla tasolla olevilla ihmisillä	Ihmiset, jotka ovat samalla tasolla kohtaavat samanlaisia vaikuttimia /interventioita, jotka auttavat heitä etenemään. Tekijät, jotka ovat vastuussa siirtymistä tasolta toiselle voivat olla sidoksissa tiettyyn käyttäytymiseen: eri faktorit liittyvät erityyppiseen käyttäytymiseen.
4)	Erilaiset tekijät/attribuutit eri tasoilla olevilla ihmisillä	Tekijät /attribuutit ovat taso-sidonnaisia (stage –specific): jotkut tekijät /vaikuttimet ovat tärkeämpiä siinä vaiheessa, kun henkilö päättää toimia ja toisenlaisia tekijöitä/vaikuttimia tarvitaan ennen kuin henkilö toteuttaa tämän päätöksen.

LIITE 3. AIEMPI TUTKIMUSKIRJALLISUUS, OSA 2

Tekijä	Koti/työkonteksti (K/T)	Tutkimusmenetelmät ja kuvaus aineiston keruusta ja analyysista	Taustateoriat, muuttujat ja tutkimuksen päätulokset
Anderson & Agarwal (2010)	K	**Ryhmä 1: kysely** **Ryhmä 2: kokeellinen tutkimus** Kyselyn kohderyhmänä Internet palvelujen tilaajia ja liiketoiminnan opiskelijoita. (N=594) Analysointityökaluna PLS. Kokeen kohderyhmänä markkinoinnin opiskelijoita (N=101). Analysointi toteutettiin varianssianalyysilla (ANOVA).	
Boss & Kirsch et al. (2009)	T	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laisen terveyskeskuksen työntekijät (N=1698). Analysointityökaluna PLS.	Taustateoriat: Control theory, Mandatoriness Muuttujat: Tietoturvapolitiikkojen määrittely (specification) Ohjeiden noudattamisen arviointi (evaluation) Palkkio ohjeiden noudattamisesta (reward) Tietoisuus tietoturvapolitiikkojen pakollisuudesta (mandatoriness) Suojaustoimet (precautions) Tietokoneen käytön miellyttävyys (CSE) Välinpitämättömyys (apathy)

			Tietoturvapoliiikkojen määrittely ja ohjeiden noudattamisen arviointi vaikuttavat tietoisuuteen tietoturvapolitiikkojen pakollisuudesta, mikä vaikuttaa suojaustoimien käyttöönottoon.
Bryant & Campbell (2006)	K	**Ryhmä 1: kysely** Kohderyhmänä australialaiset liiketoiminnan opiskelijat (N = 884). Aineiston analyysi toteutettiin ei-parametrisillä testeillä.	Taustateoriat:- Muuttujat: - Tulokset osoittavat, että useat tietokoneen käyttäjät ovat tietoisia hakkereiden ja virusten aiheuttamista riskeistä ja ottavat ensiaskeleita välttääkseen niitä, esimerkiksi laativat salasanoja, jotka ovat yli 8 merkkiä pitkiä. Toisaalta tietokoneen käyttäjät eivät ymmärrä riskejä, joita puutteellisiin salasanakäytänteihin liittyy ja mitä tietoturvarikkomuksista voi seurata. Esimerkiksi helposti arvattavien salasanojen käyttö on yleistä.
Bulgurcu, Cavusoglu, & Benbasat (2010)	T	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laisisten organisaatioiden työntekijät (N=928). Aineiston analyysimenetelmänä PLS.	Taustateoriat: Theory of planned behavior (TPB), Rational choice theory Muuttujat: Tietoturvatietoisuus (information security awareness) Tietoisuus ohjeiden noudattamisen hyödyistä (perceived benefit of compliance) Tyytyväisyys (intrinsic benefit)

	Resurssien turvallisuus (safety of resources) Palkkiot (rewards) Tietoisuus ohjeiden noudattamisen haitoista (perceived cost of compliance) Työn este (work impediment) Tietoisuus noudattamattomuuden haittapuolista (perceived cost of noncompliance) Tyytymättömyys tietoturvaohjeiden noudattamattomuudesta (intrinsic cost) Resurssien haavoittuvaisuus (vulnerability of resources) Rangaistukset (sanctions) Asenne (attitude) Normatiiviset uskomukset (normative beliefs) Luottamus omiin kykyihin noudattaa ohjeita (self-efficacy to comply) Aikomus noudattaa ohjeita (intention to comply) Asenne, normatiiviset uskomukset ja luottamus omiin kykyihin tietoturvaohjeiden noudattamisessa vaikuttavat merkittävästi aikomukseen noudattaa tietoturvaohjeita.

Bunnel et al (1997)	K	**Ryhmä 1: kysely** Tutkimukseen osallistui 2 ryhmää: varsinaiset vastaajat (N= 90) ja heille merkittävät henkilöt (84). Varsinaiset vastaajat olivat U.S.A: laisia psykologian opiskelijoita. Pääasiallisena analyysimenetelmänä varianssianalyysi.	Taustateoriat:- Muuttujat: - Tutkimuksessa selvitettiin salasanan laatimistekniikoita (kognitiiviset salasanat ja sana-assosiaatiot) ja kuinka tekniikoiden avulla laaditut salasanat muistetaan ja toisaalta kuinka hyvin ne ovat ulkopuolisten arvattavissa. Faktoihin perustuvat kognitiiviset yksiköt muistettiin paremmin kuin mielipiteisiin perustuvat. Toisaalta ihmiset jotka olivat läheisiä koehenkilöille, pystyivät arvaamaan useita faktoihin perustuvia yksiköitä. Sana-assosiaatioihin perustuvat yksiköt olivat vaikeasti ulkopuolisten arvattavissa mutta toisaalta niiden muistaminen oli vaikeaa.
Caldwell. & McGarvey (2013)	K	**Ryhmä 1: kysely** Kohderyhmänä lukio-opiskelijat ja tavalliset tietokoneen käyttäjät. Analyysimenetelmä konfirmatorinen faktorianalyysi (AMOS).	Taustateoria: Theory of planned behavior Muuttujat: Asenne tietoturvauhkia kohtaan (attitude towards cyberthreats) Tietoisuus vertaisryhmästä (perceptoins of peer group) Tietoisuus kyvystä ehkäistä uhkaa (perceived ability to prevent threat) Aikomus (intention) Käyttäytyminen (behavior)

			Tietokoneen käyttäjien aikomuksiin käyttäytyä tietoturvallisesti eivät merkittävästi vaikuta heidän asenteensa, tietoisuus kyvystä ehkäistä uhkaa tai tietoisuus vertaisryhmästä.
Chan, Woon et al. (2005)	T	**Ryhmä 1: kysely** Kohderyhmänä logistiikka- ja petrokemian alan työntekijät (N=119). Aineisto analysoitu PLS työkalulla.	Taustateoria: safety climate Muuttujat: Ylemmän johdon käytännöt (upper managament practices) Oman esimiehen käytännöt (direct supervisory practices) Työtovereiden toiminta (co-worker socialization) Tietoisuus tietoturvailmapiiristä (perception of information security climate) Luottamus omiin kykyihin (self-efficacy) Tietoturvaohjeiden noudattaminen (compliant behavior) Johdon käytännöt, oman esimiehen käytännöt ja työtovereiden toiminta vaikuttavat työntekijöiden tietoisuuteen siitä, millainen tietoturvailmapiiri organisaatiossa on. Tietoisuus tietoturvailmapiiristä ja luottamus omiin kykyihin vaikutti positiivisesti tietoturvaohjeiden noudattamiseen
D'Arcy, Hovav, & Galletta (2009)	T	**Ryhmä 1: kysely**	Taustateoria: General deterrence

		Kohderyhmänä U.S.A: laisten organisaatioiden työntekijät (N=304). Aineiston analyysissa käytetty PLS- työkalua.	theory (GT) Muuttujat: Aikomus väärinkäyttää tietojärjestelmiä (IS misuse intention) Tietoisuus seuraamusten varmuudesta (perceived certainty of sanctions) Tietoisuus seuraamusten vakavuudesta (perceived severity of sanctions) Tietoturvapolitiikat (security policies) Tietoturvakoulutus- ja tietoisuus ohjelma (SETA program) Tietokoneenkäytön seuranta (computer monitoring) Tietojärjestelmien väärinkäyttöä estävät työntekijän tietoisuus tietoturvapolitiikoista, tietoturvakoulutus – ja tietoisuusohjelma sekä tietokoneenkäytön seuranta. Tietoisuus seuraamusten vakavuudesta vähentää tehokkaammin väärinkäyttöä kuin tietoisuus seuraamusten varmuudesta.
Dinev et al. (2009)	K	**Ryhmä 1: kysely** Kohderyhmänä oli U.S.A:laiset tietojärjestelmien asiantuntijat sekä opiskelijat etelä-Koreassa ja U.S.A:ssa. (N=559). Analyysissa on käytetty SEM-mallinnusta (li-	Taustateoria: Theory of planned behavior Muuttujat: Aikomus (behavioral intention) Asenteet tietoturvaa kohtaan (attitudes toward behavior)

		säksi multigroup analysis).	Sosiaalinen paine (subjective norm) Tietoisuus suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (Perceived behavioral control) Helppokäyttöisyys (ease of use) Tietoisuus hyödyllisyydestä (perceived usefulness) Tietoisuus (awareness) Tietoisuus kontrolloitavuudesta (controllability) Luottamus omiin kykyihin (self-efficacy) Maskuliinisuus (masculinity) Epävarmuuden välttäminen (uncertainty avoidance) Individualismi (individualism) Etäisyys vallasta (power distance) Pitkäkestoinen orientaatio (long-term orientation) Tutkimuksessa selvitettiin kulttuuristen moderaattorien (epävarmuuden välttäminen, etäisyys vallasta, maskuliinisuus, individualismi ja pitkäkestoinen orientaatio) vaikutusta tietokoneen käyttäjien asenteisiin ja suojaustoimenpiteiden käyttöön etelä-Koreassa ja U.S.A:ssa. Tutkimus osoitti, että individualismi, masku-

			liinisuus, etäisyys vallasta ja epävarmuuden välttäminen vaikuttavat merkitsevästi tietokoneenkäyttäjien asenteisiin ja suojaustoimien käyttöön.
Dinev & Hu (2007)	K	**Ryhmä 1: kysely** Kohderyhmänä U:S.A:laiset tietojärjestelmäasiantuntijat ja opiskelijat (N=339). Analysointityökaluna rakenneyhtälömalli (SEM), ja Lisrel	Taustateoria: theory of planned behavior Muuttujat: Teknologiatietoisuus (technology awareness) Tietoisuus hyödyllisyydestä (perceived usefulness) Tietoisuus helppokäyttöisyydestä (perceived ease of use) Luottamus omiin kykyihin (self-efficacy) Tietoisuus kontrolloitavuudesta (controllability) Asenne (attitude) Sosiaalinen paine (subjective norm) Tietoisuus suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (Perceived behavioral control) Aikomus ottaa suojaustoimenpide käyttöön (behavioral intention) Aikomukseen käyttää suojaavia teknologioita vaikuttaa tietoisuus uhkista, joita negatiiviset teknologiat kuten vakoiluohjelmat tuovat

			mukanaan. Sosiaalisen paineen vaikutus on vahvempi edistyneemmillä tietokoneenkäyttäjillä kuin tavallisilla tietokoneen käyttäjillä.
Dodge et al. (2007)	K	Tutkimusmenetelmää ei mainita Kohderyhmänä U.S.A: laisen sotakorkeakoulun opiskelijat. Tutkimuksen 1. vaiheessa N = 4118 ja toisessa vaiheessa N = 4136. Analyysimenetelmää ei mainita	Taustateoriat: - Muuttujat: - Tutkimuksessa tehtiin harjoitus, jossa arvioitiin opiskelijoiden alttiutta vastata sähköpostitse saapuviin tiedon kalasteluyrityksiin. Opiskelijat luovuttivat sellaista tietoa luvattomille käyttäjille, jota ei olisi saanut luovuttaa ja asettivat itsensä haitalliselle koodille avaamalla sähköpostin liitetiedostoja. Vanhemmat opiskelijat vastasivat huomattavasti harvemmin kalastelyrityksiin kuin 1. vuoden opiskelijat ja toisaalta myös raportoivat kalasteluyrityksistä enemmän eteenpäin.
Furnell, Tsaganidi & Phippen (2008)	K	**Ryhmä 3: haastattelu** Kohderyhmänä tietokoneen käyttäjät Iso-britanniasta (N = 20 haastateltavaa).	Taustateoriat: - Muuttujat: - Vaikka tietokoneen käyttäjät ovat tietoisia ongelmista, joita tietoturvan laiminlyöminen aiheuttaa, se ei motivoi heitä ottamaan suojatoimenpiteitä käyttöön. Tietokoneen käyttäjien tietoisuus siitä, että he ovat itse vastuussa tietokoneensa suojaamisesta, ei

			aiheuta huolta siitä, mitä tietoturvaongelmista voi seurata.
Furnell et al. (2007)	K	**Ryhmä 1: kysely** Kohderyhmänä kotitietokoneen käyttäjät (N=415). Analyysimenetelmää ei mainita	Taustateoriat: - Muuttujat: - Tietokoneen käyttäjät tuntevat tietoturvauhat, jotka kohdistuvat heidän henkilökohtaiseen tietokoneeseensa ja käyttävät monia suojaustoimia, mutta kuitenkin monilla alueilla toivottava tieto ja ymmärrys puuttuu. Aloittelevilta tietokoneen käyttäjiltä puuttui tietoa ja itsevarmuutta suojautua ongelmilta mutta myös kokeneilla tietokoneen käyttäjillä oli puutteita tiedoissa ja ymmärryksessä, esimerkiksi ohjelmistopäivitysten ja sovellusten tietoturvaominaisuuksien suhteen.
Furnell, Jusoh & Katsabas (2006)	K	**Ryhmä 1: kysely** Kohderyhmänä Microsoftin ohjelmistojen (Windows XP, IE, Word ja outlook express) loppukäyttäjät (N=342). Analyysimenetelmää ei mainita	Taustateoriat: - Muuttujat: - Tietokoneen käyttäjät kohtaavat ongelmia, kun he yrittävät ymmärtää ja käyttää tunnettujen ohjelmistosovellusten tietoturvaominaisuuksia. Tämän seurauksena tietoturvaominaisuuksia ei käytetä tai ne konfiguroidaan väärin.
Furnell (2005)	K	Tutkimusmenetelmää ei mainita Tutkimuksessa käytetään Microsoft Word-ohjelmistoa tarjoamaan esimerkkejä tyypillisistä	Taustateoriat: - Muuttujat: - Sovellusten ja tietojärjestelmien tietoturvaominaisuuksien esille-

		ongelmista, joita käyttäjät kohtaavat erilaisia sovelluksia ja tietojärjestelmiä käyttäessään. Analyysimenetelmää ei mainita	tuonti ja käytettävyys on puutteellista. Käyttäjät kohtaavat ongelmia, kun he yrittävät löytää, ymmärtää ja käyttää tietoturvaominaisuuksia.
Guo et al. (2011)	T	**Ryhmä 1: kysely** Kohderyhmänä erilaisten organisaatioiden työntekijät (N=335). Analyysi-työkaluna PLS.	Taustateoriat: The composite behavior model, Theory of reasoned action (TRA), The theory of planned behavior (TPB) Muuttujat: Asenne tietoturvapolitiikkaa kohtaan (Attitude toward security policy) Hyöty työn kannalta (relative advantage for job performance) Tietoisuus tietoturvariskistä (perceived security risk) Tietoisuus seuraamuksista (perceived sanctions) Työyhteisön normit (workgroup norm) Tietoisuus tietoturvapolitiikkojen sopivuudesta ammatilliseen imagoon (perceived identity match) Asenne (attitude towards NMSV Aikomus rikkoa tietoturvapolitiikkoja (NMSV intention) Tulokset osoittivat että hyöty työn kannalta (relative advantage for job performance), tietoisuus toetoturvariskistä (perceived security

			risk), työyhteisön normit (work-group norm) ja tietoisuus tietoturvapolitiikkojen sopivuudesta ammatilliseen imagoon (perceived identity match)ovat keskeisiä asioita, jotka vaikuttavat siihen, aikooko työntekijä rikkoa tietoturvaohjeita ilman aikomusta vahingontekoon.
Harrington, Anderson & Agarwal (2006)	K	**Ryhmä 2: kokeellinen tutkimus** Kohderyhmänä U.S.A: laiset yliopisto-opiskelijat (N=101) Tutkimusaineiston analyysissa käytetty varianssianalyysia (ANOVA).	Taustateoriat: goal frame ja self-view Muuttujat: - Tutkimuksessa koehenkilöitä kehotettiin avaamaan web-sivu, jonka viesti oli joko positiivisesti tai negatiivisesti sävyttynyt. Tämän jälkeen heille tehtiin sivustoon liittyviä kysymyksiä. Tulosten mukaan ne että viestit, jotka korostivat tietoturvallisen käyttäytymisen positiivisia vaikutuksia olivat tehokkaita lisäämään aikomusta toteuttaa tietoturvaa kotikontekstissa.
Harrington, S. J. (1996)	T	**Ryhmä 1: kysely** Kohderyhmänä U.S.A:laiset työntekijät (N=219). Aineiston analysoinnissa käytetty ANOVA-analyysia, Spearmanin korrelaatioanalyysia ja yleistettyä lineaarista mallia (GLM).	Taustateoria: general deterrence theory (GT) Muuttujat: Eettiset ohjeet (codes of ethcs) Vastuun kieltäminen (denial of responsibility) Aikomus toteuttaa tietoturvaloukkaus (computer abuse intention)

			Tietoturvaloukkauksen oikeutus (computer abuse judgment) Organisaation eettiset ohjeet voivat vaikuttaa epäeettistä käytöstä vähentävästi niihin työntekijöihin, jotka kieltävät oman vastuunsa käyttäytymisestään. Tietojärjestelmiä koskevilla ohjeilla oli suora vaikutus tietoturvarikkomusten harkintaan ja aikomukseen tehdä rikkomus tasaisesti kaikkien työntekijöiden kohdalla. Tulokset osoittivat, että oman vastuun kieltäminen on suoraan yhteydessä harkintaan tehdä tietoturvarikos.
Herath et al. (2014)	K	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laiset yliopisto-opiskelijat (N=144). Aineiston analysointi toteutettu PLS-työkalulla.	Taustateoriat: TAM ja TTAT Muuttujat: Tietoisuus riskeistä (EmailRisk perception) Tehokkuus (EmailScreen efficacy) Asenne (aAuth_Attitude) Hyödyllisyys (eAuth_Usefulness) Helppokäyttöisyys (eAuth_Ease of use) Reagointi (eAuth_Responsiveness) Huoli yksityisyydestä (Privacy concern) Yksityisyysasioiden esilletuominen (Privacy Notification)

			Aikomus käyttää suojaustoimea (eAuthAdopt Intention) Helppokäyttöisyys ja hyödyllisyys ovat merkittäviä suojaustoimenpiteen valintaan vaikuttavia tekijöitä. Tietoisuus riskeistä vaikuttaa merkittävästi hyödyllisyyteen ja aikomukseen käyttää suojaustoimenpidettä eAuth (Email authentication service).
Herath & Rao (2009a)	T	**Ryhmä 1: kysely** Kohderyhmänä USA: laiset työntekijät eri ammattiryhmistä (N=312). Aineiston analyysi toteutettu PLS-menetelmällä.	Taustateoriat: General deterrence (GDT), Protection motivation theory (PMT), Theory of planned behavior (TPB), Decomposed theory of planned behavior (DTPB), Organizational commitment (OC) Muuttujat: Rangaistuksen vakavuus (punishment severity) Kiinnijäämisen varmuus (detection certainty) Tietoisuus tietoturvarikkoumuksen mahdollisuudesta (perceived propability of security breach) Tietoisuus tistoturvarikkomksen vakavuudesta (perceived severity of security breach) Huoli tietoturvarikkomuksesta (security breach concern level) Suojaustoimenpiteen tehokkuus

		(response efficacy) Kustannukset (response cost) Aikomus noudattaa tietoturvaohjeita) (security policy compliance intention) Asenne tietoturvapolitiikkaa kohtaan (security policy attitude) Luottamus omiin kykyihin (self-efficacy) Sosiaalinen paine (subjective norm) Tietoisuus muiden käytöksestä (decriptive norm) Resurssien saatavuus (resource availability) Sitoutuminen työhön (organizational commitment) Tulokset osoittivat, että asenteisiin tietoturvapolitiikkaa kohtaan vaikuttavat tietoisuus uhasta ja rikkomusten vakavuudesta, suojatoimen tehokkuus, luottamus omiin kykyihin ja suojaustoimen kustannukset. Työhön sitoutuminen ja sosiaaliset seikat vaikuttavat merkittävästi aikomukseen noudattaa tietoturvaohjeita Resurssien saatavuus (esim. tie-

			tourvaohjeet) vaikuttaa merkittävästi luottamukseen omiin kykyihin, mikä taas on merkittävä ennustaja aikomukselle noudattaa ohjeita.
Herath & Rao (2009b)	T	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laiset työntekijät (N=312). Aineiston analyysissa käytetty PLS- työkalua.	Taustateoriat: Principal agent theory, General Deterrence (GT), Socio-economic theory of compliance Muuttujat: Rangaistuksen vakavuus (severity of penalty) Suojaustoimenpiteiden varmuus (certainty of detection) Normatiiviset uskomukset (normative beliefs) yötovereiden käyttäytyminen (peer behavior) Tietoisuus suojaustoimen tehokkuudesta (perceived effectiveness) Tulokset osoittivat, että tietoturvakäyttäytymistä säätelevät niin sisäiset kuin ulkoisetkin motivaatiotekijät. Sosiaalinen paine ja työtovereiden käytös vaikuttavat työntekijöiden tietoturvakäyttäytymiseen. Tietoisuus siitä, kuinka tehokasta suojaustoimen käyttö on, vaikuttaa aikomukseen noudattaa tietoturvaohjeita. Myös suojaustoimen varmuus vaikutti

			merkittävästi aikomukseen noudattaa tietoturvaohjeita.
Hsu, Shih, Hung, and Lowry (2015)	T	**Ryhmä 1: kysely** Kohderyhmänä taiwanilasten yritysten esimiehet (N=78) ja alaiset (N=260). Analyysimenetelmänä PLS.	Taustateoria: social control theory (SCT) Muuttujat: Osallistuminen (involvement) Kiintymys (attachment) Uskomus (belief) Sitoutuminen (commitment) Määrittely (specification) Arviointi (evaluation) Palkkio (reward) Sosiaalinen valvonta (social control) Formaali valvonta (formal control) Tietoturvaohjeiden noudattaminen (in-role behaviors) Tietoturvaohjeisiin liittymätön tietoturvakäyttäytyminen (extra-role behaviors) Tietoturvaohjeisiin liittymätön tietoturvakäyttäytyminen on tärkeää ottaa huomioon tietoturvapolitiikkoja tehostettaessa. Formaalit valvontamenettelyt samoin kuin sosiaalinen kontrolli vahvistavat niin tietoturvaohjeiden noudattamista kuin niihin liittymätöntä tietoturvakäyttäytymistäkin.
Hu, Xu., Dinev & Ling (2011)	T	**Ryhmä 1: kysely**	Taustateoriat: Rational choice,

		Kohderyhmänä kiinalaiset työntekijät 5 organisaatiossa (N=227). Analyysimenetelmänä PLS.	Self-control, Deterrence, Shame, Moral beliefs Muuttujat: Alhainen itsekontrolli (low self-control) Moraaliset uskomukset (moral beliefs) Tietoisuus seuraamusten varmuudesta (perceived certainty of sanctions) Tietoisuus rangaistuksen vakavuudesta (perceived severity of sanctions) Tietoisuus rangaistuksen nopeudesta (perceived celerity of sanctions) Tietoisuus materiaalisista hyödyistä (perceived extrinsic benefits) Tietoisuus ei- materiaalisista hyödyistä (perceived intrinsic benefits) Tietoisuus formaaleista riskeistä (perceived formal risk) Tietoisuus informaaleista riskeistä (perceived informal risk) Tietoisuus häpeäntunteen riskistä (perceived risk of shame) Aikomus toteuttaa loukkaus (intention to commit violation) Tutkimuksessa laaditaan tietoturvarikkomusten tekemistä selittävä

			malli, joka pohjautuu useisiin kriminologian teorioihin. Tutkimuksessa myös testataan mallia empiirisesti. Tulokset osoittivat, että tietoturvakäyttäytymiseen vaikuttaa pelotteita enemmän itsekontrolli ja moraaliset uskomukset.
Johnston & Warkenting (2010)	T	**Ryhmä 2: kokeellinen tutkimus** Kohderyhmänä USA:laisen yliopiston työntekijät ja opiskelijat (N=311). Analyysimenetelmänä PLS.	Taustateoriat: Protection motivation theory (PMT), Fear appeal theory Muuttujat: Suojaustoimenpiteen tehokkuus (response efficacy) Sosiaalinen vaikutus (social influence) Luottamus omiin kykyihin (self-efficacy) Tietoisuus alttiudesta (perveived threat susceptibility) Tietoisuus vakavuudesta (perceived severity) Tutkimus osoitti, että pelkoa sisältävät elementit (fear appeals) vaikuttavat tietokoneen käyttäjän aikomukseen noudattaa suositeltuja tietoturvaohjeita.
Kritzinger & von Solms (2010)	K	Tutkimusmenetelmää ei mainita Analyysimenetelmää ei mainita	Taustateoriat: - Muuttujat: - Tutkimuksessa esitetään malli tietoturvatietoisuuden lisäämisek-

			si. Malli on 2-osainen: 1. osassa esitetään tietoturvaan liittyvä informaatiota ja toisessa osassa käyttäjän oletetaan omaksuvan 1. osassa omaksutun asian täytäntöön.
Kumar et al. (2008)	K	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laiset yliopisto-opiskelijat (N=130). Analyysimenetelmänä konfirmatorinen faktorianalyysi (PLS).	Taustateoria: Technology acceptance model (TAM) Muuttujat: Tietoisuus hyödyllisyydestä (perceived usefulness) Tietoisuus helppokäyttöisyydestä (perceived ease of use) Aikomus käyttää palomuuria (intention to use firewall) Asenne palomuurin käyttöön (attitude towards using firewall) Huoli tietokoneesta (computer anxiety) Tietoisuus suojaustoimenpiteistä (awareness of security measures) Huoli tietojen yksityisyydestä (concern for information privacy) Huoli tietokoneesta, tietokoneen käyttäjän tietoisuus yleisimmistä suojaustoimenpiteistä ja huoli tiedon yksityisyydestä vaikuttavat palomuurin käyttöönottoon kotikontekstissa.
La Rose et al. (2008)	K	**Ryhmä 1: kysely** **Ryhmä 2: kokeellinen tutkimus**	Taustateoriat: - Muuttujat: - Henkilöt, jotka kokevat että Inter-

		Kyselyssä kohderyhmänä U.S.A: laiset opiskelijat (N=566). Analyysi toteutettu chi-square -analyysilla. Kokeen kohderyhmänä lukio-opiskelijat (N= 206).	netin käyttöön liittyvä tietoturva on heidän omalla vastuullaan, suojaavat tietojaan merkittävästi enemmän kuin ne, jotka eivät ajattele tällä tavalla. Koehenkilöiden tietoturvan edistäminen lisääntyi sen jälkeen, kun he osallistuivat interventioihin, joissa korostettiin sitä, että tietoturva on heidän omalla vastuullaan.
Lee & Kozar (2005)	K	**Ryhmä 1: kysely** Kohderyhmänä Internetin käyttäjät, jotka ovat ottaneet käyttöön/harkitsevat virustorjuntaohjelman käyttöönottoa (N=212). Aineisto analysoitiin PLS-menetelmällä.	Taustateoria: Theory of planned behavior (TPB) Muuttujat: Asenne (attitude) Sosiaalinen vaikutus (social influence) Tietoisuus suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (Perceived behavioral control) Aikomus ottaa suojaustoimenpide käyttöön (adoption intention) Suojaustoimenpiteen käyttöönotto (adoption) Hyöty (relative advantage) Moraalinen yhteensopivuus (moral compatibility) Helppokäyttöisyys (ease of use) Sosiaalinen paine (subjective norm) Näkyvyys (visibility)

			Sosiaalinen asema (image) Kokeiltavuus (trialability) Tietokoneen teho (computer capacity) Tietoisuus kustannuksista (perceived cost) Hyöty, moraalinen yhteenspivuus, näkyvyys, sosiaalinen asema, kokeiltavuus sekä tietokoneen teho vaikuttavat merkittävästi virustorjuntaohjelman käyttöönottoon.
Lee & Kozar (2008)	K	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laiset tietokoneen käyttäjät 1. vaiheessa N = 373, 2. vaiheessa N= 305. Aineisto analysoitiin PLS-työkalulla.	Taustateoriat: Theory of planned behavior (TPB), innovation diffusion theory, IT ethics/morality Muuttujat: Asenne (attitude) Sosiaalinen paine (subjective norm) Tietoisuus suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (Perceived behavioral control) Hyöty (relative advantage) Helppokäyttöisyys (ease of use) Yhteensopivuus (compatibility) Näkyvyys (visibility) Sosiaalinen asema (image) Kokeiltavuus (trialability) Luottamus omiin kykyihin (self-efficacy) Tietokoneen teho (computer capa-

			city) Tietoisuus kustannuksista (perceived cost) Moraalinen velvollisuus (moral oblication) Vastuun kieltäminen (denial of responsibility) Asenne (attitude), sosiaalinen paine (subjective norm), tietoisuus suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (perceived behavioral control) ja vastuun kieltäminen (denial of responsibility) vaikuttavat merkittävästi virustorjuntaohjelman käyttöönottoon.
Lee, Lee & Yoo (2004)	T	**Ryhmä 1: kysely** Kohderyhmänä korealaiset Mba-opiskelijat ja keskitason johtajat (N= 182). Analyysimenetelmät: path analysis ja maximum likelihood estimation	Taustateoriat: Theory of reasoned action (TRA), Theory of planned behavior (TPB) Muuttujat: Tietoturvapolitiikka (security policy) Tietoturvatietoisuus (security awareness) Tietoturvajärjestelmä (physical security system) Liittyminen (attachment) Sitoutuminen (commitment) Osallistuminen (involvement) Säännöt (norms) Suojautuminen (self defence)

			Väärinkäytön kontrollointi (induction control) Ulkopuolisen hyökkääjän väärinkäytös (invaders' abuse) Organisaation jäsenen väärinkäytös (insider' s abuse) Pelote-tekijät (tietoturvapolitiikka, tietoturvatietoisuus, tietoturvajärjestelmä) vaikuttavat aikomukseen puolustautua tietoturvauhkilta ja organisaatiotekijät (liittyminen, sitoutuminen, osallituminen ja säännöt) vaikuttavat merkittävästi siihen, aikooko työntekijä tehdä tietoturvaan liittyviä väärinkäytöksiä.
Liang & Xue (2010)	K	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laiset opiskelijat (N=152). Aineiston analyysissa käytetty PLS -työkalua.	Taustateoria: Technology threat avoidance theory (TTAT) Muuttujat: Tietoisuus alttiudesta (perveived susceptibility) Tietoisuus vakavuudesta (perceived severity) Tietoisuus uhasta (perceived threat) Suojaustoimen tehokkuus (safeguard effectiveness) Suojaustoimen kustannukset (safeguard cost) Luottamus omiin kykyihin (self-efficacy)

			Motivaatio tietoturvaongelman välttämiseen (avoidance motivation) Tietoturvaongelmien välttäminen (avoidance behavior) Tietoisuus uhkasta, suojaustoimen tehokkuus, suojaustoimen hinta ja luottamus omiin kykyihin vaikuttavat motivaatioon välttää tietoturvauhkia.
Lowry, Posey, Bennett and Roberts (2014)	T	**Ryhmä 1: kysely** Kohderyhmänä työntekijät pankki-, finanssi- ja vakuutusalalta (N=533) Analyysimenetelmänä PLS regressio.	Taustateoriat: Fairness theory (FT), Reactance theory (RT), Deterrence theory (DT) Muuttujat: Tietoturvapolitiikkojen rajoittavuus (restricteveness of enhanced ISP) Organisaation tietoturvatietoisuus ja -koulutus (organizational SETA initiatives) Tiedottaminen muutoksista ennakkoon (advance notification of changes) Ulkoinen ohjaus (external control) Vapauden rajoitukset (freedom restrictions) Selityksen riittävyys (explanation adequacy (EA) Luottamus organisaatioon (organizational trust)

			Tietokoneen väärinkäyttö (reactive computer abuse) Luottamus organisaatioon voi vähentää tietokoneen väärinkäyttöä.
Limayem & Hirt (2003)	T	**Ryhmä 1: kysely** Kohderyhmänä hongkongilaiset yliopisto-opiskelijat (N = 60). Aineiston analyysi toteutettu PLS-menetelmällä.	Taustateoria: Theory of planned behavior (TPB) Muuttujat: Käyttäytyminen (behavior) Aikomus (Behavioral intention) Helpottavat olosuhteet (facititating conditions) Sosiaaliset tekijät (social factors) Tietoisuus seurauksista (perceived consequences) Tapa (habit) Tunne (affect) Tulokset korostavat sitä, että käyttäytymisen selittämisessä on tärkeää ottaa huomioon tietoiset (aikomukset) ja tiedostamattomat tekijät (tavat)
Myyry, Siponen, Pahnila, Vartiainen & Vance (2009)	T	**Ryhmä 1: kysely** Kohderyhmänä suomalaiset toimistotyöntekijät ja työssäkäyvät opiskelijat (N = 163). Aineiston analysointiin on käytetty regressioanalyysia.	Taustateoria: Theory of cognitive moral development, Theory of motivational types of values Muuttujat: Pre-konventionaalinen päättely (preconventional reasoning) Konventionaalinen päättely (conventional reasoning)

			Post-konventionaalinen päättely (postconventional reasoning) Avoimuus muutokselle (openness to change) Säilyttäminen (conservation) Oletettu noudattaminen (hypothetical compliance) Todellinen noudattaminen (actual compliance) Henkilöt, jotka ovat prekonventinaalisella tasolla (jotka pelkäävät rangaistusta jos loukkaavat tietoturvaa tai jotka pitävät salasanan jakamista henkilökohtaisena riskinä) noudattavat todennäköisemmin tietoturvaohjeoita kuin henkilöt jotka ovat ylemmillä tasoilla. Vastaajat jotka pitivät tärkeänä avoimuutta muutokselle, eli seuraavat omia emotionaalisia ja älyllisiä intressejä, noudattivat ohjeita vähiten todennäköisimmin.
Möller et al. (2011)	K	**Ryhmä 2: kokeellinen tutkimus** Kohderyhmänä tietokoneen käyttäjät (N = 20). Analyysimenetelmänä varianssianalyysi ANOVA.	Taustateoriat: - Muuttujat: - Tutkimuksessa laaditaan simulaatiomalli, jolla analysoidaan ja ennustetaan käyttäytymistä tilanteissa, joissa käyttöliittymä sisältää turvallisuuteen liittyviä toimintoja. Simulaatioiden pohjalta saatua

			tietoa verrataan empiiriseen dataa kokeellisesta tutkimuksesta. Vertailut osoittavat, että tietokoneen käyttäjän käyttäytymistä tietoturvaan liittyvissä tilanteissa voidaan ennustaa.
Ng, Kankahalli, & Xu, (2009)	T	**Ryhmä 1: kysely** Kohderyhmänä työssä käyvät opiskelijat ja IT-alan työntekijät (N=134). Analyysimenetelmänä on käytetty usean muuttujan regressioanalyysiä.	Taustateoria: Health belief model Muuttujat: Käyttäytyminen (behavior) Tietoisuus alttiudesta (perveived susceptibility) Tietoisuus vakavuudesta (perceived severity) Tietoisuus hyödyistä (perceived benefits) Tietoisuus esteistä (perceived barriers) Aktivoivat seikat (cues to action) Yleinen tietoturvaan orientoituminen (general security orientation) Luottamus omiin kykyihin (self-efficacy) Tekniset valvontakeinot (technical controls) Tietoturvan tuttuus (security familiarity) Tietoisuus alttiudesta, tietoisuus hyödyistä, ja luottamus omiin kykyihin määrittävät sähköpostin käyttöön liittyvää tietoturvakäyttäytymistä

Ng & Rahim (2005)	K	**Ryhmä 1: kysely** Kohderyhmänä yliopisto- opiskelijat (N=233). Vastaukset analysoitiin PLS-menetelmällä.	Taustateoria: Theory of planned behavior (TPB) Muuttujat: Aikomus käyttää suojaustoimenpidettä (Intention) Asenne (attitude) Sosiaalinen paine (subjective norm) Tietoisuus suojaustoimenpiteen käytön helppoudesta tai vaikeudesta (perceived behavioral control) Tietoisuus hyödyllisyydestä (perceived usefulness) Perheen ja vertaisjoukon vaikutus (family and peer influence) Median vaikutus (media influence) Luottamus omiin kykyihin (self-efficacy) Helpottavat olosuhteet (facilitating conditions) Asenne ja sosiaalinen paine vaikuttavat merkittävästi aikomukseen ottaa suojaustoimenepide käyttöön. Tietoisuus hyödyllisyydestä, perheen ja vertaisjoukon sekä median vaikutus sekä luottamus omiin kykyihin vaikuttavat merkittävästi aikomukseen ottaa

			suojaustoimenpide käyttöön.
Puhakainen & Siponen (2010)	T	**Ryhmä 6: toimintatutkimus**	Taustateoriat: universal constructive instructional theory ja elaboration likelihood model Muuttujat: - Tutkimuksessa kehitetty teoriapohjainen tietoturvakoulutusohjelma tuotti positiivisia tuloksia ja toimi käytännössä. Lisäksi toteutettu koulutus todisti, että tietoturvakoulutuksen tulisi hyödyntää sisältöjä ja menetelmiä, jotka aktivoivat ja motivoivat oppijoita koulutuksessa saamansa tiedon kognitiiviseen prosessointiin.
Shaw, R.S. et al. (2009)	T	**Ryhmä 2: kokeellinen tutkimus** Kohderyhmänä olivat taiwanilaiset yliopisto-opiskelijat (N=154) Aineisto analysoitiin SPSS menetelmällä.	Taustateoriat: - Muuttujat: - Tutkimuksessa selvitettiin hypermedian, multimedian ja hypertekstin vaikutusta tietoturvatietoisuuteen. Tutkimuksessa löydettiin positiivinen yhteys median monipuolisuuden ja tietoturvatietoisuuden kehittymisen välillä. Tutkimuksessa löydettiin myös syy-seuraussuhde eri tietoisuuden tasojen välillä (tietoisuus, ymmärrys, ennakointi), ja siksi tietoturvatietoisuusohjelmien pitäisi kohdentua kaikkiin näihin tasoihin.
Siponen & Vance (2010)	T	**Ryhmä 1: kysely**	Taustateoriat: Neutralization theory, Deterrence theory (GT)

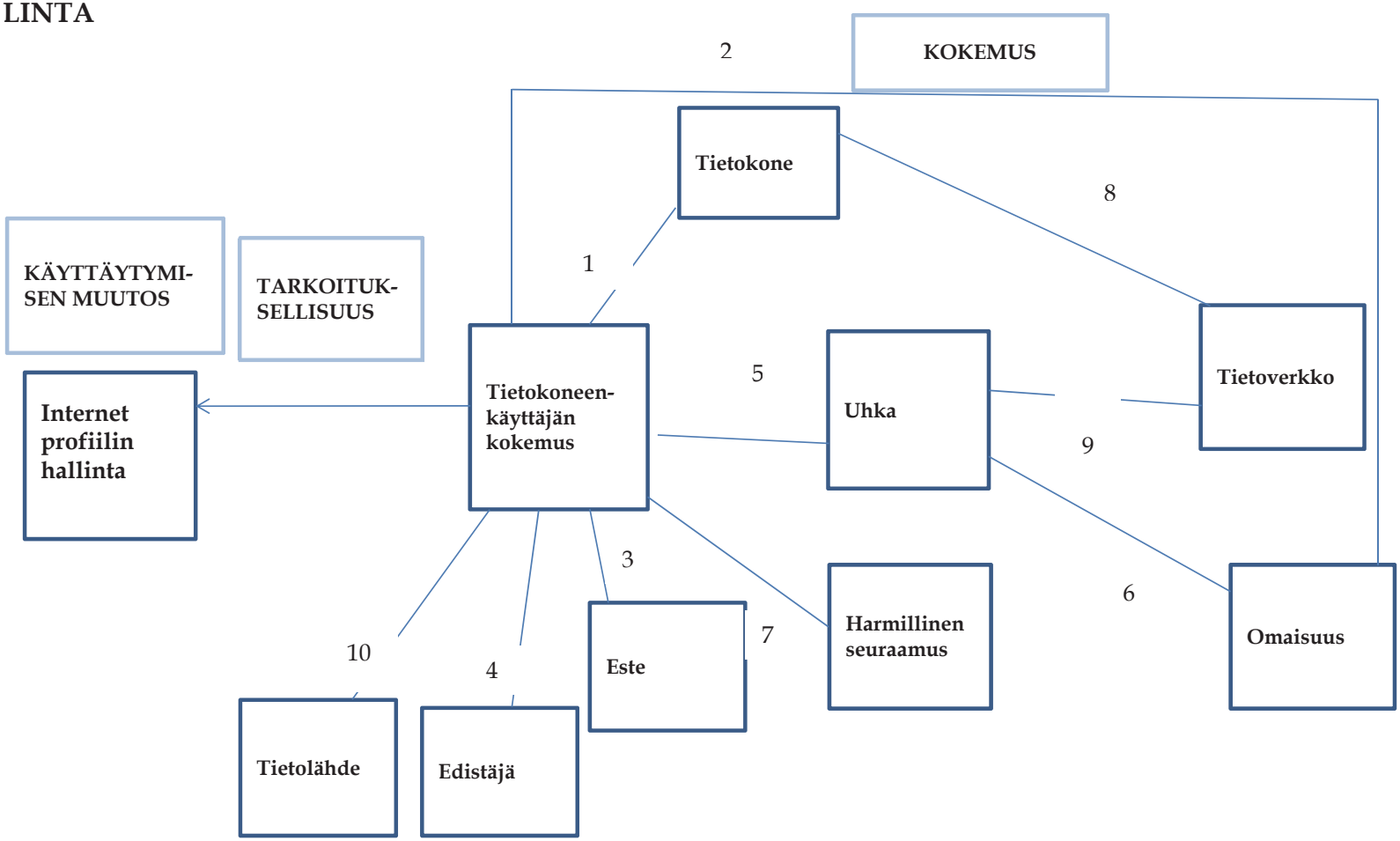
		Kohderyhmänä suomalaiset työntekijät erityyppisissä organisaatioissa (N=395). Analyysimenetelmä PLS.	Muuttujat: Välttämättömyyden puolustaminen (defense of necessity) Vetoaminen ylempiin tahoihin (appeal to higher loyalties) Kohteen tuomitseminen (condemn the condemners) Rikkomusten puolustaminen aiemmilla hyvillä teoilla (metaphor of the ledger) Vahingon kieltäminen (denial of injury) Vastuun kieltäminen (denial of responsibility) Virallinen seuraamus (formal sanctions) Epävirallinen seuraamus (informal sanctions) Häpeä (shame) Neutralisointitekniikat (kuten esimerkiksi oman vastuun kieltäminen) vaikuttavat työntekijöiden aikomukseen rikkoa tietoturvaohjeita, minkä takia neutralisaatio kannattaa ottaa huomioon organisaation tietoturvaohjeita ja käytäntöjä kehitettäessä ja toteutettaessa.
Son, J. (2011)	T	**Ryhmä 1: kysely** Kohderyhmänä USA: laisten organisaatioiden työntekijät (N=602). Aineiston analysointi-	Taustateoria: General deterrence theory (GDT) Muuttujat: Tietoturvaohjeiden noudattami-

		työkaluna PLS.	nen (compliance) Pelotteen varmuus (deterrent certainty) Pelotteen vakavuus (deterrent severity) Tietoturvaohjeiden oikeutus (legitimacy) Arvojen samankaltaisuus (value congruence) Muuttujat, jotka pohjatuvat sisäisen motivaation malliin (tietoturvaohjeiden oikeutus, arvojen samankaltaisuus) selittivät työntekijöiden tietoturvaohjeiden noudattamista merkittävästi enemmän kuin ulkoisen motivation mallin muuttujat (pelotteen varmuus ja vakavuus)
Stanton, Stam, Mastrangelo & Jolton (2005)	T	**Ryhmä 1: kysely** Kohderyhmänä U.S.A: laiset työntekijät (N= 2011) Analyysissa käytetty yksinkertaista korrelaatiota	Taustateoriat: - Muuttujat: - Salasanakäyttäytyminen vaihteli eri organisiaatiossa, yleisesti ottaen se oli huonolla tasolla. Toisaalta koulutuksella, tietoisuudella seurannalla ja motivoinnilla voidaan salasanakäyttäytymiseen vaikuttaa.
Straub, D.W. (1990)	T	**Ryhmä 1: kysely** Kohderyhmänä U.S.A:laiset organisaatiot (N=1211).	Taustateoria: Theory of general deterrence Muuttujat: Tietokoneen väärinkäyttö (compu-

		Aineiston analyysissa on käytetty LISREL: iä, korrelaatiotestejä ja analyysia vahvistavia testejä kuten Kruskal Wallisin testi.	ter abuse) Pelotteen varmuus (deterrent certainty) Pelotteen vakavuus (deterrent severity) Suojaukset (preventives) Motivaatiotekijät (motivational factors) Ympäristötekijät (environmental factors) Tietoturvaohjelmistot vähentävät tietokoneen väärinkäyttöä työpaikalla samoin kuin tieto siitä, millaisia rangaistuksia tietoturvaohjeiden noudattamattomuudesta työntekijöille seuraa. Tietoturvaa edistävän henkilökunnan aktiivisuus ja tietoturvaan sitoutuminen myös parantavat organisaation tietoturvaa.
Wang et al. (2010)	K	**Ryhmä 5: seurantatutkimus** Kohderyhmänä Internetin hakukoneen (AOL) käyttäjät (N=658000) Analyysimenetelmänä dynaaminen regressio-analyysi	Taustateoria: - Muuttujat: - Tutkimuksessa seurattiin koehenkilöiden hakukoneen (AOL) käyttöä 3 kuukauden ajan. Tulokset osoittavat, että verkkohyökkäysten yleisyys ja voimakkuus ovat positiivisesti yhteydessä tietoturvaan liittyvän tiedon etsimiseen Internetistä. Kun tietokoneen käyt-

			täjät kokevat hyökkäyksiä, tämä saa heidät aktiivisesti etsimään tietoturvaan liittyvää tietoa.
Woon, Tan, & Low, R. (2005)	K	**Ryhmä 1: kysely** Kohderyhmänä yliopiston tutkijat, opiskelijat sekä teollisuudessa työstentelevät osa-aikaiset opiskelijat (N=215). Analyysimenetelmänä logistinen regressioanalyysi.	Taustateoria: Protection motivation theory (PMT) Muuttujat: Tietoisuus haavoittuvaisuudesta (perceived vulnerability) Tietoisuus seurausten vakavuudesta (perceived severity) Suojaustoimenpiteen tehokkuus (response efficacy) Luottamus omiin kykyihin (self-efficacy) Kustannukset (response cost) Tietokoneen käyttäjien päätökseen ottaa suojaustoimenpiteitä käyttöön vaikuttavat merkittävästi tietoisuus seurausten vakavuudesta, suojaustoimenpiteen tehokkuus, luottamus omiin kykyihin ja suojaustoimenpiteen kustannukset.

LIITE 4. MALLI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ INTERNET-PROFIILIN HALLINTA

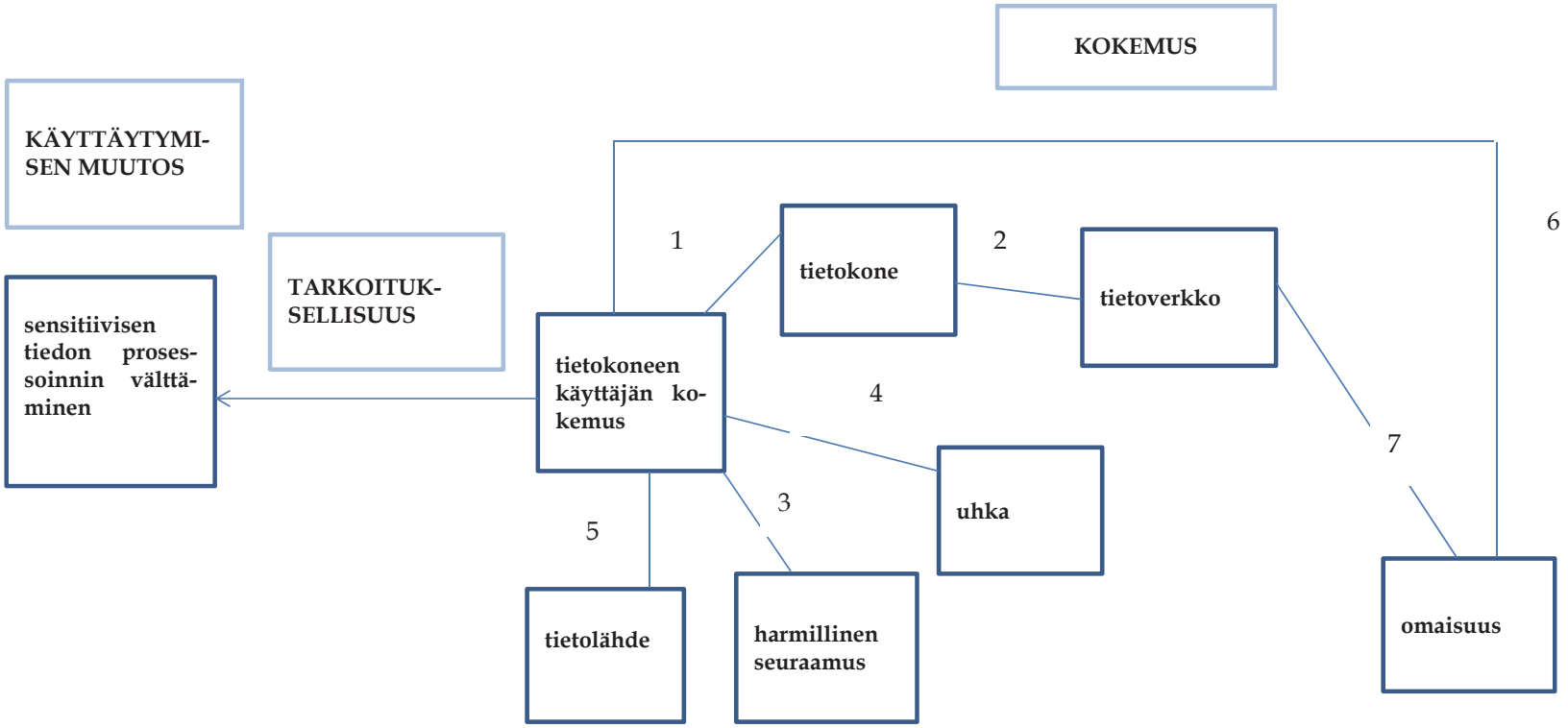


INTERNET-PROFIILIN HALLINTA	
Elementti	**Elementin variaatiot**
uhka	roskaposti, hakkerointi, facebook-tunnusten väärinkäyttö, identiteetti-varkaus, henkilö, joka levittää sensitiivistä tietoa eteenpäin
harmillinen seuraus	tietojen häviäminen sosiaalisesta mediasta, facebook-profiilin kopiointi, tietojen vuotaminen ulkopuolisille, väärän tiedon levittäminen, oma kuva päätyy ei-halutuille www-sivuille, kuvajakopalvelun kuvia vuotaa julkisuuteen, erikoiset kaveripyynnöt facebookissa ja tuntemattomien ihmisten päivitysten näkeminen, vääristyneen kuva muodostuminen Internetissä olevien tietojen perusteella
tietolähde	LinkedIn – koulutus, perhe, sosiaalinen media, ystävät, media, koulu ja poliisi
edistäjä	hakukoneen avulla voi etsiä itseään koskevaa tietoa Internetistä
este	tietokoneen käyttäjä ei osaa käyttää kuvanjako palvelua niin että kuvat eivät leviäisi julkisesti saataville, tietokoneen käyttäjä ei hallitse yksi-tyisyysasetusten määrittelemistä facebookissa
omaisuus	tiedot, joita tallettaa sosiaaliseen mediaan (yksityiset ja työhön liittyvät), yksityisyys, oma nimi, sähköpostitiedot, lopputyöhön liittyvään yrityk-seen ja tuotteeseen liittyvät tiedot
tietokone	laitteet joilla sosiaalista mediaa käytetään
tietoverkko	Internet
tietokoneenkäyttäjän kokemus	tietokoneen käyttäjän kokemukset liittyen oman profiilin hallintaan Internetissä

INTERNET-PROFIILIN HALLINTA		
Yhteys #	**Yhteyden tyyppi**	**Yhteyden kuvaus**
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta yhteydenpitoon ystäviensä kanssa, oman työn markkinointiin, viihtymiseen, tiedon saamiseen ja oppimiseen. Tietokoneen käyttötarve on liittymistarve ja toimeentulon tarve (Alderfer), Maslowin hierarkiassa yhteenkuuluvuuden tarve sekä tietämisen ja itsensä toteuttamisen tarve.
2	Omistaminen	Tietokoneen käyttäjän omaisuutta ovat esimerkiksi kuvat, sähköpostitiedot, sosiaalisen median päivitykset, työhön liittyvät tiedot, identiteetti, lopputyöhön liittyvään yritykseen ja tuotteeseen liittyvät tiedot
3	Käyttäytymisen muutoksen hidastuminen	Tietokoneenkäyttäjän omien tietojen hallintaa Internetissä haittaa esimerkiksi se, jos hän unohtaa merkitä sosiaaliseeen mediaan laittamansa kuvan, ja se päätyy julkiseksi.
4	Käyttäytymisen muutoksen nopeutuminen	Tietokoneen käyttäjän omien tietojen hallintaa edistää mm. se, että hakukoneiden avulla (esimerkiksi Google-kuvahaku) käyttäjä pystyy etsimään itseään koskevaa tietoa Internetistä.
5	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen uhkista, esim. että roskaposti, hakkerointi, facebook-tunnusten väärinkäyttö ja identiteettivarkaus uhkaavat sosiaalisen median käyttöä.
6	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen omaisuuteensa kohdistuvista uhista, mm. siitä, että hänen sensitiivistä tietoa/kuvia voidaan linkittää ei-halutuille sivuille.
7	Harmillisten seuraamusten ymmärtäminen	Tietokoneen käyttäjä unohtaa merkitä kuvansa facebookissa tietylle ryhmälle kuuluvaksi, joten se päätyy julkisesti saatavaksi ja ei-

		halutuille sivuille. Tietokoneen käyttäjä ei aseta sosiaalisen median yksityisyysasetuksia tarpeeksi tiukoiksi joten hän alkaa saamaan kaveripyyntöjä ja epäolennaista tietoa. Tietoja voi hävitä sosiaalisesta mediasta tai facebook-profiii voidaan kopioida. Sosiaalisessa mediassa olevia tietoja voi vuotaa ulkopuolisille. Tietokoneenkäyttäjästä voidaan levittää väärää tietoa. Tietokoneen käyttäjän kuvanjakopalvelun laittamia kuvia päätyy julkiseksi Tietokoneen käyttäjästä on väärää tieto Internetissä, joten hänestä muodostuu vääristynyt kuva näiden tietojen perusteella.
8	6) Edellytykset	Tietokone on yhteydessä tietoverkkoon.
9	6) Edellytykset	Tietoturvauhka sijaitsee Internetissä.
10	4) Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä saa tietoa Google-kuvahausta LinkedIn-kurssilta. Hän keskustelee sukulaisten kanssa siitä, kuinka omia tietoja voidaan etsiä Internetistä. Ystävät kertovat, kuinka facebookin tietoturva-asetuksia voidaan määritellä. Facebook järjestää kampanjan, jossa kerrotaan, kuinka facebookin tietoturva-asetuksia voidaan määritellä.

LIITE 5. MALLI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ SENSITIIVISEN AINEISTON PROSESSOINTI

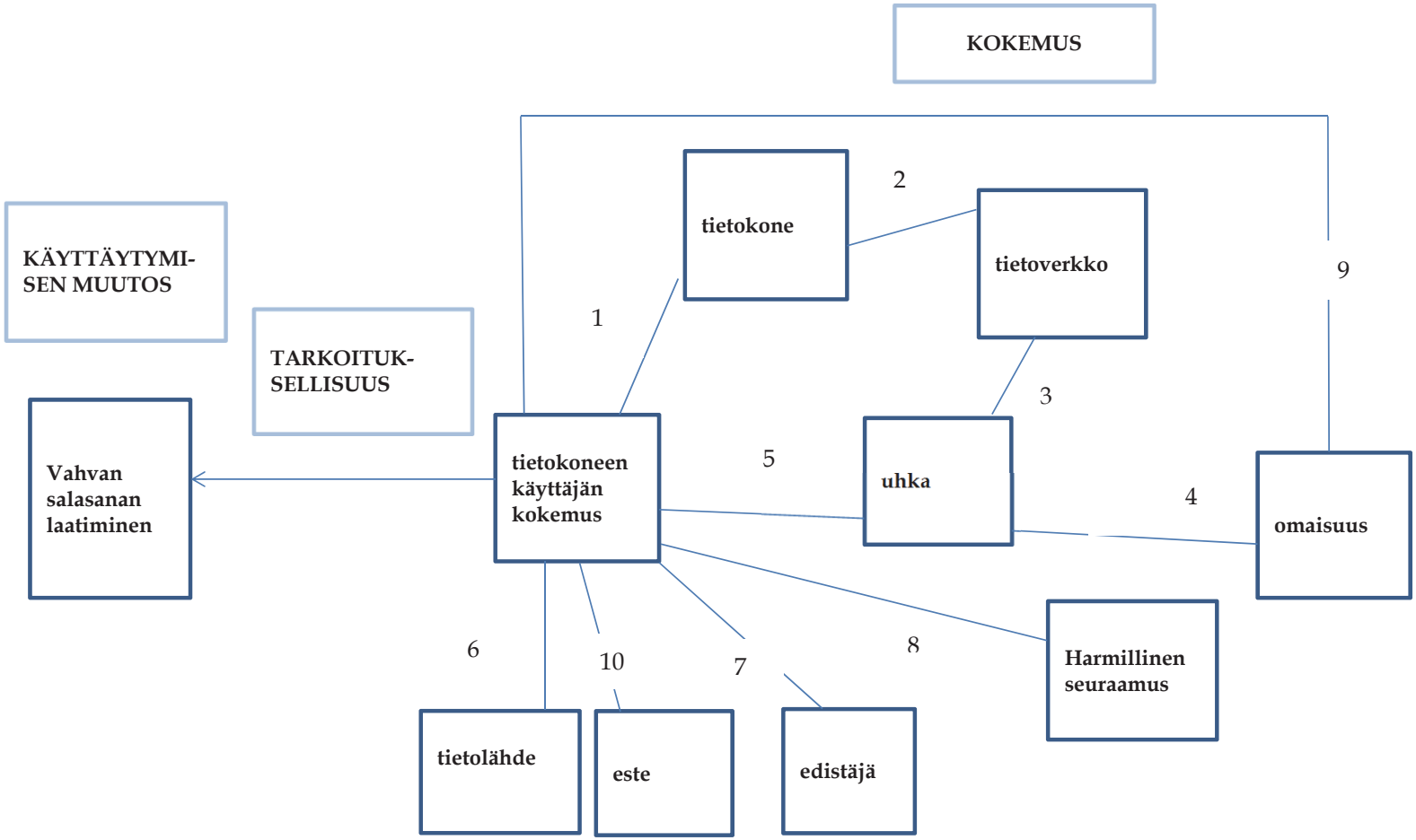


SENSITIIVISEN AINEISTON PROSESSOINTI	
Elementti	**Elementin variaatiot**
tietolähde	ystävä, TV, Internet, työpaikka, koulu, sukulaiset, tietokonealan lehdet
harmillinen seuraamus	sensitiivisen tiedon vuotaminen ulkopuolisille ja tietojen väärinkäyttö, tietojen häviäminen sosiaalisesta mediasta, pankkitietojen väärinkäyttö, ei-toivotut yhteydenotot, tilausten tekeminen toisen nimellä, Chat – keskustelun kaappaus, nettikiusaaminen
uhka	pahantahtoinen henkilö, joka varastaa ja levittää tietoja, identiteettivarkaus
omaisuus	sensitiivinen tieto, esimerkiksi tilinumero, potilastiedot, henkilötunnus, verkkokauppaan liittyvät tiedot, puhelinnumero, koti, osoite, työhön tai työnhakuun liittyvät dokumentit, pankkitiedot, identiteetti, ihmissuhteisiin liittyvät tiedot, käyttäjätunnus ja salasana
tietokone	laite, jota käytetään sähköpostin lähettämiseen ja sosiaalisen median käyttöön
tietoverkko	Internet
tietokoneenkäyttäjän kokemus	tietokoneen käyttäjän kokemukset liittyen sensitiivisen aineiston prosessointiin

SENSITIIVISEN AINEISTON PROSESSOINTI		
Yhteys #	**Yhteystyyppi**	**Yhteyden kuvaus**
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta yhteydenpitoon ystäviensä kanssa sekä asioiden toimittamiseen. Hänellä on liittymisen tarve (Alderfer) ja yhteenkuuluvuuden tarve, tietämisen tarve ja itsensä toteuttamisen tarve (Maslow) sekä asioinnin tarve.
2	Edellytykset	Tietokone on yhteydessä Internetiin.
3	Harmillisten seuraamusten ymmärtäminen	Tietokoneen käyttäjä tulee tietoiseksi sensitiivisen tiedon vuotamisen seurauksista, esimer-

		kiksi kun ystävän viesti päätyy ulkopuolisille ja tietokoneen käyttäjän chat – keskustelu facebookissa kaapataan ja päätyy keskustelun ulkopuolisille.
4	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä tulee tietoiseksi uhista kuten esimerkiksi siitä, että on olemassa pahantahtoisia henkilöitä, jotka haluavat välittää sensitiivistä tietoa eteenpäin tai varastaa tietoja.
5	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä saa tietoa sensitiivisen tiedon lähettämisen vaaroista TV:stä, Internetistä, työpaikalta, koulusta, sukulaisilta ja ystäviltä.
6	Omistaminen	Tietokoneen käyttäjä omistaa sensitiivistä tietoa kuten esimerkiksi tilinumero, sähköpostiviesti, potilastiedot, henkilötunnus, verkkokauppaan liittyvät tiedot, puhelinnumero, osoite.
7	Toiminta	Tietokoneen käyttäjä välittää sensitiivistä tietoa tietoverkon välityksellä.

LIITE 6. MALLI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VAHVAN SASANAN LAATIMINEN

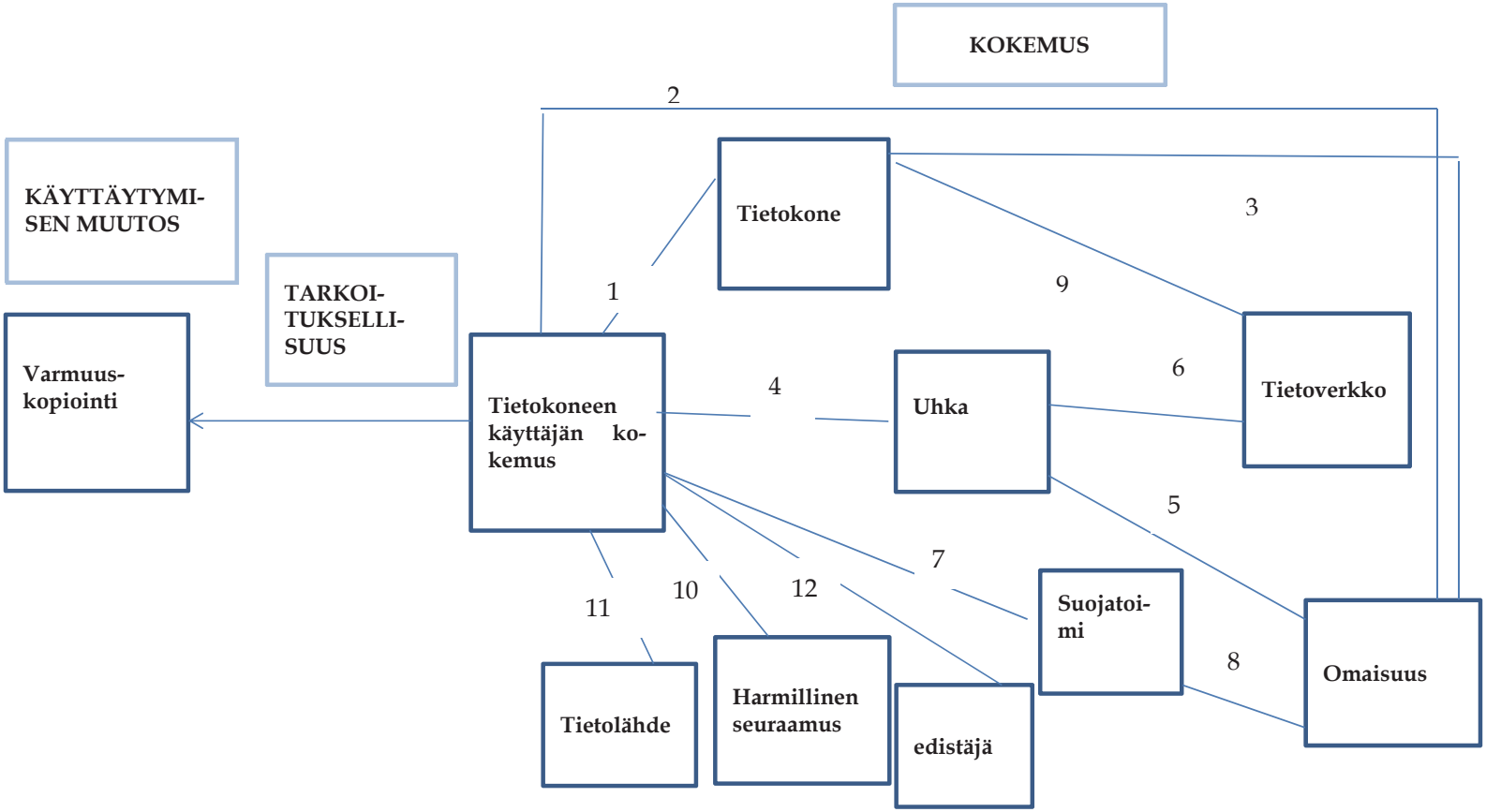


VAHVAN SALASANAN LAATIMINEN	
Elementti	**Elementin variaatiot**
tietokone	tietokone jota käytetään viestintään ystävien kanssa, harrastuksiin liittyvän tiedon tiedon välittämiseen, asiointiin sekä verkkopankkiasiointiin
tietoverkko	Internet
tietolähde	palveluntarjoaja, pankki, ystävät, koulu, työ, kollegat, ohjeet, joita on saatu mm. uutisista ja Internetistä, esimerkiksi palveluiden foorumeista
omaisuus	tietokonelaite, raha, identiteetti, yksityisyys, henkilöhistoria, kriittinen informaatio sähköpostissa kuten esimerkiksi henkilökohtaiset viestit ja ostokuitit, verkkokaupan tiedot, henkilökohtaiset tiedot ja tiedostomateriaalit
harmillinen seuraamus	tietojen menetys, sähköpostin käyttäminen ja lähettäminen omissa nimissä, Somer-tilin tai peli-tilin kaappaus ja väärinkäyttö, tietokoneella olevien henkilökohtaisten tietojen menetys, tiedostomateriaalin päätyminen vääriin käsiin, salasanojen vuotaminen ja varastaminen
edistäjä	pankin järjestelmä ohjaa vahvan salasanan laatimisessa, verkkopalvelu pakottaa laatimaan vahvan salasanan jotta palvelua pääsee käyttämään, Internetistä löytyy ohjeita vahvan salasanan laatimiseen, palvelu pyytää vahvistamaan salasanaa, selain tallettaa salasanat, joten niitä ei tarvitse muistaa
uhka	hakkerointi, esimerkiksi sähköpostin hakkerointi Bruce forte – hyökkäyksellä, ”olan yli katseleminen” ja salasanan selville saaminen.
este	vahvan salasanan laatimista ehkäisee laiskuus ja välinpitämättömyys sekä se, että vahvan salasanan muistaminen on hankalaa
tietokoneenkäyttäjän kokemus	tietokoneen käyttäjän kokemukset liittyen vahvan salasanan laatimiseen

VAHVAN SALASANAN LAATIMINEN		
Yhteys #	Yhteystyyppi	Yhteyden kuvaus
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta yhteydenpitoon ystävien kanssa, asiointiin, esim. pankkiasiointiin sekä harrastuksiin liittyvän tiedon jakamiseen. Yhteydenpito perustuu liittymistarpeeseen (Alderfer) ja pankkiasiointi itsensä toteuttamisen tarpeeseen (Maslow). Tietokoneen käyttötarpeita ovat myös asioinnin tarve sekä tutkimisen, tietämisen ja ymmärtämisen tarve (Maslow). Myös esteettisyyden tarve (Reiss) korostuu.
2	Edellytykset	Tietokone on yhteydessä Internetiin.
3	Edellytykset	Tietokoneen käyttäjä on tietoinen siitä, että tietoverkossa on uhkia.
4	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen siitä, että salasanojen hakkerointi uhkaa sähköpostin tietoja ja rahaa.
5	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen uhista kuten salasanojen hakkeroinnista brute force-hyökkäyksellä, salasanojen varastamisesta ja ”olan yli katselusta”, jonka seurauksena salasana voi päätyä ulkopuolisille.
6	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä saa tietoa vahvoista salasanoista ja niiden merkityksestä mm. pankilta ja uutisista, Internetistä, lähipiiriltä ja työstä, palveluiden foorumeista sekä hakkeroinnin haitallisista seuraamuksista ystävältä. Palveluntarjoaja tiedottaa sähköpostitilin hakkeroinnista.
7	Käyttäytymisen muutoksen helpottuminen/ nopeutuminen	Järjestelmät, esimerkiksi pankin järjestelmä ohjaa käyttäjää laatimaan vahvan salasanan.

		Internet-selain tallettaa salasanat, joten niitä ei tarvitse muistaa.
8	Harmillisten seuraamusten ymmärtäminen	Tietokoneen käyttäjä tulee tietoiseksi hakkeroinnin haitallisista seurauksista, esimerkiksi sen myötä, että ystävä kokee tietojen menetyksen/ tiedostomateriaalin päätymisen vääriin käsiin hakkeroinnin seurauksena tai kun tietokoneen käyttäjän oma sähköposti hakkeroidaan, eikä hän pääse kirjautumaan sähköpostiinsa/ viestejä lähetetään hänen nimissään.
9	Omistaminen	Tietokoneen käyttäjä omistaa rahaa ja kriittistä informaatiota sähköpostissa (henkilökohtaiset viestit, henkilöhistoria, ostokuitit).
10	Käyttäytymisen muutoksen hidastuminen	Vahvan salasanan laatimista hidastaa se, että tietokoneen käyttäjä ei viitsi laatia vahvoja salasanoja ja että salasanoja on vaikea muistaa.

LIITE 7. MALLI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VARMUUSKOPIOINTI



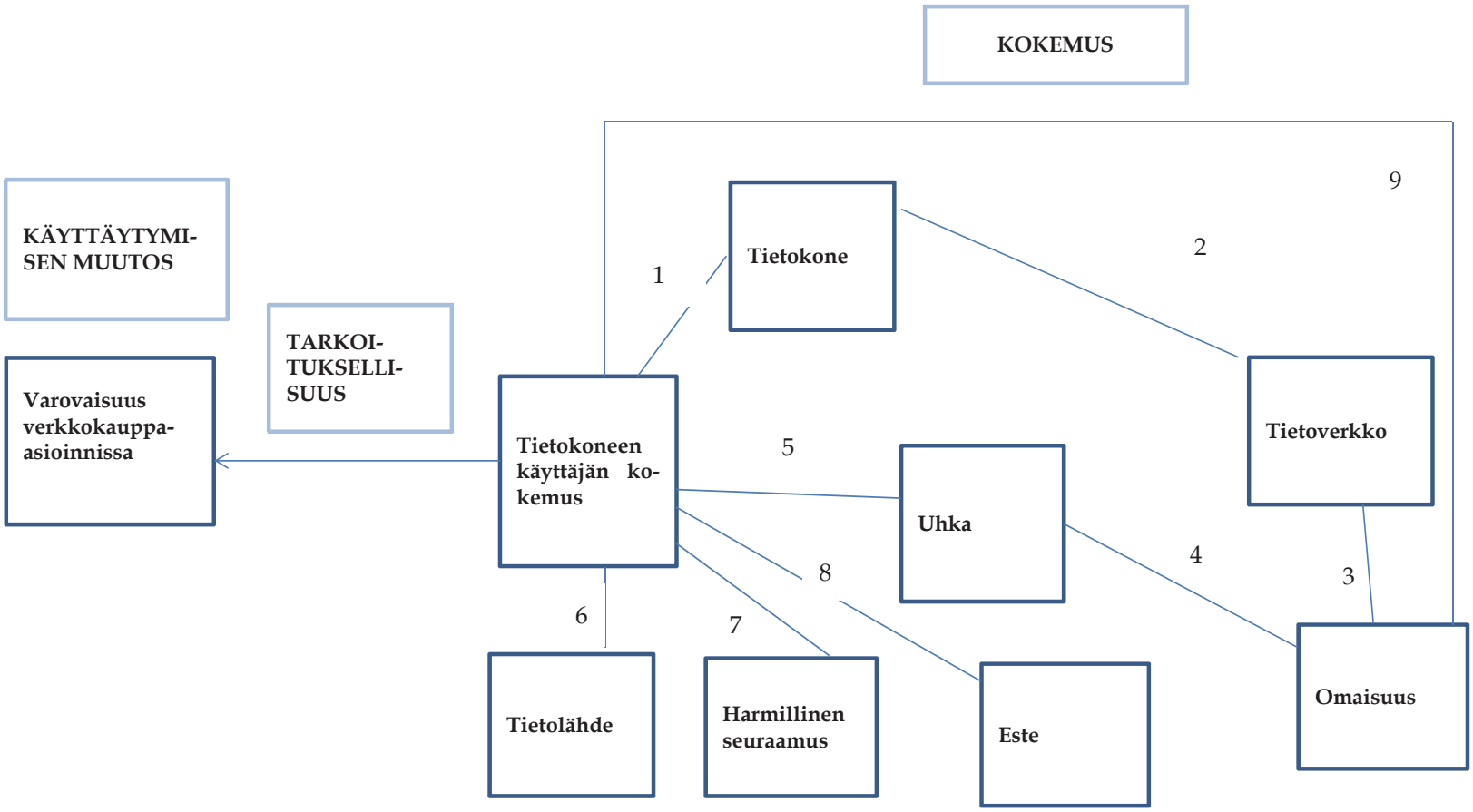
VARMUUSKOPIOINTI	
Elementti	**Elementin variaatiot**
Omaisuus	liiketoiminta-asiakirjat, opiskeluun liittyvät asiakirjat, kuvat, työnhaku-dokumentit, chattilogit, artikkelipohjat
Harmillinen seuraamus	tietojen menetys tai muuttuminen käyttökelvottomaksi, sähköpostin ja liitetiedoston katoaminen
Uhka	virukset, jotka tuhoavat tiedostoja, tietokoneen rikkoutuminen ja kuluminen, varmuuskopioinnin unohtaminen
Tietolähde	ystävä, Internet-keskustelut, koulu, työpaikka
Suojatoimi	antivirus-ohjelmisto
Tietokone	tietokone, jolle omaisuus kuten liiketoiminta-asiakirjat, opiskeluasiakirjat ja kuvat on tallennettu
Tietoverkko	Internet
Edistäjä	varmuuskopiointi on helppoa
Tietokoneenkäyttäjän kokemus	tietokoneen käyttäjän kokemus liittyen varmuuskopioiden laatimiseen

VARMUUSKOPIOINTI		
yhteys #	**Yhteystyyppi**	**Yhteyden kuvaus**
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta liiketoiminnan kehittämiseen, yhdistystoimintaan, työntekoon, opiskeluun ja tallennukseen (esim. kuvat, muistiinpanot, ideat ja musiikki). Liiketoiminnan edistäminen perustuu kehittymisen tarpeeseen (Maslow), työnteko toimeentulon tarpeelle (Alderfer) Opiskelu sekä sukuhistoria tallentaminen sekä ideoiden ja muistiinpanojen tallennus tallettaminen pohjautuu tietämisen ja ymmärtämisen tarpeeseen (Maslow). Opiskeludokumenttien ja muistiinpanojen tallentamista selittää myös ajan ja vaivan säästämisen

		tarve. Yhdistystoiminta pohjautuu itsensä toteuttamisen tarpeelle Kuvien, videoiden ja musiikin tallentaminen taas pohjautuu esteettisyyden eli kauneuden kokemisen tarpeelle (Maslow ja Reiss). valokuvien sekä musiikin tallentaminen itsensä toteuttamisen tarpeelle jos henkilöllä on harrastuksena valokuvaus tai musiikin teko. Valokuvien tallentamista selittää myös liittymisen tarve siinä tapauksessa että valokuvia halutaan jakaa lähipiirille
2	Omistaminen	Tietokoneen käyttäjä omistaa esim. liiketoiminta-asiakirjoja, opiskeluun ja työhön liittyviä asiakirjoja, esimerkiksi työnhakudokumentteja, artikkelipohjia ja kuvia sekä musiikkitiedostoja.
3	Toiminta	Tietokoneen käyttäjä tallentaa mm. liiketoiminta-asiakirjoja, kuvia ja opiskeluun liittyviä asiakirjoja tietokoneelleen.
4	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä tulee tietoiseksi uhkista, joita ovat mm. koneen saastuminen viruksesta, koneen rikkoutuminen/kuluminen ja varmuuskopioinnin unohtaminen.
5	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen asioista jotka uhkaavat hänen omaisuuttaan, kuten esimerkiksi liiketoimintadokumentteja.
6	Edellytykset	Virukset sijaitsevat ja leviävät Internetissä.
7	Toiminta	Tietokoneen käyttäjällä on käytössään virustorjuntaohjelmisto.
8	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä tietää, että virustorjuntaohjelma auttaa suojaamaan omaisuutta, kuten esimerkiksi liiketoiminta-asiakirjoja.

9	Edellytykset	Tietokone on yhteydessä Internetiin.
10	Harmillisten seuraamusten ymmärtäminen	Tietokoneen käyttäjä ymmärtää mitä harmillisia seurauksia uhkat voivat aiheuttaa. Tietokoneen käyttäjä esimerkiksi kokee tietojen menetyksen viruksen tai tietokoneen rikkoutumisen seurauksena. Tietokoneen käyttäjän ystävän tietokone rikkoutuu/ saastuu viruksesta, mistä seuraa tietojen menetys. Tietokoneen käyttäjä kuulee kuinka opiskeludokumentteja on kadotettu varmuuskopioinnin puuttumisen vuoksi Tietokoneenkäyttäjän ystävä menettää tärkeän sähköpostiviestin ja liitetiedoston
11	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjän ystävä neuvoo käyttämään pilvipalveluita varmuuskopiointiin. Myös koulun, työpaikan ja Internet-keskustelujen kautta tietokoneen käyttäjä kuulee varmuuskopioinnin tärkeydestä
12	Käyttäytymisen muutoksen helpottuminen / nopeutuminen	Varmuuskopioinnin helppous helpottaa sen käyttöönottamista

LIITE 8. MALLI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VERKKOKAUPPA-ASIOINTI



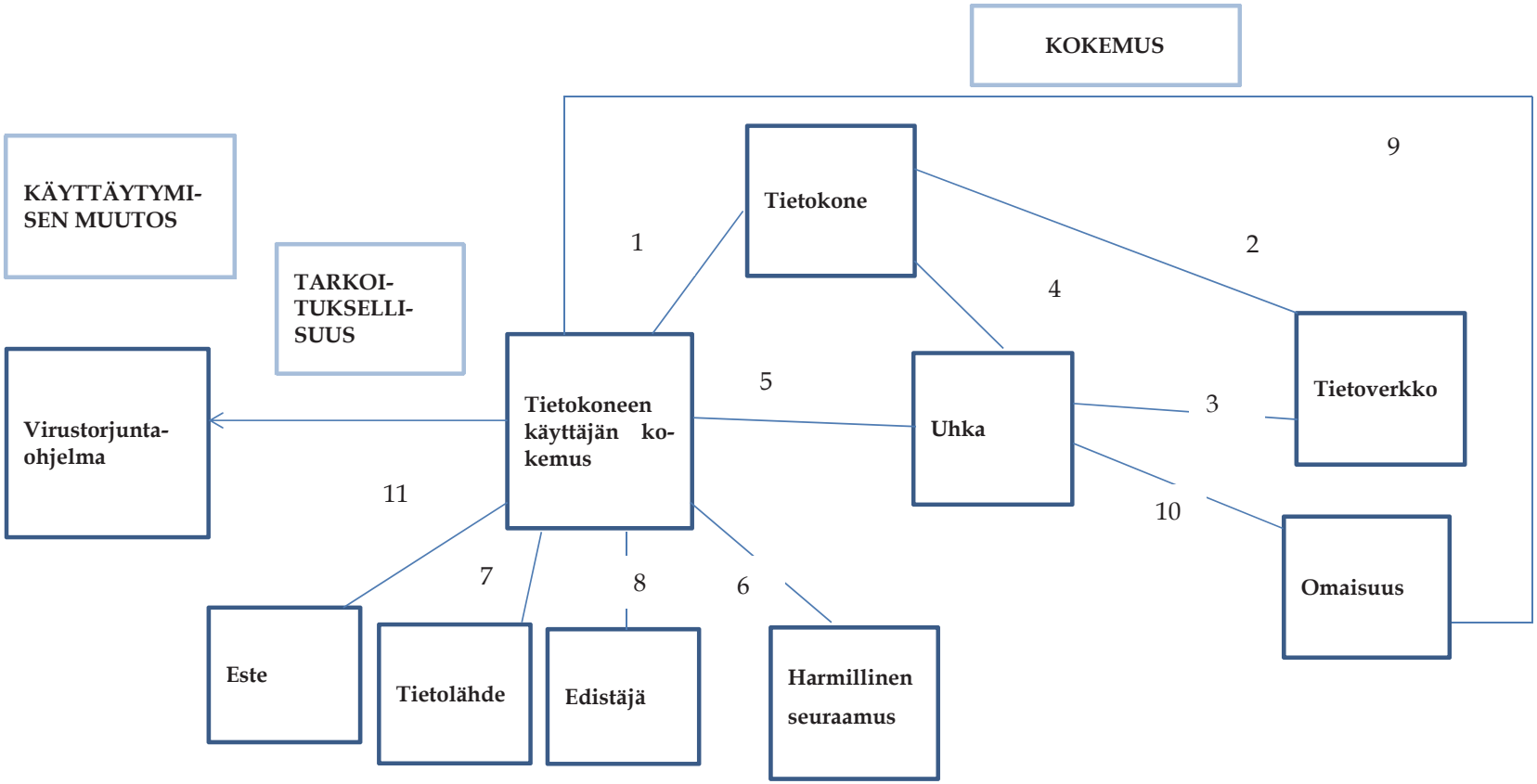
VAROVAISUUS VERKKOKAUPASSA	
Elementti	**Elementin variaatiot**
tietokone	tietokone jota käytetään verkkokauppa-asioinnissa
tietoverkko	Internet
omaisuus	luottokorttinumero ja -tiedot, raha, verkkopankkitunnukset, pankkitiedot
este	ongelmat englanninkielisten ohjeiden ymmärtämisessä
harmillinen seuraamus	rahan menetys tililtä, tilin käyttö estyy, pitkät selvittelyajat, ostoksiin tulee ylimääräisiä lisiä, luottokorttitietoja tai verkkopankkitunnuksia vuotaa julkisuuteen, rahan menetys tekaistulta verkkosivulta tehdyn ostoksen seurauksena, joku toinen tilaa google playsta tavaraa omalla nimellä, verkkokaupasta ostetusta elektroniikkalaitteesta ei mene takuu läpi
tietolähde	ystävät, sukulaiset, firman asiakkaat, verkkokauppa, luottokunta, Internetin keskustelufoorumi
uhka	huijaus, hakkerointi, verkkokaupan toimintaongelmat, musiikkipalvelun tili jää auki, verkkokaupan tietokantaan murtautuminen, luottokortin hakkerointi
tietokoneenkäyttäjän kokemus	tietokoneenkäyttäjän kokemus liittyen verkkokauppa-asiointiin

VAROVAISUUS VERKKOKAUPASSA		
Yhteys #	**Yhteyden tyyppi**	**Yhteyden kuvaus**
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta verkkokauppa-asiointiin, pelaamiseen ja musiikin kuuntelun. Nämä kaikki pohjautuvat itsensä toteuttamisen tarpeeseen (Maslow). Pelaamista selittävät myös liittymisen tarve (Alderfer) ja Maslowin luokittelussa sosiaalisen arvostuksen motiivit. Pelaaminen selittyy myös tarpeella sosiaalisiin yhteyksiin (Social

		contact) ja hyväksyntään (acceptance) (Reiss). Verkkokaupan käyttö pohjautuu lisäksi ajan ja vaivan säästämisen tarpeeseen. Uteliaisuuden tarve korostuu, jos halutaan nähdä mitä uutuuksia on saatavilla.
2	Edellytykset	Tietokone on yhteydessä Internetiin.
3	Toiminta	Tietokoneen käyttäjä välittää luottokorttitietoja ja maksutietoja tietoverkon välityksellä ostaessaan tuotteita verkkokaupasta.
4	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä tulee tietoiseksi siitä, että uhat kuten huijaus, hakkerointi ja verkkokaupan toimintaongelmat uhkaavat luottokorttitietoja.
5	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä tulee tietoiseksi verkkokaupankäynnin uhista kuten huijauksesta, verkkokaupan toimintaongelmista sekä siitä, että verkkokaupan tietokantaan voidaan murtautua ja luottokortti hakkeroida. Myös toisen nimellä voidaan tilata tuotteita.
6	Tietoturvatietoisuuden lisääntyminen	Esimerkiksi tietokoneen käyttäjän ystävät ja firman asiakkaat kertovat kokemistaan harmillisista seuraamuksista, joita verkkokaupan käyttöön liittyy (luottokortin hakkerointi, rahanmenetys). Verkkokauppa, luottokunta ja nettifoorumi tiedottavat verkkokaupan tietokannan hakkeroinnista. Tietokoneen käyttäjä lukee lehdestä kuinka joku oli tilannut toisen nimissä google playsta tavaraa
7	Harmillisten seuraamusten ymmärtäminen	Tietokoneen käyttäjä kokee esimerkiksi rahanmenetyksen verkkokauppa-asioinnin seu-

		rauksena. Verkkokaupasta tilattaessa ostoksiin tulee ylimääräisiä lisiä. Ystävän luottokortti hakkeroidaan mistä seuraa rahanmenetys, pitkä selvittelyaika ja tilin käyttö estyy. Tietokoneen käyttäjän luottokorttitietoja vuotaa julkisuuteen verkkokaupan tietokantamurron seurauksena. Tietokoneen käyttäjä ystävä menettää rahaa kun vuokraa loma-asunnon tekaistulta verkkosivulta. Tietokoneen käyttäjän ystävä tilaa elektroniikkaa verkkokaupasta. Laitteeseen tulee vika mutta takuun kanssa tulee ongelmia.
8	Käyttäytymisen muutoksen hidastuminen	Verkkokaupan turvallista käyttöä hidastaa se, että verkkokaupan englanninkielisiä ohjeita on vaikeita ymmärtää.
9	Omistaminen	Tietokoneenkäyttäjä omistaa mm. luottokorttinumeron ja rahaa.

LIITE 9. MALLI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VIRUSTORJUNTA



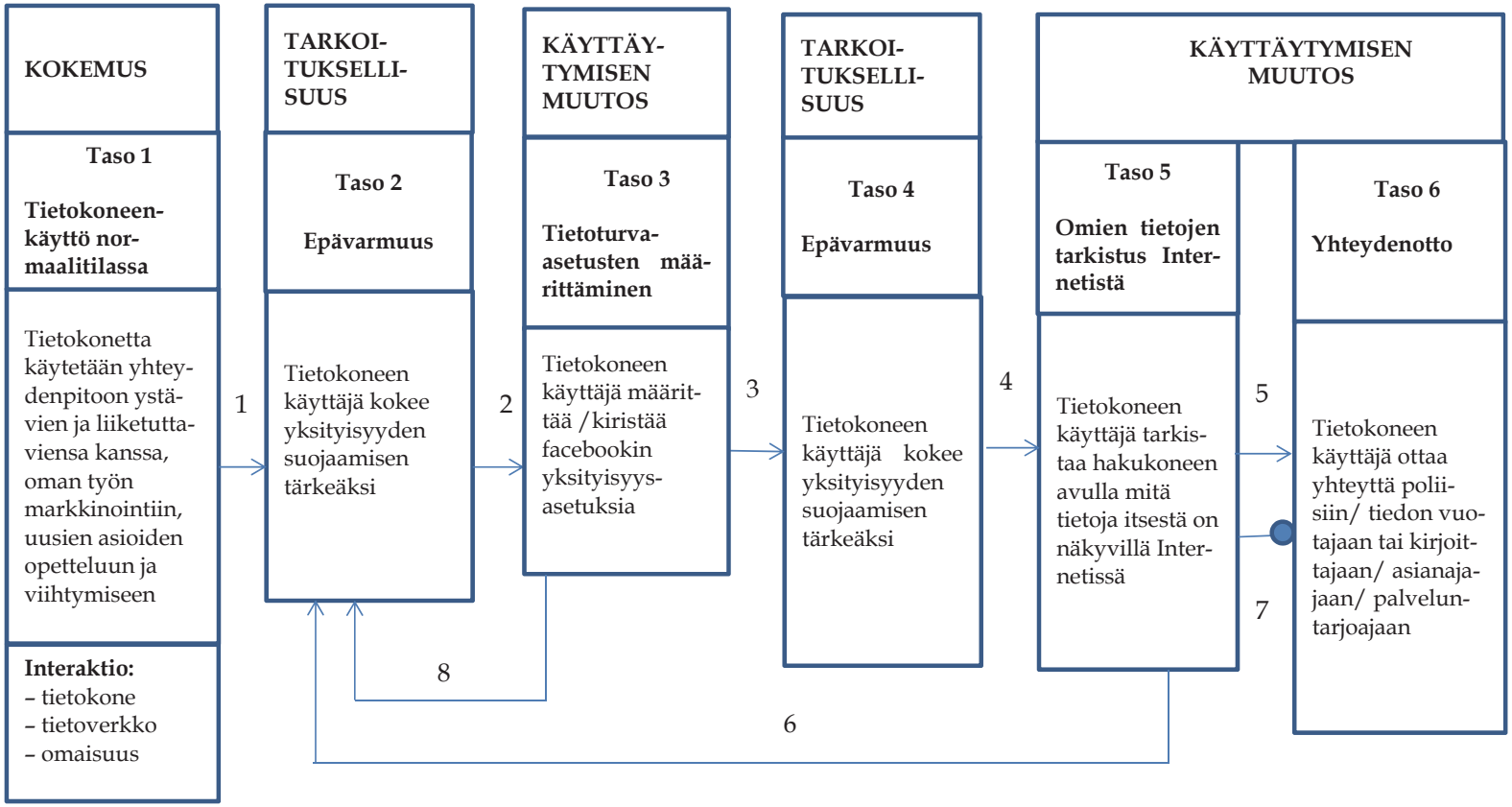
VIRUSTORJUNTA	
Elementti	**Elementin variaatiot**
tietokone	laite, jota käytetään Internet-sivujen selaamiseen
tietoverkko	Internet
uhka	haittaohjelmat, virukset
omaisuus	tietokone ja sinne talletetut tiedot kuten, salasanat ja pankkitunnukset, pankkitiedot, yksityisyys
tietolähde	ystävät, Internet, Internet-keskustelut, media, sukulaiset ja muu lähipiiri
edistäjä	tietoturvaohjelmisto, esimerkiksi virustorjuntaohjelmisto, on helppo asentaa ja helppo käyttää, ohjelmisto on ilmainen, ohjeet helposti ymmärrettävissä
harmillinen seuraamus	koneen saastuminen, koneen hidastuminen, pop-up ikkunat, selaimen aloitussivun vaihtuminen, sähköpostitunnusten kaappaaminen, koneen hallinnan menettäminen
este	tietokoneen ikä ei mahdollista modernin virustorjuntaohjelman asentamista, puutteelliset taidot virustorjuntaohjelmien etsimiseen internetistä ja asennusohjeiden ymmärtämiseen, virustorjuntaohjelman maksullisuus, tietokoneenkäyttäjä epäilee virustorjunnan tehokkuutta

VIRUSTORJUNTA		
yhteys #	**Yhteyden tyyppi**	**Yhteyden kuvaus**
1	Tarve tietokoneen käytölle	Tietokoneen käyttäjä käyttää tietokonetta lnternet-sivustojen selaamiseen. Tiedonhaku perustuu uteliaisuuden tarpeeseen (Reiss), itsensä toteuttamisen tarpeeseen ja tutkimisen, tietämisen ja ymmärtämisen (Maslow) ja henkilökohtaisen kasvun tarpeeseen (Alderfer)) sekä liittymisen tarpeeseen.

2	Edellytykset	Tietokone on yhteydessä Internetiin.
3	Edellytykset	Tietokoneen käyttäjä on tietoinen siitä, että virukset sijaitsevat ja leviävät Internetissä.
4	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen siitä, että virukset ovat uhka tietokoneelle.
5	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen uhasta eli viruksista ja haittaohjelmista.
6	Harmillisten seuraamusten ymmärtäminen	Tietokoneen käyttäjä huomaa, että tietoturvaohjelmisto (F-secure) ei suojaa kaikilta haittaohjelmilta. Kone hidastuu, koneen aloitussivu vaihtuu. Seuraa myös käynnistysongelmia ja popup-ikkunoita. Tietokoneen käyttäjän sähköpostitili kaapataan ja sähköpostitiliä väärinkäytetään. Tietokoneen käyttäjä kuulee, että vakoiluohjelmia on liikkeellä niissä tietokonelaitteissa, joita hän käyttää.
7	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjän ystävä neuvoo käyttämään spybot-ohjelmistoa virustorjunnan lisäksi. Tietokoneen käyttäjä löytää Internetistä tietoa virustorjuntaohjelmista. Myös media, sukulaiset ja muu lähipiiri toimivat tietolähteenä.
8	Käyttäytymisen muutoksen helpottuminen / nopeutuminen	Virustorjuntaohjelmiston käyttöönottoa helpottaa se, että ohjelmisto on helppo asentaa ja käyttää ja että ohjeet on helposti ymmärrettävissä.
9	Omistaminen	Tietokoneen käyttäjä omistaa tietokoneen sekä salasanoja, pankkitunnuksia ja muita pankkitietoja.
10	Tietoturvatietoisuuden lisääntyminen	Tietokoneen käyttäjä on tietoinen siitä, että virukset ovat uhka tietokoneelle ja siihen tal-

		lennetuille/siellä oleville tiedoille.
11	Käyttäytymisen muutoksen hidastuminen	Tietokoneen ikä ei mahdollista modernin virustorjuntaohjelman asentamista Tietokoneen käyttäjä epäilee virustorjunnan tehokkuutta

LIITE 10. PROSESSI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ INTRENET-PROFIILIN HALLINTA



Yhteydet tasojen välillä

#	Yhteyden kuvaus
1	Tietoturvaan liittyvä kokemus Tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa: - tietokone - tietoverkko - uhka - harmillinen seuraamus - omaisuus - tietolähde a) Tietokoneen käyttäjä ottaa käyttöönsä facebookin. Koska hän ei ole tottunut olemaan julkisesti esillä, hän ei halua jakaa tietojaan julkisesti saataville. b) Tietokoneen käyttäjä saa lisätietoa facebookin tietoturva-asetusten käytöstä esimerkiksi facebook-kampanjan myötä ja ystäviltä, jotka varoittelevat että tiedot saattaa facebookissa hävitä c) Tietoturvatapahtuman voi muodostaa myös harmillinen seuraus, esimerkiksi facebook-profiilin kopiointi, hakkerointi ja facebook-tunnusten väärinkäyttö tai se, että tietokoneen käyttäjä unohtaa salata 2 henkilön välisen informaation sosiaalisessa mediassa ja tämän johdosta tietoja vuotaa ulkopuolisille d) Tietokoneen käyttäjä kuulee että identiteettivarkauksia tapahtuu ja sen seurauksena voidaan levittää väärää tietoa.
2	Ratkaisuinteraktio. Tietokoneenkäyttäjä on tietoinen siitä, että Facebookin tietoturva-asetuksia pystyy muokkaamaan niin ettei kuvat näy julkisesti kaikille. Käyttäytymisen muutoksen esteeksi voi muodostua se, että tietokoneen käyttäjä ei hallitse yksityisyysasetusten määrittelemistä facebookissa. Tietokoneen käyttäjä ei välttämättä osaa käyttää kuvanjakopalvelua niin että kuvat eivät leviäisi julkisesti saataville.
3	Tietoturvatapahtuma Tässä vaiheessa tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa – tietokone – tietoverkko – omaisuus – tietolähde

	Tietokoneen käyttäjä osallistuu LinkedIn - koulutukseen ja saa tietoa google-kuvahausta. Tietokoneen käyttäjä keskustelee lähipiirinsä kanssa siitä kuinka omia tietoja voi etsiä Internetistä. Tietokoneen käyttäjä hakee työpaikkaa /aloittaa työt uuden työnantajan palveluksessa
4	Ratkaisuinteraktio: Tietokoneenkäyttäjä on tietoinen siitä, että omia tietoja voi tarkistaa Internetistä hakukoneiden avulla Tietojen etsimistä helpottaa se, että henkilö oppii käyttämään kuvahakua omien tietojen etsimiseen Internetissä.
5	Tietokoneen käyttäjä löytää Internetistä oman kuvan tai tiedon, joka on päätynyt ei-toivotuille sivuille.
6	Tietokoneen käyttäjä löytää Internetistä oman kuvan tai tiedon, joka on päätynyt ei-toivotuille sivuille.
7	Tietokoneen käyttäjä löytää itsestään kuvia ei-toivotuilla sivuilla mutta ei koe tätä niin häiritseväksi että se aiheuttaisi toimenpiteitä/ haluaa välttää sen että asiasta nousee kohu.
8	Tietoturvaan liittyvä kokemus: Facebookiin tulee saataville uusia yksityisyysasetuksia. Myös tietoturvaongelma voi saada tarkistamaan yksityisyysasetuksia. Tietokoneen käyttäjä esimerkiksi saa sosiaalisessa mediassa outoja kaveripyyntöjä ja näkee tuntemattomien ihmisten julkaisuja

Tasojen kuvaus sekä kuvaus interaktiosta, joka eri tasoihin sisältyy

Taso 1. Käyttötarkoitus

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko
- omaisuus

Tietokoneen käyttäjä käyttää tietokonetta yhteydenpitoon ystäviensä ja liiketuttaviensa kanssa, oman työn markkinointiin, uusien asioiden opetteluun ja viihtymiseen. Tietokoneen käyttäjä ei ole tietoinen uhkista ja sosiaalisen median käytön /kuvien lisäämisen mahdollisista haitallisista seuraamuksista tässä vaiheessa. Hän välittää myös sensitiivistä tietoa sosiaalisessa mediassa.

Taso 2. Tarkoituksellisuuden pohtiminen

Tietokoneen käyttäjällä on kokemus facebook-profiilin kopioinnista. Hän haluaa jatkossa välttää identiteetin kopioimisen ja sen, että hänestä levitetään vääriä tietoja, jotka voivat koitua harmiksi myöhemmin esim. työtä haettaessa. Hän haluaa myös välttää roskapostin saamisen ja nolostumisen, joka sensitiivisen tiedon leviämisestä seuraa.

Facebookin järjestämän kampanjan seurauksena tietokoneen käyttäjä hoksaa, että hänen pitäisi määritellä yksityisyysasetuksia, ja miten tieto tulee näkyville facebookiin.

Siinä tapauksessa, että tietokoneen käyttäjä vasta aloittelee sosiaalisen median käyttöä, hän pohtii siihen liittyviä yksityisyysasioita. Hän ei halua että ulkopuoliset näkevät hänen kuviaan ja päivityksiään Facebookissa. Jos ei ole kokemusta julkisesti esillä olemisesta, ei myöskään haluta Internetin kautta levittää tietojaan kaikkien luettavaksi ja nähtäväksi.

Taso 3: Sosiaalisen median tietoturva-asetusten määrittäminen

Tietokoneen käyttäjä määrittää sosiaalisen median ja kuvanjakopalvelun asetukset niin, että hänen tietojaan ja päivityksiään eivät pääse näkemään ulkopuoliset henkilöt vaan ainoastaan tietty lähipiiri ja kaverit.

Taso 4. Tarkoituksellisuuden pohtiminen

Tietokoneen käyttäjä on lisännyt sosiaaliseen mediaan materiaalia ja kokee, että oman yksityisyytensä suojelemiseksi ja työnhaun kannalta on tärkeää tarkistaa mitä hänestä on julkisesti näkyvillä Internetissä. Internet profiilin hallinnan avulla tietokoneen käyttäjä haluaa välttää omien tietojen päätymisen ei-toivotuille sivuille. Hän haluaa estää sen että itsestä tulee vääristynyt kuva sen perusteella mitä Internetissä on hänestä näkyvillä. Tietokoneen käyttäjä haluaa myös suojata työnantajaansa liittyviä tietoja.

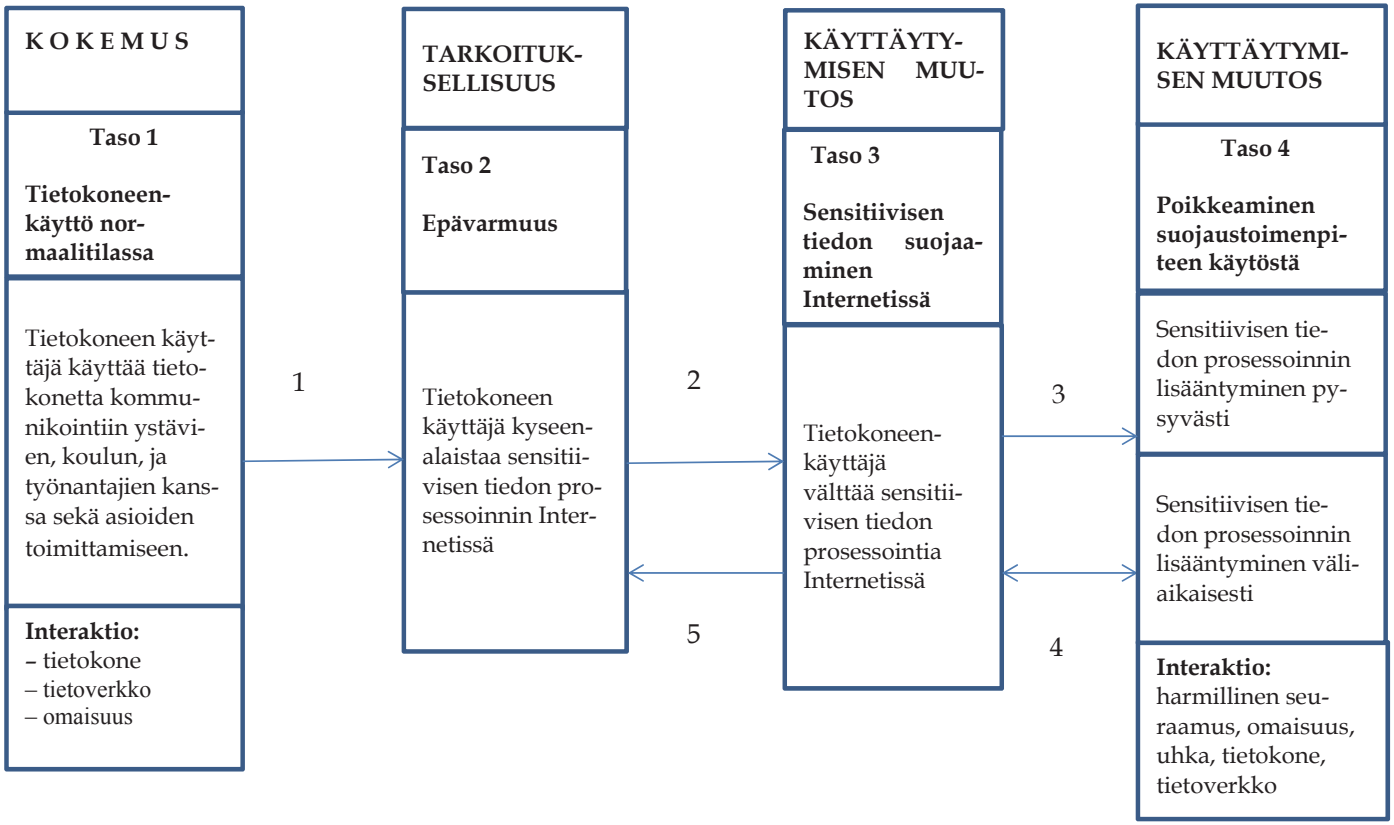
Taso 5. Omien tietojen tarkistus Internetistä

Tietokoneen käyttäjä tarkistaa hakukoneen avulla, mitä hänestä on näkyvillä Internetissä, esimerkiksi keskustelupalstoilla. Hän käyttää myös kuvahakua, jolla näkee onko oma kuva päätynyt ei-toivotuille sivuille.

Taso 6. Yhteydenotto

Yhteydenotto poliisin, palveluntarjoajaan tai tiedon levittäjään auttaa selvittämään tietovuotoa, ja kuka tietoa on levittänyt. Yhteydenotto asianajajaan auttaa selvittämään, mitkä ovat omat oikeudet tietovuototapauksessa.

LIITE 11.PROSESSI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ SENSITIIVISEN AINEISTON PROSESSOINTI



Yhteydet tasojen välillä

#	Yhteyden kuvaus
1	Tietoturvaan liittyvä kokemus, esimerkiksi 1) Tietokoneen käyttäjän ystävä lähettää sähköpostissa sensitiivistä tietoa, ja se päätyy ulkopuolisille. 2) Tietokoneen käyttäjä kuulee tv:stä, Internetistä, tietokonealan lehdistä ja koulussa, että sensitiivistä tietoa, esimerkiksi potilastietoja, ei saa lähettää sähköpostissa/ laittaa sosiaaliseen mediaan ja että ne voidaan varastaa. 3) Tietokoneen käyttäjä lähettää arkaluontoista tietoa (esim. tilinumeron) sähköpostissa. Sukulainen varoittaa, ettei niin kannata tehdä. 4) Turvallisuustietous lisääntyy käytön lisääntymisen myötä. 5) Facebook tulee markkinoille ja sen myötä tietokoneen käyttäjä kuulee varoittavia esimerkkejä siitä, miten tiedot saattaa sieltä hävitä. 6) Facebookin chat- keskustelu kaapataan 7) Facebookissa ulkoiset palvelut pyytävät saada käyttää tietoja 8) Tietokoneenkäyttäjä kuulee nettikiusaamisesta tiedotusvälineistä 9) Tietokoneenkäyttäjä lähtee kouluttautumaan ammattiin 10) Oma päättely ja pohdinta: tietojen päivittämisessä sosiaaliseen mediaan ei tunnu olevan järkeä Tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa: – tietokone – uhka – tietoverkko – harmillinen seuraamus – omaisuus – tietolähde

2	Ratkaisuinteraktio: Tietokoneenkäyttäjä on tietoinen siitä, että arkaluontoisen tiedon päätymistä ulkopuolisille voi välttää harkitsemalla, mitä netissä julkaisee ja mitä sähköpostiin kirjoittaa ja lisäämällä sinne ainoastaan sellaista materiaalia mistä ei ole haittaa jos se päätyy ulkopuolisille.
3	Pysyvä poikkeaminen Riippumattomuus: tunne ettei kuitenkaan voi miellyttää kaikkia Uhkan kokemuksen väheneminen: koska tietokoneenkäyttäjälle ei tule harmillisia seuraamuksia Internetiin tai sähköpostiin kirjoittamisesta, hän alkaa kirjoittaa sinne vapaammin
4	Väliaikainen poikkeaminen Tietokoneenkäyttäjä poikkeaa omaksutusta suojaustoimenpiteestä seuraavissa tilanteissa Mikään muu viestintäväline ei kelpaa toiselle osapuolelle Tarve toimittaa tietty asia, esimerkiksi pankkiasia Vahinko: Tietokoneen käyttäjä esimerkiksi lähettää vahingossa arkaluontoisen viestin sosiaalisessa mediassa tai lisää tietoja vahingossa väärään kanavaan Tietokoneenkäyttäjä unohtaa salata tietoja, esimerkiksi ihmissuhteisiin liittyviä tietoja facebookissa tai unohtaa merkitä kuvan että se näkyy vain tietylle ryhmälle Tietokoneenkäyttäjä käyttää palvelua, jossa mukana vain lähipiiri, joten kirjoittaa vapaammin Tietokoneenkäyttäjä osallistuu keskusteluun pelimaailmassa, jossa käytössä online-persoona.
5	Tietoturvaongelmat, esimerkiksi hakkerointi, lisääntyy

Tasojen kuvaus sekä kuvaus interaktiosta, joka eri tasoihin sisältyy

Taso 1. Käyttötarkoitus

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- omaisuus
- tietoverkko

Tietokoneen käyttäjä käyttää henkilökohtaista tietokonettaan kommunikointiin mm. ystävien, koulun ja työnantajien kanssa sekä asiointiin. Hän välittää viesteissä myös sensitiivistä tietoa eikä ole tietoinen tähän liittyvistä uhista kuten tietojen vuotamisesta ulkopuolisille. Tietokoneen käyttäjä ei osaa varautua siihen, mitä haitallisia seuraamuksia arkaluontoisen asian käsittelystä Internetissä voi seurata.

Taso 2. Tarkoituksellisuuden pohtiminen

Tällä tasolla tietokoneen käyttäjä pohtii kokemusten merkitystä oman tietoturvansa kannalta. Hän on kuullut mitä siitä seuraa, jos arkaluontoisia viestejä päätyy ulkopuolisille ja haluaa välttää joutumisen samanlaiseen tilanteeseen. Tietokoneen käyttäjän sosiaalisessa mediassa välittämää tietoa vuotaa ulkopuolisille. Uutiset nettikiusaamisesta saavat pohtimaan, kuinka tärkeää on välttää omien tietojen laittamisen Internetiin. Tietokoneen käyttäjä kokee tärkeäksi estää sen, ettei hänen tietojaan vuoda ulkopuolisille. Myös sosiaalisen median ja sähköpostin käytön aloitus saavat pohtimaan sitä, kuka omiin tietoihin pääsee käsiksi, samoin kuin se että henkilö lähtee kouluttautumaan ammattiin. Tällöin hän alkaa pohtimaan sitä mitenkä asiat vaikuttaa esimerkiksi työhön tai tulevaan työhön, tulevaan koulutukseen.

Tietokoneen käyttäjä lähettää tilinumeronsa pikaviestipalvelun/ sosiaalisen median kautta. Ystävät ja sukulaiset varoittelevat tästä. Tietokoneen käyttäjä kokee tärkeäksi jatkossa välttää sensitiivisen tiedon välittämistä sosiaalisessa mediassa /pikaviestipalvelussa.

Tietokoneen käyttäjä on osallistunut tietoturvaluennoille. Hän kokee tärkeäksi noudattaa saatuja ohjeita, koska ei halua riskeerata tulevaisuuttaan lähettämällä potilastietoja sähköpostissa.

Taso 3. Sensitiivisen tiedon suojaaminen Internetissä

Tällä tasolla tietokoneen käyttäjän tietoturvakäyttäytyminen muuttuu. Hän esimerkiksi lopettaa lähettämästä sensitiivisiä viestejä sähköpostissa ja alkaa käyttämään tähän tarkoitukseen esim. skypeä. Hän on varovaisempi siitä, mitä tietoja itsestään kirjoittaa Internetissä.

Taso 4. Poikkeaminen omaksutusta toimintatavasta

Tietokoneen käyttäjä voi poiketa omaksutusta toimintatavasta joko väliaikaisesti tai pysyvästi. Esimerkiksi tilanteessa, että hän maksaa laskunsa vahingossa väärän liikkeen tilille hän joutuu lähettämään tilinumeronsa sähköpostissa, koska kokee ettei ole muuta keinoa toimittaa kyseistä asiaa.

Sensitiivistä tietoa voi lisätä Internetiin myös vahingossa. Sosiaaliseen mediaan voidaan laittaa epähuomiossa kuva, jonka lisäämistä myöhemmin kadutaan. Tietokoneen käyttäjä voi unohtaa merkitä kuvan niin että se näkyisi vain tietylle ryhmälle tai laittaa tietoja vahingossa väärään kanavaan.

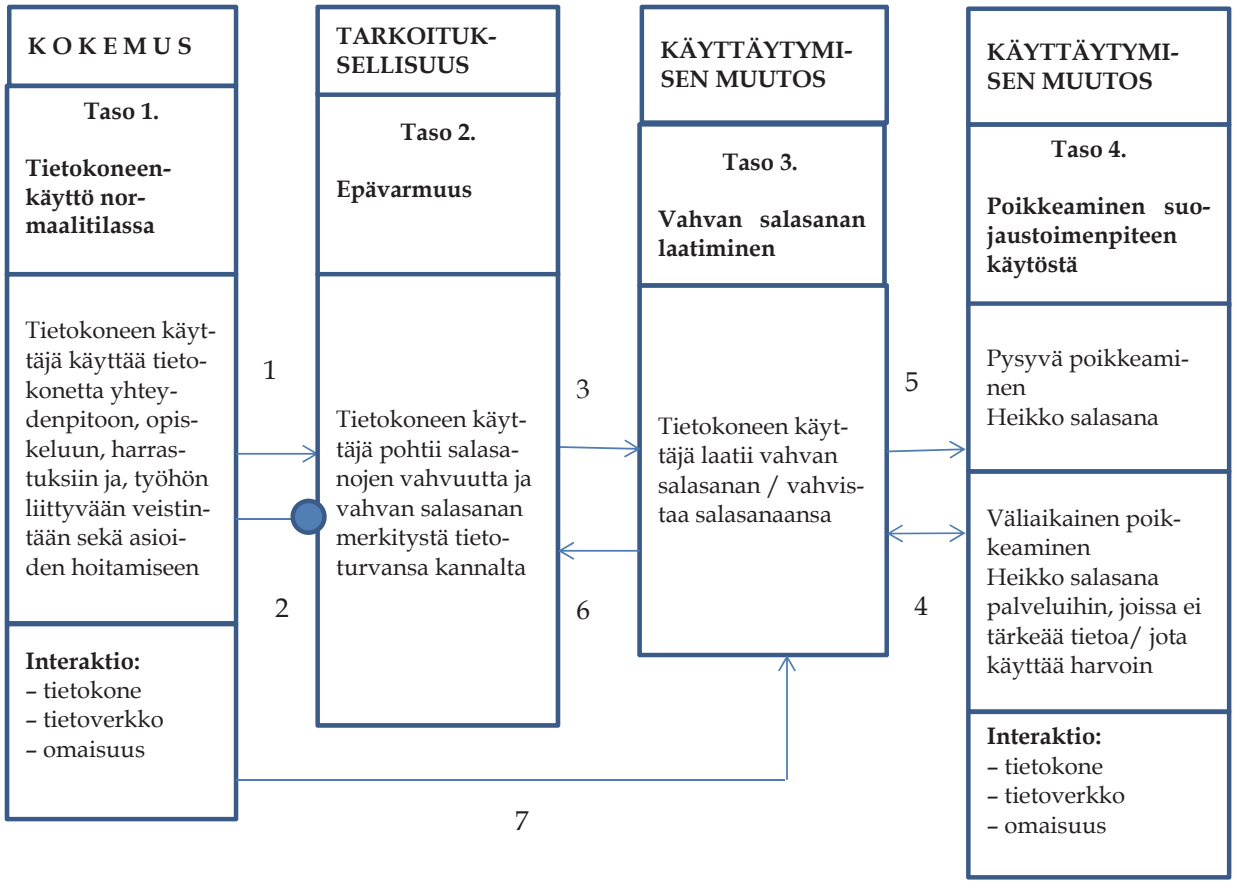
Joihinkin some-palveluihin lisätään sensitiivisempää tietoa kuin muihin. Esimerkiksi Twitteriin ja Instagramiin laitetaan asiallisempaa kuin sellaisiin palveluihin, joissa viestitellään lähipiirin kanssa. Samoin peleissä voidaan välittää sensitiivisempää tietoa kuin esimerkiksi facebookissa, koska käytössä on online-persoona.

Omaksutusta käyttäytymistavasta voidaan poiketa myös pysyvästi. Kun tietokoneen käyttäjä alkaa käyttämään sosiaalista mediaa hän miettii tarkemmin, mitä sinne kirjoittelee mutta ajan kuluessa tämä pohdinta vähenee. Myös tunne siitä, ettei kuitenkaan voi miellyttää kaikkia ja johtaa siihen, että henkilö alkaa lisäämään sensitiivisempää tietoa uudestaan

Tällä tasolla tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko
- omaisuus
- uhka
- harmillinen seuraamus

LIITE 12. PROSESSI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VAHVAN SALASANAN LAATIMINEN



Yhteydet tasojen välillä

#	Yhteyden kuvaus
1	Tietoturvaan liittyvä kokemus Käyttäjä on interaktiossa seuraavien elementtien kanssa: – tietokone – uhka – tietoverkko – omaisuus – tietolähde – edistäjä – harmillinen seuraamus Tietokoneen käyttäjä alkaa käyttämään tietokonetta verkkopankkiasiointiin. Tietokoneen käyttäjän ystävän sosiaalisen median tili kaapataan Tietokoneen käyttäjän henkilökohtainen sähköposti hakkeroidaan/yritetään hakkeroida. Tietokoneen käyttäjä ottaa käyttöönsä google mailin ja ajattelee, että kerää sinne kaikki tärkeät sähköpostit, joten laatii siihen myös vahvan salasanan. Tietokoneen käyttäjä saa koulusta, pankista ja työpaikalta tietoa vahvojen salasanojan merkityksestä ja siitä, millaisia salasanoja ei kannata käyttää. Keskusteluissa ystävien ja kollegoiden kanssa välittyy tietoa vahvoista salasanoista. Tietokoneen käyttäjä lukee aiheeseen liittyviä ohjeita ja tutkimuksia. Tietokoneen käyttäjä pitää pitkään samaa salasanaa ja kirjautuu julkisille koneille esimerkiksi kirjastossa. WWW-palvelu, esimerkiksi sähköpostipalvelu, pakottaa laatimaan vahvan salasanan. Tietokoneen käyttäjä aloittaa ammatillisen koulutuksen ja alkaa käyttää sähköpostia virallisempaan viestintään ja asiakirjojen lähetykseen Tietokoneen käyttäjän ystävä on myymässä tietokonetta jota myös tietokoneen käyttäjä on käyttänyt ja salasanoja on saattanut tallentua koneelle Tietokoneen käyttäjä ostaa uuden tietokoneen, jota varten täytyy laatia uusi tili, jonka takana on kalenteri, sähköposti ja yhteystiedot Muutos elämäntilanteessa. Perheenlisäyksen saaminen aiheuttaa sen, että tie-

	tokoneen käyttäjä kokee tärkeäksi laatia vahvan salasanan pilvipalveluun jossa kuvia omasta lapsesta. Salasanan paljastumien ”olan yli katselun” seurauksena Sähköpostin hakkerointi ja sähköpostin väärinkäyttö
2	Tieto vahvojen salasanojen merkityksestä tai hakkerointi ei vaikuta tietokoneen käyttäjään siten, että hän alkaisi laatimaan vahvoja salasanoja. Syy heikon salasanan käyttämiseen voi olla se, että se on hauska tai että järjestelmä ei vaadi käyttäjältä vahvaa salasanaa.
3	Ratkaisuinteraktio. Tietokoneenkäyttäjä on tietoinen siitä, että salasanojen hakkerointia voi aktiivisesti estää laatimalla palveluihin vahvat salasanat. Käyttäytymisen muutosta edistää se, että pankin järjestelmä ohjaa vahvan salasanan laatimisessa ja että verkkopalvelu pakottaa laatimaan vahvan salasanan jotta palvelua pääsee käyttämään tai pyytää vahvistamaan salasanaa. Internetistä löytyy ohjeita vahvan salasanan laatimiseen. Salasanojen muistamista helpottaa se, jos selain tallettaa salasanat, joten niitä ei tarvitse muistaa. Käyttäytymisen muutosta hidastaa laiskuus
4	Tietokoneen käyttäjä kirjautuu sellaiseen www-palveluun (esim. keskustelupalstalle) jota käyttää vain muutaman kerran tai harvoin tai ottaa käyttöön sellaisen palvelun (esim. Netflix tai suoratoistopalvelut) jossa ei ole niin tärkeää tietoa kuin esimerkiksi sähköpostissa, sosiaalisessa mediassa tai nettipokerisovelluksessa.
5	Tietokoneen käyttäjä ei muista sähköpostin salasanaansa
6	Tietoturvaan liittyvä tapahtuma, esimerkiksi hakkerointi
7	Järjestelmä pakottaa vaihtamaan salasanan

Tasojen kuvaus sekä kuvaus interaktiosta, joka eri tasoihin sisältyy

Taso 1. Käyttötarkoitus

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- omaisuus
- tietoverkko

Tietokoneen käyttäjä käyttää henkilökohtaista tietokonettaan viestintään ystäviensä kanssa, asioiden hoitamiseen kuten esimerkiksi verkkopankkiasiointiin, opiskeluun, harrastuksiin ja työhön liittyvään viestintään.
Tällä tasolla henkilöllä voi olla sähköpostissa käytössään heikko salasana tai vahva salasana, jota tulee myöhemmin tarvetta vahvistaa.

Taso 2: Tarkoituksellisuuden pohtiminen

Tasolla 2 tietokoneen käyttäjä pohtii kokemuksen merkitystä itselleen. Hän alkaa käyttämään verkkopankkia, ja hän kokee, että on tärkeää laatia vahva salasana verkkopankkiin jotta rahat säilyvät tallessa. Verkkopankin käytön aloitus ja tiedon lisääntyminen vahvoista salasanoista saavat tietokoneen käyttäjän pohtimaan vahvojen salasanojen merkitystä myös henkilökohtaisessa sähköpostissa, jonka kautta välittää sensitiivistä aineistoa. Tietokoneen käyttäjä uskoo pankin ohjeita, koska luottaa pankkiin. Tietokoneen käyttäjän ystävä on myymässä tietokonettaan, jota myös tietokoneen käyttäjä on käyttänyt. Hän pohtii tietokoneen salasanojen päätymisen mahdollisuutta ulkopuolisille.

Oman tai ystävän sähköpostin hakkerointi voi vaikuttaa henkilöön siten, että hän alkaa pohtimaan omien salasanojensa vahvuutta. Hän haluaa vahvistaa salasanojaan ja estää tärkeän tiedon ja tiedostojen katoamisen ja päätymisen ei-toivotuille henkilöille ja www-sivuille hakkeroinnin seurauksena. Hän haluaa estää myös omalla identiteetillä esiintymisen esimerkiksi sähköpostien lähettämisen omissa nimissä.

Koska tietokoneen käyttäjä on pitänyt pitkään samaa salasanaa ja kirjautunut julkisille koneille, hän kokee tärkeäksi lisätä salasanaansa ”digitejä” jotta se olisi vahvempi.

Taso 3. Vahvan salasanan laatiminen

Tällä tasolla tietokoneen käyttäjän tietoturvakäyttäytyminen muuttuu. Tietokoneen käyttäjä on pohtinut vahvojen salasanojen merkitystä itselleen ja laatii vahvan salasanan sekä verkkopankkiin että henkilökohtaiseen sähköpostiin.

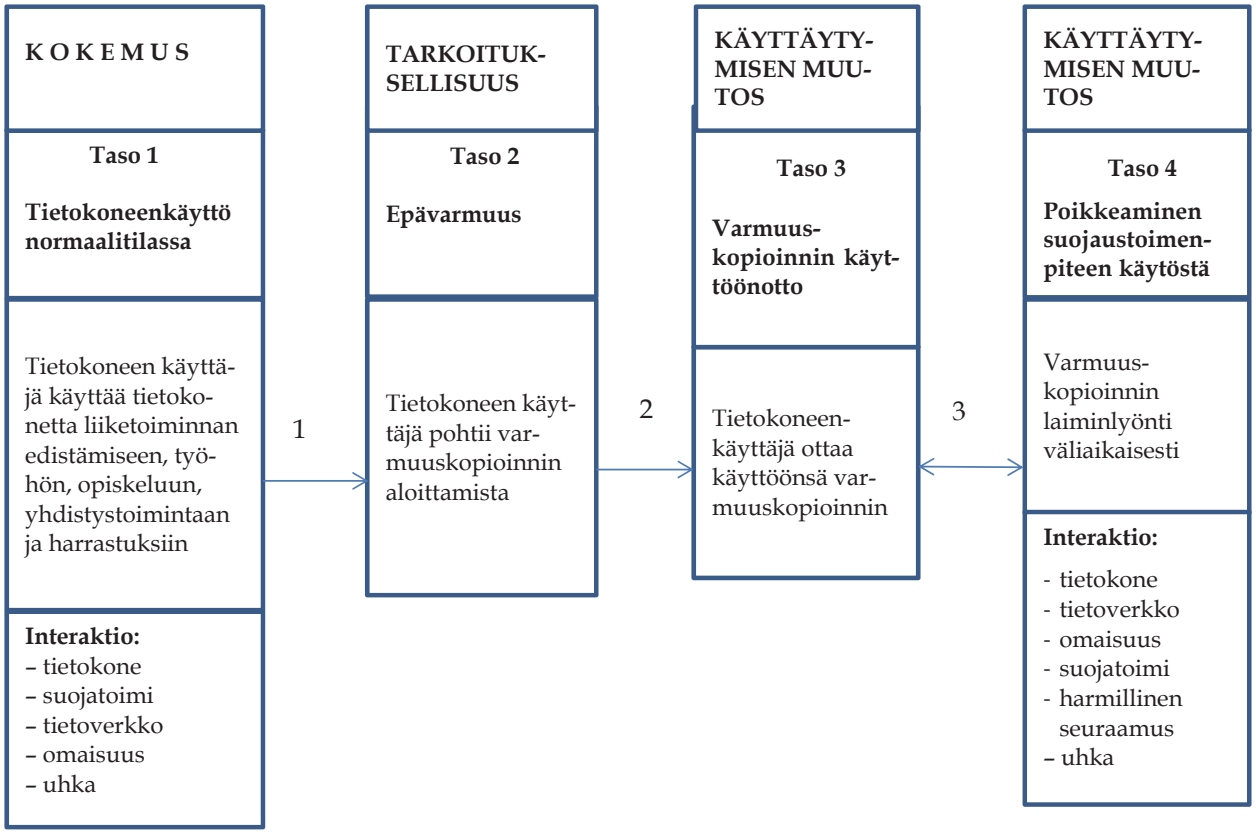
Taso 4. Poikkeukset

Tasolla 4 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko
- omaisuus

Vaikka henkilö on omaksunut vahvojen salasanojen käyttämisen, hän voi poiketa tästä toimintavasta väliaikaisesti. Esimerkiksi siinä tapauksessa, että henkilö kirjautuu keskustelufoorumeille, joihin tietää osallistuvansa vain yhdesti tai kahdesti, hän ei ole huolissaan salasanan vahvuudesta. Myös joihinkin verkkokauppoihin voidaan laatia heikko salasana, jos siellä ei koeta olevan tärkeää tietoa. Myös Netflix ja suoratoistopalvelut ovat sellaisia, joissa ei käytetä vahvaa salasanaa kuten myös lehtiyhtiön sivustot, joita käytetään ehkä muutaman kerran vuodessa. Kun salasana on helppo se on myös helppo muistaa. Vastaavasti sähköpostissa, esimerkiksi koulun sähköpostissa, ja somepalveluissa koetaan olevan tärkeämpää tietoa joten niiden salasanan valinnassa ollaan tarkempia. Samoin salasanat joiden takana on työasioita. Jotkut verkkokaupat ovat sellaisia joihin laitetaan vahva salasana, samoin nettipokerisovellukset joissa käytetään rahaa

LIITE 13. PROSESSI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VARMUUSKOPIOINTI



Yhteydet tasojen välillä

#	Yhteyden kuvaus
1	Tietoturvaan liittyvä kokemus: Tietokoneen käyttäjän koneeseen tulee virus ja hän menettää tärkeitä liiketoiminta-dokumentteja/ kuvia/ opiskeluun liittyviä tiedostoja. Tietokone hajoaa/ ystävän tietokone hajoaa, mistä seuraa tietojen menetys. Tietokoneen tietoja on vaarassa kadota (koneen päälle kaatuu juomaa/ kone hidastuu, mikä on merkki siitä, että tiedot ovat vaarassa yms.) Tietokoneen käyttäjän ystävä neuvoo käyttämään varmuuskopiointia. Opiskeluun liittyvä dokumentti katoaa varmuuskopioinnin puuttumisen takia Tietokoneen käyttäjä on vaarassa kadottaa tärkeitä kuvia puhelimestaan Tietokoneen käyttäjä alkaa laatimaan opiskeluasiakirjoja, ja hän haluaa säilyttää ne tallessa ja välttyä uudelleenkirjoittamiselta Tietokoneen käyttäjä alkaa tekemään isompaa opiskeluun liittyvää dokumenttia Tietokoneen käyttäjä kuulee että opiskeludokumentteja voi kadota varmuuskopioinnin puuttumisen takia Tietokone vanhenee ja heikkenee Sähköpostiviesti ja liitetiedosto katoaa Tietokoneenkäyttäjällä alkaa omistamaan enemmän suojattavaa tietoa **Interaktio:** – harmillinen seuraamus – omaisuus – uhka – tietokone – tietoverkko – tietolähde
2	Ratkaisuinteraktio. Tietokoneenkäyttäjä on tietoinen siitä että tärkeiden tietojen menettämisen voi estää tallentamalla tiedot useampaan paikkaan Siirtymistä tasolle 3 edistää se, että varmuuskopiointiohjelmisto on helppo asentaa ja että varmuuskopiointi yleensäkin on helppoa.
3	Tietokoneenkäyttäjä unohtaa tai ei hoksaa ottaa varmuuskopioita vaikka onkin omaksunut tämän toimintatavan.

	Tietokone ei ole verkossa varmuuskopioinnin aikana joten tiedosto ei tallennu pilvipalveluun Tallennettava tieto ei ole tärkeä. Tallennettava työ on keskeneräinen Varmuuskopiointi epäonnistuu vahingossa Välinpitämättömyys: tietokoneenkäyttäjä ei välitä tai viitsi tehdä varmuuskopioita Tietokoneenkäyttäjä lähettää dokumentin jollekulle toiselle, jolta on vastaus odotettavissa viestiin. Tietokoneenkäyttäjä palaa turvalliseen toimintatapaan väliaikaisen poikkeamisen jälkeen. Tietokoneen käyttää esimerkiksi kuulee muistutteluja varmuuskopioinnin tärkeydestä. Ystävä menettää tietoja mikä muistuttaa varmuuskopioinnin tärkeydestä. Tietokoneenkäyttäjä varmuuskopioi tärkeän dokumentin ja samalla sitten sellaisetkin jotka eivät ole niin tärkeitä Henkilö voi myös itse hoksata, ettei ole varmuuskopioinut tiedostojaan vähään aikaan.

Tasojen kuvaus sekä kuvaus interaktiosta, joka eri tasoihin sisältyy

Taso 1. Käyttötarkoitus

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- omaisuus
- tietoverkko
- uhka
- suojatoimi: virustorjunta

Tietokoneen käyttäjä käyttää henkilökohtaista tietokonettaan liiketoiminnan edistämiseen ja harrastuksiin (esimerkiksi kuvien ja musiikin tallennukseen), työntekoon (esimerkiksi freelancerit) sekä opiskeluun. Hän tallentaa koneelle liiketoiminta-asiakirjoja, työhön ja työnhakuun liittyviä tiedostoja, kaunokirjallisia tekstejä, musiikkia ja kuvia sekä opiskeluun liittyviä töitä, chattilogeja ja artikkelipohjia.

Tietokoneen käyttäjällä voi olla tällä tasolla käytössään antivirusohjelma, koska hän on tietoinen viruksista. Hän uskoo, ettei tarvitse varmuuskopiointia, koska hänellä on virustorjuntaohjelma käytössään.

Taso 2. Tarkoituksellisuuden pohtiminen

Tällä tasolla tietokoneen käyttäjä pohtii kokemusten merkitystä itselleen. Hän on itse menettänyt tietojaan varmuuskopioinnin puuttumisen seurauksena tai on kuullut että ystävät ovat menettäneet tietojaan (esimerkiksi ainutkertaiset kuvat tai työhön tai opiskeluun liittyvät tiedot). Ystävät, koulu, työ ja Internet on tarjonnut tietoa ja varmuuskopiointiin liittyen. Tietokoneen käyttäjän tietokone on kulunut ja vanha joten on vaarassa että tietoja katoaa. Tasolla 2 tietokoneen käyttäjä pohtii, mitä kokemukset merkitsevät hänen oman tilanteensa ja tietoturvansa kannalta. Hän pohtii varmuuskopioinnin aloittamista. Tietokoneen käyttäjä kokee tärkeäksi suojata tietonsa varmuuskopioinnilla. Jos esimerkiksi kovalevy hajoaa niin tiedot ovat ainakin jossain toisessa paikassa tallessa eikä töitä tarvitse tehdä uudestaan.

Taso 3. Varmuuskopiointi

Tällä tasolla tietokoneen käyttäjän tietoturvakäyttäytyminen muuttuu. Tietokoneen käyttäjä on pohtinut varmuuskopioinnin merkitystä tietojensa suojaamisessa ja päätyy ottamaan sen käyttöön.

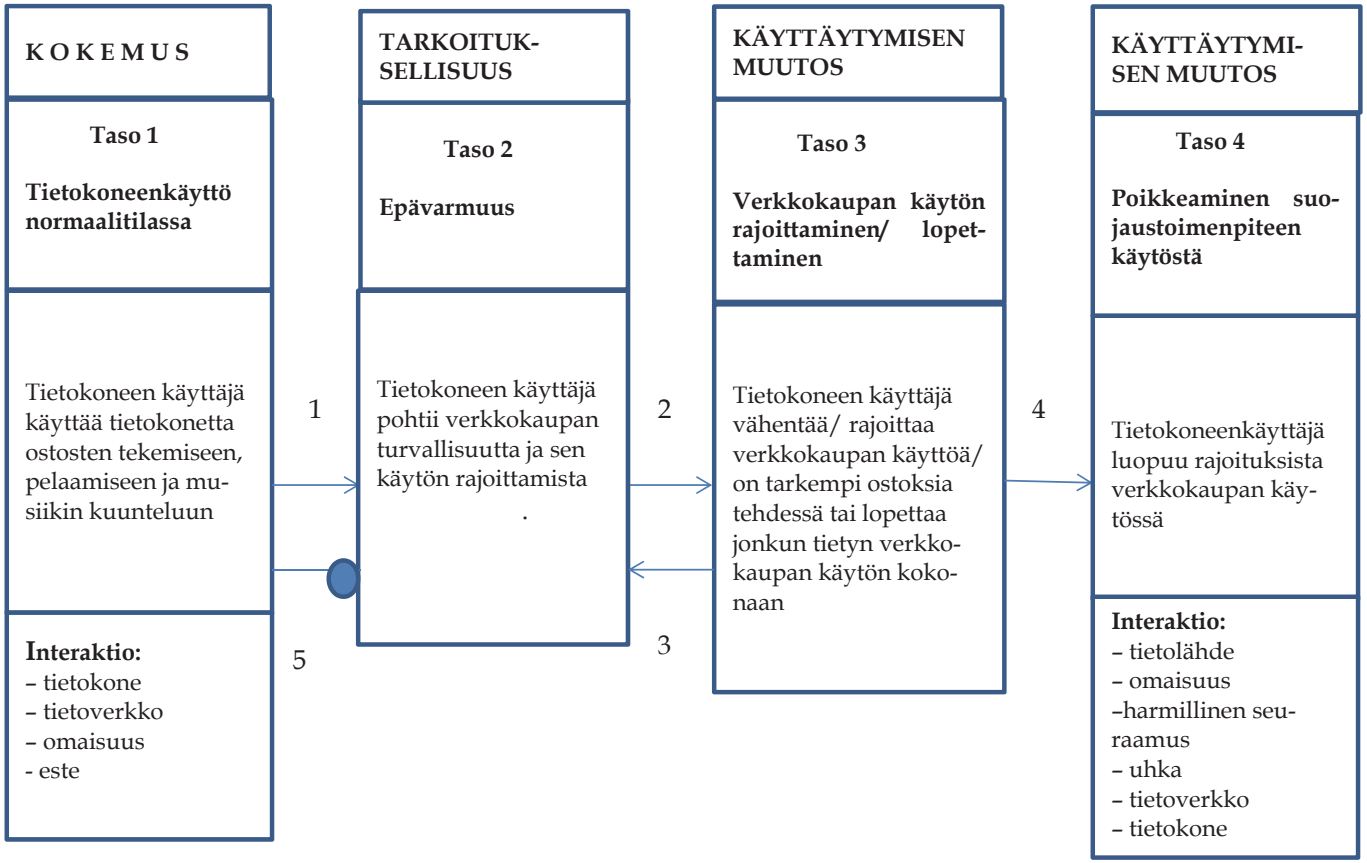
Taso 4. Poikkeukset

Vaikka tietokoneen käyttäjä on omaksunut varmuuskopioinnin, se ei aina ole systemaattista. Varmuuskopiointi saatetaan unohtaa ja esimerkiksi tietoturvaongelman sattuessa muistetaan varmuuskopioinnin tärkeys. Tietokoneen käyttäjä ei varmuuskopioi kaikki tietoja vaan arvioi niiden tärkeellisyyden ja tärkeimmät tallentaa moneen paikkaan, esimerkiksi työhön tai opiskeluun liittyvät dokumentit tai viralliset dokumentit. Välillä tietokoneen käyttäjä hoksaa tiedostoja tarkastellessaan ettei ole varmuuskopioinut niitä pitkään aikaan mihinkään ja laittaa silloin tärkeät tiedot talteen. Aina varmuuskopiointi ei onnistu ja varmuuskopioinnin aikana saattaa tietoja kadota huolimattomuuden takia. Tietokoneenkäyttäjä ei varmuuskopio sellaisia dokumentteja, jotka eivät ole tärkeitä tai keskeneräisiä ja joihin on odotettavissa esim. sähköpostilla palautetta.

Tasolla 4 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko
- omaisuus
- suojatoimi
- harmillinen seuraamus
- uhka

LIITE 14. PROSESSI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VERKKOKAUPPA-ASIOINTI



Yhteydet tasojen välillä

#	Yhteyden kuvaus
1	Tietoturvatapahtuma Tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa: – omaisuus – uhka – harmillinen seuraamus – tietoverkko – tietokone – tietolähde Tietokoneen käyttäjän tili musiikkipalvelussa jää auki. Musiikkipalvelun käytössä ja ohjeissa on ongelmia ja epäselvyyksiä. Tietokoneen käyttäjän luottokortilta velotetaan pieni summa rahaa. Tietokoneen käyttäjä tilaa suoravelotuksella ulkomaiselta palveluntarjoajalta lentolipun, johon tulee ylimääräisiä lisiä. Amerikkalaisen verkkokaupan tietokanta murretaan ja luottokorttinumeroita vuotaa julkisuuteen. Verkkokauppa, luottokunta ja nettifoorumit tiedottaa asiasta. Tietokoneenkäyttäjä kuulee verkkokaupan salasanojen hakkeroinnista Tutusta hotelliketjusta varastetaan luottokorttitietoja Ystävä varaa loma-asunnon tekaistulta verkkosivulta ja menettää paljon rahaa Tietokoneen käyttää kuulee kuinka google playsta voi tilata toisen henkilön nimissä tavaraa Ystävä tilaa verkkokaupasta elektroniikkaa, ja takuun kanssa tulee ongelmia
2	Ratkaisuinteraktio. Tietokoneenkäyttäjä on tietoinen siitä, että verkkokaupankäynnin turvallisuutta voi parantaa - välttämällä luottokortin käyttöä verkkokaupassa - lopettamalla epäluotettavan verkkokaupan käytön. - kieltämällä luottokorttinumeroiden säilytyksen verkkokaupassa. - ottamalla käyttöön pay pal: in verkkokaupassa maksettaessa - tarkistamalla millainen salaus on verk-

	ko-kaupassa, eli onko ns. turvallisempi moodi päällä - tarkistamalla maksuvaihtoehdot - ottamalla epävarmuutta aiheuttavissa asioissa yhteyttä suoraan yritykseen Este Verkkokaupan englanninkielisiä ohjeita on vaikeita ymmärtää, mikä muodostuu esteeksi turvallisen verkkokaupan käytölle
3	Tietoturvaongelma, esimerkiksi ystävän luottokortti hakkeroidaan hänen tilattuaan pelejä verkkokaupasta ja hän saa ison laskun, jonka selvittelyyn menee aikaa.
4	Tietokoneen käyttäjä kohtaa vakavia ongelmia verkkokaupan käytössä, esim. luottokortin hakkeroinnin tai rahan häviämisen tililtä. Tietokoneenkäyttäjän suhtautuminen verkkokauppoihin muuttuu myönteisemmäksi verkkokauppojen yleistymisen myötä
5	Huono kokemus verkkokaupassa ei välttämättä saa rajoittamaan sen käyttöä

Tasojen kuvaus sekä kuvaus interaktiosta, joka eri tasoihin sisältyy

Taso 1. Käyttötarkoitus

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko
- omaisuus
- este

Tietokoneen käyttäjä käyttää tietokonetta ostosten tekemiseen. Hän lataa musiikkia, pelejä ja ostaa mm. matkoja, vaatteita, elektroniikkaa ja loma-asuntoja. Hän käyttää asioinnissa luottokorttia. Tietokoneen käyttöä verkkopankkiasioissa haittaa se, että vieraskieliset ohjeet ovat vaikeasti ymmärrettäviä.

Taso 2: Tarkoituksellisuuden pohtiminen

Negatiiviset kokemukset verkkokauppa-asioinnissa (esim. rahanmenetys musiikkipalvelussa, luottokortin hakkerointi ja huijaus asunnon vuokraamisen yhtey-

dessä) vaikuttavat käyttäjän ajatteluun siten, että hän alkaa pohtia verkkokaupan turvallisuutta.

Hän haluaa toimia luotettavien toimijoiden kanssa ja luottaa siihen ettei tapahdu mitään yllätyksiä. Tietokoneen käyttäjä ei halua tulla huijatuksi eikä menettää rahaa. Hän ei halua myöskään ylimäärästä vaivaa, kun pitää selvitellä rahanmenetystä ja tiliä ei voi käyttää vähään aikaan.

Taso 3: Varovaisuus verkkokaupassa lisääntyy

Käyttäytyminen muuttuu. Tietokoneen käyttäjä rajoittaa verkkokaupan käyttöä. Hän esimerkiksi lopettaa maksullisen musiikin tilaamisen verkkokaupasta ja vähentää luottokortin käyttöä verkkokauppa-asioinnissa.

Tietokoneen käyttäjä välttää tilaamasta tietyistä verkkokaupoista, esimerkiksi ulkomaisista/ pienistä/ epäluotettavista verkkokaupoista eikä anna säilyttää luottokorttinumeroita verkkokaupassa. Hän ottaa käyttöön pay pal:in verkkokauppamaksuissa. Jos henkilö tilaa luottokortilla, hän tarkistaa, millainen salaus on verkkokaupassa, eli onko ns. turvallisempi moodi päällä ennen kun lähtee antamaan mitään tietoja.

Tietokoneen käyttäjä tarkistaa maksuvaihtoehdot ja on tarkempi ostosten teossa verkkokaupassa, esimerkiksi jos on tekemässä sellaista tilausta, josta jollain toisella on huonoja kokemuksia, ottaa yhteyttä suoraan yritykseen.

Siinä tapauksessa että tietokoneen käyttäjä kohtaa yhtä vakavia ongelmia kuin ystävänsä ja tuttavansa, jotka menettivät paljon rahaa verkkokaupassa tai kokee rahojen häviämisen tililtä, verkkokaupan käyttö voi loppua. Henkilö ajattelee: ”en tilaa mitään”.

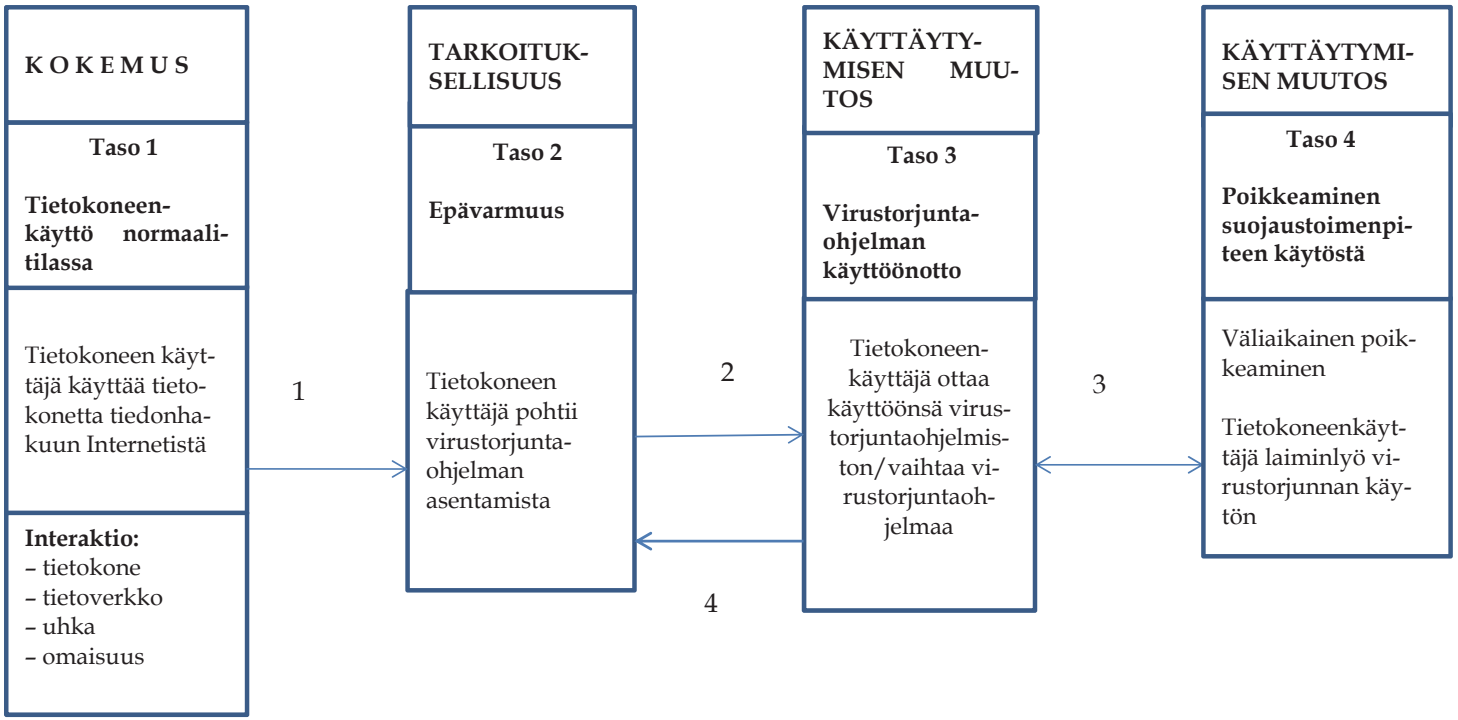
Taso 4. Poikkeaminen omaksutusta toimintatavasta

Tasolla 4 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietolähde
- omaisuus
- harmillinen seuraamus
- uhka
- tietoverkko
- tietokone

Verkkokaupan yleistymisen myötä luottamus verkkokauppaan voi lisääntyä. Tämän johdosta tietokoneen käyttäjä poikkeaa aiemmin omaksutusta turvallisemmasta toimintavasta ja vähentää verkkokauppaan liittyviä rajoituksia, esimerkiksi luopumalla paperilaskusta.

LIITE 15. PROSESSI KÄYTTÄYTYMISEN MUUTOKSESTA, ESIMERKKINÄ VIRUSTORJUNTA



Yhteydet tasojen välillä

#	Yhteyden kuvaus
1	Yhteys 1 muodostaa tietoturvaan liittyvän kokemuksen Käyttäjä on interaktiossa seuraavien elementtien kanssa: – harmillinen seuraamus – suojatoimi – uhka – tietoverkko – tietokone – omaisuus – tietolähde Tietoturvatapahtuma voi olla se, että tietokoneenkäyttäjä kuulee julkisuudesta tietomurroista tai että haittaohjelmat voivat kaapata tietokoneita tai että liikkeellä on viruksia / vakoiluohjelmia niissä laitteissa, joita hän käyttää sillä hetkellä. Tietokoneen käyttäjä saa ystävältä/sukulaiselta neuvoja virustorjuntaohjelman valintaan.
2	Ratkaisuinteraktio. Tietokoneenkäyttäjä on tietoinen siitä, että tietokoneen ja siinä olevat tiedot voi suojata viruksilta virustorjuntaohjelmalla. Lisäksi, virustorjuntaohjelmaa vaihtamalla voi saada koneelleen tehokkaamman suojan. Siirtymistä tasolle 3 edistää se, että ohjelmisto on helppo asentaa, käyttää ja ymmärtää jos käyttöohjeet ovat suomeksi. Ohjelmiston ilmaisuus edesauttaa sen käyttöönottoa. Hidastava tekijä on se, että tietokoneenkäyttäjä epäilee virustorjunnan tehokkuutta Esteeksi uuden virustorjuntaohjelman käytölle voi muodostua virustorjunnan maksullisuus ja se, että tietokoneen ikä ei mahdollista modernin virustorjuntaohjelman asentamista. Tietokoneen käyttäjällä voi olla puutteelliset taidot virustorjuntaohjelmien etsimiseen Internetistä ja asennusohjeiden ymmärtämiseen.
3	Sovelluksen asentaminen/testaaminen (sovellus ei toimi, joten sitä pitää testata ottamalla virustorjunta hetkeksi pois päältä)
4	Tietoturvaan liittyvä tapahtuma Virustorjuntaohjelma ei pysty poistamaan virusta eikä estä kaikkia tietoverkon välityksellä koneelle tulevia haittaohjelmia. Puutteellinen toiminnallisuus (esimerkiksi virustorjuntaohjelma blokkaa liikaa) Luotettava taho, esimerkiksi ystävä tai

	lähipiiri, suosittelee toista virustorjuntaohjelmistoa. Tietokoneen käyttäjä kuulee Internetin keskustelupalstoilta arviointeja siitä, mikä on hyvä / huono suojausohjelmisto. Mainokset/ lisäominaisuudet/ virheilmoitukset ärsyttävät Toinen virustorjuntaohjelmisto on ilmainen Virustorjuntaohjelman vapaan version vuosittainen uusiminen ei onnistu

Tasojen kuvaus sekä kuvaus interaktiosta, joka eri tasoihin sisältyy

Taso 1. Käyttötarkoitukset

Tasolla 1 tietokoneen käyttäjä on interaktiossa seuraavien elementtien kanssa:

- tietokone
- tietoverkko
- suojatoimi
- uhka
- omaisuus

Tietokoneen käyttäjä käyttää tietokonetta Internet-sivujen selailuun, esimerkiksi uutisten ja lehtien lukemiseen. Hänellä ei ole käytössään virustorjuntaohjelmaa, koska hän ajattelee, että virukset ja vakoiluohjelmat ovat sen verran harvinaisia Mac-tietokoneissa, ettei tarvitse virustorjuntaohjelmaa.

Taso 2. Tarkoituksellisuuden pohtiminen

Tasolla 2 tietokoneen käyttäjä pohtii kokemuksen merkitystä itselleen ja hänen ajattelunsa muuttuu. Hän on kokenut tietoturvaongelman, Hänen koneensa on saastunut viruksista/ kone on mennyt epäkuntoon viruksen takia. Hän on kuullut julkisuudesta siitä, mitä haittaohjelmat voi saada aikaan ja saanut tietoa ja neuvoja virustorjuntaohjelmistoista Internetin keskustelupalstoilta, ystäviltä ja lähipiiriltä.

Tasolla 2 hän pohtii, mitä em. asiat merkitsevät hänen oman tietoturvansa kannalta. Tietokoneen käyttäjä kokee tärkeäksi suojata koneensa viruksilta ja haitta ohjelmilta tehokkaammin. Hän haluaa suojata myös sen, ettei kukaan pääse pankkitietoihin käsiksi. Hän pohtii virustorjuntaohjelman asentamista, koska ei halua, että kun latailee ohjelmia, niissä on ”kylkiäisiä” matkassa ja että kone saastuu haittaohjelmista. Hän haluaa välttää ne ongelmat, joita on aiemmin kokenut haittaohjelmien takia, esimerkiksi koneen hidastuminen, sekä lisäksi pankkitunnusten ja salasanojen kaappauksen.

Taso 3. Virustorjuntaohjelman käyttöönotto

Käyttäytyminen muuttuu. Tietokoneen käyttäjä on miettinyt suojauksen hankkimista viruksia vastaan tietokoneelleen ja päätyy ottamaan käyttöönsä virustorjuntaohjelmiston.

Taso 4. Poikkeaminen omaksutusta toimintatavasta

Jos tietokoneen käyttäjä haluaa asentaa tietyn ohjelman, virustorjunta pitää ottaa hetkeksi pois päältä jotta sovelluksen saa toimimaan

LIITE 16. KÄYTTÄYTYMISEN MUUTOKSEEN VAIKUTTAVAT TUNTEET

Tapahtuma	**Tunne**	**Esimerkki aineistosta**	**Tunteen vaikutus käyttäytymiseen**
Identiteettivarkaus	huoli omasta ammatillisesta tulevaisuudesta	*I: Yeah. So do you think these accidents what you have had.. influence on your behavior, somehow made you more secure or..* *R: Yes, and more careful, I hide more things, in Facebook. But I think, only my friends have to see, no one else have to see my birth year or my emails or.. (--) [0:22:45.7]* *I: So.. what kind of consequences you see.. you would have because of this kind of identity theft, what kind of harm (--)?* *R: Not.. perhaps if I go.. to a.. I want to work at someplace and employer googles my name and finds stuff that I haven't done, in fact many people do it nowadays, and.. someone has, written something under my name, something, perhaps, racistic or politic and these things that employers want to know and it could affect the.. if they hire me or not.*	Internet -profiilin hallinta: Sosiaalisen median yksityisyysasetusten tiukentaminen
Tietokoneenkäyttäjä kuulee että sähköpostiviestit ovat salaamattomia	epävarmuus, pelko ja huoli liittyen tietoihin joita välittää sähköpostissa	*V: Kyllä se herätti tietenki semmosta epävarmuutta.* *K: : Tuliko huolta tai pelkoa?* *V : Tuli, tietenki tuli.* *K: Miten tämä sun ajatuksiin tai*	Sensitiivisen aineiston prosessointi: Tietokoneenkäyttäjä välttää sensitiivisen tiedon laittamista sähkö-

		käyttäytymiseen nyt sitte jatkossa...? *V: Varmaan se vaikuttaa aika voimakkaasti nyt. Tulee vähemmän [?? 01:15:12].* -- *V: Saattaa olla, että mä alan kirjottamaan niitä kaunokirjallisia kirjeitä enemmän sitten. Ingmar Bergmanhan muuten kirjotti kaikki käsikirjotukset käsin.*	postiin
Valokuvien häviäminen puhelimesta	hätäännys joka aiheutuu tärkeiden kuvien katoamisesta	*K: Minkälaisia ajatuksia tunteita tämä herätti tämä tämmönen tietoturvakokemus?* *V: Se herätti just siihen tajuamaan, että hetkinen, että se voi yhellä ainoalla painauksella hävitä kaikki.* *K: Minkälaisia tunteita siihen liitty?* *V: Se oli aivan, jotenki musta tuntu, että...* *K: Oliko hätäännys tai joku semmonen?* *V: Tuli. Just nimenomaan se hätäännys.*	Varmuuskopiointi: Tietokoneenkäyttäjä alkaa tallentamaan kuvat kahteen paikkaan
Valokuvien menetys	kauhu koska menetti tärkeitä valokuvia	*K: Kiinnostaa, minkälainen oli sun reaktio [?? 00:46:05] tämä tapahtu. Mitä sää aattelit, minkälaisia tunteita se ehkä herätti?* *V: Kyllä se herätti kauhua, siellä oli valokuvat ja muistot. Se oli kauhun tunne.* *K: Mitä sää aattelit siinä?* *V: Että onko nämä nyt kaikki oikeasti poissa. Sillon tuli mieleen, että kyllä*	Varmuuskopiointi: Varmuuskopioinnin aloittaminen

		nostalgiset ajatukset, että ennen vanhaan oli kyllä paljon paremmin, kun ne oli siellä albumeissa turvallisesti. Paperikuvina. Ku siellä oli siis semmosia kuvia sitte, mitä mää en ollu vielä ehtiny teettää paperikuviksikaan, että ne ois sitte menny... *K: Elikkä nimenomaan sen tapahtuman jälkeen alko se tuplakopiointi?* *V: Kyllä.*	
Nettikiusaaminen	suru joka aiheutuu uutisista liittyen nettikiusaami-seen	*V: Nii, sanottaisiinko, että minä olen kyllä kuullut tässä monia varoittavia esimerkkejä sisällön lataamisesta.* *K: No kerro muutama.* *V: No minä… Siis tämähän ei minuun niin päde, koska minä en ole nainen. Mutta kuitenkin muistan muun muassa Briteistä erään surullisen esimerkin, jossa eräs teinityttö kyberkiusaamisen takia teki itsemurhan.* *--* *K: Vaikuttiko se sinun käyttäytymiseen sitte, tietoturvakäyttäytymiseen, ja millälailla jos vaikutti?* *V: Sanottaisiinko, että se oli osa semmoista, että olin merkittävästi varovaisempi siitä, millaista nettiin lataan ja se on yksi niistä syistä muun muassa, miksi minä en ole Facebookissa ollenkaan. Minä henkilö… Niin aivan aidosti henkilökohtaista tietoa jaan kuitenkin hyvin kitsaasti netissä.*	Sensitiivisen aineiston prosessointi: Tietokoneenkäyttäjä on varovaisempi sensitiivisen tiedon prosessoinnissa

Tietokoneenkäyttäjä kuulee opiskelu-dokumentin menetyksestä	myötätunto, jota tunnetaan toisen opiskelijan menetettyä tärkeän opiskeludokumentin	*K: Muistakko nää sillon, ku kuulit, että oli tämmönen isompi onnettomuus tapahtunu että mitä nää aattelit, mitä ehkä tunteita nousi esille? Mikä reaktio?* *V: Ei siinä muuta ku myötätunto vaan. Että ois tosi ilkeää, jos itelle tapahtu sellanen. Toivos, ettei kenellekään muullekaan tapahtuis.*	Varmuuskopiointi: Tietokoneenkäyttäjä alkaa varmuuskopioimaan tärkeät opiskeludokumentit
Salasanojen hakkerointi	välinpitämättö-myys: tietokoneenkäyttäjä ei koe että salasanojen hakkerointi on vakava asia	*I: So did you change your behaviour somehow after this hacking experience?* *R: Maybe it affected my behaviour but, in the time I didn't think this is serious problem. I don't know the reason why I changed it, my password to complicated password*	Ei vaikutusta
Salasanojen hakkerointi	turhautuminen joka on seurausta hakkerointiuuti-sista	*K: Sitte kyselisin taas sitä, että minkälaisia reaktion, minkälaisia tunteita nämä tiedot aiheutti, ni mitä sä sillon mietit tai minkälaisia tunteita se aiheutti, ku kuulit tämmösestä?* *V: No enempi turhautumista, et joku ny sitte viittii ja tietenki minä aattelin, että tuskin ny sitte meikäläisen, eläkeläisen salasanoista ny kovin paljon mitää irti saa, et siinä ei kuitenkaan rahan kanssa ollu tekemissä, siis kaikista salasanoista. Siellä ani harva voi johtaa mihinkää, että pystyy tilaamaan jotaki taikka muuta. Et en ollu pitäny niitä sillä tavalla merkit-*	Vahvan salasanan laatiminen: Tietokoneenkäyttäjä vaihtaa heikot salasanansa vahvoiksi

		tävänä, mutta sit aattelin, että minä varmuuden vuoksi nämä nyt vaihdan kuitenkin, että jos siinä jotaki häikkää tulee.	
Nettisivuston kaappaus ja verkkokauppahuijaus	ihmettely, viha joita koetaan verkkokauppa-huijauksen yhteydessä	*K: Tuliko jotain muita erityisiä tunteita siinä pintaan, minkälainen reaktio oli, ku tämä tapahtu?* *V: Ihmettelin sitä vaan, että koskaan ollu ajatellu sitä, että kokonainen tavallaan tommosen yrityksen nettisivusto voiaan kaapata ihan autenttisen [?? 00:52:59], että siinä kaikki oli ihan oikeeta tietoja, et se oli kaapattu ihan semmosenaan, ainoostaan oli muutettu vaan tilinumerot.* -- *K: Oliko joku semmonen viha, raivo siinä päällimmäisenä?* *V: No kyllä se on, todellakin otti päähän. Ja sitte yllätys kyllä, että itelläkään koskaan osannu ajatella, että tommonen sivusto, jossa on muuten kaikki täydellistä, toimii ja kaikki, että sitä ei osaa oikein epäillä, että onko tämä aito vai kopio.*	Varovaisuus verkkokaupassa: Varovaisuus lisääntyy merkittävien varausten tekemisessä
Ongelma verkkokaupassa	ärtymys joka aiheutuu ongelmista verkkokaupassa	*K: Kuvaile sitte sitä, mitä sää ajattelit sen ongelman yhteyessä? Mikä oli reaktio? Mitä tunteita ehkä siinä heräs?* *V: Paska homma, ärsytti ja muuta, mutta oli mulla itellä seki mielessä myös, että samaan saattaa joutua ihan paikallisessa kivijalkaliikkeessäki. Ei*	Varovaisuus verkkokaupassa: Henkilö katsoo tarkemmin mistä verkkokaupasta ostaa

		siinä sinällään. *K: Nää kerrot, että nää aloit sitte vähä tarkemmin kattomaan, mistä nää ostat.* *V: Joo. Sinällään, että jos kyseisellä... No nettiinki sitte alkanu ilmestymään näitä arvostelupaikkoja, vertailupaikkoja, nii käyn sieltä vähän katellu, että jos hintavertailua kattoo, nii ei sitte ehkä se kympin pari halvempi hinta enää paina siinä vaiheessa.*	
Tietoisuuden lisääntyminen salasanoista	vähättely, ärtymys, välinpitämättö-myys, huoli, jotka johtuvat siitä että tietokoneen-käyttäjä saa tietoa vahvoista salasanoista	*K: Mikä tunne vois kuvata sitä [?? 00:53:36].* *V: Että eikö se nyt riitä, että ei sitä kuitenkaan nyt kukaan. Kuka siitä nyt on kiinnostunu sen kummemmin. Mutta sitte kuitenki kai siihen sitte se huoli.* *K: Välinpitämättömyyen tunne?* *V: Vähän ehkä oli semmonen välinpitämätön ja sitte ehkä kuitenki vähä semmonen huoli, että jos se nyt on käytäntö ,nii miksipä sitä nyt ei, mutta se tietysti mietitytti ja vähän aiheutti ärtymystä, ku joka paikassa nykyään pitää olla joku tietty salasana tai koodi tai numerosarja, että niitä on sitte loppujen lopuks niin paljon, mitä pitää muistaa. Että miten ne kaikki muistaa, miten muistaa aina, mitä on laittanu mihinki. Tietty sitäki suunnitellaan, että niitä on eri, että ne on eri salasanoja eri paikois, ettei oo sama.*	Vahva salasana: Tietokoneenkäyttäjä laatii vahvan salasanan

		Se, että miten niitä muistaa, semmonen vähä aiheutti semmosta päänvaivaa, että tämmöstä turhanpäivästä monimutkasuutta. *K: Mikä sitte oli se kaikista tärkein asia, mikä sinut sai vakuuttuneeksi? Sää kuitenki laadit sen vahvemman salasanan. Mikä oli siinä motiivina?* *V: Turvallisuuden tarve ja just se, että ei tartte sitten sen kummemmin sitä pohtia tai miettiä.*	
kuvien vuotaminen kuvanjako palvelusta	Pettymys kuvanjakopal-veluun	*K: Minkälaisia ajatuksia tai tunteita tämä sitte herättää, ku se ei ookkaan pysyny siellä (kuvanjakopalvelussa)?* *V: Sanotaan niin, että valitettavasti, en tiiä, löytyykö se jossaki niissä sitten, kun niissä hyväksytyissä, niin mitä on sovellutuksilla hyväksyny, mutta ainaki minä oon pettyny siihen, että ne pitää selkeemmin sanoo ne, tavallaan sen, että miten se toimii joku kuvanjakopalvelu ja mihin se voi se tieto sitten päätyä. Pitää ne rajotukset kertoo selkeesti, eikä missään semmosessa, että 50 sivua, ni sitähä ei kukkaan jaksa…* -- *V: Mä en etes tiedä, tiedän vaan, että sieltä jotakiha on saatavissa kuulemma pois, mutta niin monimutkanen prosessi tuntuu olevan ja epävarmaa, että se nyt varmasti poistuu. Sanon, että minä nyt tiedä sitte, että kannat-*	Sensitiivisen aineiston prosessointi: Tietokoneenkäyttäjä varoo laittamasta sensitivistä aineistoa Internetiin

		taako siihen ryhtyä [?? 01:00:55], enempi varoo siinä, että kun mitä aineistoa sinne panee. Et on vaan harmitonta aineistoa, jos menee, niin menee.	
sähköpostin hakkerointi	huvittuneisuus liittyen hakkeroinnin epäonnistumiseen	*K: Niin siihen vielä, miten nä huomasit sen, että se oli yritetty hakkeroida se sun…* *V: Yleensä niistä tulee jonku näkönen viesti, että on…* *K: Sieltä palvelun tarjoojalta?* *V: Niin. Tai että on otettu jostaki toisesta ip:stä, että täältä on yritetty, tavanomaisesta poikkeavasta kohteesta on yritetty kirjautua tänne ja se ei oo onnistunu. Aika moni lähettää nykyään semmosen viestin noista isommista palveluntarjoajista niinku Google ja pelifirmat on monesti kans semmosia.* *K:Mitä nä siinä tilanteessa aatelit, että minkälaisia fiiliksiä herätti?* *V: Lähinnä naurahdin, ku mulla on se kaksvaihe autentifikaatio, siinäpähän yrittävät.*	Ei vaikutusta
ongelma liian laajan kaveripiirin suhteen sosiaalisessa mediassa	hämmennys joka on seurausta yksityisyysasetusten puutteellisesta määrittelystä sosiaalisessa mediassa	*K: Joo, miks sää aloit tarkistelemaan niitä sitte niitä asetuksia?* *V: Varmaan ku tuli outoja kaveripyyntöjä, niitä tuli yhessä välissä aika paljon, nii se vähä häiritsi ja sitte ku itekki näki jottai iha tuntemattomien ihmisten julkasuja, nii mää olin sillee, että ei mun tarvi nähä näitä, että vaan*	Internet-profiilin hallinta: Sosiaalisen median yksityisyysasetusten tiukentaminen

		kaverit näkee. *K: Joo, mitä ajatuksia tai tunteita siihen sitte liitty?* *V: No hämmennystä tosi paljo, että miksi tullee tämmösiä ku ei niinku oo mitään kontaktia näihin ihmisiin, se oli tosi outoa. Mutta sitte tein näin, nii sitte ne loppu kyllä siihen*	
tietoisuus lisääntyy vahvoista salasanoista	epävarmuus, häpeä, harmi jotka ovat seurausta siitä että henkilö saa uutta tietoa salasanoihin liittyen	*V: Ei ehkä, se oli semmosta… saatto siinä olla semmosta pientä epävarmuutta ja sitte semmosta tavallaan harmitusta, että kun luki niitä juttuja, että miksi heleppoja salasanoja ei kannata käyttää ja sitten mietti, että niin, minä oon aina käyttäny näin helppoja.* -- *K: Joo, no miksi ne sitten vaikutti ne uutiset, mikä niissä sai tavallaan… mikä niissä vaikutti sun käyttäytymiseen, miks se oli tärkeetä noudattaa niitä?* *V: Tavallaan sitä huomasi, että miten pöljästi sitä on tehny, että justiin kun oli tämmösiä niinku oikeita sanoja ja muita.*	Vahvan salasanan laatiminen Tietokoneenkäyttäjä alkaa laatimaan vahvoja salasanoja
sosiaalisen median käytön aloitus	epäluulo joka liittyy omien tietojen näkyvyyteen Internetissä	*V: Koska siitä oli jotenki syvä epäluulo että jos ei, ei ehkä niin tietoturva-asioista tai en mä tiedä miten tietoturva, mitä kaikkea se käsittää mutta mulla oli syvä epäluulo siitä että jos mä sit päivitän sinne jotakin niin ketkä kaikki näkkee niitä mun tietoja.*	Internet profiilin hallinta: Sosiaalisen median yksityisyysasetusten määrittäminen

		Niitä mä selvitin aika paljon ennen ku alkoin käyttämään.	
virus	ihmettely, raivo jotka johtuvat viruksesta omalla koneella	*V: Niin, no kyllä se varmasti justiisa se yllätyshän se (virus) on aina sitten ja yhden kerran yllätyin sitte, ku vaihdoin uuden koneen ja oli vähän aikaa, ku siirsin ohjelmia toiselle, niin se usko oli vielä sitte siinä ei ollu vielä ladattuna mitään siinä vaiheessa, kun mä luulin vaan, että kun mä siirrän vaan, että se ei mee nettiin. Ni se oli vähän aikaa, ni kuitenki se nettiytti sen siihen, siihenhä tuli ryökäleet troijalaisia jo sitten. Se muutaman minuutin aikana.* *K: Noppeesti ne löytää sitte.* *V: Ne oli tosi vaikeita poistettavia, että kyllä ne sitte ilmaantu, ku sai sen virusohjelman, ni se kyllä skannasin sen, ni se kerto ne. Niissä oli kans vaikeuksia löytää niitä. Kyllä se tietenki raivoahan se herättää siis, että viittivät vaan tahallaan tehä niitä. Raivoo, yllätystä ja sitte todellaki…*	Virustorjunta: Tietokoneenkäyttäjä asentaa virustorjuntaohjelman
omien tietojen lisääminen sosiaaliseen mediaan	painostava tunne liittyen tietojen jakamiseen sosiaalisessa mediassa	*V: No just vähä semmonen, onko ahistava ehkä liian radikaali sana… Semmonen painostava tunne, että en halua…* *K: Semmonen epämiellyttävä?* *V: Epämiellyttävä, kyllä, että en halua, että ihmiset tietää musta asioita liikaa. Vaikka eihän siis, en mitään henkilökohtasta kirjottanu sinne mit-*	Internet-profiilin hallinta: Sosiaalisen median yksityisyysasetusten tiukentaminen

	tää vaan semmosia perusjuttuja, että oli kiva päivä tai jottai, tein tämmöstä ja tämmöstä. Mutta siltiki tuntu, että se on vähä… *K: Joo, sulle tuli semmonen tunne, jotenki epämukava tunne?* *V: Nii. Sillee just ihmiset tarkkailee, vaikka ei ne silti tarkkaile, ne on vaa sillee että kiva että oot käyny ulkona ja jotain semmosta normaalia, tämmöstä ihan perusjuttua. Nii sitte ehkä ei tarvikaan.*	