Henri Perämäki
Juha-Matti Sulander

TYÖASEMIEN LUKITSEMISEEN VAIKUTTAMINEN: PITKITTÄINEN INTERVENTIOTUTKIMUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Perämäki, Henri ja Sulander, Juha-Matti
Työasemien lukitsemiseen vaikuttaminen: pitkittäinen interventiotutkimus
Jyväskylä: Jyväskylän yliopisto, 2018, 140 s.
Tietojärjestelmätiede, Pro Gradu -tutkielma
Ohjaaja(t): Siponen, Mikko ja Rönkkö, Mikko

Tässä Pro Gradu -tutkielmassa tutkittiin työasemien lukitsemiseen vaikuttamista sähköpostitse lähetettyjen interventioviestien avulla. Työaseman lukitseminen on tärkeä käyttäjän vastuulla oleva tietoturvatoimi ja sen laiminlyöminen voi mahdollistaa ulkopuolisen pääsyn järjestelmiin ja tietoon. Aiempi tietoturvakäyttäytymisen tutkimus on keskittynyt suurelta osin kyselytutkimuksiin, joilla on selvitetty käyttäytymisen aietta. Todellista käyttäytymistä oikeassa organisaatioympäristössä havainnoivia ja siihen vaikuttamaan pyrkiviä tutkimuksia on tehty hyvin vähän. Tässä työssä raportoidussa tutkimuksessa organisaation henkilökunnalle lähetettiin sähköpostitse interventioviesti, jonka tarkoituksena oli lisätä työasemien lukitsemista. Viestin lähetys toistettiin yhteensä kolme kertaa ja viestien vaikutusta todelliseen lukitsemiskäyttäytymiseen havainnoitiin yhteensä noin vuoden ajan.

Viestien sisällön vaikutusta tutkittiin viestejä manipuloimalla. Kirjallisuuskatsauksen perusteella viestien pohjaksi valittiin kaksi eri teoriaa: suojelumotivaatioteoria sekä prospektiteorian mukainen viitekehyksen vaikutus. Suojelumotivaatioteoriaan perustuvia viestejä manipuloimalla pyrittiin vaikuttamaan uhka-arvioon ja selviytymisarvioon. Viitekehyksen huomioivissa viesteissä käytettiin negatiivista ja positiivista kehystämistä. Molempien teoriapohjien osalta manipuloitiin myös uhkan henkilökohtaisen relevanssin painotusta sekä kuvailun tarkkuuden tasoa.

Interventioilla saatiin vaikutettua positiivisesti työasemien lukitsemiseen. Kaksi ensimmäistä interventiota lisäsi työasemien päivittäistä lukitsemista keskimäärin yhteensä lähes 30 % kolmannen intervention vaikutuksen jäädessä vähäisemmäksi. Ei yhtään lukitusta sisältäneiden kirjautumissessioiden päivittäinen osuus kaikista sessioista laski havaintojakson aikana yhteensä noin 40 %.

Ensimmäisen intervention osalta selittävien tekijöiden vaikutusta tutkittiin regressioanalyysin ja marginaalivaikutusten avulla. Tutkimuksessa havaittiin viitekehysvaikutuksen olevan suojelumotivaatioteoriaa tehokkaampi. Suojelumotivaatioteorian uhkan korostaminen tehosi jo ennestään paljon lukitseviin käyttäjiin ja selviytymisarvioon vaikuttaminen puolestaan vähän lukitseviin. Viitekehysvaikutuksen osalta positiivinen kehys oli negatiivista tehokkaampi. Henkilökohtaisen relevanssin korostaminen saattoi hieman lisätä intervention vaikutusta vähän lukitsevilla. Kuvailun tarkkuuden tasoilla ei havaittu tehoeroa.

Asiasanat: tietoturva, tietoturvakäyttäytyminen, työaseman lukitseminen, viitekehysvaikutus, suojelumotivaatioteoria, interventio

ABSTRACT

Perämäki, Henri and Sulander, Juha-Matti
Improving the locking of workstations: a longitudinal intervention study
Jyväskylä: University of Jyväskylä, 2018, 140 p.
Information Systems, Master's Thesis
Supervisor(s): Siponen, Mikko and Rönkkö, Mikko

In this Master's Thesis the efficacy of an email intervention in improving the locking of workstations was investigated. Locking the workstation is a crucially important security measure that the user is responsible for. Neglecting this could result in unauthorized access to the information systems by a 3rd party. Previous research on information security behavior has focused mainly on survey studies that have used behavioral intention as the dependent variable. Studies observing actual behavior in a real organizational context have received significantly less attention. In this experiment an email message was sent to the staff of an organization in attempt to increase the locking of workstations. The intervention was repeated three times in total and the actual behavior was observed for a period of one year.

The effect of message content was studied by manipulating the messages according to two different theories. The theories used in this study were Protection Motivation Theory (PMT) and Prospect Theory based message framing effect. Regarding PMT, the aim was to affect the cognitive threat appraisal and coping appraisal processes. With message framing both positive and negative framing was used. In addition, personal relevance of the threat and the amount of details included in the messages were manipulated.

The interventions had a positive effect on the locking of workstations. The first two interventions increased the amount of daily locks by approximately 30 % combined. A small but positive change was observed for the third intervention. The relative daily amount of sessions with no lock events decreased by 40 percent.

Multiple linear regression and average marginal effects were used to study the relationship between the manipulations made to the messages and the observed change in the locking of workstations in the first intervention. Messages that were based on framing effect were found more effective than messages based on PMT. Emphasizing the threat was effective on users who locked workstations more than an average user, whereas affecting the coping appraisal was effective on users who locked workstations less. Positive message framing was more effective than negative message framing. Emphasizing the personal relevance increased the effect of the intervention on those who locked workstations less than an average user. Manipulating the amount of detail did not have a noticeable effect.

Keywords: information security, workstation locking, information security behavior, protection motivation theory, framing effect, intervention

KUVIOT

KUVIO 1 Suojelumotivaatioteoria (mukaillen Rogers, 1983)..... 19
KUVIO 2 Valintakehys (mukaillen Levin, Schneider & Gaeth, 1998) 27
KUVIO 3 Ominaisuuskehys (mukaillen Levin, Schneider & Gaeth, 1998)..... 28
KUVIO 4 Tavoitekehys (mukaillen Levin, Schneider & Gaeth, 1998)..... 29
KUVIO 5 Tutkimuksen eteneminen vuokaaviona esitettynä 39
KUVIO 6 Interventiokokeen eteneminen aikajanalla kuvattuna..... 40
KUVIO 7 Yhden session aikana tehtyjen lukitsemisten kappalemäärien jakauma esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen. 55
KUVIO 8 Sessioiden keston jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen. 56
KUVIO 9 Yksittäisen lukituksen keston jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen. 57
KUVIO 10 Yhden session aikana tehtyjen lukitusten yhteiskeston jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen. 58
KUVIO 11 Sessiokohtaisesti määritetyn keskimääräisen lukitsemisaktiivisuuden jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen. 59
KUVIO 12 Käyttäjien jakautuminen käyttäjäluokkiin lukitsemisaktiivisuuden perusteella esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen..... 60
KUVIO 13 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä (yhteensä 1881 uniikkia käyttäjää)..... 62
KUVIO 14 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 0 käyttäjille (yhteensä 339 uniikkia käyttäjää)..... 63
KUVIO 15 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 1 käyttäjille (yhteensä 253 uniikkia käyttäjää)..... 63
KUVIO 16 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 2 käyttäjille (yhteensä 372 uniikkia käyttäjää)..... 64
KUVIO 17 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 3 käyttäjille (yhteensä 345 uniikkia käyttäjää)..... 65
KUVIO 18 Keskimääräinen lukitsemisaktiivisuus päivittäin kaikille käyttäjille (yhteensä 1881 uniikkia käyttäjää)..... 66
KUVIO 19 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 0 käyttäjille (yhteensä 339 uniikkia käyttäjää)..... 67
KUVIO 20 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 1 käyttäjille (yhteensä 253 uniikkia käyttäjää)..... 68
KUVIO 21 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 2 käyttäjille (yhteensä 372 uniikkia käyttäjää)..... 69
KUVIO 22 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 3 käyttäjille (yhteensä 345 uniikkia käyttäjää)..... 69
KUVIO 23 Nollalukkosessioiden osuus kaikista sessioista..... 70

KUVIO 24 Keskimääräinen lukitsemisaktiivisuus päivittäin kontrolliryhmälle (yhteensä 81 uniikkia käyttäjää). 71

TAULUKOT

TAULUKKO 1 Tietoturvakäyttäytymisen luokittelu (Stanton ym., 2005)..... 14
TAULUKKO 2 Aasialaisen taudin ongelma (Tversky & Kahneman, 1981) 25
TAULUKKO 3 Varman ja epävarman rahan saamisen ongelma (Tversky & Kahneman, 1981)..... 25
TAULUKKO 4 Andersonin ja Agarwalin (2010) tutkimuksen viestien kehystämisen esimerkkejä..... 31
TAULUKKO 5 Barlow ym. (2013) tutkimuksen viestien kehystämisen esimerkkejä..... 32
TAULUKKO 6 Havaintoaineiston rajaamisessa käytetyt ehdot..... 51
TAULUKKO 7 Sessioihin liittyvät tiedot havaintoaineistossa..... 52
TAULUKKO 8 Käyttäjien luokittelu esitarkkailujakson lukitsemisaktiivisuuden perusteella..... 54
TAULUKKO 9 Käyttäjien jakautuminen luokkiin esitarkkailujakson ja viimeisen intervention (I_3) jälkeen ristiintaulukoituna, prosenttiosuudet suhteessa esitarkkailujakson luokitukseen. 61
TAULUKKO 10 Regressioanalyysissä ja korrelaatiotaulukossa käytetyt muuttujat ja niiden selitykset..... 74
TAULUKKO 11 Muuttujien korrelaatiot 75
TAULUKKO 12 Intervention vaikutus session keskimääräiseen lukitsemisaktiivisuuteen yleisesti..... 77
TAULUKKO 13 Intervention keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen kontrolliryhmässä 78
TAULUKKO 14 Suojelumotivaatioteorian ja viitekehysvaikutuksen vertailu regressiolla. Riippuvana muuttujana keskimääräinen lukitsemisaktiivisuus.... 79
TAULUKKO 15 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja käytetyn teorian funktiona..... 80
TAULUKKO 16 Suojelumotivaatioteorian faktorien vaikutus keskimääräiseen lukitsemisaktiivisuuteen interventiossa..... 81
TAULUKKO 17 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja uhkan vakavuuden ja todennäköisyyden faktorin funktiona..... 82
TAULUKKO 18 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja henkilökohtaisen relevanssin faktorin funktiona..... 83
TAULUKKO 19 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja kuvailun tarkkuuden faktorin funktiona 83

TAULUKKO 20 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja vastatoimen tehokkuuden ja minäpystyvyyden faktorin funktiona..... 84
TAULUKKO 21 Viitekehysvaikutuksen faktorien vaikutus keskimääräiseen lukitsemisaktiivisuuteen interventiossa..... 85
TAULUKKO 22 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja viitekehysvaikutuksen näkökulman faktorin funktiona..... 86
TAULUKKO 23 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja henkilökohtaisen relevanssin faktorin funktiona..... 87
TAULUKKO 24 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja kuvailun tarkkuuden faktorin funktiona..... 87
TAULUKKO 25 Yhdistettyjen faktorien kuvailun tarkkuus ja henkilökohtainen relevanssi vaikutus keskimääräiseen lukitsemisaktiivisuuteen interventiossa.. 89
TAULUKKO 26 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja yhdistetyn henkilökohtaisen relevanssin faktorin funktiona..... 90
TAULUKKO 27 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja yhdistetyn kuvailun tarkkuuden faktorin funktiona..... 90

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

TAULUKOT 5

SISÄLLYS 7

1 JOHDANTO 9
1.1 Tutkimuksen tarve 9
1.2 Tutkimuksen tavoitteet, rajaus ja tutkimuskysymykset 10
1.3 Tutkielman rakenne 11

2 TIETOTURVA ORGANISAATIOSSA 12
2.1 Tietoturva organisaatiossa 12
2.2 Tietoturvakäyttäytyminen 13
2.3 Tietoturvaviestinnällä vaikuttaminen 15
2.4 Yhteenveto tietoturvasta organisaatiossa 16

3 PELKOON VETOAVA VIESTINTÄ 17
3.1 Pelkoon vetoaminen 17
3.2 Suojelumotivaatioteoria 19
3.3 Suojelumotivaatioteoria tietoturvatutkimuksessa 21
3.4 Pelkoon vetoavan viestinnän yhteenveto 22

4 VIITEKEHYSVAIKUTUS VIESTINNÄSSÄ 24
4.1 Prospektiteoria ja päätöskehys 24
4.2 Päätöskehyksestä viitekehysvaikutuksen kategorisointiin 26
4.3 Viitekehysvaikutus IT-tutkimuksessa 30
4.4 Yhteenveto viitekehysvaikutuksesta viestinnässä 32

5 PUUTTEITA AIEMMASSA TIETOTURVAKÄYTTÄYTYMISEN TUTKIMUKSESSA 34

6 KIRJALLISUUSKATSAUKSEN YHTEENVETO 37

7 TUTKIMUKSEN TOTEUTUS 39
7.1 Tutkimusmenetelmä 40
7.2 Kohdeorganisaatio 42
7.3 Interventiot 42
7.3.1 Faktorien ja tasojen valinta 43

7.3.2 Viestien muotoilu ja viimeistely 43
7.3.3 Interventioviestin vastaanottajien rajaaminen ja ryhmittely 45
7.3.4 Viestien lähettäminen ja datan kerääminen 45
7.4 Datankeruujärjestelmä 46
7.4.1 Suunnittelu, toteutus ja testaus..... 46
7.4.2 Tietoturva ja yksityisyys 47
7.5 Havaintoaineiston muodostaminen kerätystä datasta 48
7.5.1 Sessioiden muodostaminen 48
7.5.2 Työaseman lukitsemisten yhdistäminen sessioihin..... 49
7.5.3 Sessioiden rajaaminen analyysiä varten 49

8 ANALYYSI JA TULOKSET..... 52
8.1 Lukitsemisaktiivisuus..... 52
8.2 Käyttäjien luokittelu 54
8.3 Esitarkkailujakson ja viimeisen intervention jälkeisen kuukauden vertailu..... 54
8.4 Lukitsemiskäyttäytyminen päivittäin tarkasteltuna..... 61
8.4.1 Lukitsemisten ja käyttäjien kokonaismäärät 61
8.4.2 Päivittäinen lukitsemisaktiivisuus 65
8.4.3 Nollalukkosessioiden osuus 70
8.4.4 Kontrollin päivittäinen lukitsemisaktiivisuus..... 71
8.5 Intervention vaikutuksen selittäminen..... 71
8.5.1 Usean selittäjän lineaarinen regressio..... 72
8.5.2 Keskimääräinen marginaalivaikutus 72
8.5.3 Datan rajaus ja muuttujien valinta analysointia varten..... 72
8.5.4 Intervention vaikutus kontrolliryhmään..... 76
8.5.5 Suojelumotivaatioteorian ja viitekehyksen vaikutuksen vertailu..... 78
8.5.6 Suojelumotivaatioteorian faktoreiden vaikutus..... 80
8.5.7 Viitekehysvaikutuksen faktorien vaikutus..... 84
8.5.8 Kuvailun tarkkuuden ja viestin henkilökohtaisen relevanssin vaikutus 88

9 YHTEENVETO..... 91
9.1 Kokeen reliabiliteetti ja validiteetti..... 94
9.2 Tulosten merkitys 96
9.2.1 Tutkimukselle 96
9.2.2 Käytännölle 97
9.3 Jatkotutkimusideoita 97

LÄHTEET 99

LIITE 1 SUOJELUMOTIVAATIOTEORIAAN POHJAUTUVAT INTERVENTIOVIESTIT 104

LIITE 2 VIITEKEHYSVAIKUTUS-POHJAISET INTERVENTIOVIESTIT 128

1 JOHDANTO

Iso osa tietoturvatutkimuksesta on keskittynyt tietoturvaan teknisistä lähtökohdista yrittäen luoda turvallisempia algoritmeja tai parempia menetelmiä kehittää tietoturvallisia järjestelmiä (Stanton, Stam, Mastrangelo, & Jolton, 2005). Yhä enenevissä määrin on kuitenkin havahduttu siihen, että pelkästään tekniset ratkaisut eivät ole riittäviä vaan vähintään yhtä keskeisessä osassa on järjestelmiä käyttävien ihmisten käyttäytyminen (Pfleeger & Caputo, 2012). Käyttäjän kannalta pieneltä tuntuva tietoturvan laiminlyönti voi pahimmassa tapauksessa auttaa ulkopuolista tahoa ohittamaan tietojärjestelmän teknisen tietoturvan kokonaan.

Eräs tärkeimmistä käyttäjien vastuulle jäävistä tietoturvatoimista on työaseman lukitseminen tai uloskirjautuminen työaseman luota poistuttaessa (Vance, Siponen, & Pahnila, 2012). Työaseman lukitsemisella tarkoitetaan työaseman sulkemista niin, että työaseman käytön jatkaminen vaatii salasanaa. Kertakirjautumisen (engl. single sign-on, SSO) ja muiden järjestelmien käyttöä helpottavien teknologioiden yleistyminen on entisestään korostanut työaseman lukitsemisen tärkeyttä. Kertakirjautumista hyödynnettäessä eri järjestelmiin kirjautuminen tapahtuu automaattisesti työasemalle kirjautuneen tunnuksen tiedoilla, minkä ansiosta käyttäjätunnusta ja salasanaa ei tarvitse erikseen syöttää uudelleen. Lukitsematonta työasemaa käyttämällä voi olla siis mahdollista päästä laajastikin käsiksi organisaation järjestelmiin ja tietoon. Tällaista väärinkäyttöä on lisäksi vaikea havaita, sillä se ei vaadi teknisten suojausten murtamista.

1.1 Tutkimuksen tarve

Tietoturvakäyttäytymiseen, kuten työaseman lukitsemiseen, vaikuttavia tekijöitä on tutkittu laajasti. Tutkimus on rajoittunut tyypiltään kuitenkin paljolti kyselytutkimuksiin, joissa pyritään selittämään henkilön itsensä raportoiman käyttäytymisen aietta erilaisia teorioita hyödyntäen. Sen sijaan vähemmälle huomiolle ovat jääneet todellisen käyttäytymisen havainnointi sekä tutkimukset, joissa

käyttäytymiseen yritetään vaikuttaa. Muun muassa kyselyihin tiedonkeruumenetelmänä liittyvien ongelmien sekä käyttäytymisen aikeen ja todellisen käyttäytymisen välisen epäselvän yhteyden vuoksi onkin olemassa tarve tutkimuksille, joissa todellista käyttäytymistä havainnoidaan pitkällä ajanjaksolla. (Crossler ym., 2013; Lebek, Uffen, Breitner, Neumann & Hohler, 2013).

Suojelumotivaatioteoria on yksi tietoturvakäyttäytymisen kontekstissa eniten tutkituista teorioista. Eri tutkimuksista saadut tulokset ovat kuitenkin olleet keskenään epäyhteneväisiä ja jopa osittain ristiriidassa keskenään (Menard, Bott, & Crossler, 2017). Lisäksi useat tahot ovat huomauttaneet organisaation tietojärjestelmiin kohdistuvien uhkien henkilökohtaisen relevanssin puutteen aiheuttamista ongelmista teorian soveltamisen kannalta (Johnston, Warkentin & Siponen, 2015; Menard ym., 2017). Tietoturvakäyttäytymisen tutkimuksessa on pohdittu myös negatiivisten seurausten konkreettisuuden vaikutusta. Abstraktit seuraamukset eivät välttämättä riitä motivoimaan toimimaan tietoturvallisesti (Pfleeger & Caputo, 2012).

Eräs vähemmän tietoturvatutkimuksessa huomiota saaneista aiheista on prospektiteorian mukaisen viitekehyksen vaikutuksen tutkiminen. Halutun toiminnan kehystämisen eli esittämisen joko huonojen seurausten välttämisenä tai toimintana hyötyjen saavuttamiseksi on havaittu vaikuttavan ihmisten päätöksentekoon myös tietoturvan kontekstissa. (Anderson & Agarwal, 2010; Shropshire, Warkentin, & Johnston, 2010)

Organisaatioissa sähköposti on nykyisin laajasti käytetty viestinnän väline. Sen avulla on mahdollista lähestyä kerralla suurta vastaanottajajoukkoa hyvin pienillä tai lähes olemattomilla kustannuksilla. Käytännön kannalta olisikin tärkeää saada tietoa sähköpostiviestinnän vaikutuksesta todelliseen tietoturvakäyttäytymiseen oikeassa organisaatioympäristössä. Mikäli sähköpostiviestillä saadaan aikaan konkreettisia parannuksia organisaation tietoturvaan, voidaan sen käyttöä pitää hyöty-kustannussuhteen perusteella kannattavana.

Myös koko tutkimusalan kannalta olisi tärkeää, että tietoturvan tutkimus tuottaisi käytännön kannalta relevanttia tietoa, sillä informaatioteknologian merkitys organisaatioille on suuri ja jatkuvasti kasvava. Käytäntöön sovellettavaa tietoa tuottamalla vältetään päätymästä tilanteeseen, jossa tutkimusta tehtäisiin vain sen itsensä vuoksi (Rosemann & Vessey, 2008).

1.2 Tutkimuksen tavoitteet, rajaus ja tutkimuskysymykset

Tämän tutkimuksen tavoitteena on vaikuttaa tietoturvainterventiolla työasemien lukitsemiseen positiivisesti oikeassa organisaatiossa. Interventiot toteutetaan sähköpostiviesteillä, joiden sisältöä manipuloimalla tutkitaan kahteen eri teoriaan perustuvan viestityypin tehokkuutta. Interventio toistetaan useita kertoja toiston vaikutuksen tutkimiseksi. Suojelumotivaatioteorian osalta tutkitaan uhkan vakavuuden ja todennäköisyyden sekä vastatoimen tehokkuuden ja minäpystyvyyden korostamisen vaikutusta. Viestin viitekehyksen osalta vertaillaan

negatiivista ja positiivista kehystämistä. Kummankin viestityypin kohdalla tutkitaan lisäksi uhkan kohdistumisen henkilökohtaisen relevanssin sekä kuvailun yksityiskohtaisuuden vaikutusta.

Tutkimus toteutetaan pitkittäisenä kenttätutkimuksena, jossa dataa todellisesta lukitsemiskäyttäytymisestä kerätään pitkältä ajanjaksolta. Kerättävän aineiston perusteella pyritään selvittämään, miten toistettu sähköposti-interventio vaikuttaa organisaation henkilökunnan todelliseen lukitsemiskäyttäytymiseen. Tutkimuksessa painotetaan tutkimusasetelman tosielämän vastaavuutta sekä havaintojen käytännön hyödynnettävyyttä.

Tutkimusongelman selvittämiseksi ja tutkimuksen rajaamiseksi edelleen käytetään seuraavia tutkimuskysymyksiä:

Kysymys 1: Voidaanko sähköposti-interventiolla lisätä työasemien lukitsemista ja onko vaikutus pysyvä?

Kysymys 2: Onko sähköposti-intervention toistamisesta hyötyä?

Kysymys 3: Eroaako suojelumotivaatioteoriaan pohjautuvan intervention teho viitekehysvaikutukseen perustuvan intervention tehosta?

Kysymys 4: Miten suojelumotivaatioteorian mukaisen uhkan vakavuuden ja todennäköisyyden sekä vastatoimen tehokkuuden ja minäpystyvyyden korostaminen vaikuttaa lukitsemiskäyttäytymiseen interventiossa?

Kysymys 5: Miten viestin viitekehyksen valinta vaikuttaa työasemien lukitsemiseen interventiossa?

Kysymys 6: Miten henkilökohtaisen relevanssin korostaminen tai kuvailun yksityiskohtaisuuden lisääminen vaikuttaa työasemien lukitsemiseen interventiossa?

1.3 Tutkielman rakenne

Tämän tutkielman rakenne on seuraava. Työ jakautuu aiempaan kirjallisuuteen perustuvaan osuuteen ja kokeelliseen osuuteen. Kirjallisuusosuudessa käydään läpi tutkimuksen teoreettisen taustoittamisen sekä tutkimuksen motivoimisen kannalta oleellista aiempaa kirjallisuutta. Kokeellisessa osassa kuvataan ensin tutkimuksen toteutus ja sen jälkeen havaintoaineiston analysointi ja tulokset. Tutkielman lopussa annetaan lyhyt yhteenveto tuloksista sekä pohditaan kokeeseen liittyneitä rajoituksia. Tämän tutkielman työmäärällisesti selkeästi suurin kokonaisuus oli kokeellisen tutkimuksen suunnittelu ja toteutus sekä kerätyn aineiston analysointi.

2 TIETOTURVA ORGANISAATIOSSA

Tässä luvussa käsitellään tietoturvaa organisaation kontekstissa. Osion aluksi esitellään tietoturvan ja tietoturvakäyttäytymisen käsitteet, jonka jälkeen käsitellään tietoturvaviestinnällä vaikuttamisen keinoja.

2.1 Tietoturva organisaatiossa

Nykyään organisaation tietojärjestelmiä ja tietojärjestelmissä käsiteltävää tietoa pidetään kriittisenä organisaation toiminnalle. Näiden tietojen suojaaminen voi olla organisaatiolle yhtä tärkeää, kuin esimerkiksi organisaation talousresurssien, fyysisen omaisuuden ja työntekijöiden suojaaminen. Organisaation tietojärjestelmissä sijaitsevan tiedon arvo voi jopa ylittää organisaation fyysisen omaisuuden arvon, koska nykyajan organisaatiot toimivat yhä enemmän verkossa ja ovat riippuvaisia tietojärjestelmien jatkuvasta toiminnasta. (Andress, 2014; Peltier, 2014.)

Tietopääoman suojaamisen tarve ei myös rajoitu pelkästään järjestelmien ja järjestelmissä säilytettävän tiedon tietoturvaan, vaan tietoturva koskee lisäksi muuta organisaation tietopääomaa, kuten paperisia arkistoja sekä muita tietovarastoja. (Peltier, 2014.)

Tietoturvaan organisaation kontekstissa sisältyy kaiken organisaation tiedon ja järjestelmien suojaaminen sijainnista riippumatta. Tietoturvan tasoa voidaan arvioida kolmen käsitteen kautta: tiedon luottamuksellisuus (engl. confidentiality), tiedon eheys (engl. integrity) ja tiedon saatavuus (engl. availability). Näistä kolmesta käsitteestä muodostuvaa mallia kutsutaan englanninkielisten käsitteiden mukaan CIA-malliksi, joka on osa myös ISO27002-tietoturvastandardia. Tiedon luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain henkilöt, joilla on siihen oikeus. Tiedon eheydellä tarkoitetaan tiedon oikeellisuutta sekä täydellisyyttä. Tiedon saatavuudella tarkoitetaan tiedon jatkuvaa ja katkotonta saatavuutta aina, kun tietoa tarvitaan. (Andress, 2014.)

Työaseman lukitsematta jättämisen muodostama tietoturvauhka koskettaa kaikkia CIA-mallin tietoturvan osa-alueita. Tiedon luottamuksellisuuden toteutuminen edellyttää siis esimerkiksi sitä, etteivät ulkopuoliset pääse käsiksi käyttäjien omiin tiedostoihin tai työasemalle. Ulkopuolisen päästessä käsiksi tiedostoihin tai työasemalle on myös tiedon eheys ja saatavuus uhattuna: tiedostoja ja työaseman tietoja on mahdollisuus muokata luvatta.

Tietoturvan parantaminen ja hallinta edellyttävä usean eri osatekijän huomioimisen. Näitä ovat muun muassa:

- Menettelyt ja käytänteet (esimerkiksi tietoturvapolitiikka)
- Ihmiset (esimerkiksi mahdollisuus vaikuttaa koulutuksella)
- Laitteistot (esimerkiksi palomuuri)
- Ohjelmistot (esimerkiksi tiedon salausohjelma)

- Data (esimerkiksi datan luokittelu)

Nämä osatekijät muodostavat perustan organisaation tietoturvalle ja mahdollistavat tiedon luottamuksellisuuden, eheyden ja saatavuuden suojaamisen (Whitman & Mattord, 2011). Tekijöistä tärkeimpänä pidetään tietoturvapolitiikkaa. Organisaation tietoturvapolitiikka määrittää organisaation henkilökunnalle ja johdolle, miksi organisaatio tarvitsee tietoturvaa ja miten tietoturva tukee organisaation toimintaa. Tietoturvapolitiikka määrittää myös yleiset tietoturvaperiaatteet, joiden mukaan henkilöstön odotetaan toimivan. Tietoturvaperiaatteilla määritetään siis millä toimilla henkilöstö suojelee organisaation tietoa ja mikä toiminta on sallittua. Tietoturvapolitiikka määrittää usein myös rikkomusten seuraukset. (Höne & Eloff, 2002.) Käytännössä piittaamattomuus ja epätietoisuus tietoturvapolitiikoista organisaatioissa on hyvin yleistä. Käyttäjien on tutkimuksissa usein havaittu toimivan mieluummin tietoturvapolitiikan vastaisesti, vaikka he olisivat tietoisia tietoturvallisesta oikeasta toimintatavasta. (Moody, Siponen, & Pahnila, 2018.)

Tietoturvan kohdalla sanonta ”ketju on yhtä vahva kuin sen heikoin lenkki” pitää hyvin paikkaansa. Yksikin heikko kohta, kuten työaseman lukitsematta jättäminen, voi vaarantaa tietoturvan ja mahdollistaa asiattoman pääsyn organisaation resursseihin. Esimerkiksi vuonna 2017 lähes 30 % tietomurroista oli seurausta organisaation oman henkilökunnan toiminnasta (Verizon Enterprise, 2018). Pelkkä tietoturvapolitiikan määrittely ei siis paranna organisaation tietoturvaa, vaan henkilöstö on saatava myös sitoutettua noudattamaan tietoturvallisia toimintatapoja. Tietoturvan laiminlyönti voi johtua useista eri syistä. Käyttäjät kokevat yleisesti tietoturvan olevan toisarvoista käsillä olevaan tehtävään verrattuna. Jos tietoturvan huomioiminen haittaa ensisijaisen tehtävän suorittamista, saatetaan se sivuuttaa kokonaan. Lisäksi käyttäjät usein luottavat teknisten taustajärjestelmien huolehtivan tietoturvasta heidän puolestaan. (Pfleeger & Caputo, 2012.)

2.2 Tietoturvakäyttäytyminen

Tietoturvakäyttäytymisellä tarkoitetaan mitä tahansa käyttäytymistä, jolla voi olla vaikutusta tietoturvan kannalta. Tietoturvakäyttäytyminen voi olla hyödyllisen käyttäytymisen lisäksi haitallista ja organisaation tietoturvapolitiikan vastaista. Stanton ym. (2005) esittävät tietoturvakäyttäytymisen jakautuvan kuuteen eri luokkaan tarkoituksellisuuden ja osaamisen tason mukaan. Nämä on esitetty taulukossa 1.

TAULUKKO 1 Tietoturvakäyttäytymisen luokittelu (Stanton ym., 2005)

Osaamisen taso	Tarkoituksellisuus	Luokan nimi	Luokan kuvaus
Korkea	Pahantahtoinen (engl. malicious)	Tahallinen vahingoittaminen (engl. intentional destruction)	Käytös vaatii teknistä osaamista yhdistettynä vahvaan aikeeseen aiheuttaa harmia organisaation IT:lle ja resursseille. Esimerkki: Työntekijä murtautuu työnantajan suojattuihin tiedostoihin tarkoituksenaan varastaa liikesalaisuuksia.
Matala	Pahantahtoinen (engl. malicious)	Vahingollinen väärinkäyttö (engl. detrimental misuse)	Käytös vaatii vain vähän teknistä osaamista, mutta tarkoituksena on kuitenkin aiheuttaa harmia, häirintää, sääntöjen rikkomista ym. Esimerkki: Työnantajan sähköpostin käyttö roskapostiviestien lähettämiseen oman sivutyön markkinointiin.
Korkea	Neutraali (engl. neutral)	Riskialtis toiminta (engl. dangerous tinkering)	Vaatii teknistä osaamista, mutta ei aietta aiheuttaa harmia organisaation IT:lle tai resursseille. Esimerkki: Työntekijä konfiguroi langattoman reitittimen, joka tahattomasti päästää ulkopuoliset organisaation verkkoon.
Matala	Neutraali (engl. neutral)	Naiivit vahingot (engl. naive mistakes)	Vaatii vain vähän teknistä osaamista ja ei aietta vahingoittaa organisaation IT:tä tai resursseja. Esimerkki: Huonon salasanan valinta, kuten "salasana".
Korkea	Hyväntahtoinen (engl. beneficial)	Valveutunut tarkastelu (engl. aware assurance)	Vaatii teknistä osaamista ja aikeen tehdä hyvää suojellakseen organisaation IT:tä ja resursseja. Esimerkki: Työntekijä tunnistaa työasemalla olevan takaoven tarkkailemalla oman työaseman toimintaa.
Matala	Hyväntahtoinen (engl. beneficial)	Yleinen huolellisuus (engl. basic hygiene)	Ei vaadi teknistä osaamista, mutta sisältää aikeen suojella organisaation IT:tä ja resursseja. Esimerkki: Osaava ja valveutunut työntekijä tunnistaa ja raportoi sosiaalisen manipuloinnin yrityksen vastaanottaessaan puhelun väitetysti it-tuesta, jossa kysellään salasanaa.

Crossler ym. (2013) esittävät, että tietoturvakäyttäytymistä tarkasteltaessa pitää huomioida myös toiminnan tahallisuus ja tahattomuus. Tahaton, käyttäjän vahingossa tekemä tietoturvarike voi olla pahimmillaan yhtä haitallinen kuin tahallinen tietoturvarike. Tahattomia tietoturvarikkeitä voivat olla esimerkiksi

tietoturvan tietämyksen puutteesta johtuva tietojen tai salasanan luovuttaminen henkilölle, joka ei todellisuudessa ole oikeutettu tietoihin. Lisäksi käyttäjät voivat esimerkiksi tahattomasti klikata linkkejä, jotka asentavat käyttäjän työasemalle haittaohjelman. Työaseman lukitseminen sen luota poistuttaessa on tehokas tapa estää työaseman luvaton käyttö. Työaseman lukitsemista kuitenkin saatetaan laiminlyödä tietoisesti tai lukitseminen saatetaan yksinkertaisesti unohtaa. Lisäksi on mahdollista, että osa käyttäjistä ei välttämättä tiedä mitä työaseman lukitseminen tarkoittaa. Työaseman lukitseminen tai lukitsematta jättäminen voi siis olla tahatonta tai tahallista ja se sijoittuu Stanton ym. luokittelussa kategorioihin yleinen huolellisuus sekä naiivit vahingot.

2.3 Tietoturvaviestinnällä vaikuttaminen

Organisaation sisällä tapahtuvien tietoturvarikkeiden suuren määrän vuoksi tarvitaan tehokkaita tapoja vähentää epäturvallista käyttäytymistä. D 'arcy, Hovav ja Galletta (2009) toteavat kolmen asian vähentävän tietoturvarikkeiden määrää organisaatiossa: käyttäjän tietoisuus tietoturvapolitiikasta; tietoturvakoulutus, -harjoitus ja tietoisuusohjelmat (engl. Security education, training, and awareness programs, SETA); sekä tekninen valvonta. Vance ym. (2012) painottavat olevan tärkeää, että työntekijä osaa tunnistaa tietoturvauhkia ja uhkista koituvia riskejä organisaatiolle. Työntekijöille tulee kertoa organisaation altistuvan tietoturvauhkille, mikäli tietoturvaa ei oteta tosissaan ja sitä ei huomioida kaikessa toiminnassa. Lisäksi työntekijän on ymmärrettävä, että tietoturvapolitiikan noudattaminen on osa työntekijän vastuuta. Organisaatioiden täytyy myös varmistaa, että tietoturvakäytänteet ja prosessit eivät ole liian vaikeita toteuttaa. (Vance ym., 2012.) Tietoturvatoimien ei pidä siis olla rasitteena käyttäjille. Päivän aikana tehtävien tietoturvatoimien määrän ja niiden vaatiman vaivannäön pitää pysyä maltillisena, jotta tietoturvatoimien tekeminen ei kuluta käyttäjän energiaa turhaan. Myös tunnolliset, tavallisesti tietoturvallisia toimintatapoja noudattavat käyttäjät voivat alkaa toimimaan epäturvallisella tavalla, jos tietoturvatoimien määrä ja niiden vaatima vaivannäkö kasvaa liian suureksi. (Beautement, Sasse, & Wonham, 2009.)

Tietoturvatoimien aiheuttamaa kognitiivista kuormaa voidaan vähentää suunnittelemalla tietojärjestelmiä niin, että toimet tuntuvat käyttäjistä helpoilta. Mielikuvaan helppoudesta voidaan vaikuttaa myös viestinnällä. Helppoutta korostavaa lähestymistapaa käytetään paljon esimerkiksi mainonnassa: mainoksissa usein korostetaan kuinka helppoa ja vaivatonta tuotteen käyttö on. (Pfleeger, Sasse, & Furnham, 2014.)

Tietoturvakäyttäytymiseen vaikuttamisen ja tietoturvatietoisuuden lisäämisen keinoja voivat olla muun muassa esitykset, tietoturvakurssit, demotilaisuudet, videojulkaisut, tiedottaminen ja tiedotevihkoset. Keskeistä on kuitenkin saada organisaation tavoitteiden mukainen tietoturvaviesti perille tehokkaasti. Tehokas tietoturvaviestintä vaatii vaikuttamisen keinon valinnan kohderyhmän mukaan. Tietoturvaviestintä ei lisäksi ole kertaluonteista, vaan suunnitelmallista

ja jatkuvaa. Tietoturvaviestinnän pitää myös mukautua organisaation tavoitteisiin, huomioida muuttuvat tietoturvatarpeet ja sen täytyy olla perustellusti tarpeellista. (O'Leary, 2014.) Tietoturvaviestin täytyy herättää lukijan mielenkiinto, lukijan pitää ymmärtää viestin sisältö, viestin asian pitää tuntua tärkeältä ja asian pitää olla helposti muistettavissa (Bada & Sasse, 2014). Käyttäjien tietoturvakäyttäytymisen parantaminen vaatii inhimillisten käyttäytymistä ohjaavien tekijöiden ymmärtämistä. Erityisesti tärkeää olisi tunnistaa tekijät, jotka vaikuttavat tietoturvakäyttäytymiseen käytännössä (Pfleeger ym., 2014).

2.4 Yhteenveto tietoturvasta organisaatiossa

Tietoturvaa voidaan pitää kriittisen tärkeänä organisaatiolle, koska niiden toiminta on usein riippuvaista tietojärjestelmistä ja tietojärjestelmissä sijaitsevasta tiedosta. Tietoturvaa voidaan parantaa ja hallita monen tekijän avulla. Tärkeimpänä hallinnan välineenä on pidetty tietoturvapolitiikkaa. Tietoturvapolitiikka määrittää miksi organisaatio tarvitsee tietoturvaa, miten tietoturva tukee organisaation toimintaa ja se määrittää myös yleiset tietoturvaperiaatteet, joilla pyritään ohjaamaan käyttäjien tietoturvakäyttäytymistä. Organisaation tietoturvapolitiikan mukaisesti toimiminen on kuitenkin kiinni myös yksilön omasta halusta ja osaamisesta. Tietoturvakäyttäytymiseen voidaan pyrkiä vaikuttaa muun muassa lisäämällä käyttäjien tietoisuutta ja osaamista kouluttamalla, tiedottamalla ja ohjeistuksella. Tässä tutkielmassa tarkastellaan lähemmin pelkoon vetoavaa tietoturvaviestintää sekä positiivisessa tai negatiivisessa viestikehyksessä esitettyä tietoturvaviestintää, joilla pyritään vaikuttamaan positiivisesti työasemien lukitsemiseen.

3 PELKOON VETOAVA VIESTINTÄ

Pelkoon vetoaminen on yleisesti erilaisissa asiayhteyksissä käytetty ja paljon tutkittu vaikuttamisen keino. Pelkoon vetoavaa viestintää hyödynnetään usein erityisesti terveyden ja turvallisuuden kontekstissa, kuten esimerkiksi erilaisissa valistuskampanjoissa. Sen vaikutuksen tutkimisella on pitkät perinteet käyttäytymispsykologian, viestinnän ja terveystieteiden tieteenaloilla (Floyd, Prentice-Dunn & Rogers, 2000; Ruiter, Kessels, Peters & Kok, 2014). Parin viimeisen vuosikymmenen aikana pelkoon vetoava viestintä on saanut huomiota myös tietojärjestelmätieteen tutkimuksessa (Boss, Galletta, Lowry, Moody, & Polak, 2015; Sommestad, Karlzén, & Hallberg, 2015).

Tässä luvussa käsitellään ensin pelkoon vetoavaa viestintää yleisesti. Sen jälkeen esitellään yksi eniten huomiota saanut teoria, suojelumotivaatioteoria, joka pyrkii selittämään pelkoon vetoavan viestinnän vaikutusmekanismeja. Luvun lopuksi käsitellään suojelumotivaatioteorian soveltamista tietoturvatutkimuksessa.

3.1 Pelkoon vetoaminen

Pelkoon vetoamisella viitataan tekniikkaa, jonka tavoitteena on motivoida ihmisiä toimimaan halutulla tavalla herättämällä heissä pelkoa. Pelkoon vetoamisen tarkka määritelmä vaihtelee hieman kontekstista ja määrittelijästä riippuen (Stiff & Mongeau, 2003). Tavallisesti sen määritellään tarkoittavan viestintää, jonka tarkoituksena on vaikuttaa ihmisten käyttäytymiseen esittämällä lukijaa henkilökohtaisesti koskeva uhka sekä toimintaohje uhkan välttämiseksi (Witte, 1992).

Pelkoon vetoamisen voidaan Stiffin ja Mongeaun (2003) mukaan nähdä erikoistapauksena tunteisiin (engl. emotion) vetoamisesta. Tunteen, kuten pelon, voidaan katsoa koostuvan useasta eri komponentista. Tunteeseen liittyy kognitiivinen komponentti, joka kuvaa henkilön tulkintaa muutoksista ympäristössään. Tulkintoihin liittyvää arvioita siitä, ovatko muutokset hyviä vai huonoja kutsutaan affektiksi (engl. affect). Tunteeseen liittyy usein myös fysiologinen reaktio, kuten esimerkiksi sykkeen nouseminen tai pupillien laajentuminen. Ihmisten käyttäytymiseen vaikuttamisen kannalta tärkein komponentti on tunteeseen liittyvä käyttäytymisreaktio. Esimerkkinä Stiff & Mongeau kuvailevat tilanteen, jossa retkeilijä kohtaa metsässä karhun. Usein karhun kohtaaminen tulkitaan tilanteeksi, joka uhkaa henkilön elämää. Tulkintaan liittyy negatiivinen affekti ja se saa henkilössä aikaan fysiologisen taistele tai pakene -reaktion. Tilanteen aiheuttama pelon tunne saa retkeilijän pakenemaan. (Stiff & Mongeau, 2003.)

Muita tutkimuksessa tunnistettuja diskreettejä tunteita ovat esimerkiksi rakkaus, viha, syyllisyys, kateus ja ilo (Fehr & Russell, 1984). Näistä muun muassa syyllisyyden on havaittu joissain tietyissä konteksteissa voivan olla tehokas motivoija (Hibbert, Smith, Davies & Ireland, 2007).

Tunteisiin, kuten pelkoon, vetoamisen käyttäminen ihmisiin vaikuttamiseksi ei ole missään tapauksessa uusi asia. Jo Aristoteles esitti yhä erittäin arvostetussa teoksessaan ”Retoriikka” tunteisiin vetoamisen tekijänä, joka yhdessä loogisten argumenttien sekä puhujan luonteen kanssa saavat aikaan puheen vakuuttavuuden.

Pelkoon vetoamisen vaikutusmekanismien tutkimuksen katsotaan saaneen alkunsa 1950-luvulla. Hovlandin, Janisin ja Kelleyn (1953) esittämän mallin mukaan pelko on epämiellyttävä mielentila, josta ihminen haluaa päästä eroon. Pelkoa herättävän viestinnän seurauksena syntynyt pelko siis motivoi ihmistä toimimaan viestissä ehdotetulla tavalla pelon lieventämiseksi. Mikäli ehdotettu käyttäytyminen onnistuu vähentämään pelon tunnetta, käyttäytymismalli vahvistuu ja on todennäköisempää, että henkilö käyttäytyy samoin myös tulevaisuudessa. Jos taas ehdotettu käyttäytyminen ei vähennä pelkoa, henkilö saattaa pelkoa lieventääkseen siirtyä vaihtoehtoisiin keinoihin, kuten asian välttelyyn tai uhkan olemassaolon kieltämiseen. (Hovland ym., 1953)

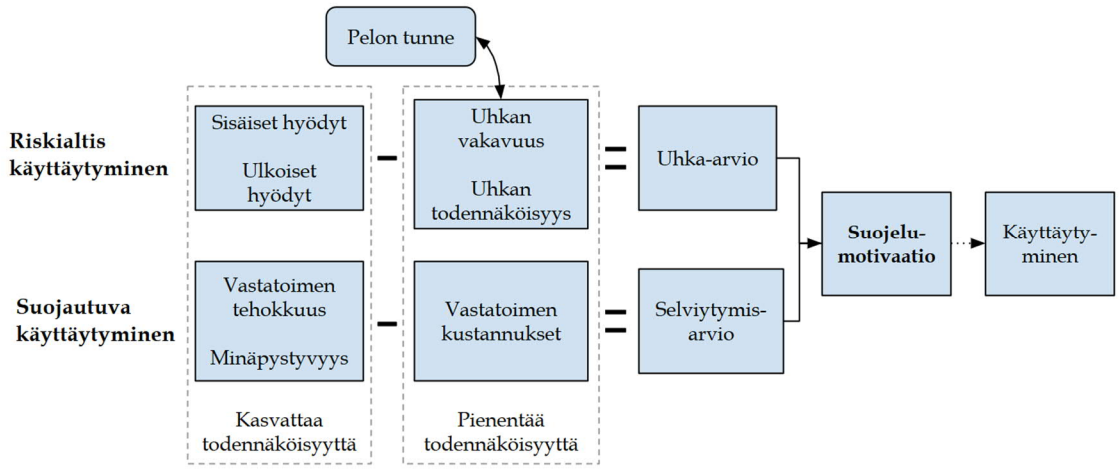
Janis (1967) laajensi Hovlandin ym. (1953) mallia pelosta epämiellyttävänä ja toimintaan motivoivana mielentilana. Hän arveli, että pelon tunteen lisääntyessä henkilö saattaisi alkaa suhtautua pelkoa herättävän viestin suosituksiin kriittisemmin. Tämän vuoksi Janis postuloi, että pelkotilan voimakkuuden ja viestin suositusten hyväksymisen välinen riippuvuus olisi käänteisen U-kirjaimen muotoinen funktio. Pelon tunteen kasvaminen lisäisi siis suositeltua käyttäytymistä tiettyyn optimaaliseen raja-arvoon asti, jonka jälkeen kriittisen suhtautumisen vaikutus alkaisi voimistua vähentäen viestin suositusten noudattamista (Janis, 1967). Kokeellista näyttöä Janisin postuloimalle käänteiselle U:lle ei myöhemmissä tutkimuksissa kuitenkaan ole löytynyt (Rogers, 1983).

Leventhal (1970) esitti omaan tutkimukseensa perustuen mallin, jonka mukaan pelkoon vetoaminen voisi aiheuttaa ihmisessä kaksi erillistä yhtäaikaista prosessia: pelkotilan lieventämiseen tähtäävän prosessin (engl. fear control) ja/tai vaaran välttämiseen tähtäävän prosessin (engl. danger control). Leventhalin mallissa käyttäytymisen muutos tapahtuu pääasiallisesti vaaran välttämiseen tähtäävän prosessin seurauksena, eikä siten pelkotilan syntyminen tai pyrkimys pelkotilan lieventämiseen ole edellytys muutokselle. Leventhalin mukaan näin kahden prosessin välillä voi kuitenkin olla vuorovaikutuksia.

Janisin (1967) ja Leventhalin (1970) esittämiin teorioihin sekä niistä kertyneeseen tutkimusnäyttöön pohjautuen Rogers (1975; 1983) muodosti 1970-luvulla suojelumotivaatioteoriaksi nimeämänsä teorian. (engl. Protection Motivation Theory, PMT). Se on pelkoon vetoamisen tutkimuksessa sovelletuista teorioista laajimmin käytetty teoria (Ruiter, Kessels, Peters & Kok, 2014). Suojelumotivaatioteoriaa on sovellettu lukuisissa eri konteksteissa, kuten esimerkiksi syövän ja AIDSin ehkäisyssä, terveellisiin elintapoihin kannustamisessa, tupakointiin ja alkoholin kulutukseen liittyen, uhanalaisten eläinlajien suojelussa ja hyönteismyrkkyjen turvalliseen käyttöön kannustamisessa (Floyd ym., 2000).

3.2 Suojelumotivaatioteoria

Suojelumotivaatioteorian (Rogers, 1983) mukaan pelkoon vetoava viesti tai muusta lähteestä saatu informaatio käynnistää yksilössä kaksi toisistaan riippumatonta rinnakkaista kognitiivista prosessia (engl. cognitive mediating processes): uhka-arvion (engl. threat appraisal) ja selviytymisarvion (engl. coping appraisal). Niiden välityksellä tieto uhkasta aikaansaa suojelumotivaation (engl. protection motivation), jonka voidaan mieltää tarkoittavan aikomusta toimia uhkalta suojautumiseksi. Suojelumotivaation siis ajatellaan ohjaavan ja ylläpitävän yksilön käyttäytymistä, joka voi olla yksittäinen toimi tai useita toimia. Toimet voidaan suorittaa kerran tai toistuvasti useita kertoja. Lisäksi toimi voi olla tyypiltään johonkin ryhtyminen tai ryhtymättä jättäminen. Kuviossa 1 on esitettynä suojelumotivaatioteoria kaavion muodossa.



KUVIO 1 Suojelumotivaatioteoria (mukaillen Rogers, 1983)

Kognitiiviset prosessit aloittavan informaation lähde voi olla joko henkilön ympäristöstä tuleva tai henkilön sisäinen. Ulkoisina informaation lähteinä voi olla pelkoon vetoavan viestinnän lisäksi esimerkiksi toisia havainnoimalla opittu tieto. Henkilön sisäisenä informaation lähteenä voi toimia esimerkiksi persoonallisuuteen liittyvät tekijät tai aiempi kokemus vastaavista uhkista.

Ensimmäinen kognitiivisista prosesseista, uhka-arvioprosessi, arvioi riskialttiin käyttäytymisen, kuten esimerkiksi tupakoinnin, jatkamista tai sen aloittamista. Prosessissa uhkan, kuten keuhkosyövän, vakavuutta (engl. threat severity) ja todennäköisyyttä uhkan toteutumiselle (engl. vulnerability) verrataan kyseiseen käyttäytymiseen liittyviin sisäisiin ja ulkoisiin hyötyihin (engl. internal and external rewards). Mikäli uhkan todennäköisyyden ja vakavuuden merkityksen arvioidaan ylittävän käyttäytymisestä saadut hyödyt, katsotaan sen pienentävän riskialttiin käyttäytymisen todennäköisyyttä. Mikäli käyttäytymisestä saadut hyödyt taas arvioidaan tärkeämmiksi, kasvaa todennäköisyys riskialttiiseen

käyttäytymiseen. Eräs esimerkki sisäisestä hyödystä voisi olla riskialttiin käyttäytymisen tuottama nautinto. Ulkoinen hyöty taas voisi olla esimerkiksi riskialttiin käyttäytymisen tuoma sosiaalinen hyväksyntä. Kuten Leventhalin (1970) mallissa, Rogersinkaan suojelumotivaatioteoriassa pelon tunteen syntyminen ei ole välttämätöntä käyttäytymisen muuttumisen kannalta, vaan pelko toimii uhka-arvion osana lisäten motivaatiota omaksua riskiltä suojautumiseen pyrkivä käyttäytyminen.

Toisessa kognitiivisista prosesseista, selviytymisarvio-prosessissa, arvioidaan uhkalta suojautumaan tähtäävän käyttäytymisen omaksumista. Siinä vaihtoehtoisen, uhkalta suojautuvan käyttäytymisen eli vastatoimen (engl. adaptive response) kustannuksia (engl. response costs) verrataan vastatoimen tehokkuuteen (engl. response efficacy) uhkalta suojautumisessa sekä käyttäjän minäpystyvyyteen (engl. self-efficacy) näiden toimen suorittamiseksi. Vastatoimen tehokkuudella tarkoitetaan henkilön arviota siitä, kuinka tehokkaasti vastatoimi auttaa suojautumaan uhkalta. Minäpystyvyys viittaa henkilön käsitykseen siitä, pystyykö henkilö omaksumaan uhkalta suojautumaan pyrkivän käyttäytymisen. Vastatoimen kustannuksia ovat esimerkiksi käyttäytymisen suorittamisen vaikeus tai sen henkilön muuta elämää häiritsevä vaikutus.

Rogersin (1983) mukaan kummankin kognitiivisen prosessin sisällä esiintyvillä tekijöillä ei ole keskenään korkeamman asteen vuorovaikutuksia. Eri prosessien välillä tekijöillä taas voi olla toisen asteen keskinäisiä vuorovaikutuksia suojelumotivaatioon. Tämä havaitaan erityisesti tilanteessa, jossa vastatoimen tehokkuus tai minäpystyvyys arvioidaan matalaksi. Tällöin lisäyksellä uhkan vakavuuden tai todennäköisyyden arviossa ei ole joko lainkaan vaikutusta tai se vahvistaa aikomusta jatkaa riskialtista käyttäytymistä. Rogers selittää ilmiötä psykologisen kontrollin tunteen käsitteellä (engl. perceived control): helpottaakseen tilanteen aiheuttamaa avuttomuuden tunnetta henkilö päättää tietoisesti sitoutua riskialttiiseen käyttäytymiseen. Tällöin henkilö voi kokea uhkalle altistavan käyttäytymisen olevan hänen oma valintansa.

Suojelumotivaatioteorian konstrukteista minäpystyvyyden on todettu olevan selvästi voimakkain suojelumotivaatiota määrittävä tekijä (Floyd ym., 2000). Vastatoimen tehokkuuden, uhkan vakavuuden ja todennäköisyyden sekä vastatoimeen liittyvien kustannusten on sen sijaan todettu olevan merkitykseltään keskenään lähes saman suuruisia ja minäpystyvyyden vaikutusta vähäisempiä.

Rogersin suojelumotivaatioteorian mukaan siis tieto uhkasta synnyttää kahden rinnakkaisen kognitiivisen prosessin välityksellä suojelumotivaation, joka ohjaa ja ylläpitää yksilön toimia uhkalta suojautumiseksi. Suojelumotivaatioteoria on kehitetty terveys- ja turvallisuusuhkien kontekstissa, jossa uhkat kohdistuvat yksilön omaan jatkuvuuteen tai hyvinvointiin ja ovat siten universaalisti henkilökohtaisesti relevantteja. Teoriaa on kuitenkin sovellettu laajasti myös muilla tieteenaloilla ja konteksteissa, joihin liittyvien uhkien kokeminen henkilökohtaisesti relevantiksi on hyvin subjektiivista ja vaihtelevaa. Eräs näistä tieteenaloista on tietoturvakäyttäytymisen tutkimus.

3.3 Suojelumotivaatioteoria tietoturvatutkimuksessa

Suojelumotivaatioteoria on saanut tietojärjestelmätieteessä paljon huomiota viimeisen parin vuosikymmenen aikana, erityisesti tietoturvaan liittyvän käyttäytymisen tutkimuksessa. Aiemmasta tutkimuksesta on esitetty useita kattavia koosteita eri julkaisuissa.

Sommestad ym. (2015) tunnistivat meta-analyysissään aiemmasta kirjallisuudesta 43 tutkimusta, joissa tutkittiin vähintään yhden suojelumotivaatioteorian konstruktin vaikutusta käyttäytymisen aikeeseen. Näistä 28 artikkelissa raportoitiin tulokset riittävällä tarkkuudella meta-analyysiä varten. Analysoitavaksi valitut artikkelit oli julkaistu vuosien 2005 ja 2013 välillä. Sommestad ym. (2015) havaitsivat, että suojelumotivaatioteoria selittää käyttäytymistä paremmin uhkan ja vastatoimen ollessa konkreettisia tai spesifisiä sekä uhkan ollessa henkilökohtaisesti relevantti eikä pelkästään organisaatioon tai muihin ihmisiin kohdistuva. He myös huomauttivat, että arvioiduista tutkimuksista vain kolme oli interventiotutkimuksia, ja peräänkuuluttivat tarvetta tehdä lisää tutkimuksia, joissa tietoturvakäyttäytymiseen yritetään vaikuttaa suojelumotivaatioteoriapohjaisella interventiolla. Interventiotutkimusten avulla on mahdollista saada tietoa siitä, miten tietoturvakäyttäytymisen parantamiseen tähtäävä pelkoon vetoava viestintä tulisi muotoilla, jotta se olisi mahdollisimman tehokasta.

Bossin ym. (2015) tutkimuksen kirjallisuuskatsaus käsitti 26 artikkelia, jotka sovelsivat ainakin osittain suojelumotivaatioteoriaa. Artikkelit olivat vuosilta 2009 – 2014. Bossin mukaan aiempi tutkimus koostuu pääosin tutkimuksista, joissa käytetyt tutkimusmallit on muodostettu lisäämällä tai korvaamalla suojelumotivaatioteorian konstrukteja muista käyttäytymisen teorioista lainatuilla konstrukteilla. He pitävät tätä huonona asiana, sillä näin toimittaessa ei voida selkeästi osoittaa, parantavatko tehdyt muutokset tai lisäykset alkuperäisen suojelumotivaatioteorian selitysvoimaa tietoturvaan liittyvän käyttäytymisen kontekstissa. Boss ym. toteavat, että tarvittaisiin enemmän tutkimusta, jossa pelkoon vetoavan viestinnän tehokkuutta testattaisiin manipuloimalla vähintään uhkan vakavuutta sekä uhkan todennäköisyyttä. Näin saataisiin tietoa siitä, onko pelkoon vetoaminen toimiva vaikuttamisen tapa tietoturvan kontekstissa.

Menard, Bott ja Crossler (2017) artikkelin kirjallisuuskatsaus huomioi 22 tutkimusartikkelia, jotka oli julkaistu vuosina 2008 - 2015. He toteavat saatujen tulosten olevan epäyhteneviä ja keskenään ristiriitaisia. Menard ym. muistuttavat, että suojelumotivaatioteoria on alun perin kehitetty terveysuhkien kontekstissa, jossa uhkat ovat oleellisesti henkilökohtaisia. Tietoturvan kontekstissa uhkat taas kohdistuvat yleensä organisaation resursseihin, jolloin uhkilla ei ole välitöntä henkilökohtaista relevanssia. Tämä esitetään potentiaalisena selityksenä saatujen tulosten ristiriitaisuuteen.

Menardin ym. (2017) ja Sommestadin ym. (2015) näkemyksen tietoturvauhkan henkilökohtaisen relevanssin puutteesta jakavat myös esimerkiksi Johnston, Warkentin ja Siponen (2015). He esittävät saman ongelman koskevan kaikkia tie-

toturvauhkia kontekstista riippumatta, sillä tietoresurssien (engl. information assets) käsittäminen henkilökohtaisesti relevanteiksi on hyvin subjektiivista ja vaihtelevaa. Sen sijaan esimerkiksi tupakoinnin aiheuttama keuhkosyöpä on uhka henkilön omalle olemassaololle ja siten universaalisti henkilökohtaisesti relevantti. Johnstonin ym. mukaan suojelumotivaatioteoria ei huomioi eroja uhkan luonteessa vaan se olettaa kaikkien uhkien olevan henkilölle relevantteja.

Johnston ym. (2015) pyrkivät huomioimaan tietoturvakontekstin erikoispiirteet tutkimuksessaan, jossa testattiin kolmen eri pelkoon vetoavan viestin vaikutusta aikomukseen noudattaa viestin suosituksia erään suomalaisen kaupungin hallinnossa. Viestit koskivat hyvän salasanan käytön tärkeyttä, USB-muistitikkujen salaamista tietovarkauden estämiseksi sekä työasemalta uloskirjautumista tai työaseman lukitsemista aina sen luota poistuttaessa. Jokaiseen viestiin oli lisätty myös maininta siitä, että viestin suositusten noudattamatta jättämiseen liittyy formaaleja ja epäformaaleja sanktioita. Tutkimus toteutettiin lähettämällä organisaation työntekijöille sähköpostitse kutsu osallistua webpohjaiseen tutkimukseen, jossa osallistujille näytettiin satunnaisesti jokin kolmesta viestistä ja pyydettiin sen jälkeen vastaamaan nimettömästi kyselyyn. Osa osallistujista toimi kontrolliryhmänä ja vastasi vain kyselyyn. Kerätyn aineiston perusteella havaittiin, että rangaistusten vakavuuden ja todennäköisyyden ottaminen mukaan tutkimusmalliin lisäsi sen kykyä selittää käyttäytymisen aietta verrattuna pelkkiä taustamuuttujia ja suojelumotivaatioteorian konstrukteja käyttäneeseen malliin. Tuloksen katsottiin tukevan sitä, että tietoturvalliseen käyttäytymiseen kannustavan viestin kuvailemalla uhkalla tulisi olla myös henkilökohtainen ulottuvuus.

Suojelumotivaatioteorian tietojärjestelmätieteessä saamasta huomiosta huolimatta aihetta ei voida pitää läheskään loppuun käsiteltynä. Eri tutkimuksissa saadut tulokset eivät ole olleet keskenään yhteneväisiä, minkä on arveltu johtuvan siitä, että tietoturvauhkat varsinkaan organisaation kontekstissa eivät kohdistu suoraan yksilöön itseensä. Näin ollen ne eivät välttämättä täytä suojelumotivaatioteoriaan sisältyvää implisiittistä oletusta siitä, että uhka on henkilökohtaisesti relevantti. Tutkimuksessa käytettyjen tutkimusasetelmien osalta puutteena on nähty se, ettei interventiotutkimuksia tai suojelumotivaatioteorian konstrukteja, kuten uhkan vakavuutta, manipuloimaan pyrkiviä tutkimuksia ole juuri tehty.

3.4 Pelkoon vetoavan viestinnän yhteenveto

Pelkoon vetoaminen on paljon käytetty ja tutkittu vaikuttamisen keino. Nimensä mukaisesti sen tarkoituksena on ohjata käyttäytymistä haluttuun suuntaan esittämällä henkilölle pelkoa herättävä uhka ja toimintamalli uhkan välttämiseksi. Pelkoon vetoamisen vaikutusta selittämään kehitetyistä teorioista suojelumotivaatioteoria on vakiinnuttanut asemansa usealla eri tieteenalalla, kuten myös tietoturvatutkimuksessa.

Suojelumotivaatioteorian mukaan tieto uhkasta synnyttää kaksi toisistaan riippumatonta kognitiivista prosessia, jotka arvioivat uhkaa ja selviytymiskeinoja uhkan välttämiseksi. Uhka, joka koetaan vakavaksi ja todennäköiseksi ja jolta suojautumiseksi on olemassa tehokas vastakeino, aikaansaa vastakeinon toteuttamaan pystyvässä henkilössä suojelumotivaation. Suojelumotivaatio ohjaa ja ylläpitää henkilön käyttäytymistä uhkalta suojautumiseksi.

Tietojärjestelmätieteessä suojelumotivaatioteorian tutkimus ei ole kyennyt tuottamaan yhtenäistä kuvaa siitä, mitkä tekijät saavat yksilön suojautumaan tietoturvauhkilta. On esitetty, että suojelumotivaatioteorian tutkimusta tietoturvauhkien kontekstissa tulisi laajentaa kokeilla, joissa suojelumotivaatioteorian konstrukteja manipuloimalla pyritään selvittämään niiden vaikutusta henkilön käyttäytymiseen ja näin löytää tehokas tapa vaikuttaa käyttäytymiseen. Myös tietoturvauhkien henkilökohtaisen relevanssin subjektiivisuus on esitetty asiana, joka tulisi ottaa huomioon, kun tietoturvakäyttäytymiseen pyritään vaikuttamaan.

4 VIITEKEHYSVAIKUTUS VIESTINNÄSSÄ

Tässä luvussa käsitellään viitekehysvaikutuksen (engl. framing effect) käyttöä viestinnässä. Viitekehysvaikutuksen määritelmänä käytetään Tverskyn ja Kahnemanin (1981) näkemystä prospektiteorian pohjalta ja Levinin, Schneiderin ja Gaethin (1998) kategorisointia eri viitekehysluokista. Määritelmää ja kategorisointia tarkastellaan tarkemmin omassa alaluvussaan. Luvun alku käsittelee määritelmän muodostumista ja luvun lopussa tarkastellaan aiempaa tutkimusta yleisesti ja tietoturvaviestinnän kontekstissa.

4.1 Prospektiteoria ja päätöskehys

Viitekehysvaikutus perustuu Kahnemanin ja Tverskyn (1979) luomaan Nobelpalkittuun prospektiteoriaan. Prospektiteoria pyrkii selittämään henkilön valinnan muodostumista epävarmoissa tilanteissa. Prospektiteorian juuret ovat odotetun hyödyn teoriassa (engl. expected utility theory), joka on normatiivinen malli ja postuloi henkilön aina valitsevan maksimaalisen hyödyn tuottavan vaihtoehdon. Kahneman ja Tversky (1979) kuitenkin havaitsivat, että joissain tapauksissa henkilö toimii vastoin maksimaalisen hyödyn tavoittelua ja ylipainottavat lopputuloksia, jotka ovat varmoja muiden epävarmojen lopputulosten joukosta. Lisäksi tutkimuksessa havaittiin ihmisten olevan alttiimpia ottamaan riskejä, jos varmoja vaihtoehtoja ei ole.

Ihmiset käsittävät teorian mukaan lopputulokset (engl. outcomes) joko saavutuksina tai saatuina etuina (engl. gains), tai vaihtoehtoisesti menetyksinä (engl. losses). Kahneman ja Tversky (1979) esittävät, että prospektiteorian mahdollisuudet (engl. prospect) ovat lähtökohtaisesti arvomuutoksia varallisuudessa tai hyvinvoinnissa, ei niinkään lopullinen olotila. Aistien kaltaisesti käsitys hakee jonkin referenssipisteen, kuten lämpötilan, tarkkailee sen muutosta ja päättely lämpötilasta on suhteessa referenssitilaan. Esimerkkinä sama absoluuttinen varallisuus voi tarkoittaa toiselle köyhyyttä ja toiselle suurta rikkautta, riippuen yksilön nykyisestä varallisuudesta. Todellista arvoa arvioidaan siis kahden argumentin kautta: Lähtökohta toimii referenssipisteenä ja muutoksen suuruus, joko positiivinen tai negatiivinen, arvioidaan referenssipisteestä. Keskeinen seikka asenteista muutokseen varallisuuden tapauksessa on se, että häviöt koetaan voimakkaammin kuin saavutukset. Esimerkiksi rahan menetyksestä aiheutuva tunne on voimakkaampi kuin saman summan saamisesta aiheutuva tunne.

Toisessa tutkimuksessaan Tversky ja Kahneman (1981) pyrkivät prospektiteorian avulla esittämään ongelmia, jotka rikkovat käsitystä siitä, että rationaalinen ajattelu pyrkii jatkuvasti konsistenssiin ja koherenssiin ajattelussa. Tutkijat viittaavat päätöskehykseen (engl. decision frame), jolla tarkoitetaan päätöksentekijän mielikuvaa toimista, tuloksista ja oheisvaikutuksista liittyen tiettyyn valin-

taan. Tämä päätöskehys muodostuu ongelman asettelusta sekä normeista, tavoista ja yksilöllisistä ominaispiirteistä. Tutkimuksessa esimerkkeinä käytettiin ihmishenkiin kohdistuvaa tapahtumaa sekä rahallisiin saamisiin ja häviöihin kohdistuvaa tapahtumaa.

Tversky ja Kahneman (1981) havainnollistavat kehysvaikutusta yleisesti käytetyn esimerkin kautta. Tutkimushenkilöille esitetään tilanne, jossa 600 henkilöä sairastuu epidemian seurauksena ja tutkimushenkilöiden täytyy valita kahdesta lääkeohjelmasta. Tutkimus esitettiin kahdelle ryhmälle, joista toiselle ratkaisu esitettiin positiivisessa valossa ja toiselle negatiivisessa valossa. Taulukossa 2 on esitetty ongelman asettelu suomennettuna.

TAULUKKO 2 Aasialaisen taudin ongelma (Tversky & Kahneman, 1981)

1. ryhmä	2. ryhmä
(Ohjelma A) 200 henkilöä pelastuu.	(Ohjelma C) 400 henkilöä kuolee.
(Ohjelma B) 1/3 mahdollisuus, että 600 henkilöä pelastuu. 2/3 mahdollisuus että kukaan ei pelastu.	(Ohjelma D) 1/3 mahdollisuus, että kukaan ei kuole. 2/3 osa mahdollisuus, että kaikki kuolevat.

Valtaosa 1. ryhmän koehenkilöistä valitsi vaihtoehdon A, jossa 200 henkilöä pelastuu. 2. ryhmän koehenkilöistä valtaosa valitsi vaihtoehdon D, jossa 1/3 mahdollisuus ettei kukaan kuole ja 2/3 mahdollisuus, että kaikki kuolevat. Mielenkiintoista tutkimuksessa on se, että varman lopputuloksen vaihtoehtojen A ja C lopputulos on sama, kuten myös epävarman lopputuloksen vaihtoehtojen B ja D. Johtopäätöksenä todetaan, että jos vaihtoehdot sisältävät jonkin saavutettavan edun (engl. gains), ovat valinnat usein riskejä välttäviä. Jos valinnat sisältävät menetyksen (engl. loss) ovat valinnat usein riskejä ottavia.

Toisessa esimerkissä (taulukko 3) koeryhmälle esitettiin rahan saamiseen ja menettämiseen liittyvät vaihtoehdot. Tehtävässä piti valita molemmista ohjelmista yksi vaihtoehto.

TAULUKKO 3 Varman ja epävarman rahan saamisen ongelma (Tversky & Kahneman, 1981)

Ohjelma 1	Ohjelma 2
(Vaihtoehto A) saat varmasti 240$	(Vaihtoehto C) menetät varmasti 750$
(Vaihtoehto B) saat 25% varmuudella 1000$ tai 75% varmuudella et mitään.	(Vaihtoehto D) 75% varmuudella menetät 1000$ ja 25% et menetä mitään

Koehenkilöistä 73% valitsi yhdistelmän A & D. Vähiten suosittu vaihtoehto oli B & C. Kuitenkin vaihtoehtoyhdistelmistä B & C olisi ollut tilastollisesti tehokkain. Huomioiden tämän, tutkijat esittivät ongelman seuraavaksi vaihtoehtopareina:

(1) A & D. 25% mahdollisuus voittaa 240$ ja 75% mahdollisuus hävitä 760$
(2) B & C. 25% mahdollisuus voittaa 250$ ja 75% mahdollisuus hävitä 750$

Näistä koehenkilöt valitsivat kaikki vaihtoehdon 2. Tämä tuo ilmi kahden vaihtoehdon ajattelemisen yksittäisinä valintoina eikä yhtenäisenä vaihtoehtojen konjunktiona.

Päätöksen kehystämistä voidaan myös tarkastella henkilön ajatusmallina. Kuvitellaan henkilö, joka on hävinnyt raviradalla 140$ ja suunnittelee 10$ vetoa 1:15 voittosuhteella olevalle hevoselle. Tämä voidaan kehystää kahdella eri tavalla. Vedon voidaan ajatella olevan yksittäinen tapahtuma ja arvioida todennäköisyyttä sen perusteella: Vedon lopputulos voi olla 1:15 todennäköisyydellä 140$ voitto tai 14:15 todennäköisyydellä 10$ häviö. Tämänkaltainen veto on yksittäisenä tapahtumana ajateltuna todella riskialtis suuren häviämistodennäköisyyden vuoksi ja vedonlyöjä tuskin tekisi tämänkaltaista vetoa yksittäisenä vetona. Luonnollinen ja yleinen tapa ajatella asiaa kuitenkin on, että 140$ on jo hävitty ja voitolla voidaan saada takaisin nollatulos voittamalla 140$. Häviö koetaan pienempänä, kun referenssipisteenä on jo hävitty 140$ ja häviö voi kasvaa 150 dollariin. Tätä analyysiä tukee Tversky & Kahneman (1981) mukaan myös McGlothlin (1956) tutkimus, jossa todetaan epätodennäköisten vetojen olevan suosituimpia viimeisellä lähdöllä. Riski koetaan siedettäväksi, kun ajatellaan vedonlyöntiä koko päivän tulosten perusteella eikä yksittäisenä tapahtumana.

Esimerkeillä Tversky ja Kahneman (1981) tuovat esille henkilön päätöskehyksen toimivan epärationaalisesti henkilön itse sitä välttämättä huomaamatta. Lisäksi päätöskehys on altis valinnan vaihtumiselle kehystämällä asia toisella tavalla.

4.2 Päätöskehyksestä viitekehysvaikutuksen kategorisointiin

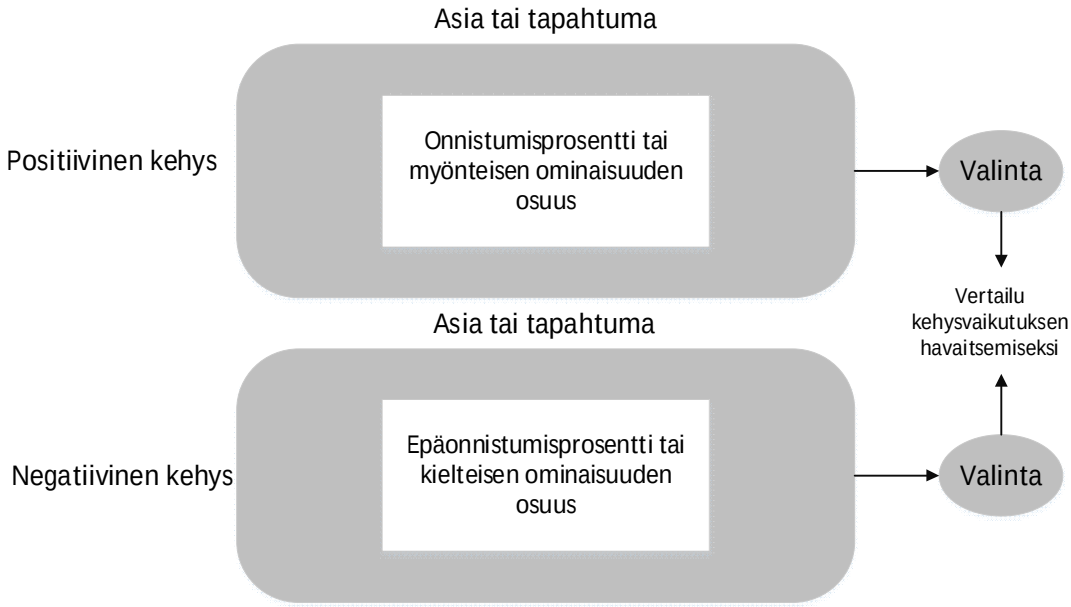
Päätöskehystä ja viitekehysvaikutusta on tutkittu laajasti eri aloilla, mutta tutkimustulokset eivät ole tuottaneet selvää käsitystä siitä, mitkä kognitiiviset prosessit ovat merkityksellisiä viitekehysvaikutuksen saamiseksi (Levin ym., 1998). Levin ym. (1998) toteavat metatutkimuksessaan viitekehystutkimuksen tulosten vaihtelevan suuresti eri konteksteissa, mutta olevan yhtenäisiä tietyn tyyppisissä tapauksissa. Levin ym. (1998) jakavat viitekehysvaikutuksen kolmeen kategoriaan: valintakehys (engl. risky choice framing), ominaisuuskehys (engl. attribute framing) ja tavoitekehys (engl. goal framing).

Näistä valintakehys on sama kuin alkuperäinen prospektiteorian mukainen päätöskehys. Valintakehyksessä varioidaan riskiä ja kuvaillaan tilanne eri tavoin. Tästä esimerkkinä Levin ym. (1998) ottavat tässä tutkielmassa aiemmin esitellyn prospektiteorian mukaisen aasialaisen taudin ongelman (kuvio 2).

KUVIO 2 Valintakehys (mukaillen Levin, Schneider & Gaeth, 1998)

Levin ym. (1998) toteavat tutkimusten, jotka kategorisoituvat valintakehykseen, olevan konsistenttejä tutkimustulosten suhteen. Henkilöt ottavat todennäköisemmin riskejä, kun vaihtoehdot korostavat mahdollisuutta välttää menetyksiä kuin saada jotain.

Ominaisuuskehys tarkoittaa jonkin asian kehystämistä esittämällä ominaisuuden prosenttiosuus tai onnistumisen mahdollisuus joko positiivisessa valossa tai negatiivisessa valossa. Esimerkkinä ominaisuuden kehystämisestä voidaan käyttää Levinin ja Gaethin (1988) tutkimusta jauhelihan subjektiivisesta mausta ja rasvapitoisuudesta. Jauhelihan todettiin maistuvan paremmalta ja vähärasvaisemmalta, kun jauhelihan kuvattiin olevan 75 % lihaa, verrattuna siihen, että jauhelihan kuvattiin olevan 25 % rasvaa. Toisena esimerkkinä ominaisuuskehyksen käytöstä onnistumisen kehystämisessä voidaan käyttää sairaalassa tehtävää toimenpidettä. Jos toimenpide esitetään selviytymisprosentin mukaan ihmiset todennäköisemmin suosittelevat toimenpidettä ja kokevat toimenpiteen vaikuttavammaksi, kuin jos toimenpide esitettäisiin kuolleisuuden mukaan. (Levin, Schnittjer & Thee, 1988.) Ominaisuuskehys on esitetty kuviossa 3.



KUVIO 3 Ominaisuuskehys (mukaillen Levin, Schneider & Gaeth, 1998)

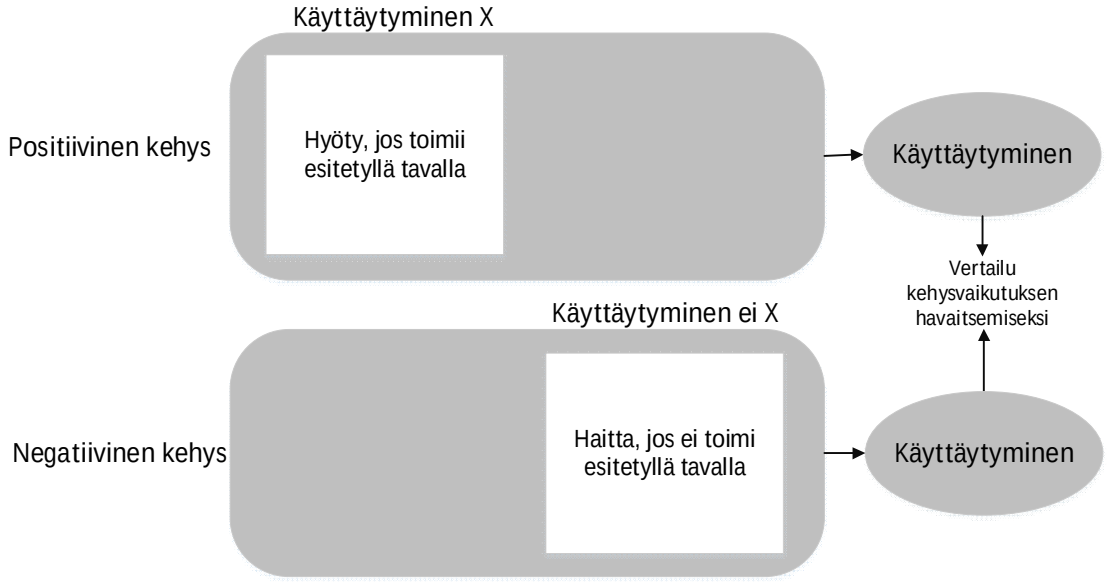
Ominaisuuskehyksessä positiivinen kehys toimii tehokkaammin kuin negatiivinen kehys. Ominaisuuskehyksen vaikutuksen esitetään johtuvan positiivisen viestin herättämistä positiivisista assosiaatioista muistissa, joka vaikuttaa asian tai tapahtuman arvioon. (Levin ym., 1998).

Tavoitekehys on viitekehysvaikutuksen teorian eniten suostuttelevassa (engl. persuasive) viestinnässä käytetty kehysmalli. Vaikuttamaan pyrkivän viestin tehon on todettu riippuvan siitä, korostaako viesti käyttäytymisen hyötyä vai käyttäytymisen laiminlyömisestä seuraavaa haittaa. Sekä positiivinen että negatiivinen kehys pyrkii siis saamaan vastaanottajan toimimaan molemmissa kehyksissä samalla halutulla tavalla kehystämällä viestin joko niin, että viestin vastaanottaja haluaa välttää haitan käyttäytymällä toivotulla tavalla tai saavuttaa jotain etua käyttäytymällä toivotulla tavalla. Tavoitekehyksen vaikutuksen esimerkkinä käytetään usein Meyerowitzin ja Chaikenin (1987) tutkimusta, jossa naisia pyrittiin motivoimaan rintojen omatarkkailuun kehystämällä viesti joko positiivisesti tai negatiivisesti. Vapaamuotoisesti suomennettuna tutkimuksessa käytetyt viestit olivat:

Positiivinen kehys: "Naiset, jotka tutkivat omatoimisesti rintojaan, havaitsevat todennäköisemmin kasvaimen aikaisessa vaiheessa, kun kasvainta voidaan vielä paremmin hoitaa."

Negatiivinen kehys: "Naiset, jotka eivät tutki omatoimisesti rintojaan, havaitsevat epätodennäköisemmin kasvaimen aikaisessa vaiheessa, kun kasvainta voidaan vielä paremmin hoitaa."

Tutkimuksessa havaittiin, että negatiivisesti kehystetty viesti toimi tehokkaammin kuin positiivisesti kehystetty viesti. Henkilöt olivat siis motivoituneempia ’välttämään haittaa’ kuin ’saamaan hyötyä’ rintojen omatarkkailulla. Tavoitekehys on esitetty kuviossa 4.



KUVIO 4 Tavoitekehys (mukaillen Levin, Schneider & Gaeth, 1998)

Tavoitekehys on muita kehyksiä alttiimpi monille kieliopillisille ja kontekstuaalisille variaatioille. Puhtaimmillaan tavoitekehys on silloin, kun voidaan käyttää positiivisen kehyksen suoraa negaatiota. Tämä tarkoittaa sitä, että esimerkiksi ”henkilö nukkuu” suora negaatio on ”henkilö ei nuku”. Asian voisi ilmaista myös sanomalla ”henkilö on hereillä”. Kieliopillisesti tavoitekehys on siis haastava; edellä mainittu esimerkki rintojen omatarkkailusta voitaisiin myös muotoilla esimerkiksi muokkaamalla negaatioksi havaitseminen (ei havaitse) tai hoitaminen (ei voida hoitaa). Kehystämisessä on huomioitava mahdollisten kieliopillisten ja kontekstuaalisten variaatioiden mahdollinen vaikutus kehyksen vaikutukseen. Lisäksi kehystämisessä on oltava tarkkana käytettävän kielen ominaispiirteiden suhteen. (Levin ym., 1998.)

Levin ym. (1998) esittää kehyksen vaikutuksen riippuvan kehyksen tyypistä (valintakehys, ominaisuuskehys, tavoitekehys), kun taas Rothman ja Salovey (1997) esittää käsityksen riskistä moderoivan kehyksen vaikutusta. Rothmanin ja Saloveyn (1997) mallia on pääasiassa sovellettu terveystieteiden tieteenalalla. Rothmanin ja Saloveyn (1997) mallissa kehyksen toimivuutta arvioidaan kahden muuttujan kautta: (1) käsitys lopputuloksen riskistä (engl. perceived outcome risk) ja (2) käsitys menettelyn riskistä (engl. perceived procedural risk). Mallissa detektiiviset, eli sairauden tunnistavat menettelyt, kategorisoitiin yleisesti ottaen riskialttiiksi (esim. rintojen omatarkkailu) ja preventiiviset, eli sairautta ennaltaehkäisevät menettelyt, kategorisoitiin turvallisiksi (esim. aurinkovoiteen käyttö). Rothman, Bartels, Wlaschin ja Salovey (2006) toteavat katsauk-

sessaan, että terveystieteiden tieteenalalla positiivisesti kehystetyn viestin voidaan todeta olevan tehokkaampi sairauden ennaltaehkäisevässä käyttäytymisessä (engl. prevent the onset of disease) ja negatiivisesti kehystetyn viestin olevan tehokkaampi sairauden tunnistamiseen tähtäävässä käyttäytymisessä (engl. detect the presence of a disease).

4.3 Viitekehysvaikutus IT-tutkimuksessa

Viitekehysvaikutusta on tutkittu vähäisesti tietojärjestelmätieteen tieteenalalla. Kaikki tässä luvussa käsitellyt tutkimukset ovat tyypiltään tavoitekehystettyjä. Andersonin ja Agarwalin (2010) tutkimuksessa koehenkilöt lukivat internetin vaaroista ja suojautumisesta kertovan internetsivun, joka oli muotoiltu tavoitekehyksen (engl. goal framing) mukaan positiivisesti tai negatiivisesti. Positiivisen kehyksen mukaan muotoiltu internetsivu korosti hyödyllisiä seurauksia tietoturvallisesta käyttäytymisestä ja negatiivinen korosti haitallisia seurauksia, jos toimitaan ohjeiden vastaisesti. Lisäksi tutkimuksessa yhtenä muuttujana oli viestin relevanssi, eli internetsivu oli muotoiltu henkilökohdennuksella (engl. independent view) tai yhteisökohdennuksella (engl. interdependent view). Taulukkoon 4 on otettu esimerkinomaisesti yksi kehystyksen eron hyvin esittävä lause ja sen variaatiot.

TAULUKKO 4 Andersonin ja Agarwalin (2010) tutkimuksen viestien kehystämisen esimerkkejä

Kehys	Suomeksi	Alkuperäinen
Henkilökohdennettu positiivinen kehys	”Nauti tunteesta, että tiedät tekeväsi oman osasi kyberavaruuden turvaamisessa - Hyödynnä edut seuraamalla näitä ehdotettuja turvallisia käytänteitä!”	“Enjoy the confidence of knowing you are doing your part to secure cyberspace – Reap the benefits by following these suggested secure online behaviors”
Henkilökohdennettu negatiivinen kehys	”Vältä henkilökohtaiset seuraukset tietoturvan laiminlyömisestä – Suojaudu seuraamalla näitä ehdotettuja turvallisia käytänteitä!”	“Avoid the personal consequences of security violations – Protect yourself by following these suggested secure online behaviors!”
Yhteisökohdennettu positiivinen kehys	”Nauti tunteesta, että tiedät kaikkien tekevän oman osansa kyberavaruuden turvaamisessa – Hyödynnä edut seuraamalla näitä ehdotettuja turvallisia käytänteitä!”	“Enjoy the confidence of knowing we are all doing our part to secure cyberspace - Reap the benefits by following these suggested secure online behaviors!”
Yhteisökohdennettu negatiivinen kehys	”Vältä tietoturvarikkeistä koituvat seuraukset internetyhteisölle – Suojaa yhteisöä seuraamalla näitä ehdotettuja turvallisia käytänteitä!”	“Avoid the consequences to the community of Internet users from security violations – Protect your community by following these suggested secure online behaviors!”

Internetsivun lukemisen jälkeen koehenkilöille esitettiin kysely. Tutkimuksen tuloksena todetaan, että positiivisesti kehystetyt viestit saattavat olla tehokkaampia vaikuttamaan tietoturvakäyttäytymiseen, kuin negatiivisesti kehystetyt viestit. Tämä vaikutus korostuu, jos viestit ovat henkilökohdennettuja.

Shropshire ym. (2010) tutkimus lähtee oletuksesta, että terveystieteen sekä psykologian tieteenalan tutkimuksessa negatiivinen kehys on ollut positiivista kehystä tehokkaampi. Tutkimus keskittyy negatiivisesti kehystetyn detektiivisen ja preventiivisen viestin vaikutuksen arviointiin. Detektiivisellä toiminnalla tarkoitetaan proaktiivisia toimia, joilla voidaan havaita tietoturvauhkia. Näitä ovat esimerkiksi virus- ja haittaohjelmien torjuntaohjelma tai roskapostisuodatin. Preventiivisellä toiminnalla tarkoitetaan aktiivisia vastatoimia, joilla voidaan estää epäsuotuisa toiminta. Näitä ovat esimerkiksi elektroniset lukot sekä automaattisen uloskirjauksen ominaisuus. Tutkijat esittelivät biometrisen näppäimistön (preventiivinen) ja mukautuvan roskapostisuodattimen (detektiivinen), ja kyselytutkimuksella tutkivat aietta ottaa teknologia käyttöön. Tutkimuksen tuloksena todetaan, että negatiivinen kehys sai vahvistusta toimivana vaikutuskeinona, ja että koehenkilöt olivat valmiimpia ottamaan käyttöön detektiivistä teknologiaa kuin preventiivistä teknologiaa.

Barlowin, Warkentinin, Ormondin ja Dennisin (2013) skenaariopohjaisessa kyselytutkimuksessa tutkittiin kehysvaikutuksen tehokkuutta tietoturvapolitiikkojen rikkomuksia vastaan. Tutkimuksessa koehenkilöille esitettiin fiktiivinen tilanne, jossa henkilö luovuttaa oman salasanansa kollegalle vastoin organisaation tietoturvapolitiikkaa. Skenaariokuvauksessa kehysten lisäksi varioitiin myös muita muuttujia samassa viestissä. Tutkimuksessa ei havaittu vaikutusta kummallakaan kehyksellä tai eroa kehysten tehon välillä. Tutkijat spekuloivat tuloksen johtuvan siitä, että skenaarion muut kohdat aiheuttivat yleisesti viestiin joko positiivisen tai negatiivisen sävyn, joka häivytti tarkoitetun kehystämisen vaikutuksen. Taulukkoon 5 on koottu tutkimuksessa käytettyjen viestien kehystämisen esimerkkejä.

TAULUKKO 5 Barlow ym. (2013) tutkimuksen viestien kehystämisen esimerkkejä

Kehys	Suomeksi	Alkuperäinen
Positiivinen kehys	... "Arvostamme apuanne tässä asiassa. Tämän tietoturvapolitiikan noudattaminen varmistaa yhtiömme turvallisuuden. Politiikan noudattaminen ei ole turhaa." ...	… "We appreciate your help and support in this effort. Through employee compliance with this policy, we can ensure the safety and security of our company. Your efforts to support the company in this manner are not trivial." …
Negatiivinen kehys	... "Vaikka ei välttämättä vaikuta siltä, salasanan jakamisella on usein haitallisia seurauksia, kuten luvaton pääsy luottamuksellisiin tietoihin. Jopa luotettavalta vaikuttava työntekijä voi käyttää salasanoja pahantekoon. Toisin sanoen seuraukset ulottuvat myös työntekijän ulkopuolelle, joka ei noudata politiikkaa." ...	... "While it may not appear to be the case, there are often real consequences of sharing passwords such as improper access to confidential information. Even seemingly honest employees gain access to passwords for malicious intent. In other words, consequences extend beyond the person disobeying the policy." ...

Esimerkkejä tarkasteltaessa voidaan todeta, että kehystäminen on vaihtelevaa: kehystäminen ei kohdistu samaan asiaan ja lauserakenteet sekä ilmaisut eivät ole toistensa vastakohtia. Kehystämisvaikutuksen vaihtelevia tutkimustuloksia tietojärjestelmätieteissä selittää osittain se, että uhkissa ei ole selvää uhria tai näkyvää vihollista. Politiikan kontekstissa on todettu, että viestin asettelu sankariin ja rikolliseen tuottaa tehokkaan viestin, mutta samaa ei ole saatu vahvistettua kyberturvallisuuden kontekstissa (de Bruijn & Janssen, 2017).

4.4 Yhteenveto viitekehysvaikutuksesta viestinnässä

Viitekehysvaikutuksella tarkoitetaan viestin kehystämisen vaikutusta valintaan, ajatukseen tai toimintaan. Viitekehysvaikutus perustuu Kahnemanin ja Tverskyn (1979) Nobel-palkittuun prospektiteoriaan. Tversky ja Kahneman ha-

vaitsivat tutkimuksessaan, että ihmisillä on taipumus ylipainottaa varmoja vaihtoehtoja epävarmojen vaihtoehtojen joukosta. Lisäksi tutkimuksessa havaittiin, että ihmiset ovat alttiimpia ottamaan riskejä, jos varmoja vaihtoehtoja ei ole. Prospektiteorian tutkimus kuitenkin tuotti eri konteksteissa ja tieteenaloilla vaihtelevia tuloksia. Levin ym. (1998) saivat katsauksessaan yhtenäistettyä tuloksia kategorisoimalla aiempia eri tyyppisiä tutkimuksia omiin kehyskategorioihin: valintakehykseen, ominaisuuskehykseen ja tavoitekehykseen. Valintakehyksessä varioidaan riskiä ja esitetään riski joko positiivisessa tai negatiivisessa valossa. Ominaisuuskehyksessä jokin asia kehystetään esittämällä ominaisuuden prosenttiosuus tai onnistumisen mahdollisuus joko positiivisessa tai negatiivisessa valossa. Tavoitekehyksessä korostetaan toiminnasta saatavaa hyötyä tai toiminnan laiminlyömisestä aiheutuvaa haittaa, tarkoituksena saada henkilö toimimaan halutulla tavalla. Tietojärjestelmätieteen tieteenalalla viitekehysvaikutusta on tutkittu vähäisesti ja tutkimusten toteutukset ja tulokset ovat olleet vaihtelevia. Tässä tutkimuksessa pyritään vaikuttamaan lukitsemiskäyttäytymiseen esittämällä lukitsemisen tarve positiivisessa kehyksessä lukitsemisesta saatuina etuina ja negatiivisessa kehyksessä lukitsematta jättämisen haittoina.

5 PUUTTEITA AIEMMASSA TIETOTURVAKÄYTTÄYTYMISEN TUTKIMUKSESSA

Lebek, Uffen, Breitner, Neumann ja Hohler (2013) selvittivät kirjallisuuskatsauksessaan 2000-luvulla julkaistuissa työntekijöiden tietoturvatietoisuutta ja -käyttäytymistä käsittelevissä tutkimuksissa sovellettuja teorioita. Arvioiduissa 113 tutkimuksessa sovellettiin yhteensä 54 eri teoriaa, joista suurinta osaa käytettiin vain yhdessä tai kahdessa tutkimuksessa. Suojelumotivaatioteoriaa soveltavia tutkimuksia Lebek ym. löysivät 10 kappaletta. Muita paljon sovellettuja teorioita olivat suunnitellun käyttäytymisen teoria (engl. Theory of Planned Behavior) 27 tutkimuksella sekä yleinen peloteteoria (engl. General Deterrance Theory), jota oli käytetty 17 tutkimuksessa. Prospektiteoriaa tai viitekehyksen vaikutusta Lebek ym. ei mainitse erikseen aiemmassa kirjallisuudessa tutkittuna teoriana.

Lebek ym. (2013) tuovat katsauksensa yhteenvedossa esiin sovelletusta teoriasta riippumattomia puutteita ja ongelmia tietoturvakäyttäytymisestä tehdyssä tutkimuksessa. Erityisesti heidän kritiikkinsä kohdistuu kyselyjen käyttämiseen pääasiallisena havaintoaineiston keruumenetelmänä. Esimerkiksi henkilön tulevan käyttäytymisen tai käyttäytymisen aikeen selvittämiseen kyselyillä liittyy monia tunnettuja ilmiöitä, jotka vinouttavat tuloksia (Podsakoff & Organ, 1986). Yksi vinouman aiheuttajista on ihmisten taipumus kaunistella vastauksiaan, jotta ne olisivat sosiaalisesti hyväksyttävämpiä (engl. social desirability bias). Kaunistelun määrä riippuu henkilöstä itsestään sekä kysymyksen aihealueesta, ollen erityisesti korostunut muun muassa riskinottamiseen liittyvissä kysymyksissä (King & Bruner, 2000). Näin ollen kaunistelu voi vääristää esimerkiksi tietoturvamääräysten rikkomista koskevien kyselyjen tuloksia.

Toinen osa Lebekin ym. kritiikistä liittyy käyttäytymisen aikeen valitsemiseen tutkittavaksi vastemuuttujaksi. Jotta tuloksia voitaisiin hyödyntää organisaation tietoturvan parantamiseen käytännössä, joudutaan tekemään oletus siitä, että aie olisi todellisen käyttäytymisen pääasiallinen selittäjä. Kuitenkin esimerkiksi Webbin ja Sheeranin (2006) meta-analyysin tuloksien perusteella aikeen ja todellisen käyttäytymisen välillä on olemassa ”kuilu” (engl. intention-behavior gap). Tällä viitataan siihen, ettei todellisen käyttäytymisen ole havaittu aina lisääntyvän käyttäytymisen aikeen lisääntyessä.

Lebek ym. löysivät katsauksessaan viisi aikeen ja käyttäytymisen välistä yhteyttä tarkastellutta tutkimusta, joissa kaikissa havaittiin merkittävä yhteys aikeen ja käyttäytymisen välillä. Kaikissa tutkimuksissa tulokset perustuivat kuitenkin kyselyillä hankittuun aineistoon. Kyselytutkimuksiin liittyviin ongelmiin ja Workmanin, Bommerin ja Straubin (2008) tutkimukseen vedoten Lebek ym. toteavat, ettei kyselyllä määritettyä käyttäytymisen aietta voida yksistään pitää riittävänä selittäjänä todelliselle tietoturvakäyttäytymiselle. Aikeen ja käyttäytymisen välisen yhteyden todetaan siis vaativan lisää tutkimusta.

Todellisen tietoturvakäyttäytymisen tarkkailun ongelmaksi Lebek ym. mainitsevat tietoturvan arkaluontoisuuden aihealueena. He toteavat Kotuliciin ja

Clarkiin (2004) viitaten organisaatioiden olevan usein haluttomia antamaan tietoa tietoturvansa nykytilasta ja pohtivat eräänä mahdollisuutena laboratorioympäristössä tehtäviä kokeellisia tutkimuksia. Näiden haasteena nähdään kuitenkin se, ettei laboratorio-olosuhteissa havaittu käyttäytyminen ehkä vastaa tosielämän käyttäytymistä organisaation oikeassa työympäristössä. Aiheen haastavuudesta huolimatta Lebek ym. (2013) peräänkuuluttavat tarvetta objektiiviselle tietoturvakäyttäytymisen pidemmän aikavälin havainnoimiselle tosielämän työympäristössä.

Todellisen käyttäytymisen tarkkailun tärkeyttä painottavat myös Crossler ym. (2013) tietoturvakäyttäytymisen tutkimuksen tulevaisuutta käsittelevässä artikkelissaan. He niin ikään toteavat aiemman tutkimuksen osoittaneen kyselytutkimusten epäluotettavuuden ja huonon tarkkuuden verrattuna havaintoihin todellisesta käyttäytymisestä. Myös Crossler ym. korostavat tarvetta pitkittäistutkimuksille, joiden avulla saataisiin tietoa käyttäytymisen teorioiden selityskyvystä todelliselle käyttäytymiselle pidemmällä aikavälillä.

Aiemmasta tutkimuksesta löytyy muutama esimerkki todellisen käyttäytymisen pitkittäistutkimuksesta. Yksi näistä on Warkentinin, Johnstonin, Shropshiren ja Barnettin (2016) tutkimus, jossa kahden yliopiston opiskelijoita varoitettiin keksitystä tietokoneviruksesta. Viruksen kuvailtiin olevan perinteisten virustorjuntaohjelmistojen ulottumattomissa, ja uhkan torjumiseksi tarjottiin kokeellista virustorjuntaohjelmistoa, joka todellisuudessa oli tutkijoiden luoma valeohjelma todellisen käyttäytymisen seuraamiseksi. Opiskelijoita opastettiin käyttämään ohjelmistoa kerran viikossa. Virus ja sen torjuntaan kehitetty ohjelma esiteltiin opiskelijoille todellisina, jotta tieto kokeen todellisesta tarkoituksesta ei vääristäisi tuloksia. Warkentin ym. mainitsevat, että kokeen aikana keksityn viruksen tai virustorjuntaohjelman nimellä internetistä hakemalla ei löytynyt yhtään relevanttia tulosta.

Yhteensä 1800 opiskelijasta 398 asensi ohjelmiston omalle tietokoneelleen ja käytti sitä ainakin kerran. Käyttöön ja käytön lopettamiseen vaikuttavien tekijöiden selvittämiseksi jokaista ohjelmistoa käyttänyttä opiskelijaa pyydettiin vastaamaan kyselyyn. Kyselyllä kartoitettiin suojelumotivaatioteorian konstruktien yhteyttä havaittuun käyttäytymiseen. Näiden lisäksi ulkopuolisten olosuhteiden vaikutus oli otettu yhdeksi tutkittavaksi tekijäksi.

Warkentinin ym. (2016) tutkimusasetelma saattaa asettaa joitain rajoituksia tulosten soveltamiselle todellisten organisaatioiden tietoturvan parantamiseen. Ensinnäkin tutkimukseen osallistuneet koehenkilöt olivat opiskelijoita, joiden käyttäytymistä tarkkailtiin heidän omilla henkilökohtaisilla tietokoneillaan. Lisäksi koehenkilöiltä odotetun tietoturvatoimen tarkoituksena oli suojata koehenkilön henkilökohtainen tietoturva. Organisaatiossa työntekijät käyttävät tyypillisesti organisaation tarjoamia laitteita, joilla he käsittelevät organisaation resursseja ja järjestelmiä. Koska näihin kohdistuvista tietoturvauhkista puuttuu suora henkilökohtainen relevanssi, on Warkentinin ym. tulosten soveltuvuus organisaatiokontekstiin kyseenalaista. Tutkimuksessa ei myöskään hyödynnetty suojelumotivaatioteoriaa tietoturvakäyttäytymiseen vaikuttamiseksi vaan ainoastaan selittämään käyttäytymistä jälkikäteisesti.

Todellista tietoturvakäyttäytymistä tutkivat myös Boss ym. (2015) kaksiosaisessa tutkimuksessaan. Tutkimuksen toisessa osassa vapaaehtoisia pyydettiin sähköpostin välityksellä osallistumaan tutkimusta varten luodun internetsivun käytettävyystutkimukseen. Kaksi minuuttia linkin avaamisen jälkeen sivusto näytti käyttäjälle virusvaroituksen, jossa kuvattiin viruksen aiheuttama uhka ja seuraukset joko vähäisinä tai suurina. Kontrolliryhmälle ei näytetty ilmoitusta lainkaan. Viruksesta varoittavassa ikkunassa kehotettiin klikkaamaan OK-painiketta viruksen poistamiseksi, mikä tulkittiin viestin ehdottaman toiminnan hyväksymiseksi. Ikkunan sulkemisen katsottiin tarkoittavan viestin ehdotuksen huomiotta jättämistä. Boss ym. havaitsivat uhkaa korostaneen viestin johtavan suositeltuun toimintaan matalan uhkan viestiä useammin.

Myös Boss ym. (2015) tutkimuksen heikkoutena voidaan pitää sen tulosten sovellettavuutta käytäntöön. Tutkimuksen kohderyhmä koostui tässäkin tutkimuksessa opiskelijoista, jotka käyttivät omia henkilökohtaisia laitteitaan. Täten tulokset eivät välttämättä ole sovellettavissa organisaatiokontekstiin. Lisäksi Bossin ym. käyttämää koeasetelmaa voidaan perustellusti pitää hieman naiivina: internetsivujen näyttämät ponnistusikkunat ovat hyvin yleinen mainostajien, haittaohjelmien levittäjien ja huijareiden käyttämä tapa käyttäjien houkuttelemiseksi. Lisäksi kokeessa käytettyä virusilmoituksen ulkoasua ei esimerkiksi mukautettu koehenkilön käyttämän oikean virustorjuntaohjelman mukaisesti. Näin ollen voidaan kyseenalaistaa, pitivätkö koehenkilöt ilmoitusta viruksesta todellisena.

Aiemman tietoturvakäyttäytymisen tutkimuksen puutteiden perusteella tarvitaan siis lisää tutkimusta, jossa tarkkaillaan todellista käyttäytymistä oikeassa organisaatioympäristössä pidemmällä aikavälillä. Näin käyttäytymisestä voidaan saada objektiivista dataa ja vältytään kyselytutkimuksilla kerättyyn dataan liittyviltä vinoumilta sekä käyttäytymisen aikeen ja todellisen käyttäytymisen väliseen yhteyteen liittyviltä ongelmilta. Tällaisen tutkimuksen asetelma tulisi myös suunnitella siten, että se vastaisi mahdollisimman hyvin todellista toimintaa organisaatiossa. Näin saatu tieto olisi arvokasta myös käytännön tietoturvatyön kannalta organisaatioissa.

6 KIRJALLISUUSKATSAUKSEN YHTEENVETO

Organisaation tietoturva koostuu teknisistä ja inhimillisistä tekijöistä. Inhimilliset tekijät, kuten organisaation jäsenten päivittäiset toimet tiedon ja tietojärjestelmien käsittelyssä, ovat kriittisen tärkeä osa tietoturvan kokonaisuutta. Yksittäisen käyttäjän epäturvallinen toimintatapa, kuten työaseman lukitsematta jättäminen, voi tehdä teknisistä tietoturvaratkaisuista tehottomia ja vaarantaa organisaation tieto-omaisuuden sekä jopa koko organisaation toiminnan. Tietoturvakäyttäytymisen vaikuttamisen keinojen tutkiminen on siis kriittistä niin käytännön kuin tutkimuksenkin kannalta, jotta tutkimus voisi vastata tosielämän tarpeisiin.

Eräs eniten tutkituista käyttäytymisen teorioista on suojelumotivaatioteoria, joka selittää pelkoon vetoamisen vaikutusta. Suojelumotivaatioteorian mukaan tieto uhkasta saa aikaan kahden toisistaan riippumattoman prosessin, uhka-arvion ja selviytymisarvion, välityksellä käyttäjän toimintaa ohjaavan suojelumotivaation. Tehdyistä tutkimuksista vain pieni osa on ollut käyttäytymiseen vaikuttamaan pyrkiviä tutkimuksia, joissa vähintään suojelumotivaatioteorian uhka-arvioprosessia manipuloimalla olisi pyritty selvittämään pelkoon vetoamisen tehokkuutta tietoturvakontekstissa. Tämä on nähty heikkoutena aiemmassa tutkimuksessa. Tutkimuksessa ei lisäksi ole huomioitu riittävällä tavalla suojelumotivaatioteoriaan sisäänrakennettua olettamusta siitä, että uhka on henkilölle itselleen relevantti. Organisaatioissa tietoturvauhkat kohdistuvat lähinnä organisaation tietoon ja järjestelmiin, jolloin uhkaa ei välttämättä koeta henkilökohtaisesti relevantiksi.

Yksi vähemmän tietojärjestelmätieteessä tutkittu, mutta potentiaalinen vaikuttamisen keino on viestin kehystämisellä vaikuttaminen eli viitekehysvaikutus. Levin ym. (1998) mallissa viitekehysvaikutus on jaettu kolmeen kategoriaan: valintakehykseen, ominaisuuskehykseen ja tavoitekehykseen. Näistä erityisesti tavoitekehys on hyvin soveltuva tietoturvauhkien kontekstiin. Tavoitekehys tarkoittaa suositellun toiminnan esittämistä joko hyötyjen saamisen tai negatiivisten seurausten välttämisen näkökulmasta. Positiivisessa kehyksessä korostetaan toiminnasta saatavaa hyötyä ja negatiivisessa kehyksessä korostetaan toiminnan laiminlyömisestä aiheutuvaa haittaa. Kummankin kehyksen tarkoitus on sama eli saada henkilö toimimaan halutulla tavalla.

Käytetystä teoriasta riippumatta tietoturvakäyttäytymisen aiemman tutkimuksen heikkoutena on pidetty sen keskittymistä lähes yksinomaan kyselytutkimuksiin, joissa on tutkittu eri tekijöiden vaikutusta käyttäytymisen aikeeseen. Kyselytutkimukset ovat tiedonkeruumenetelmänä alttiita erilaisille vinoumille, jotka voivat vääristää saatuja tuloksia. Käyttäytymisen aikeen valitseminen selitettäväksi muuttujaksi taas on ongelmallista siksi, ettei kasvu käyttäytymisen aikeessa välttämättä kuitenkaan vaikuta todelliseen käyttäytymiseen.

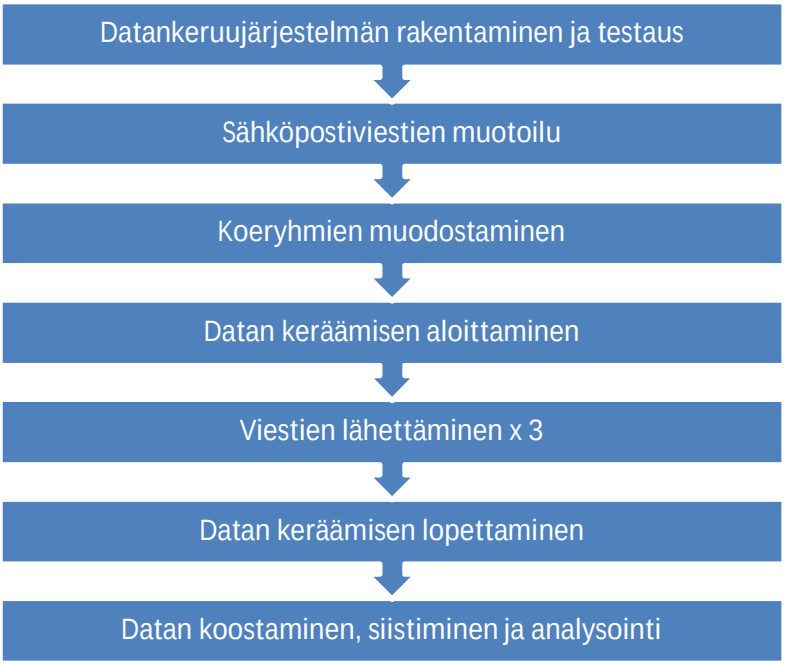
Tämän tutkimuksen tarkoituksena on vastata kirjallisuuskatsauksen perusteella havaittuihin puutteisiin koeasetelmalla, jossa käyttäytymiseen pyritään

vaikuttamaan toistetulla sähköposti-interventioilla. Tutkittavana käyttäytymisenä on työaseman lukitseminen, joka on organisaation tietoturvan kannalta tärkeä päivittäinen, käyttäjän vastuulle jäävä tietoturvatoimi. Interventioviesteissä käytetään kahta eri pohjaviestiä, joista toinen hyödyntää suojelumotivaatioteoriaa ja toinen viitekehyksen vaikutusta. Viestien sisältöä manipuloidaan, jotta voidaan tutkia sisällön vaikutusta intervention tehoon. Suojelumotivaatioteorian osalta testataan uhkan vakavuuden ja todennäköisyyden sekä vastatoimen tehokkuuden ja minäpystyvyyden vaikutusta intervention tehoon. Viitekehysvaikutuksen osalta tutkitaan positiivisen ja negatiivisen kehyksen vaikutuksen eroa. Kummankin teorian pohjalta muodostettuja viestejä manipuloidaan lisäksi henkilökohtaisen relevanssin korostamisen sekä kuvailun yksityiskohtaisuuden osalta. Viestin yksityiskohtaisuutta manipuloimalla tutkitaan, voidaanko uhka ja sen seuraukset yksityiskohtaisemmin kuvailemalla lisätä intervention tehoa. Tutkimus toteutetaan oikeassa organisaatiossa ja interventioiden vaikutuksen tutkimiseksi kerätään dataa todellisesta käyttäytymisestä organisaation tietojärjestelmiä hyödyntäen.

7 TUTKIMUKSEN TOTEUTUS

Tässä luvussa kuvataan tutkimuksen suunnittelu, toteutus ja käytetyt kokeelliset menetelmät. Kuvaus on pyritty tekemään Pfleegerin ja Caputon (2012) suosituksesta siten, että se mahdollistaa kokeen olosuhteiden ymmärtämisen riittävällä tarkkuudella sekä kokeen toistamisen tarvittaessa. Luvun alussa esitetään yleiskuvaus kokeen kulusta ja käytetystä tutkimusmenetelmästä, jonka jälkeen oleellisimpia osia tutkimuksesta tarkennetaan omissa alaluvuissaan.

Tutkimuksen eteneminen on kuvattu yleisellä tasolla vuokaaviona kuviossa 5. Tutkimuksen toteutuksen suunnittelu aloitettiin luomalla automaattinen järjestelmä, jolla Windows-käyttöjärjestelmän oletuksena ylläpitämästä työaseman tapahtumalokista saatiin siirrettyä tarpeelliset tiedot keskitettyyn tietokantaan. Järjestelmän avulla pystyttiin keräämään lokimerkinnät työasemien lukitsemisen lisäksi kirjautumisista sekä työasemien käynnistämisistä ja sammuttamisista. Datankeruun toimivuutta ja luotettavuutta testattiin keräämällä muutaman kuukauden ajan testidataa, jota ei sisällytetty tulosten analysoinnissa käytettyyn aineistoon.

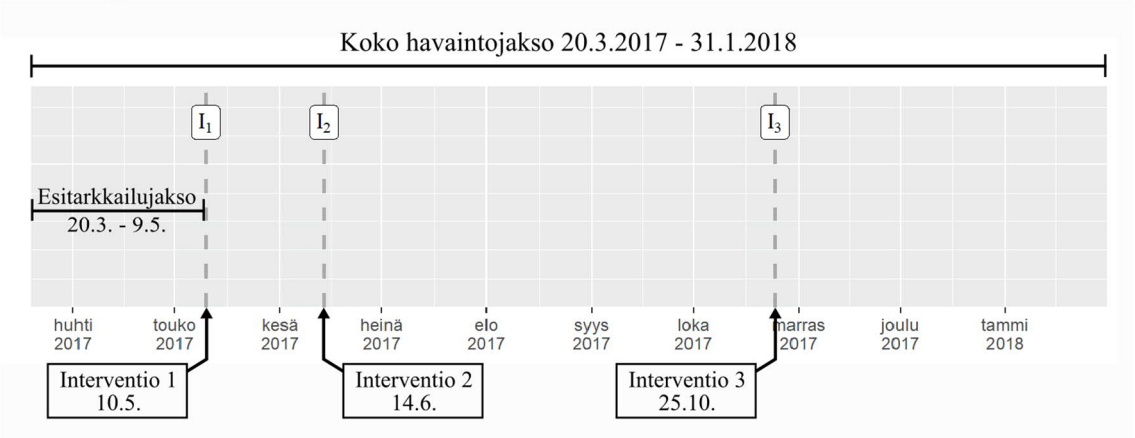


KUVIO 5 Tutkimuksen eteneminen vuokaaviona esitettynä

Kirjallisuuskatsauksen perusteella interventio päätettiin toteuttaa faktorikokeena, jossa suojelumotivaatioteoriasta valittiin kaksi tutkittavaa faktoria ja viitekehysvaikuttamisen teoriasta yksi. Näiden lisäksi valittiin kummallekin teorialle kaksi yhteistä faktoria. Kaikille faktoreille määritettiin kaksi mahdollista tasoa. Tutkimuksessa käytettiin siis 24 ($2^4 + 2^3$) erilaista sähköpostiviestiä, joilla kullakin oli oma faktorikonfiguraationsa. Sähköpostiviestit generoitiin ohjelmallisesti tekemällä viestipohjiin kunkin viestin faktorikonfiguraatiota vastaavat

muutokset ja lisäykset. Viestien ulkoasu muotoiltiin tarkasti organisaation muuta viestintää vastaavaksi ja niiden lähetys koordinoitiin organisaation oman viestintäosaston kanssa. Tutkimuksessa käytetyt sähköpostiviestit löytyvät tutkielman liitteistä 1 ja 2.

Organisaation henkilökunta jaettiin 24 interventioryhmään ja yhteen kontrolliryhmään, joka ei saanut kokeen aikana yhtään interventioviestiä. Työasemien käyttö- ja lukitsemisdatan kerääminen aloitettiin noin 7 viikon esitarkkailujaksolla ennen ensimmäistä interventiota. Intervention toiston vaikutuksen selvittämiseksi interventio tehtiin yhteensä kolme kertaa jokaiselle ryhmälle samansisältöisenä. Tarkkailujakson ja interventioiden ajallinen sijoittuminen on esitettynä kuviossa 6. Datan kerääminen lopetettiin noin 3 kuukautta viimeisen intervention jälkeen.



KUVIO 6 Interventiokokeen eteneminen aikajanalla kuvattuna

Kerätty raakadata anonymisoitiin yksisuuntaisesti siten, ettei siitä ollut mahdollista tunnistaa yksittäisiä henkilöitä tai henkilöiden käyttämiä työasemia. Tulosten analyysissä käytetty havaintoaineisto koottiin muodostamalla sessioita anonymisoiduista sisään- ja uloskirjautumistapahtumista sekä yhdistämällä lukitsemis- ja lukituksenavaamistapahtumat näin saatuihin sessioihin. Lopuksi havaintoaineisto siivottiin ja rajattiin tarkoituksenmukaisesti.

7.1 Tutkimusmenetelmä

Tehty tutkimus oli tyypiltään pitkittäinen interventiotutkimus, joka suoritettiin kenttätutkimuksena. Pitkittäisellä tutkimuksella tarkoitetaan tutkittavaan ilmiöön liittyvän pitkän aikavälin prosessin, muutoksen tai jatkuvuuden havainnointia. Pitkittäistutkimuksessa kerättävä data voi olla kvantitatiivista tai kvalitatiivista ja se on luonteeltaan jatkuvaa. Pitkittäistutkimukselle vaihtoehtona on poikittaistutkimus, jossa dataa kerätään valittuina ajankohtina ja data on tietyn ajankohdan poikkileikkaus. Pitkittäistutkimuksessa erityisesti eettiset haasteet korostuvat: tutkimukseen osallistuvista kerättävä data voi olla tyypillistä poikittais-

tutkimusta tarkempaa, jonka seurauksena yksittäinen henkilö voi olla tunnistettavissa suurestakin osallistujien joukosta. (Elliott, Holland, & Thomson, 2012.) Tässä tutkimuksessa kiinnitettiin erityistä huomioita tietosuojaan ja käyttäjien yksityisyyteen, ja kaikki tutkimuksessa käytetty aineisto oli huolellisesti anonymisoitua. Tutkimuksessa tutkittu ilmiö, työaseman lukitsemiskäyttäytyminen, vaati jatkuvaluonteista dataa lukitsemiskäyttäytymisestä, jotta intervention vaikutus käyttäytymiseen voitiin havaita. Interventioilla tutkimuksessa pyrittiin saavuttamaan positiivinen muutos lukitsemiskäyttäytymiseen luonnollisissa olosuhteissa.

Tutkimuksessa kerätty data muodosti aikasarjan. Aikajärjestyksessä olevan aineiston havaintopisteitä oli lukuisia ennen interventiota ja sen jälkeen. Aikasarjatutkimukselle ominaisesti riippuvan muuttujan kehitystä seurattiin ennen interventioita ja niiden jälkeen, ja havaintoaineistosta pyrittiin löytämään merkittävä ero ennen ja jälkeen interventioiden. Aikasarjatutkimus on lähestymistapana yksi vahvimmista tutkimusasetelmista pitkittäisen aineiston arviointiin. (Schutt, 2011)

Luonnollisissa olosuhteissa tapahtuvaa havainnointia ja aineiston keräämistä kutsutaan kenttätutkimukseksi. Kenttätutkimuksen koeasetelmassa tavoitteena on minimoida tutkimusasetelman vaikutus tutkittavaan ilmiöön ja siinä pyritään saamaan dataa eri tekijöiden vaikutuksesta niiden luonnollisessa kontekstissaan. Kenttätutkimuksessa muuttujia ei voida kontrolloida yhtä tehokkaasti kuin laboratoriotutkimuksessa, mutta sen avulla saatavaa tietoa pidetään paremmin yleistettävänä ja ilmiötä todellisuudessa kuvaavana. Eräs kenttätutkimuksessa huomioitava asia on, että tutkimuksen vaikutusten laajuutta tai kestoa tutkimusympäristössä ei voida rajata samalla tavalla kuin laboratorio-olosuhteissa. Tutkimusta tehdessä on siis oltava huolellinen, ettei epätoivottuja vaikutuksia pääse aiheutumaan. Kenttätutkimukselle tyypillistä on myös, että se vaatii usein laboratoriokoetta enemmän aikaa, rahaa ja henkilöresursseja. (Gross, 2017.)

Tutkimusasetelman vuoksi kaikkia muuttujia ei siis voitu kontrolloida ja kokeessa saattoi olla tuntemattomia lukitsemiskäyttäytymiseen vaikuttavia tekijöitä. Kokeen asetelmassa voidaankin siten nähdä piirteitä myös kvasikokeellisesta tutkimuksesta, jossa tarkoituksena ei ole kontrolloida kaikkia tutkimukseen vaikuttavia muuttujia. Kuitenkin kvasikokeellisesta tutkimuksesta poiketen tässä tutkimuksessa koehenkilöt jaettiin interventioryhmiin satunnaisesti. Puhtaasti kvasikokeelliselle tutkimukselle on tyypillistä, ettei koeryhmiä satunnaisteta, vaan koehenkilöt jaetaan ryhmiin tarkoituksenmukaisesti esimerkiksi kokeen suorittajan tai jopa koehenkilöiden itsensä toimesta. Kvasikokeellisessa tutkimuksessa myös tutkijoiden rooli on merkittävä. Kvasikokeellisen tutkimuksen perusoletus on, että tutkija osaa määrittää kausaalisen väitteen ja tutkia havainnoille vaihtoehtoisia uskottavia selityksiä, jotka voisivat mitätöidä määritetyn väitteen. Vaihtoehtoisten selitysten poissulkemiseksi aihealueen tuntemus on kvasikokeellisessa tutkimuksessa tärkeää, koska tutkijan on pystyttävä tunnistamaan vakuuttavasti juuri kyseiselle aihealueelle ominaiset vaikuttavat tekijät

(Shadish ym., 2005.) Tämän tutkimuksen tekijöillä oli kattava käytännön tuntemus tutkittavasta ilmiöstä IT-alan pitkän, yhteensä yli 20 vuoden, työkokemuksen ansiosta.

7.2 Kohdeorganisaatio

Tutkimus toteutettiin suomalaisessa korkeakoulussa (jatkossa ”organisaatio”), jossa työskenteli noin 2900 henkilöä. Organisaation toiminta keskittyi pääosin yhteen kaupunkiin, jossa sillä oli useita toimipisteitä. Henkilökunnasta valtaosa puhui äidinkielenään suomea ja noin 10% työntekijöistä oli ulkomaalaisia, jotka käyttivät kommunikointiin englantia. Organisaation sisäinen viestintä tapahtui vakiintuneen käytännön mukaisesti kaksikielisesti suomea ja englantia käyttäen.

Tutkimuksen aikana organisaatiolla oli käytössään yhteensä noin 6000 työasemaa ja kannettavaa tietokonetta (jatkossa pelkästään ”työasema”), joista tutkimuksen alussa hieman yli puolet toimi Windows 7- ja loput Windows 10-käyttöjärjestelmällä. Organisaatio oli tutkimuksen aikana siirtymässä pelkästään Windows 10 -käyttöjärjestelmän käyttöön, joten Windows 10:n suhteellinen osuus työasemista kasvoi tasaisesti. Organisaatiossa käytettiin jonkin verran myös Mac- ja Linux-työasemia, jotka kuitenkin rajattiin teknisistä syistä jo suunnitteluvaiheessa tutkimuksen tarkastelun ulkopuolelle.

Interventiotutkimukselle saatiin hyväksyntä organisaation tietoturvapäälliköltä sekä IT-osaston edustajalta. Organisaatiolla oli suunnitteilla tietoturvakampanja yleisen tietoturvan parantamiseksi, jonka yhtenä osana oli tietoturvaviestintä organisaation työntekijöille. Tutkimus siis sopi hyvin myös organisaation tavoitteisiin. Interventioviestien lähettämisestä sovittiin organisaation viestintäosaston kahden asiantuntijan kanssa, jotta viestit voitiin lähettää noudattaen organisaation vakiintunutta viestintäkäytäntöä.

Tutkimuksen aikana tutkimuksesta tietävien henkilöiden määrä organisaation sisällä pyrittiin pitämään mahdollisimman pienenä, jotta tieto tutkimuksesta ei leviäisi. Tällä varmistettiin, että interventioviestien vaikutuksesta saatavat tulokset vastaisivat todellista tilannetta. Käytäntö hyväksytettiin organisaation tietoturvapäälliköllä. Mikäli henkilökunta olisi tiennyt tutkimuksesta etukäteen, tämä olisi saattanut vaikuttaa käyttäytymiseen merkittävästi.

7.3 Interventiot

Tässä luvussa kuvataan tutkimuksessa suoritetut interventiot tarkemmin. Ensin esitellään manipuloitavaksi valitut faktorit sekä niiden tasot, jonka jälkeen kuvataan viestien muotoilu ja siinä huomioidut asiat. Tämän jälkeen määritellään, kuinka interventioviestien vastaanottajat valittiin ja jaettiin. Luvun lopuksi raportoidaan viestien lähettämiseen ja datankeräämiseen liittyneet asiat.

7.3.1 Faktorien ja tasojen valinta

Interventioviesteissä manipuloitavat faktorit valittiin kirjallisuuskatsauksen perusteella. Teoreettisena pohjana viestien muodostamiselle käytettiin suojelumotivaatioteoriaa sekä viitekehyksen vaikutuksen teoriaa. Viesteihin sisällytettyjen faktorien tasot valittiin siten, että kaikki viestit lähtökohtaisesti vaikuttaisivat positiivisesti työasemien lukitsemiseen. Viesteillä ei haluttu olevan negatiivista vaikusta organisaation tietoturvalle. Faktoreille valitut nollatasot olivat siis enintään neutraaleja korostuksissaan. Osa faktoreista oli teoriakohtaisia ja osa kummallekin yhteisiä.

Teorian testaamisen näkökulmasta olisi todennäköisesti ollut hedelmällisintä valita faktorien tasot siten, että ne olisivat olleet mahdollisimman kaukana toisistaan (esim. ”lukitsematta jätetty työasema on vakava tietoturvariski” ja ”lukitsematta jätetty työasema on vähäinen tietoturvariski”). Näin erot viestien vaikutuksessa olisivat todennäköisesti kasvaneet, mikä olisi helpottanut faktorien tasojen ja intervention tehon välisen yhteyden tutkimista. Voidaan kuitenkin pitää mahdollisena, että lukitsemisen tärkeyttä vähättelevät viestit olisivat saattaneet vähentää työasemien lukitsemista. Tämä ei olisi ollut organisaation tavoitteiden mukaista tai tutkimuseettisesti kovin hyväksyttävää.

Suojelumotivaatioteoriaan pohjautuvissa viesteissä pyrittiin vaikuttamaan kognitiiviseen selviytymisarvioprosessiin manipuloimalla minäpystyvyyden ja vastatoimen tehokkuuden yhdistettyä pystyvyysfaktoria eli kuvausta siitä, kuinka tehokas työaseman lukitseminen on vastatoimena ja kuinka kykeneväinen käyttäjä on käyttämään lukitsemistoimintoa. Valitut tasot olivat neutraali ja korostettu. Uhka-arvioprosessiin pyrittiin taas vaikuttamaan manipuloimalla uhkan todennäköisyyden ja uhkan vakavuuden yhdistettyä faktoria eli kuvausta siitä, miten vakava ja todennäköinen uhka lukitsematta jättämisen aiheuttama työaseman luvaton käyttö on. Valitut tasot olivat neutraali ja korostettu.

Viitekehyksen vaikutusta tutkiviin viesteihin valittiin faktoriksi viitekehyksen tyyppi. Faktorin tasot olivat suositellun toiminnan kuvaaminen joko epätoivottujen seurausten välttämisenä tai toimintana hyötyjen saavuttamiseksi.

Kummankin teorian osalta yhteisiksi faktoreiksi valittiin uhkan kohdistumisen faktori sekä uhkan ja seurausten kuvailun yksityiskohtaisuuden tason faktori. Uhkan kohdistumisen tasot olivat organisaatio ja organisaatio + henkilökohtainen. Kuvailun yksityiskohtaisuudelle valitut tasot olivat matala ja tarkka.

Liitteet 1 ja 2 sisältävät kokeessa käytettyjen viestien konfiguraatiomatriisit kummankin teoriapohjan osalta.

7.3.2 Viestien muotoilu ja viimeistely

Viestien muotoilu aloitettiin perehtymällä organisaation aiempaan tapaan viestiä tietoturvaan liittyvistä asioista. Näin varmistettiin, etteivät viestit poikkeaisi liikaa organisaation normaalista viestinnästä ja siten aiheuttaisi odottamattomia vaikutuksia. Aiempaa viestintää analysoitiin myös käytettyjen kirjaisintyyppien

ja muun graafisen muotoilun osalta. Lähtökohtana oli mukauttaa viestit mahdollisimman hyvin organisaation viestintäkulttuuriin. Mikäli viestit olisivat poikenneet muusta viestinnästä, tämä olisi saattanut toimia kontrolloimattomana tekijänä interventioissa.

Suojelumotivaatioteorian osalta tutkimuksessa käytettiin 16 erilaista viestiä. Kaikkien viestien pohjana käytettiin faktorien nollatasoa vastaavaa viestiä, jonka avulla muita faktorikonfiguraatioita vastaavat viestit muodostettiin pohjaa ohjelmallisesti muuttamalla. Viitekehysvaikutuksen tutkimiseksi laadittiin ensin viestin tyypin faktorin kummankin tason mukaiset viestipohjat, joihin kuvailun yksityiskohtaisuuden tason ja uhkan kohdistumisen tason faktorit lisättiin viestipohjia muokkaamalla. Kaikki eri faktorikonfiguraatioita vastaavat viestit generoitiin viestipohjien avulla ohjelmallisesti.

Päivittäisen sähköpostiviestinnän suuren määrän arveltiin vaikuttavan varsinkin pidempien tiedotteiden lukemiseen ja lukemisen huolellisuuteen. Viestejä muodostettaessa pyrittiin maksimoimaan viestien luetuksi tulemisen todennäköisyys pitämällä viestit lyhyinä ja napakoina. Myös viestien rivimäärällisen pituuden vaihtelu pyrittiin pitämään alhaisena, jotta mahdolliset erot viestien huomioiduksi tulemisessa eivät olisi vaikuttaneet merkittävästi kokeen tulokseen.

Viestien ensimmäisten versioiden laatimisen jälkeen viestien kielellinen luontevuus sekä kieliopillinen oikeellisuus varmistettiin jokaisen viestin osalta ja viesteihin tehtiin tarvittavat korjaukset. Viestien sisällön ymmärrettävyys varmistettiin luetuttamalla viestit opinnäytetyön ohjaajien lisäksi usealla organisaation ulkopuolisella henkilöllä, joiden tekninen osaamistaso vaihteli. Saadun palautteen perusteella viestien sisällön ymmärtämiseksi tarvittavaa teknistä osaamistasoa madallettiin käyttämällä mahdollisuuksien mukaan yleiskielen sanastoa ja kuvaavia, epäteknisiä ilmaisuja. Myös organisaation tietoturvapäällikkö luki viestit ja hyväksyi niiden sisällön ja ilmaisumuodot.

Koska organisaatiossa työskenteli myös suomea puhumatonta henkilökuntaa, viesteihin sisällytettiin englanninkielinen käännös tekstistä. Englanninkielisessä käännöksessä pyrittiin huomioimaan kielten erityispiirteet siten, että faktorit ja niiden tasot vastaisivat mahdollisimman hyvin toisiaan kummassakin kieliversiossa. Käännöksessä apuna käytettiin organisaation viestintäosaston kielenkääntäjää ja englanninkielisten versioiden oikeinkirjoitus varmistettiin käyttämällä ulkopuolista käännöspalvelujen tarjoajaa. Lopuksi yksi organisaation tiedotuksesta vastaava asiantuntija luki viestit ja vahvisti niiden sopivan organisaation vakiintuneeseen viestintäkulttuuriin.

Viesteihin sisällytettiin lisäksi linkki organisaation ohjesivustolle, jossa työaseman lukitsemistoiminnon käyttäminen opastettiin yksityiskohtaisesti kuvankaappausten avulla. Tällä haluttiin sekä minimoida IT-osastolle tulevat yhteydenotot sekä varmistaa, että myös teknisesti kokemattomat käyttäjät osaisivat lukita työasemansa.

Viestien muotoilua ja sisällön selkeyttä voidaan pitää onnistuneena, sillä IT-osasto ei saanut tutkimuksen aikana yhtään viesteihin liittyvää lisätietopyyntöä tai viestien autenttisuuden kyseenalaistavia yhteydenottoja. Organisaation hen-

kilökunnan tiedettiin yleisesti olevan kohtalaisen aktiivisia ilmoittamaan epäilyttävistä tietojärjestelmiin liittyvistä viesteistä, kuten erilaisista käyttäjätietojen kalasteluyrityksistä.

7.3.3 Interventioviestin vastaanottajien rajaaminen ja ryhmittely

Organisaation tietojärjestelmistä saatiin lista organisaation henkilökunnan jäsenistä sekä heidän sähköpostiosoitteistaan. Potentiaalisten vastaanottajien joukosta poistettiin tutkimuksesta tienneiden henkilöiden lisäksi organisaation koko IT-osaston henkilökunta. Tämä varotoimi tehtiin, koska pidettiin mahdollisena, että IT-osaston henkilökunta olisi saattanut keskustella viesteistä keskenään ja näin tutkimus olisi saattanut paljastua vaarantaen koko koeasetelman.

Vastaanottajaksi valitut 2841 henkilöä jaettiin satunnaisesti 25 ryhmään, jolloin yhden ryhmän kooksi tuli noin 114 henkilöä. Ryhmistä 24 sai yhden interventioviesteistä ja yksi ryhmä ei saanut lainkaan viestiä eli se toimi kontrolliryhmänä. Ilman viestiä jätetty ryhmä sisällytettiin tutkimukseen, jotta voitaisiin havaita, mikäli työasemien lukitsemisessa tapahtuisi merkittäviä, interventioviesteistä riippumattomia muutoksia.

7.3.4 Viestien lähettäminen ja datan kerääminen

Tutkimus aloitettiin noin 7 viikon esitarkkailujaksolla ennen ensimmäisen intervention suunniteltua ajankohtaa. Esitarkkailujakson tarkoituksena oli antaa tietoa nykyisestä työasemien lukitsemiskäyttäytymisestä organisaatiossa ja toimia vertailukohtana interventioiden jälkeiselle käyttäytymiselle.

Interventioiden ajankohdat eli viestien lähettämispäivät pyrittiin valitsemaan siten, että jokaista ajankohtaa seurasi riittävä aikaväli, johon ei osunut arkipyhiä. Tällä haluttiin varmistaa, että välittömästi jokaisen intervention jälkeen saataisiin riittävästi häiriötöntä dataa. Arkipyhien takia vajailla viikoilla arveltiin myös muiden päivien käyttäytymisen poikkeavan normaalista täydestä työviikosta, mihin myös esitarkkailujakson datan alustava tarkastelu viittasi.

Toinen interventio päätettiin tehdä noin kuukauden päästä ensimmäisestä viestistä, jotta sen vaikutusta ehdittäisiin havainnoimaan ennen organisaation kesälomakauden. Suhteellisen pian ensimmäisen viestin jälkeen tulevalla muistutusviestillä haluttiin myös testata, onko muistuttaminen hyödyllistä. Kolmas, ja viimeinen, interventio tehtiin kesälomakauden jälkeen uuden lukuvuoden alettua, mutta hyvissä ajoin ennen vuodenvaihteeseen ajoittuvia joululomia. Kolmannen intervention ajoittamisessa huomioitiin myös se, että havaintoaineistoissa ehtisi näkyä, mikäli kahden ensimmäisen intervention vaikutus olisi hävinnyt kesälomakauden aikana.

Intervention toistoissa jokaiselle vastaanottajalle lähetettiin sama sähköpostiviesti kuin aiemmin, mutta siten että, otsikkokenttään oli lisätty sana ”Muistutus”. Otsikon muokkaamisella yritettiin varmistaa, että myös myöhemmin tulevat viestit huomioitaisiin mahdollisimman hyvin.

Kaikki interventiot ajoitettiin keskiviikkopäiville, joiden todettiin esitarkkailujakson perusteella olevan viikon aktiivisimpia päiviä päivittäisten käyttäjämäärien perusteella. Keskiviikoille ei myöskään osunut organisaation muuta, koko henkilökuntaa koskevaa yleistä viestintää, joka olisi voinut vaikuttaa interventioihin kontrolloimattomalla tavalla. Viestien lähetysajankohta valittiin iltapäivältä yleisen lounasajan jälkeen, jolloin mahdollisimman monen käyttäjän arveltiin olevan työasemansa ääressä.

Viestit lähetettiin käyttäen organisaation virallista viestintäsähköpostiosoitetta ja lähettäminen automatisoitiin ohjelmallisesti virheiden välttämiseksi. Sähköpostijärjestelmän virheilmoitusten perusteella lähetys epäonnistui teknisistä syistä yhteensä 310 käyttäjälle vähintään yhden interventioviestin osalta. Näiden käyttäjien tutkimusta varten koostetut sähköpostiosoitteet eivät olleet enää voimassa vaan poistuneet käytöstä esimerkiksi pidemmän poissaolon vuoksi.

Kokeessa ei voitu kontrolloida sitä, ketkä vastaanottajista lukivat lähetetyt viestit. Viestin mahdollinen lukematta jättäminen tai huomaamatta jääminen toimivat siis kontrolloimattomina intervention tehoa heikentävinä muuttujina.

7.4 Datankeruujärjestelmä

Tässä luvussa kuvataan tutkimuksessa käytetty datankeruujärjestelmä sekä käsitellään sitä, kuinka tietoturva ja tietosuoja huomioitiin.

7.4.1 Suunnittelu, toteutus ja testaus

Microsoft Windows –käyttöjärjestelmä tuottaa automaattisesti lokitietoa työaseman käytöstä Windowsin tapahtumalokiin (Windows Event Log). Lokitiedot sisältävät merkintöjä muun muassa työasemalle kirjautumiseen, uloskirjautumiseen sekä työaseman sammuttamiseen ja käynnistämiseen liittyen. Jokaiseen tapahtumaan liittyvä lokimerkintä sisältää aikaleiman sekä työaseman ja käyttäjän yksilöivän tunnistetiedon. Lokimerkinnät säilyvät, kunnes työasema asennetaan uudestaan tai loki saavuttaa ennalta määritellyn ylärajan merkintöjen enimmäismäärälle, jonka jälkeen vanhimpia merkintöjä aletaan ylikirjoittaa. Työasemien tapahtumalokien merkintöjä satunnaisotantana tarkastelemalla pääteltiin, että organisaation työasemilla yläraja saavutetaan keskimäärin noin 6-12 kuukauden käytön jälkeen.

Intervention vaikutuksen seuraamista varten luotiin datankeruujärjestelmä, joka hyödynsi työasemien tapahtumalokeja. Järjestelmä voidaan jakaa kahteen komponenttiin: asiakasohjelmaan ja palvelimeen. Organisaation Windows-työasemille asennetun asiakasohjelman tehtävänä oli kerätä työaseman tapahtumalokista määrätyt lokirivit ja lähettää ne päivittäin palvelimelle prosessoitavaksi. Tämän jälkeen palvelinkomponentti käsitteli työasemien lähettämät tiedot ja tallensi ne Microsoft SQL Server –pohjaiseen tietokantaan. Järjestelmä konfiguroitiin keräämään lokirivit liittyen seuraaviin tapahtumiin:

- Sisään- ja uloskirjautuminen (Logon / Logoff)
- Työaseman lukitseminen ja lukituksen avaaminen (Lock / Unlock)
- Työaseman sammuttaminen ja kaatuminen (Power off / Power off unexpected)
- Työaseman käynnistäminen (Power on)

Tiedonkeruun kattavuuden ja tietojen eheyden seurantaa varten asiakasohjelmaan lisättiin ominaisuus, joka ilmoitti tiedonkeruupäivän lisäksi ajankohdan, josta lähtien lokitapahtumat oli kerätty. Nämä aikaleimat kerättiin palvelimella tietokantaan erilliseen tauluun, jonka avulla oli mahdollista havaita, mikäli lokitiedoissa olisi katkoja tai puutteita jonkin työaseman kohdalla.

Järjestelmän toimintavarmuuden kasvattamiseksi asiakasohjelma määriteltiin keräämään ja lähettämään lokitiedot siten, että ne sisälsivät kahden päivän päällekkäisyyden edellisen lähetyksen kanssa. Tästä aiheutuvat duplikaatit raportoiduissa tapahtumissa huomioitiin määrittelemällä tietokannan tauluun tallennettaville riveille rajoite (engl. constraint), joka vaatii jokaisen tallennettavan rivin olevan uniikki kaikilta tietokentiltään. Lisäksi taulun asetuksiin määriteltiin, että duplikaatit sivuutetaan (engl. ignore). Näin jokainen tapahtuma tallentui tietokantaan vain yhden kerran.

Datankeruujärjestelmän luotettavuuden ja tietojen oikeellisuuden varmistamiseksi työasemilta kerättiin testidataa muutaman kuukauden ajan ennen varsinaisen tutkimuksen aloittamista. Tätä dataa ei sisällytetty lopulliseen havaintoaineistoon, vaan sen ja keräämisestä tehtyjen lokimerkintöjen avulla varmistettiin, ettei kerätyissä tapahtumissa ollut katkoja ajallisesti. Datalle tehtiin myös manuaalinen tarkistus vertaamalla sitä tutkimuksen tekijöiden testikäytössä olleiden työasemien tapahtumalokien merkintöihin.

Testausvaiheen jälkeen tietokantaan sisällytettiin automatiikka, jolla kaikki kerätty data anonymisoitiin. Henkilötietoja sisältävää dataa ei käsitelty tai käytetty tämän tutkimuksen yhteydessä.

7.4.2 Tietoturva ja yksityisyys

Dataa kerättäessä ja tutkimuksen datankeruujärjestelmää suunniteltaessa kiinnitettiin erityistä huomiota järjestelmän tietoturvallisuuteen sekä organisaation työntekijöiden yksityisyyden säilyttämiseen.

Tietokantaan pääsy oli teknisesti rajattu vain organisaation turvalliseen sisäverkkoon eikä tietokantaan ollut käyttöoikeuksia muilla kuin tutkimuksen tekijöillä. Tietokannan tarkastelu oli mahdollista ainoastaan palvelinkoneelta, ja kaikki etäyhteydet tietokantapalveluun oli estetty. Työasemille asennettu datankeruukomponentti suoritti toimintonsa järjestelmätunnuksen oikeuksilla ja siirsi keräämänsä datan palvelinkomponentin käsiteltäväksi vain työaseman ollessa organisaation omassa sisäverkossa. Näiden toimien avulla varmistettiin, ettei tietoihin ollut pääsyä ulkopuolisilla. Tutkimuksessa hyödynnettiin ainoastaan sellaista tietoa, joka syntyy oletusarvoisesti työaseman käytön aikana ja vain siinä laajuudessa, kuin oli tutkimuksen kannalta tarpeellista.

Tutkimuksessa käsiteltiin ainoastaan anonymisoitua dataa, jonka sisältämiä tunnisteita ei ollut mahdollista yhdistää takaisin organisaation työntekijöihin tai heidän käyttämiinsä työasemiin eikä se siten sisältänyt mitään henkilötiedoiksi luettavaa tietoa (Yhteiskuntatieteellinen tietoarkisto, 2018). Anonymisointi toteutettiin teknisesti korvaamalla automaattisesti kaikki kerätyn datan sisältämät alkuperäiset tunnistetiedot juoksevaan numerointiin perustuvilla tunnistenumeroilla, jonka jälkeen kaikki tiedot numeroinnin ja tunnistetietojen välisestä yhteydestä tuhottiin. Samalla tavalla anonymisoitiin myös tiedot siitä, mikä interventioviesti kullekin käyttäjälle oli lähetetty. Tehty anonymisointi oli siis luonteeltaan peruuttamaton.

7.5 Havaintoaineiston muodostaminen kerätystä datasta

Tässä luvussa kuvataan tulosten analysoinnissa käytetyn havaintoaineiston muodostaminen kerätystä datasta. Kerätty raakadata koostui 3,5 miljoonasta tietokantarivistä, joista jokainen vastasi yhtä tapahtumaa havaintojaksolla eli aikavälillä 20.3.2017 – 31.1.2018. Kerätty, anonymisoitu data vietiin tietokannasta R-ohjelmistoon, jolla kaikki tutkimusta varten tehty datan käsittely ja analysointi suoritettiin[1].

Havaintoaineiston muodostaminen koostui kolmesta päävaiheesta: sessioiden muodostaminen, lukitusten liittäminen sessioihin sekä sessioiden rajaamisen analyysiä varten.

7.5.1 Sessioiden muodostaminen

Sessiolla tarkoitetaan sisäänkirjautumistapahtuman ja uloskirjautumistapahtuman välistä aikaa, jonka yksittäinen käyttäjä on ollut tietylle työasemalle kirjautuneena. Tästä voidaan käyttää myös nimitystä kirjautumissessio tai istunto. Sessio määrittää siis aikavälin, jona työasema oli kyseisen henkilön käytössä. Yhdellä käyttäjällä on mahdollista olla useita yhtäaikaisia sessioita eri työasemilla.

Sessioiden muodostamiseksi sisään- ja uloskirjautumistapahtumat järjestettiin jokaisen työaseman ja käyttäjän osalta aikaleiman perusteella. Tämän jälkeen järjestyksessä peräkkäiset sisään- ja uloskirjautumistapahtumat yhdistettiin sessioksi, jolle annettiin tunnisteeksi juokseva sessionumero. Tilanteessa, jossa sisäänkirjautumista seurasi uusi sisäänkirjautuminen ilman uloskirjautumista, katsottiin session päättyneen työaseman virran odottamattomaan katkeamiseen tai käyttöjärjestelmän kaatumiseen. Epätavallisesti päättyneiden sessioiden päättymishetken määrittämiseksi hyödynnettiin työasemien sammutus- ja käynnistystapahtumien tietoja. Tässä yhteydessä kuitenkin huomattiin, että työaseman kaatumiseen liittyvät aikaleimatiedot eivät olleet luotettavia vaan käyttöjärjestel-

[1] Lopullinen, datan lataamiseen, käsittelyyn, analysointiin ja tutkimuksessa esitettyjen kuvien piirtämiseen käytetty, R-ohjelma koostui yli 1200 rivistä koodia.

män tekemiä arviota. Koska työaseman kaatumiseen päättyneitä sessioita havaittiin olevan vain vähän verrattuna sessioiden kokonaismäärään, ne päätettiin jättää kokonaan pois havaintoaineistosta. Tutkimukseen valittiin siis vain uloskirjautumiseen päättyneet sessiot, jotka perustuivat luotettaviin havaintoihin.

Yhteensä sessioita koko havaintojaksolla oli 357 828 kappaletta. Jokaiselle sessiolle laskettiin session kesto sisään- ja uloskirjautumisen aikaleimoista minuutin tarkkuudella. Lisäksi sessiolle määritettiin aloituspäivämäärä sisäänkirjautumistapahtuman perusteella. Sessiot sisälsivät myös tiedon siitä, mikä interventioviesteistä sessioon liittyvälle käyttäjälle oli lähetetty.

7.5.2 Työaseman lukitsemisten yhdistäminen sessioihin

Jokaiselle työasemien lukitsemistapahtumalle ja lukituksen avaustapahtumalle määritettiin sessio, jonka aikana lukitseminen tai avaaminen oli tapahtunut. Lukitustapahtumat liitettiin sessioihin käyttäen sessiolle annettuja sessionumeroita.[2] Yhteensä havaintojakson sessioiden aikana tehtiin yli 1,2 miljoonaa lukitus- ja avaustapahtumaa.

Organisaation työasemaympäristön konfiguraation perusteella tiedettiin, että työasemat lukittuivat automaattisesti viimeistään kahden tunnin inaktiivisuuden jälkeen. Eräästä työasemaympäristön hallintaan käytetystä järjestelmästä oli saatavissa koko havaintojakson ajalta tunneittain koostetut tiedot, jotka määrittivät, montako minuuttia vuorokauden kunkin tunnin aikana työasema oli ollut aktiivisessa käytössä. Aktiivisuustietojen avulla todennäköisesti automaattisiksi lukituksiksi tunnistettiin noin 1,4 prosenttia kaikista lukituksista ja nämä jätettiin havaintoaineiston ulkopuolelle. On kuitenkin syytä huomioida, että havaintoaineistoon sisällytetyistä lukituksista osa oli edelleen automaattisia. Ensinnäkin käyttäjien oli mahdollista säätää itse työasemansa automaattisen lukkiutumisen aikaviivettä lyhemmäksi. Lisäksi vähintään osalla organisaation Windows 10 -työasemista lukkiutumisen viive oli jo oletuksena lyhyempi, kuin yleisen konfiguraation määrittämä kahden tunnin maksimiviive.

Vastaavalla tavalla, kuten sessioita muodostettaessa, muodostettiin lukitsemistapahtumista ja lukituksen avaustapahtumista ”lukitsemissessioita” eli aikavälejä, joina työasema oli ollut lukittuna. Näiden avulla jokaiselle kirjautumissessiolle laskettiin tehtyjen lukitusten yhteismäärä sekä lukitusten yhteiskesto minuuteissa.

7.5.3 Sessioiden rajaaminen analyysiä varten

Havaintoaineistoon sisällytettävät sessiot rajattiin seuraavaksi kuvailtavien periaatteiden mukaisesti. Rajauksessa käytetyt ehdot on koostettu taulukkoon 6.

---

[2] Neljää rinnakkaista säiettä käyttäen neljännen sukupolven Intel i5 suorittimella, 16 gigatavun keskusmuistilla ja nopealla SSD-levyllä varustettu työasema suoritti käytetyn R-koodin noin neljässä tunnissa. Lukitustapahtumat liitettiin sessioihin käymällä kaikki lukitustapahtumat läpi ja etsimällä työasema- ja käyttäjätiedon sekä aikaleiman perusteella oikea sessio.

Analyysin yksinkertaistamiseksi havaintoaineiston ulkopuolelle rajattiin yli 720 minuuttia kestäneet sessiot, joita kaikista sessioista oli noin 9%. Tätä pidemmistä sessioista suurin osa oli useamman, keskimäärin viiden, vuorokauden pituisia sessiota, joiden aikana työasema oli lukittu työpäivän päätteeksi tai esimerkiksi viikonlopun ajaksi. Rajaamalla sessiot korkeintaan yhden työpäivän pituisiksi voitiin analyysissä käyttää sessioiden aloituspäivämäärää aikasarjaan sijoittamisessa. Lisäksi kerätyn aineiston perusteella havaittiin, että pitkiä sessioita tehneet käyttäjät olivat jo valmiiksi keskimääräistä useammin työasemaansa lukitsevia eivätkä siten edustaneet interventioiden pääasiallista kohderyhmää.

Tarkasteltavien sessioiden kestolle määritettiin myös 180 minuutin alaraja. Tätä lyhyempiä sessioita koko havaintojaksolla oli 46%. Alarajan tarkoituksena oli jättää tarkastelun ulkopuolelle sessiot, joissa työasemaa oli käytetty vain hetkellisesti. Tällaiset sessiot eivät olisi välttämättä olleet vertailukelpoisia pidempien sessioiden kanssa, sillä niiden aikana käyttäjällä ei ehkä olisi ollut tarvetta poistua työaseman luota lainkaan. Tarkasteluun haluttiin valita vain sessiot, joissa työasema todennäköisesti olisi pitänyt lukita vähintään kerran.

Session aloituspäivämäärän perusteella havaintoaineistosta rajattiin pois viikonloppuna ja arkipyhinä tapahtuneet sessiot. Organisaation toiminta keskittyi pääasiassa arkipäiville, joten tarkastelu haluttiin rajoittaa vain näihin. Muiden kuin arkipäivien päivittäiset käyttäjämäärät olivat alustavan tarkastelun perusteella huomattavasti arkipäiviä alempia, joten ne olisivat aiheuttaneet dataan ylimääräistä hajontaa. Rajauksen perusteella 5,5% havaintojakson sessioista jätettiin tarkastelun ulkopuolelle.

Lopuksi havaintoaineistosta rajattiin pois sessiot niiltä 310 käyttäjältä, joille yhden tai useamman interventioviestin lähettäminen oli epäonnistunut teknisistä tai muista syistä. Näiden käyttäjien osalta tiedettiin siis varmasti, että he eivät olleet saaneet kaikkia kolmea interventioviestiä. Rajaus koski noin 5% kaikista havaintojakson sessioista.

Analyysissä käytetty lopullinen havaintoaineisto muodostui 149 538 sessiosta. Havaintoaineisto käsitti yhteensä 1881 käyttäjän tekemät sessiot, joiden aikana tehtiin yhteensä 291 705 lukitusta.

TAULUKKO 6 Havaintoaineiston rajaamisessa käytetyt ehdot

Rajaava tekijä	Ehto	Pois rajautuneiden osuus	Perustelut
Session kesto (yläraja)	t < 720 min	9 %	Analyysin yksinkertaistaminen; pitkiä sessioita tekevät valmiiksi paljon lukitsevia
Session kesto (alaraja)	t > 180 min	46 %	Lyhyiden sessioiden aikana ei todennäköistä tarvetta poistua työasemalta
Session päivämäärä	Vain arkipäivät	5,5 %	Organisaation toiminta keskittynyt pääasiassa arkipäiville
Viestien lähettäminen	Kaikkien viestin lähettäminen onnistui	5%	Vain kaikki interventioviestit vastaanottaneet käyttäjät

8 ANALYYSI JA TULOKSET

Tässä luvussa analysoidaan tutkimuksessa kerätty havaintoaineisto tutkimuskysymyksiin vastaamiseksi. Luvussa esitetyt analyysit on tehty havaintoaineistosta, jonka muodostaminen havaintojaksolla kerätystä datasta on kuvattu luvussa 7.5. Havaintoaineisto koostui sessioista, joista jokaiseen liittyi taulukon 7 mukaiset tiedot.

TAULUKKO 7 Sessioihin liittyvät tiedot havaintoaineistossa

Tieto	Kuvaus
Session alkupäivämäärä	Päivämäärä, jonka perusteella sessio sijoitetaan kaikista sessioista muodostuvaan aikasarjaan.
Sisäänkirjautumisaika	Session aloittaneen sisäänkirjautumistapahtuman aikaleima.
Uloskirjautumisaika	Session päättäneen uloskirjautumistapahtuman aikaleima.
Session kesto	Session pituus minuutin tarkkuudella.
Lukitusten määrä	Session aikana tehtyjen lukitusten kappalemäärä.
Lukitusten yhteiskesto	Minuuttimäärä, jonka työasema oli session aikana lukittuna.
Session tunniste	Session yksilöivä tunnistenumero.
Käyttäjän tunniste	Käyttäjälle anonymisoinnissa annettu tunnistenumero.
Työaseman tunniste	Työasemalle anonymisoinnissa annettu tunnistenumero.
Interventioviestin numero	Tieto siitä, mikä interventioviesti käyttäjälle lähetettiin.

8.1 Lukitsemisaktiivisuus

Intervention tarkoituksena oli parantaa organisaation tietoturvaa vähentämällä tilanteita, joissa työaseman luota poistutaan lukitsematta sitä. Organisaatiossa henkilökunnan työtehtävät saattoivat kuitenkin olla hyvin vaihtelevia, jonka seurauksena työasemien käyttökään ei ollut säännöllistä. Näin ollen käytettävissä ei ollut tietoa siitä, kuinka monta kertaa kunkin käyttäjän ideaalitilanteessa olisi pitänyt lukita työasemansa. Todellisen lukitsemistarpeen selvittämiseksi olisi vaadittu tarkkailua, joka tämän tutkimuksen mittakaavassa ei olisi ollut mahdollista. Lisäksi on hyvin todennäköistä, että tämän tyyppiseen valvontaan olisi liittynyt myös laillisia ja eettisiä ongelmia.

Yleisesti ajatellen voidaan olettaa, että todennäköisyys tarpeelle poistua työaseman luota kasvaa työasemalla vietetyn ajan funktiona. Näin ollen myös tehtyjen lukitsemisten määrän pitäisi kasvaa käyttöajan lisääntyessä. Mikäli interventiolla siis saataisiin vaikutettua työasemien lukitsemiseen, voitaisiin vaikutus havaita tarkastelemalla muutoksia lukitusten määrässä suhteessa työasemien käyttöön. Näin ei siis tarvita tietoa siitä, kuinka monta kertaa työasema kunkin session aikana olisi pitänyt lukita.

Intervention vaikutuksen analysoimiseksi määriteltiin riippuva muuttuja keskimääräinen lukitsemisaktiivisuus, joka kertoo, kuinka monta lukitsemista jokaista kahdeksaa sessiotuntia kohti on keskimäärin tehty. Se siis ilmaisee, kuinka usein työasemia keskimäärin on yhden työpäivän aikana lukittu. Lukitsemisaktiivisuus voidaan määrittää halutun analyysitason mukaisesti joko sessiokohtaisesti, käyttäjäkohtaisesti tai esimerkiksi jollekin osajoukolle sessioita.

Keskimääräinen lukitsemisaktiivisuus A kahdeksaa sessiotuntia kohden saadaan laskemalla sessiossa tai sessioissa tehtyjen lukitusten kokonaismäärä ja jakamalla se session tai sessioiden yhteiskestolla minuutteina. Näin saatu lukema kerrotaan vielä 480:lla, jolloin saadaan lukitusten määrä kahdeksaa tuntia kohti. Matemaattisessa muodossa ilmaistuna keskimääräinen lukitsemisaktiivisuus A saadaan kaavalla

$$A = \frac{\sum_{i=0}^{n} N_i}{\sum_{i=0}^{n} t_i} \times 480,$$

jossa N_i on tarkasteltavan osajoukon i:nnen session lukitsemisten määrä ja t_i vastaavan session kesto minuuteissa. Osajoukko voidaan valita tarpeen mukaan esimerkiksi käyttäjän, käyttäjäryhmän, päivämäärän, aikavälin, käytetyn työaseman tai työaseman tyypin perusteella.

Keskimääräisen lukitsemisaktiivisuuden lukuarvon suhteuttamiseksi voidaan kuvitella hypoteettinen tilanne, jossa henkilö on kahdeksan tunnin työpäivän aikana pitänyt työehtosopimuksen hänelle oikeuttaman lounastauon ja kaksi kahvitaukoa. Oletetaan, ettei henkilön ole tarvinnut poistua työasemansa luota taukojen lisäksi muista syistä. Tällöin ideaalitapauksessa lukitsemisaktiivisuus A = 3 eli työasema on lukittu joka kerta sen luota poistuttaessa. Todellisuudessa työaseman luota poistumisen tarve ei kuitenkaan ollut sama koko organisaation henkilökunnalle ja todennäköisesti vaihteli myös päivän töitten mukaan. Tämän takia yksittäisten käyttäjien tunnollisuutta työaseman lukitsemisessa ei voida arvioida tai vertailla käyttäjien välillä suoraan keskimääräistä lukitsemisaktiivisuutta käyttäen. Koska tutkimuksessa interventioryhmät jaettiin satunnaisesti ja ryhmät olivat riittävän suuria, voidaan kuitenkin olettaa, että jokainen ryhmä jätti työasemansa lukitsematta keskimäärin yhtä usein ja siten intervention potentiaalinen vaikutus olisi kaikille ryhmille keskimäärin sama. Tällöin ryhmien välinen vertailu lukitsemisaktiivisuuden perusteella on mahdollista.

8.2 Käyttäjien luokittelu

Havaintoaineiston alustavassa analyysissä huomattiin, että intervention vaikutus eniten työasemia lukinneiden käyttäjien lukitsemisaktiivisuuteen oli hyvin vähäinen. On ilmeistä, että käyttäjien tunnollisuudessa työaseman lukitsemisen suhteen on eroja ja ennestään tunnollisiin käyttäjiin intervention vaikutuspotentiaali on pieni. Havainnon katsottiin viittaavan siihen, että työasemia harvoin tai ei lainkaan lukinneet eivät olleet keskimäärin yhtä tunnollisia lukitsijoita, kuin usein työasemia lukinneet.

Aiemman lukitsemisaktiivisuuden ja intervention yhteisvaikutuksen tutkimiseksi jokaiselle käyttäjälle määritettiin esitarkkailujakson ajalta keskimääräinen lukitsemisaktiivisuus, jonka perusteella käyttäjät luokiteltiin neljään luokkaan. Luokittelun haluttiin kuvaavan vakiintunutta käyttäytymistä, joten esitarkkailujaksolla alle 20 tuntia työasemaa käyttäneet henkilöt jätettiin luokittelematta. Luokituksen määrittäminen myös hyvin vähän tai ei ollenkaan työasemia ajanjaksolla käyttäneille henkilöille olisi saattanut aiheuttaa luokitteluun virhettä.

Taulukossa 8 on esitettynä käyttäjäluokat, luokittelurajat sekä kuhunkin luokkaan kuuluvien käyttäjien lukumäärä.

TAULUKKO 8 Käyttäjien luokittelu esitarkkailujakson lukitsemisaktiivisuuden perusteella

Käyttäjäluokka	Keskimääräinen lukitsemisaktiivisuus A	Käyttäjiä
Luokka 0 (ei lukituksia)	$A = 0$	339
Luokka 1 (alle 1 lukitus)	$0 < A < 1$	253
Luokka 2 (1-3 lukitusta)	$1 \leq A < 3$	372
Luokka 3 (yli 3 lukitusta)	$A \geq 3$	345
Ei luokiteltu (käyttötunteja < 20)	-	572
Kaikki käyttäjät	-	1881

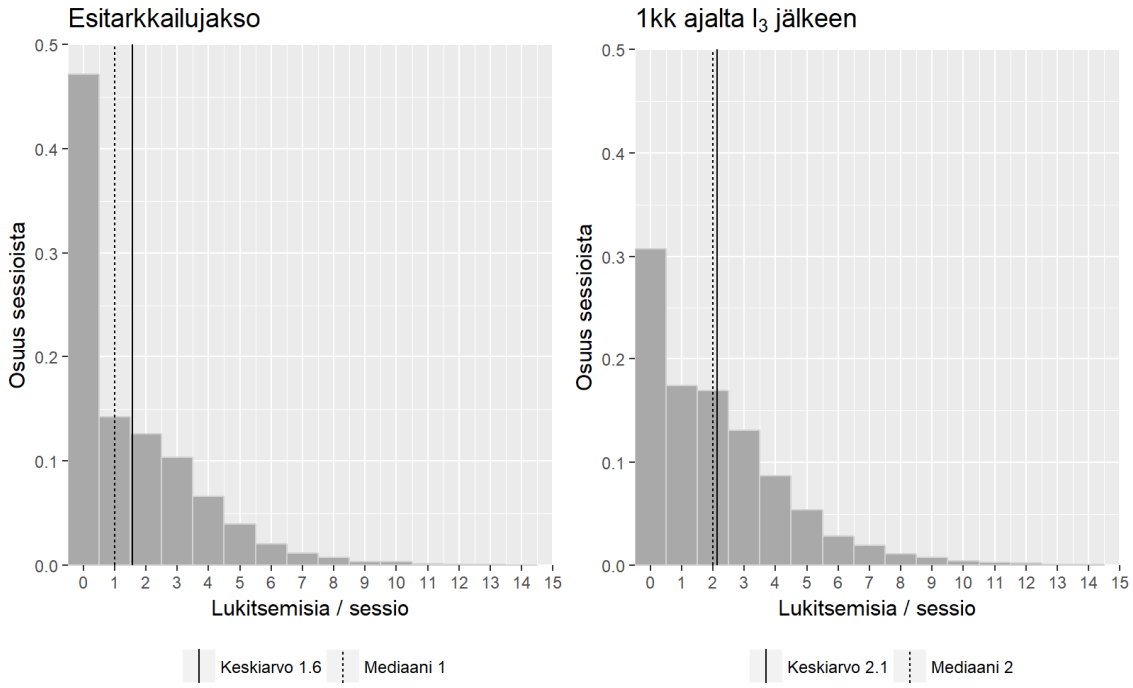
8.3 Esitarkkailujakson ja viimeisen intervention jälkeisen kuukauden vertailu

Havaintojaksolla tapahtuneen muutoksen kokonaissuuruuden hahmottamiseksi vertailtiin esitarkkailujaksoa ja kolmannen intervention jälkeistä yhden kuukauden ajanjaksoa kuuden eri tarkastelukohteen avulla. Näitä olivat yhden session aikana tehtyjen lukitusten kappalemäärä, session keston jakauma, yksittäisen lu-

kituksen keston jakauma, session aikana tehtyjen lukitusten yhteiskeston jakauma, session keskimääräisen lukitsemisaktiivisuuden jakauma sekä käyttäjien jakautuminen eri luokkiin.

Kuvioita tarkasteltaessa on syytä huomata, että ne ilmentävät vain havaitun muutosten kokonaissuuruutta. Arvioitaessa interventioiden vaikutuksen osuutta muutoksesta on huomioitava valittujen ajankohtien ajallinen etäisyys toisistaan. Esimerkiksi lukitusmäärien kokonaiskasvusta osa saattoi aiheutua Windows 10 -käyttöjärjestelmän yleistyessä mahdollisesti lisääntyneestä työasemien automaattisesta lukittautumisesta.

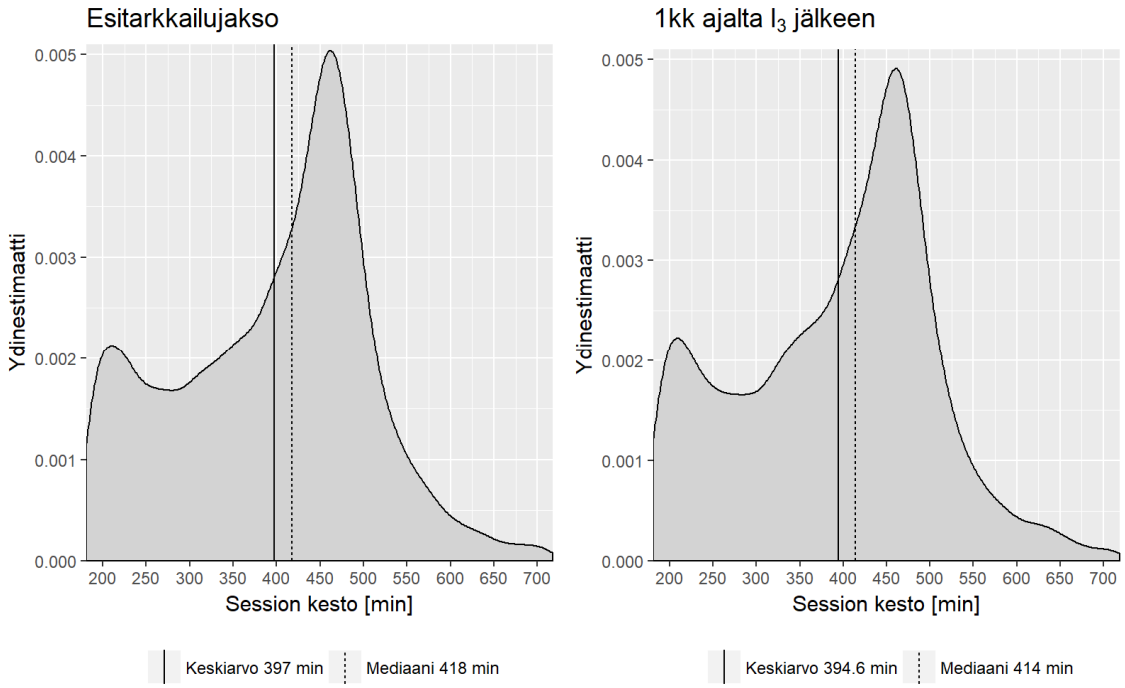
Kuviossa 7 on esitettynä histogrammina yhden session aikana tehtyjen lukitsemisten kappalemäärän jakauma esitarkkailujaksolla ja viimeisen intervention jälkeen. Lukitsemisten määrän keskiarvon ja mediaanin voidaan havaita kasvaneen selkeästi, mikä tarkoittaa työaseman lukitsemisten lisääntyneen havaintojaksolla. Histogrammista huomataan myös, että ei yhtään lukitusta sisältäneiden eli nollalukitussessioiden suhteellinen osuus laski selvästi, erityisesti yhdestä neljään lukitusta sisältäneiden sessioiden osuuden kasvaessa. Myös hyvin paljon lukituksia sisältäneiden sessioiden osuudet kasvoivat hieman.



KUVIO 7 Yhden session aikana tehtyjen lukitsemisten kappalemäärien jakauma esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen.

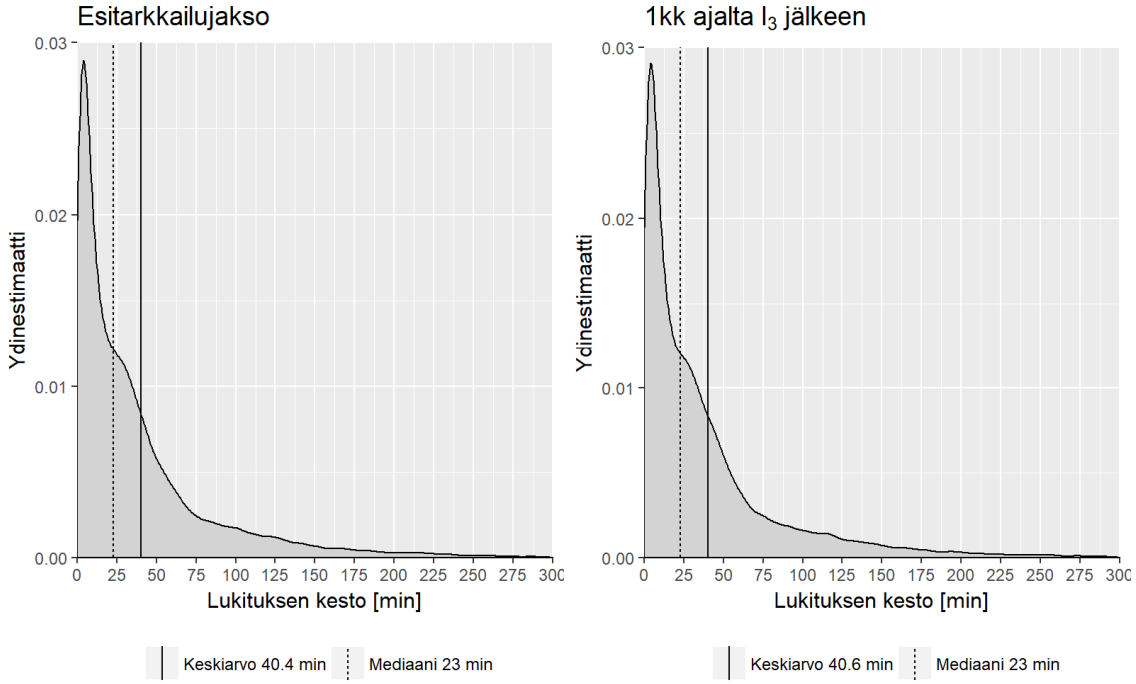
Kuviossa 8 on esitetty sessioiden keston jakauma ydinestimaattina esitarkkailujaksolla ja viimeisen intervention jälkeen. Ydinestimaatti voidaan käsittää histogrammin yleistykseksi jatkuvalle muuttujalle. Y-akselilta voidaan siis lukea tietyn pituisen session suhteellinen osuus tai yleisyys kaikista sessioista. Kuviosta havaitaan, että session keston jakaumassa ei tapahtunut merkittävää muutosta.

Interventiolla ei siis ollut tarkoittamatonta vaikutusta sessioiden kestoon. Keskimäärin yhden session pituus on molemmilla ajankohdilla hieman yli 6,5 tuntia. Sessiopituuden mediaani oli esitarkkailujaksolla 6 tuntia 58 minuuttia ja kolmannen intervention jälkeen 6 tuntia 54 minuuttia. Ydinestimaattikäyrän korkein kohta kuvaa suhteellisesti yleisintä sessiopituutta, joka oli molemmissa noin 7 tuntia 40 minuuttia. Lisäksi jakauman muodosta voidaan tehdä myös havainto siitä, että sessiopituus ei ollut normaalijakautunut. Jakaumaa tarkasteltaessa on syytä muistaa, että havaintoaineistosta on rajattu pois alle 180 minuutin ja yli 720 minuutin sessiot.



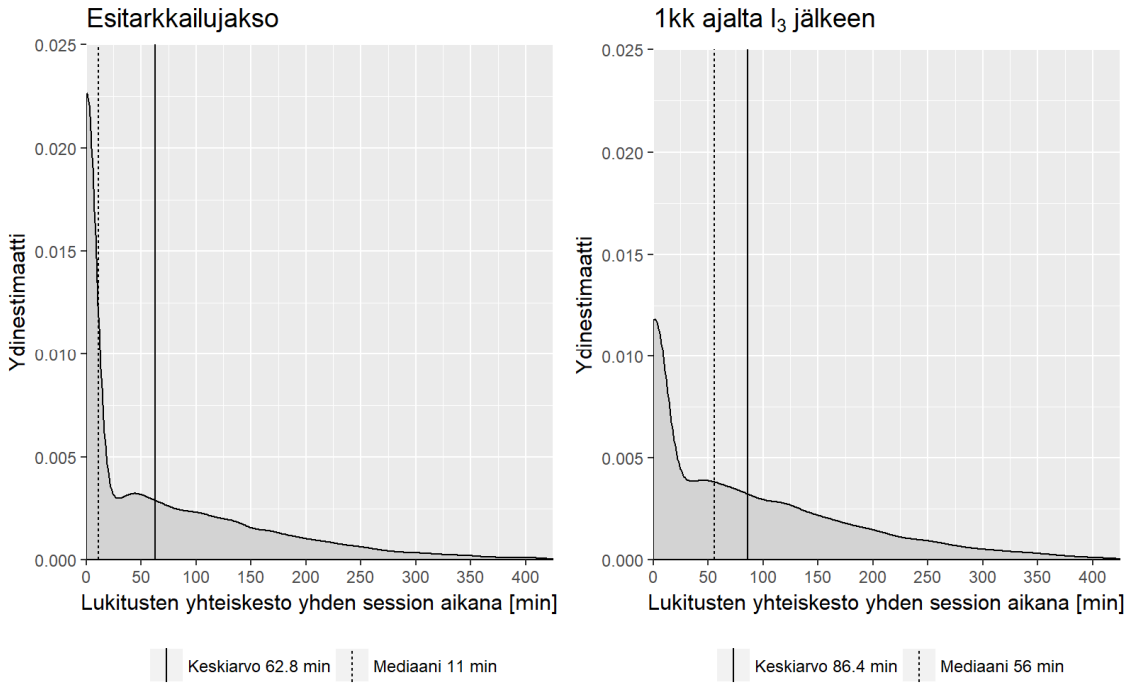
KUVIO 8 Sessioiden keston jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen.

Kuviossa 9 on yksittäisen työaseman lukituksen keston jakauma ydinestimaattina esitarkkailujaksolla ja viimeisen intervention jälkeen. Kuviosta nähdään, ettei yksittäisen lukituksen keston keskiarvo tai mediaani käytännössä muuttuneet kokeen aikana. Interventioilla ei siis ollut vaikutusta yksittäisen lukituksen kestoon, vaan mahdollinen vaikutus ilmeni lukitusten määrään lisääntymisenä. Jakauman muodosta nähdään, että suurin osa lukituksista oli melko lyhyitä kummallakin jaksolla.



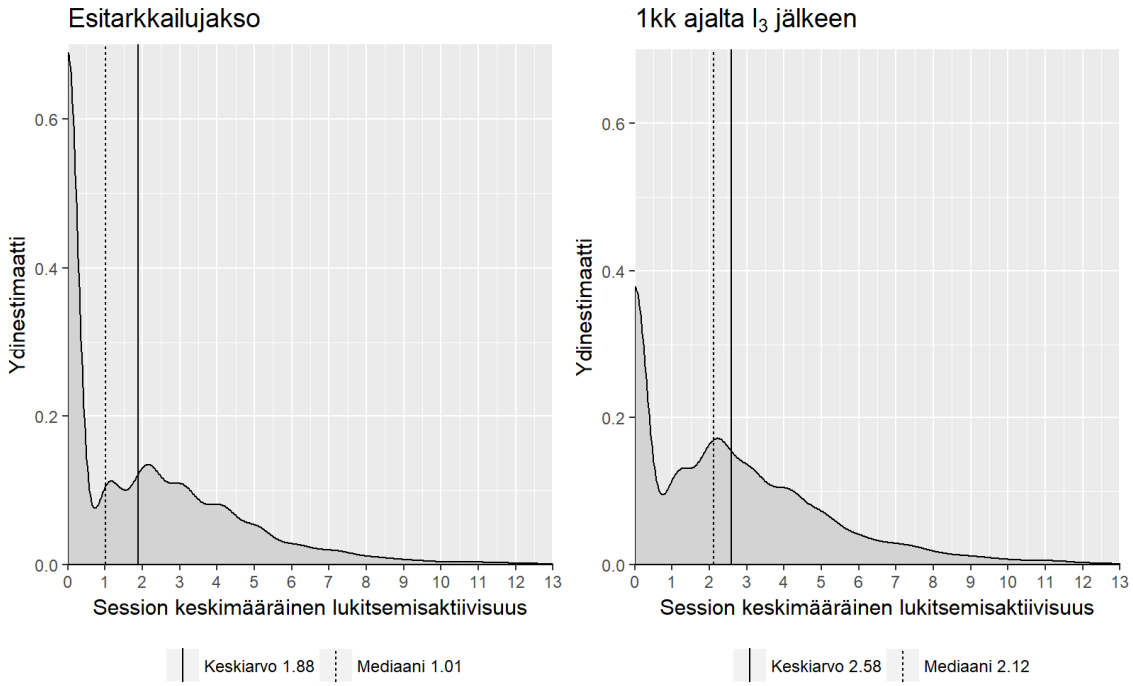
KUVIO 9 Yksittäisen lukituksen keston jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen.

Kuviossa 10 on esitettynä yhdessä sessiossa tehtyjen lukitusten yhteiskeston jakauma ydinestimaattina esitarkkailujaksolla ja viimeisen intervention jälkeen. Keskiarvon ja varsinkin mediaanin havaittiin kasvaneen merkittävästi. Viimeisen intervention jälkeen työasemat olivat siis suuremman osan sessiosta lukittuna kuin esitarkkailujaksolla. Lisäksi jakauman muotoja vertailemalla havaitaan, että hyvin vähän tai ei lainkaan lukittunaoloaikaa sisältäneiden sessioiden suhteellinen osuus väheni merkittävästi.



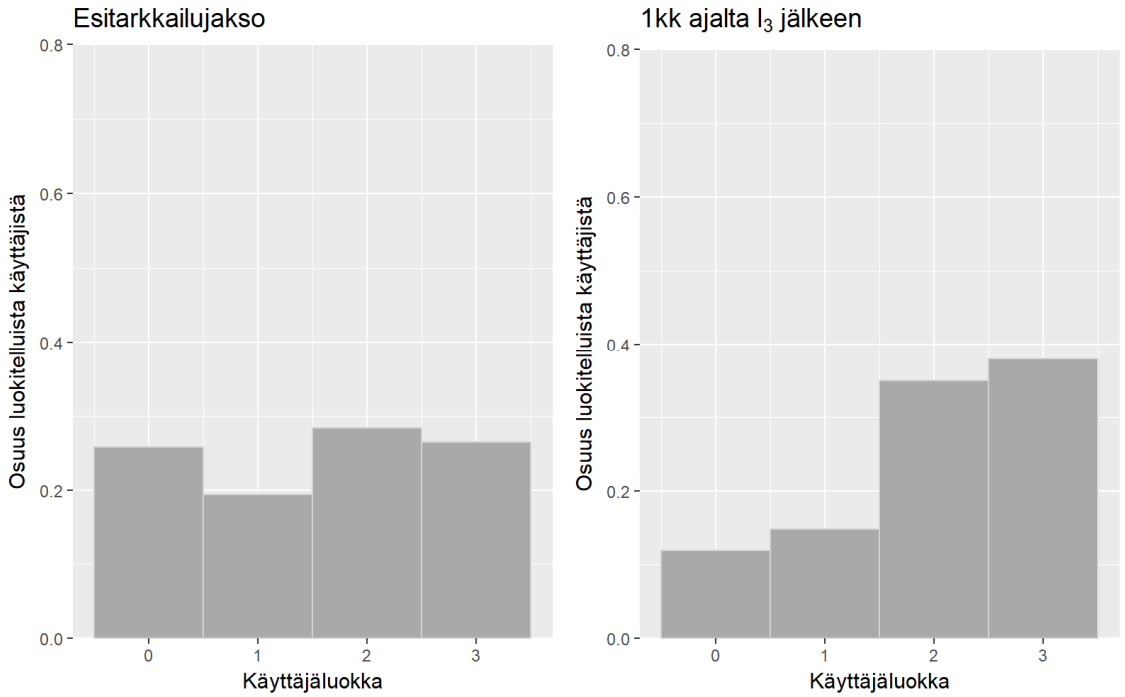
KUVIO 10 Yhden session aikana tehtyjen lukitusten yhteiskeston jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen.

Kuviossa 11 on esitettynä sessiokohtaisen keskimääräisen lukitsemisaktiivisuuden jakauma ydinestimaattina esitarkkailujaksolla ja viimeisen intervention jälkeen. Jakauma on muodostettu laskemalla aluksi kummankin ajanjakson jokaiselle sessiolle keskimääräinen lukitsemisaktiivisuus, eli kuinka monta lukitusta sessiossa oli kahdeksaa tuntia kohden. Tämän jälkeen keskimääräisestä lukitsemisaktiivisuudesta laskettiin ydinestimaattijakaumat molemmille jaksoille. Jakaumasta voidaan siis nähdä, kuinka suuressa suhteellisessa osassa sessioista oli tietty keskimääräinen lukitsemisaktiivisuus. Mediaanin ja keskiarvon havaittiin kasvaneen huomattavasti. Kun vertaillaan lisäksi jakauman muodon ja painopisteen muutosta, huomataan lukitsemisaktiivisuuden parantuneen. Tästäkin kuviosta voidaan nähdä, että täysin lukitsemattomien sessioiden suhteellinen osuus pieneni.



KUVIO 11 Sessiokohtaisesti määritetyn keskimääräisen lukitsemisaktiivisuuden jakauma ydinestimaattina esitettynä esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen.

Kuviossa 12 on käyttäjien jakautuminen käyttäjäluokkiin lukitsemisaktiivisuuden perusteella esitarkkailujaksolla ja viimeisen intervention jälkeen. Kummallakin ajanjaksolla luokitus määritettiin luvun 8.2 määrittelyn mukaisesti ja histogrammit muodostettiin luokkien kokojen suhteellisista osuuksista. Histogrammeissa ei huomioitu luokittelematta jääneitä käyttäjiä. Kuviosta nähdään luokkien 2 ja 3 suhteellisen osuuden kasvaneen merkittävästi ja luokkien 0 ja 1 osuuksien pienentyneen. Kokonaisuudessaan käyttäjien luokitus parani siis selvästi.



KUVIO 12 Käyttäjien jakautuminen käyttäjäluokkiin lukitsemisaktiivisuuden perusteella esitarkkailujaksolla ja viimeisen intervention (I_3) jälkeen.

Käyttäjien luokitukset esitarkkailujaksolla ja viimeisen intervention jälkeen ristiintaulukoitiin luokkien välisten siirtymien selvittämiseksi. Ristiintaulukointi on esitettynä taulukossa 9. Taulukosta voidaan lukea kustakin luokasta toiseen siirtyneiden määrä sekä suhteellinen osuus esitarkkailujakson luokkien koosta. Ristiintaulukoinnin avulla havaittiin, että suurin osa käyttäjistä paransi luokitustaan tutkimuksen aikana. Osalle esitarkkailujaksolla luokitelluille käyttäjille ei voitu määrittää viimeisen intervention jälkeistä luokitusta lainkaan, koska heidän kohdallaan 20 tunnin käyttöehto ei täyttynyt.

TAULUKKO 9 Käyttäjien jakautuminen luokkiin esitarkkailujakson ja viimeisen intervention (I_3) jälkeen ristiintaulukoituna, prosenttiosuudet suhteessa esitarkkailujakson luokitukseen.

	I_3 jälkeen					
Esitarkkailu-jakso	Luokka 0	Luokka 1	Luokka 2	Luokka 3	Ei luokiteltu	Yhteensä
Luokka 0	109 32,2%	74 21,8%	51 15,0%	46 13,6%	59 17,4%	339 18,0%
Luokka 1	16 6,3%	84 33,2%	84 33,2%	32 12,6%	37 14,6%	253 13,5%
Luokka 2	3 0,8%	13 3,5%	205 55,1%	99 26,6%	52 14,0%	372 19,8%
Luokka 3	1 0,3%	3 0,9%	43 12,5%	257 74,5%	41 11,9%	345 18,3%
Ei luokiteltu	22 3,8%	18 3,1%	64 11,2%	50 8,7%	418 73,1%	572 30,4%
Yhteensä	151 8,0%	192 10,2%	447 23,8%	484 25,7%	607 32,3%	1881

Lukitsemiskäyttäytymisen kokonaismuutos oli siis positiivista, kun vertaillaan viimeisen intervention jälkeistä kuukautta esitarkkailujaksoon. Vertailun perusteella havaittiin lukitsemisen lisääntyneen ja käyttäjien pääosin parantaneen luokitustaan. Session keskimääräinen kesto ja yksittäisen lukituksen kesto eivät muuttuneet kokeen aikana.

8.4 Lukitsemiskäyttäytyminen päivittäin tarkasteltuna

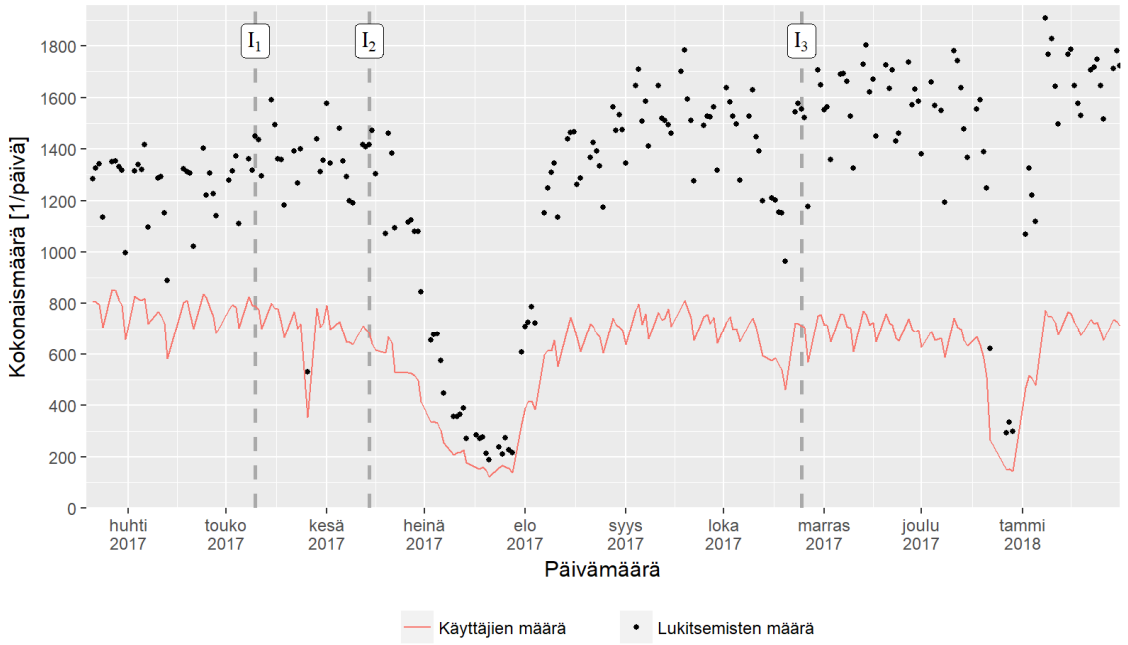
Tässä luvussa tarkastellaan päivittäistä lukituskäyttäytymistä tutkimuksen havaintojaksolla sekä arvioidaan interventioiden keskimääräistä vaikutusta lukitsemiseen ja täysin lukitsemattomien sessioiden määrään. Lopuksi käsitellään kontrolliryhmän lukitsemiskäyttäytymistä.

8.4.1 Lukitsemisten ja käyttäjien kokonaismäärät

Tässä alaluvussa esitetään päivittäisten lukitusten ja työasemia käyttäneiden käyttäjien kokonaismäärät kaikille käyttäjille sekä luvun 8.2. luokittelun mukaisesti jaoteltuna jokaiselle luokalle erikseen. Kaikkien käyttäjien joukko sisältää myös luvun 8.2 rajauksen perusteella luokittelematta jäävät käyttäjät. Tarkastelussa on huomioitu sessiot vain niiltä käyttäjiltä, joille lähetettiin jokin interventioviesteistä.

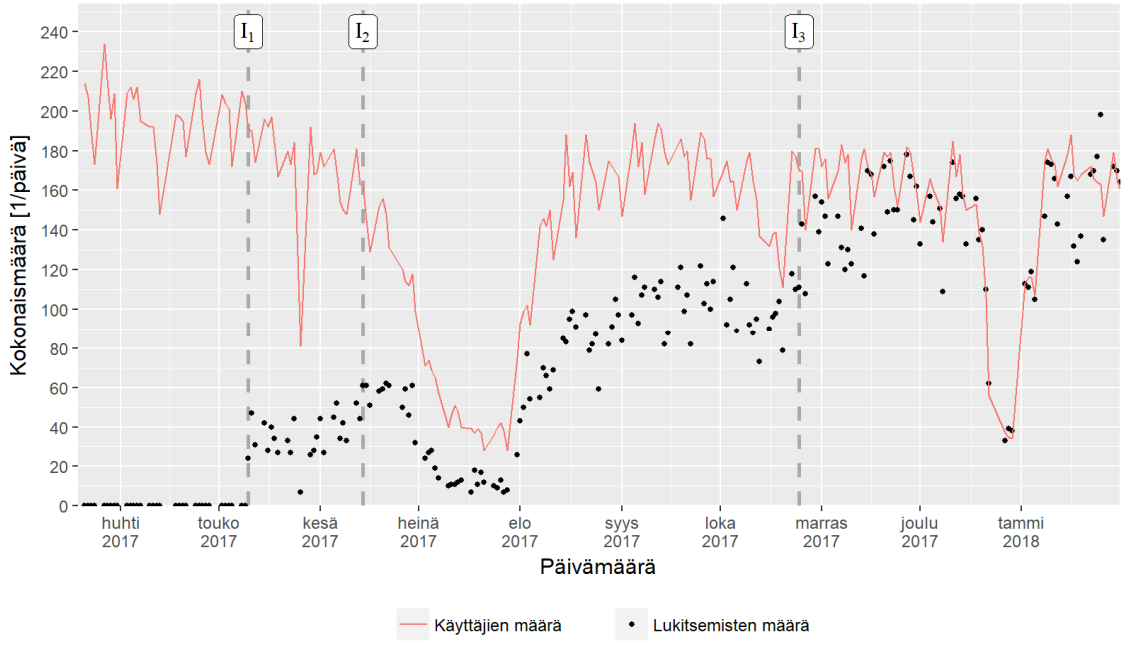
Kuviossa 13 on esitettynä kaikkien intervention kohteena olleiden käyttäjien päivittäiset lukitsemismäärät sekä käyttäjien määrät havaintojaksolla. Kuviosta havaitaan, että työasemia käyttäneiden käyttäjien päivittäinen kokonais-

määrä vaihteli merkittävästi viikonpäivän mukaan. Sen sijaan käyttäjien kokonaismäärän viikoittainen vaihtelu oli kesäloma-aikaa sekä joulua lukuun ottamatta pienehköä. Lukitsemisten päivittäisessä kokonaismäärässä havaitaan ensimmäisen intervention kohdalla nopea kasvu sekä kesäloman jälkeen jatkuva nouseva trendi. Kuvasta nähdään selvästi, että lukitusten päivittäistä kokonaismäärää voidaan pitää huonona mittarina intervention vaikutuksen arviointiin, koska päivittäiset käyttäjämäärät vaihtelivat havaintojaksolla. Tarkastelu otettiin mukaan kuitenkin, sillä se antaa hyvän yleiskuvan lukitsemiskäyttäytymisestä ja työasemien käytöstä havaintojaksolla.



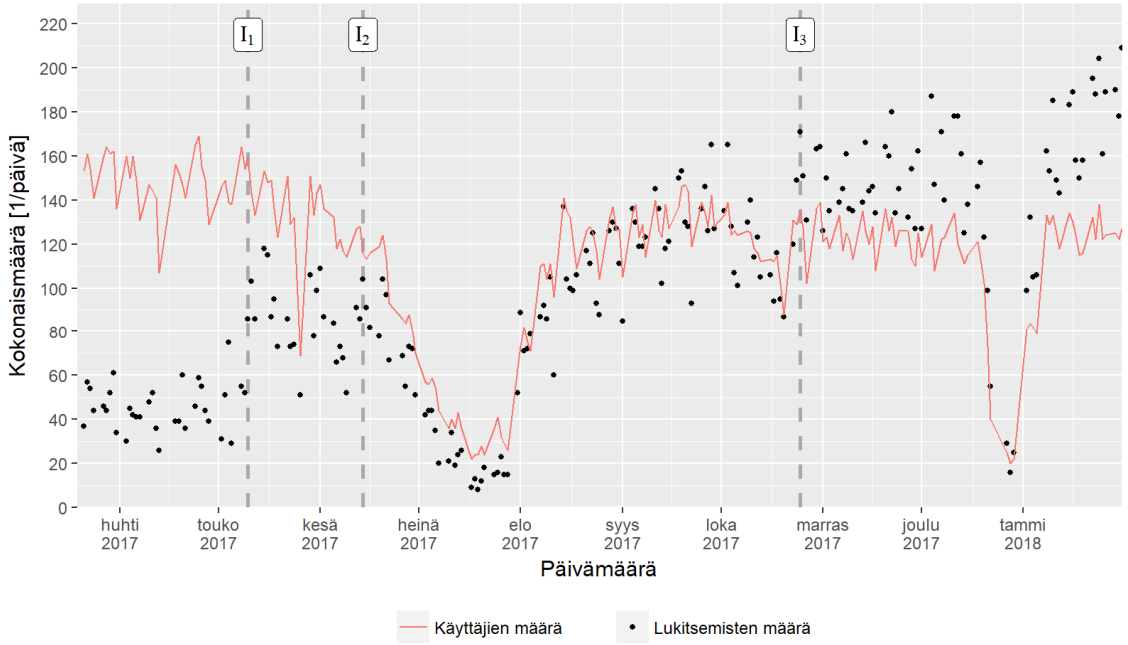
KUVIO 13 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä (yhteensä 1881 uniikkia käyttäjää).

Kuviossa 14 on esitettynä päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 0 käyttäjille. Tähän luokkaan kuului yhteensä 339 käyttäjää. Kuviosta havaitaan selvä lukitusten kokonaismäärien kasvu ensimmäisen ja kolmannen intervention kohdalla. Myös toisen intervention kohdalla lukitusmäärissä on havaittavissa kasvua, mikäli huomioidaan päivittäisten käyttäjien voimakkaasti laskeva trendi. Osa ensimmäisen intervention kohdalla tapahtuvasta noususta on luokkaan kuuluvien käyttäjien valinnasta johtuvaa harhaa, sillä luokka koostui käyttäjistä, jotka eivät olleet lukinneet työasemia kertaakaan ennen ensimmäisen intervention päivämäärää. Vastaava valinnasta johtuva harha vaikuttaa myös muista luokituksista tehtyihin kuvioihin. Päivittäisissä käyttäjien määrissä oli kuvion perusteella suurta vaihtelua tämän luokan osalta.



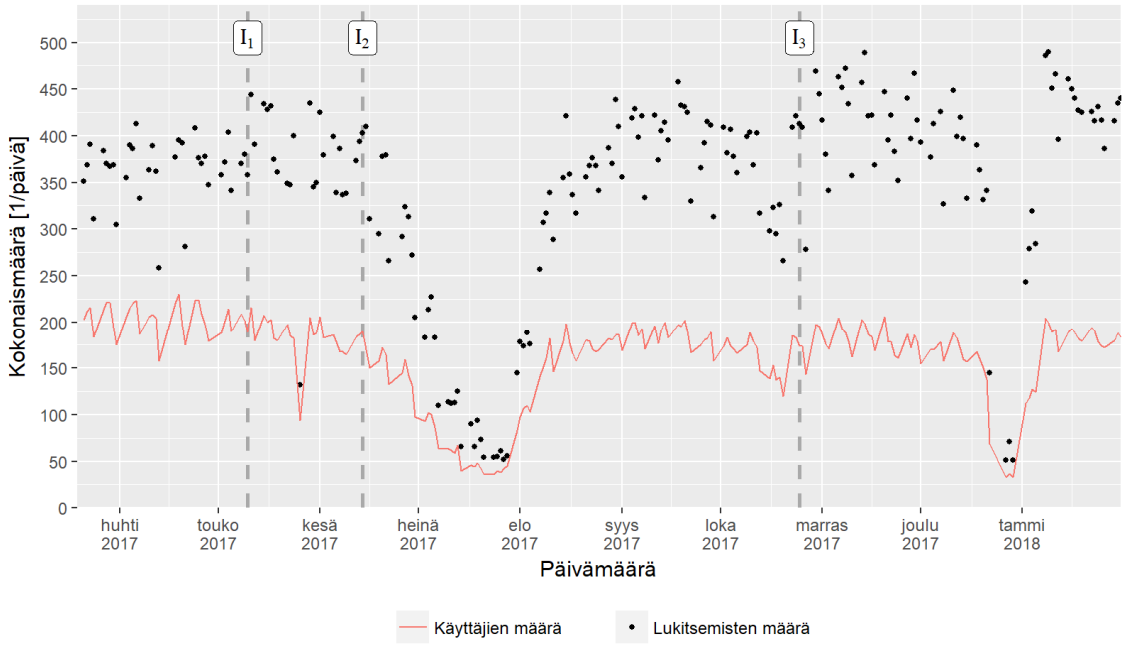
KUVIO 14 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 0 käyttäjille (yhteensä 339 uniikkia käyttäjää).

Kuviossa 15 on päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 1 käyttäjille, joita oli yhteensä 253 kappaletta. Ensimmäisen intervention kohdalla lukitsemisten kokonaismäärissä tapahtui selvä nousu. Toisesta ja kolmannesta interventiosta ei voida tehdä päätelmiä päivittäisten käyttäjämäärien vaihtelun vuoksi.



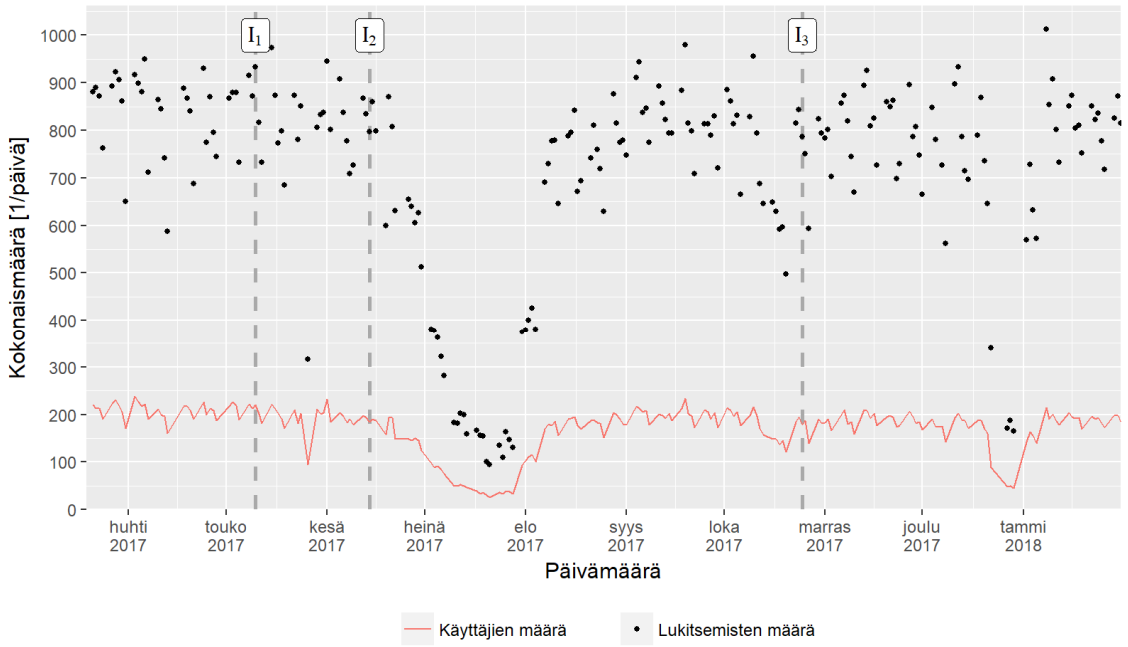
KUVIO 15 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 1 käyttäjille (yhteensä 253 uniikkia käyttäjää).

Kuviossa 16 on esitettynä luokan 2 päivittäisten lukitsemisten ja käyttäjien kokonaismäärät. Luokka koostui yhteensä 372 käyttäjästä. Kuviosta nähdään, että ensimmäisen intervention ajankohdalle ajoittui pieni nousu lukitusmäärissä. Toisen ja kolmannen intervention osalta vastaavaa päätelmää on hankala tehdä käyttäjämäärien vaihtelun vuoksi.



KUVIO 16 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 2 käyttäjille (yhteensä 372 uniikkia käyttäjää).

Kuviossa 17 on esitettynä päivittäiset lukitsemisten ja käyttäjien kokonaismäärät luokan 3 käyttäjille, joita oli yhteensä 345 kappaletta. Kuvion perusteella näyttäisi, ettei interventioilla ollut juurikaan vaikutusta kokonaismääriin tässä luokassa.



KUVIO 17 Päivittäinen lukitsemisten ja käyttäjien kokonaismäärä luokan 3 käyttäjille (yhteensä 345 uniikkia käyttäjää).

Lukitsemisten ja käyttäjien päivittäisten kokonaismäärien tarkastelun perusteella sekä käyttäjien että lukitsemisten kokonaismäärissä oli suurta päivittäistä ja kausittaista vaihtelua. Lukitsemisten kokonaismäärän suuri hajonta vaikeuttaa tulkintojen tekemistä tämän luvun kuvioiden perusteella. Näyttäisi kuitenkin siltä, että intervention vaikutus oli alemman luokituksen saanneille käyttäjille suurempi kuin korkeimman luokan käyttäjille.

8.4.2 Päivittäinen lukitsemisaktiivisuus

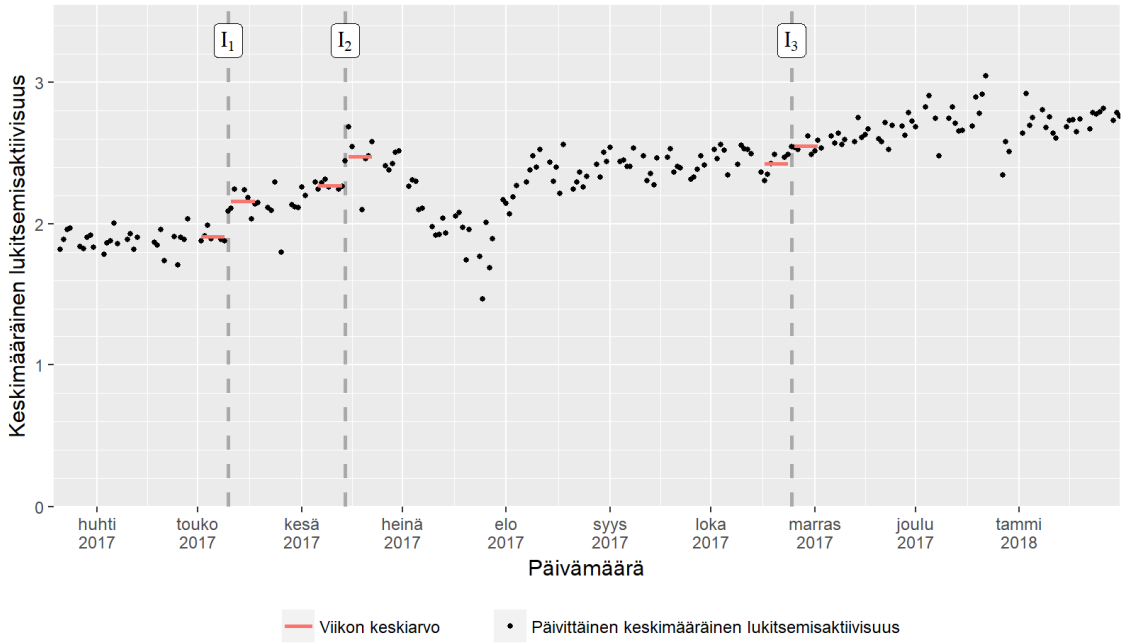
Lukitsemiskäyttäytymisen kehittymistä tarkkailujakson aikana tarkasteltiin myös laskemalla havaintojaksolle päivittäinen keskimääräinen lukitsemisaktiivisuus luvun 8.1 mukaisesti kunakin päivänä tehdyistä sessioista. Päivittäisten lukitsemisaktiivisuuden keskiarvojen lisäksi laskettiin vastaavasti myös viikoittaiset keskiarvot viikon ajalta ennen ja jälkeen jokaisen intervention (I_1-I_3).

Intervention potentiaalinen vaikutus lukitsemisaktiivisuuteen voidaan jakaa välittömään, porrasmaiseen muutokseen päivittäisessä lukitsemisessa sekä pidemmällä aikavälillä ilmenevään nousevaan tai laskevaan trendiin. Kokeessa ei kontrolloitu sähköpostiviestien lukemisajankohtaa, joten osa käyttäjistä saattoi reagoida viestiin vasta jonkin aikaa intervention jälkeen.

Tässä luvussa rajoituttiin tarkastelemaan lähinnä intervention lyhyen ajan keskimääräisiä vaikutuksia vertailemalla viikoittaisia keskiarvoja interventioiden kohdalla. Välittömiä vaikutuksia tarkasteltaessa mahdollisten kontrolloimattomien tekijöiden vaikutuksen voidaan olettaa olevan pieni ja lukitsemisaktiivisuuden porrasmaisen nousun ajallisesta korrelaatiosta interventioiden

kanssa voidaan siten tehdä myös kausaalisia päätelmiä. Pidemmän aikavälin tarkastelussa tutkimusasetelman tuntemattomien ja kontrolloimattomien tekijöiden mahdollinen vaikutus tekee interventioiden ja havaittujen muutostrendien välisen kausaalisen yhteyden tulkinnasta epävarmempaa. Tulkinnassa apuna käytettiin vertailua kontrolliryhmään, jonka päivittäinen lukitsemisaktiivisuus havaintojaksolla on esitetty luvussa 8.4.4. Vertailua vaikeutti jonkin verran kontrolliryhmän pienestä koosta johtuva hajonta.

Kuviossa 18 on esitettynä kaikkien käyttäjien keskimääräinen lukitsemisaktiivisuus havaintojaksolla. Viikoittaisen keskimääräisen lukitsemisaktiivisuuden muutokset interventioiden seurauksena olivat 0,25 (13 %), 0,20 (9 %) ja 0,12, (5 %). Kahden ensimmäisen intervention vaikutus näkyy kuviossa melko selvinä hyppyinä ja tämän perusteella voidaan todeta, että interventio vaikutti lukitsemiseen ja sen toistaminen vähintään yhden kerran oli kannattavaa. Yhteensä kaksi ensimmäistä interventiota nosti lukitsemisaktiivisuutta lähes 30%, mitä voidaan pitää huomattavana parannuksena. Kolmannen intervention kohdalla tapahtunut hyppy oli pienempi, mutta interventio näyttäisi aloittavan ainakin vuodenvaihteeseen jatkuvan nousevan trendin. Kesälomakaudella näkyvän muutoksen lukitsemisaktiivisuudessa arveltiin johtuvan todennäköisesti kesäajan pienemmästä tarpeesta poistua työpisteeltä.

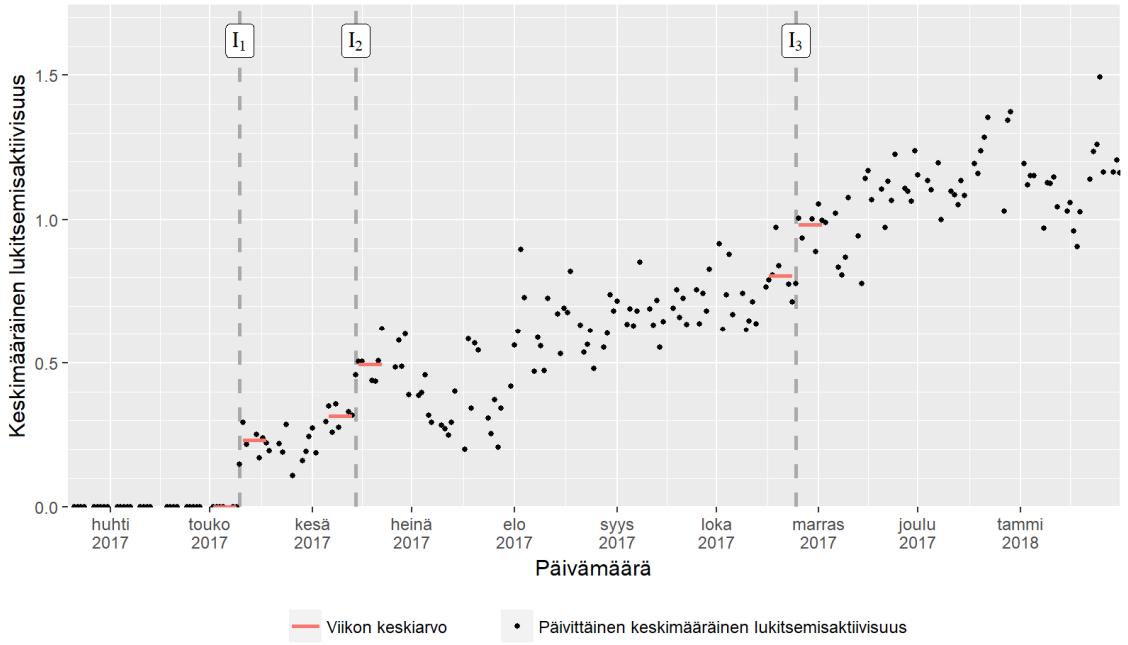


KUVIO 18 Keskimääräinen lukitsemisaktiivisuus päivittäin kaikille käyttäjille (yhteensä 1881 uniikkia käyttäjää).

Kuviossa 19 on esitettynä luokkaan 0 kuuluvien käyttäjien keskimääräinen päivittäinen lukitsemisaktiivisuus havaintojaksolla. Viikoittaisten keskiarvojen muutokset tässä luokassa olivat 0,23, 0,18 (57 %) ja 0,17 (22 %). Ensimmäisen interventiota seurannutta muutosta ei voitu määrittää prosentteina, sillä luokka

koostui ei koskaan työasemaansa lukinneista käyttäjistä. Havaintoaineiston perusteella kaikki interventiot vaikuttivat merkittävästi käyttäjiin toisen intervention jälkeisen viikkokeskiarvon ollessa yli kaksinkertainen verrattuna ensimmäisen intervention jälkeiseen viikkoon. Aiemmin työasemiaan lukitsemattomien käyttäjien muutoksen tarkastelu tukee selvästi havaintoa intervention toiston hyödyllisyydestä.

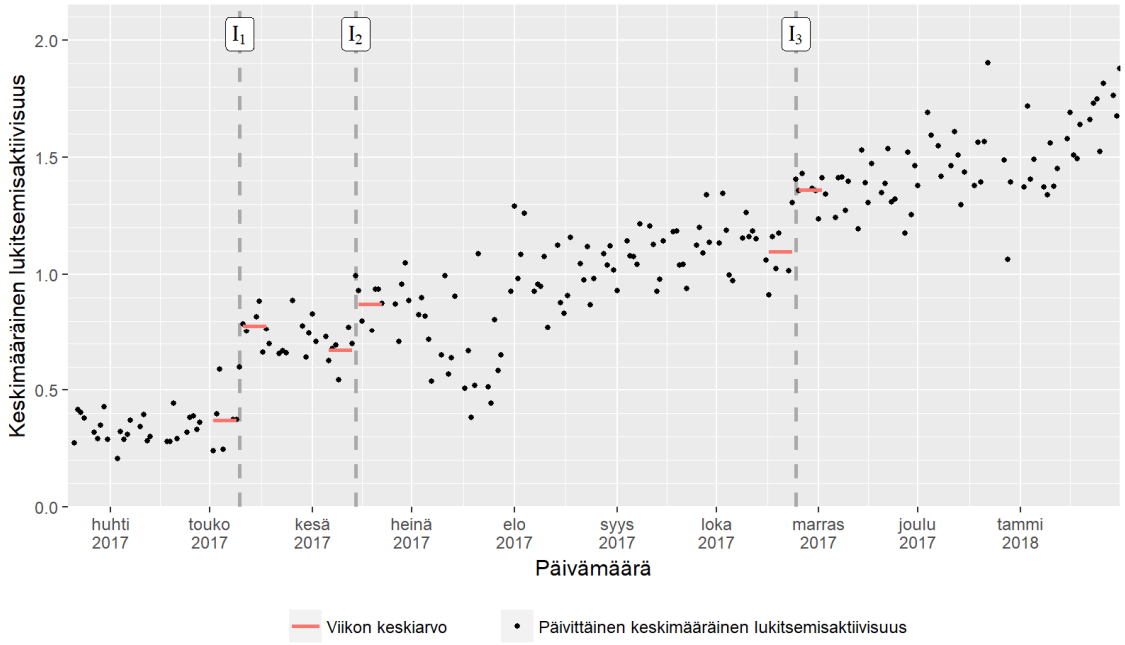
Luokan 0 käyttäjien lukitsemisaktiivisuudessa havaittiin voimakas nouseva trendi toisen intervention jälkeen. Tämän arveltiin vähintään osittain johtuneen Windows 10:n aiheuttamien automaattisten lukitsemisten lisääntymisestä. Kyseisessä käyttäjäluokassa päivittäiset lukitsemisaktiivisuudet olivat hyvin alhaisia, työasemia lukittiin intervention 2 jälkeen keskimäärin kerran kahdessa työpäivässä, joten yksikin päivittäinen automaattilukitus vaikuttaa keskiarvoon suuresti.



KUVIO 19 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 0 käyttäjille (yhteensä 339 uniikkia käyttäjää).

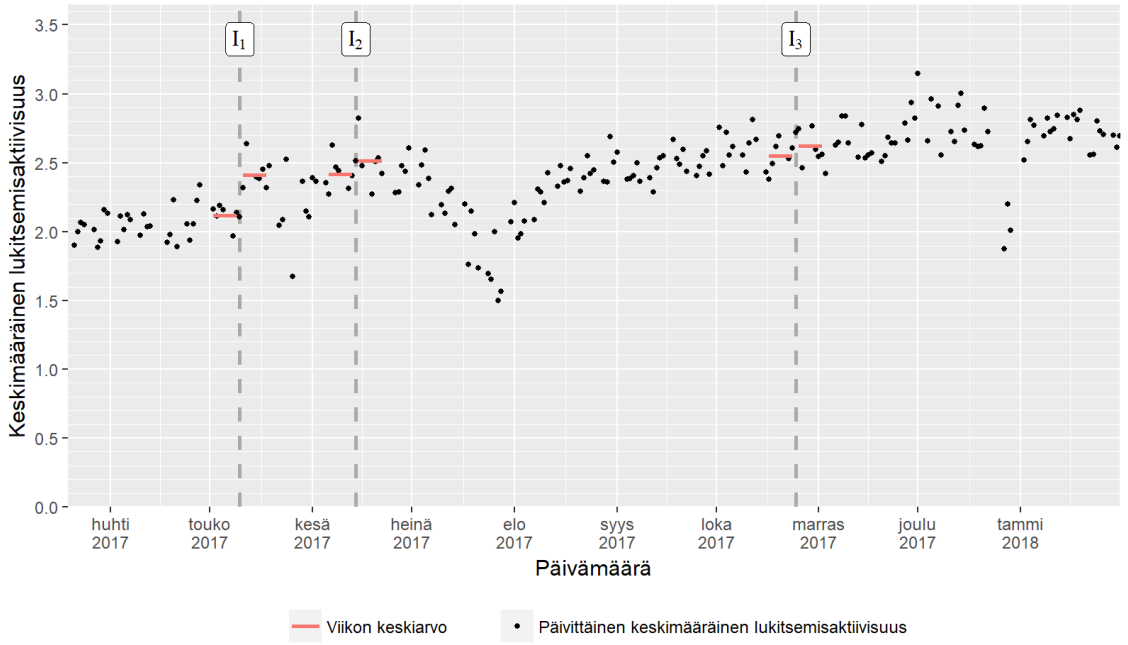
Kuviossa 20 on esitettynä luokkaan 1 kuuluvien käyttäjien keskimääräinen lukitsemisaktiivisuus havaintojaksolla. Viikoittaiset keskiarvot muuttuivat interventioissa 0,41 (109 %), 0,20 (30 %) ja 0,26 (24 %). Kuten luokan 0 osalta, myös käyttäjäluokassa 1 jokainen intervention toisto nosti merkittävästi työasemien lukitsemista ensimmäisen intervention yli tuplatessa aktiivisuuden. Ensimmäisen ja toisen intervention välistä ajanjaksoa tarkasteltaessa havaittiin pieni laskeva trendi. Havainto voisi viittaisi siihen, että tässä käyttäjäluokassa ensimmäisen intervention välitön vaikutus saattoi kääntyä laskuun intervention jälkeen. Eräs syy vaikutuksen vähentymiselle voisi olla esimerkiksi interventioviestin suositusten unohtuminen ajan kuluessa. Lukitsemisaktiivisuuden lasku oli kuitenkin

melko vähäistä, joten sen todellinen aiheuttaja saattoi hyvin olla myös jokin tuntemattomaksi jäänyt tekijä. Tämänkin käyttäjäluokan lukitsemisaktiivisuudessa havaittiin toisen intervention jälkeen alkava nouseva trendi.



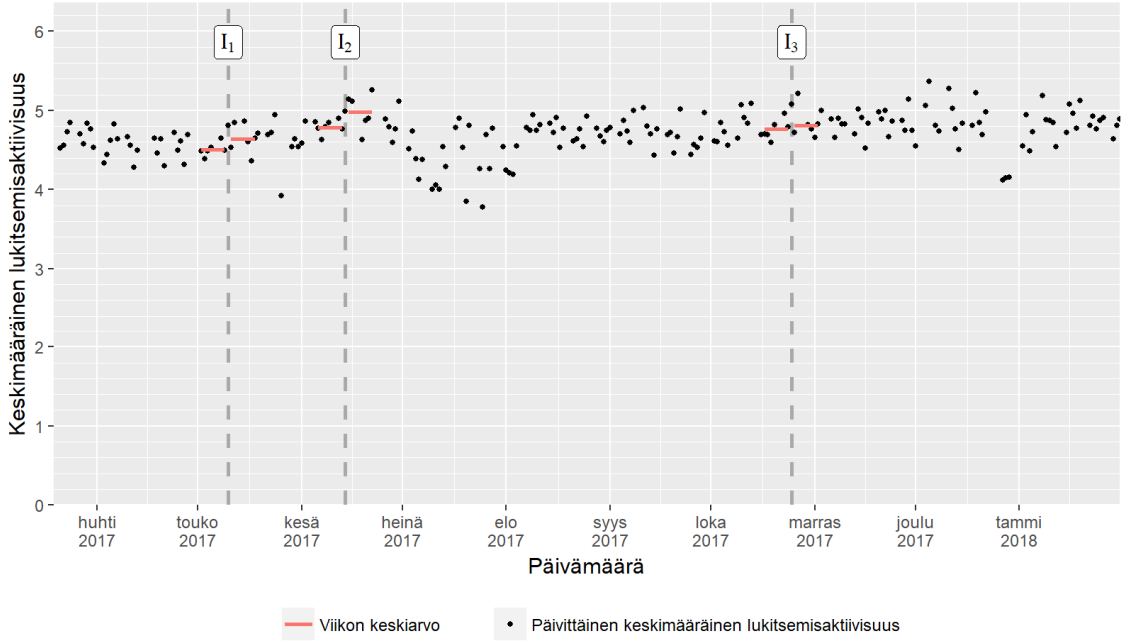
KUVIO 20 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 1 käyttäjille (yhteensä 253 uniikkia käyttäjää).

Kuviossa 21 on esitettynä luokkaan 2 kuuluvien käyttäjien keskimääräinen päivittäinen lukitsemisaktiivisuus. Viikoittaiset keskiarvot muuttuivat 0,29 (14 %), 0,10 (4 %) ja 0,07 (3%). Ensimmäisen intervention havaittiin vaikuttaneen selvästi lukitsemisaktiivisuuteen, mutta toisen ja kolmannen intervention kohdalla lukitsemisaktiivisuudessa ei havaittu selviä hyppyjä. Tälle luokalle intervention toistaminen ei siis välttämättä juuri lisännyt lukitsemista. Toistamisella ei kuitenkaan havaittu olevan negatiivisia vaikutuksia, joten muistutusviestien lähettämistä voitiin edelleen pitää kannattavana käytäntönä.



KUVIO 21 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 2 käyttäjille (yhteensä 372 uniikkia käyttäjää).

Kuviossa 22 on esitettynä aktiivisimpaan luokkaan 3 kuuluvien käyttäjien keskimääräinen päivittäinen lukitsemisaktiivisuus havaintojaksolla. Viikoittaisten keskiarvojen muutokset interventioissa olivat 0,14 (3 %), 0,20 (4 %) ja 0,01 (1 %). Havaintojen perusteella kahdella ensimmäisellä interventiolla saattoi olla lukitsemista lisäävä vaikutus, lukitseminen lisääntyi näissä yhteensä noin 8 prosenttia. Kolmannen intervention kohdalla ei havaittu kasvua lukitsemisaktiivisuudessa.

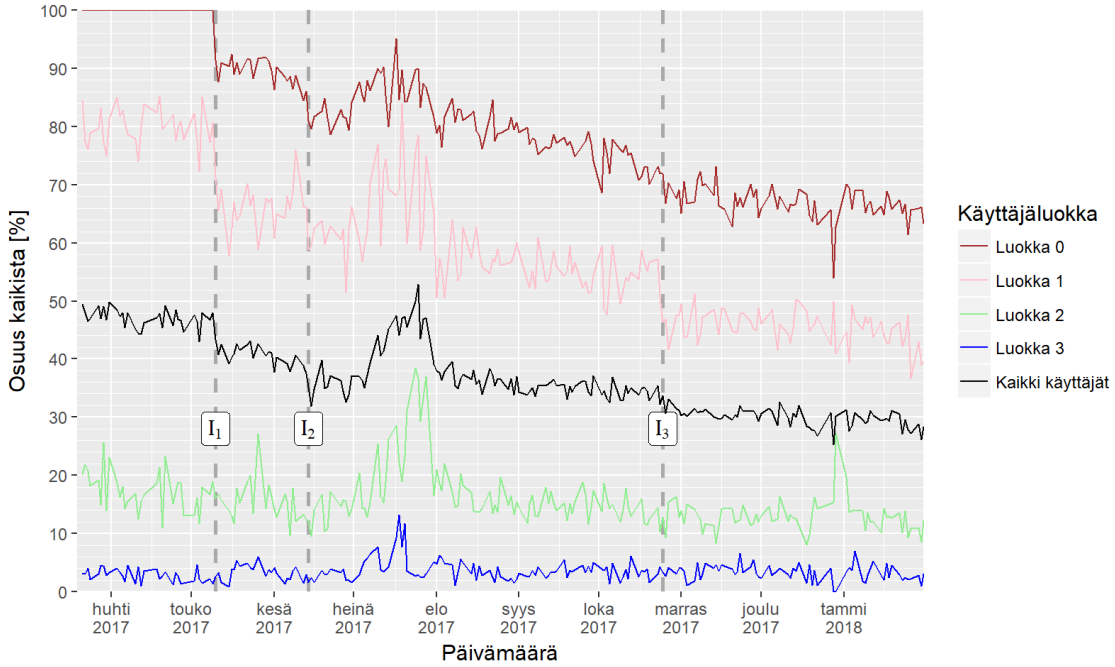


KUVIO 22 Keskimääräinen lukitsemisaktiivisuus päivittäin luokan 3 käyttäjille (yhteensä 345 uniikkia käyttäjää).

Päivittäistä lukitsemisaktiivisuutta ja viikoittaisia lukitsemisaktiivisuuden keskiarvoja tarkastelemalla huomattiin, että vähintään kahdella ensimmäisellä interventiolla oli selvä vaikutus työasemien lukitsemiseen. Kolmannen intervention vaikutus oli havaittavissa kahden alimman luokituksen käyttäjien joukossa. Tulokset osoittavat siis sen, että sähköpostitse tehtävällä tietoturvaviestinnällä voidaan vaikuttaa käyttäjien lukitsemiskäyttäytymiseen ja lähettämällä sama viesti useampaan kertaan voidaan tehostaa viestin vaikutusta.

8.4.3 Nollalukkosessioiden osuus

Kuviossa 23 on esitettynä nollalukkosessioiden eli kokonaan lukituksia sisältämättömien sessioiden osuus kaikista sessioista havaintojakson aikana.



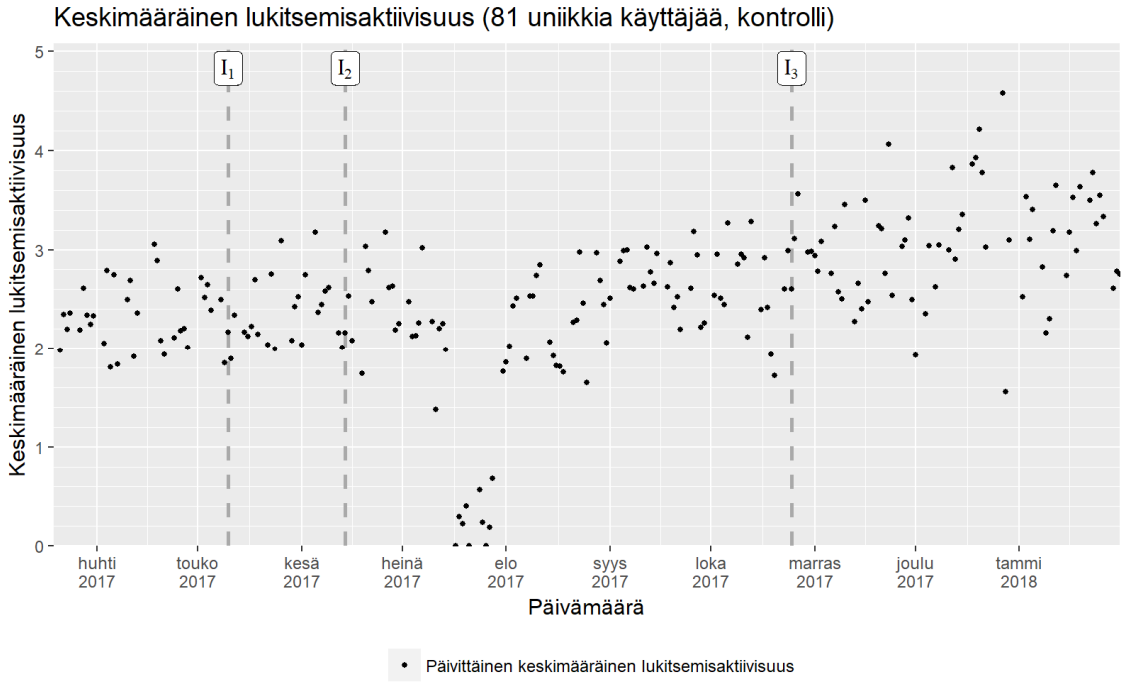
KUVIO 23 Nollalukkosessioiden osuus kaikista sessioista.

Kuviosta havaitaan, että kaikkien käyttäjien joukossa nollalukkosessioiden osuus oli lievässä laskussa jo ennen ensimmäistä interventiota. Ensimmäisen intervention kohdalla nollalukkosessioiden osuudessa tapahtui selvä pudotus kahden alimman käyttäjäluokan kohdalla, mikä näkyi myös kaikkien käyttäjien sessioita tarkasteltaessa. Myös toisen intervention vaikutus oli havaittavissa luokissa 0 ja 1 sekä kaikkien käyttäjien osalta. Kolmannen intervention vaikutus näkyi selkeästi vain luokan 1 käyttäjissä. Interventiot eivät vaikuttaneet selvästi luokan 2 ja 3 käyttäjien tekemien nollalukkosessioiden osuuksiin.

Kokonaisuudessaan havaintojaksolla kaikkien käyttäjien tekemien nollalukkosessioiden osuus kaikista sessioista pieneni lähes 20 prosenttiyksikköä. Toisin sanoen päivittäisten nollalukkosessioiden osuus siis aleni noin 40 prosenttia. Interventio ja sen toistaminen olivat täten tehokkaita myös täysin lukituksia sisältämättömien sessioiden määrän laskemisessa.

8.4.4 Kontrollin päivittäinen lukitsemisaktiivisuus

Kuviossa 24 on esitettynä intervention ulkopuolelle jätetyn kontrolliryhmän päivittäinen keskimääräinen lukitsemisaktiivisuus. Kuvasta nähdään, että lukitsemisaktiivisuuden päivittäinen vaihtelu oli suurta eikä ajallisesti interventioiden läheisyydessä ollut selkeää nousua lukitsemisaktiivisuudessa. Kontrolliryhmän käyttäytyminen tukee päätelmää siitä, että intervention saaneiden lukitsemiskäyttäytymisessä interventioiden kanssa ajallisesti korreloivat äkilliset muutokset olivat interventiosta johtuvia. Pidemmällä aikavälillä myös kontrolliryhmän lukitsemisaktiivisuudessa voitiin havaita nouseva trendi, jonka oletettiin olevan seurausta Windows 10 -käyttöjärjestelmän osuuden kasvamisesta.



KUVIO 24 Keskimääräinen lukitsemisaktiivisuus päivittäin kontrolliryhmälle (yhteensä 81 uniikkia käyttäjää).

8.5 Intervention vaikutuksen selittäminen

Intervention vaikutuksen selittämiseksi käytettiin usean selittäjän lineaarista regressiota, jolla tutkittiin, mitkä muuttujista olivat session keskimääräisen lukitsemisaktiivisuuden selittäviä muuttujia. Tarkasteluun otettiin mukaan vain ensimmäinen interventio ja kahden muun intervention tarkastelu rajattiin tämän opinnäytetyön ulkopuolelle. Myös viestien faktorien keskinäiset vuorovaikutukset rajattiin tämän tarkastelun ulkopuolelle. Regressioanalyysi suoritettiin R:n (R

Core Team, 2013) ”lm”-komentoa käyttäen. Osana regressioanalyysejä tarkasteltiin myös keskimääräistä marginaalivaikutusta R:n ”margins”-komentoa käyttäen.

8.5.1 Usean selittäjän lineaarinen regressio

Usean selittäjän lineaarinen regressio on eniten käytetty tilastotieteellinen menetelmä yhden selitettävän muuttujan ja yhden tai useamman selittävän muuttujan välisen suhteen tutkimiseen. Menetelmä soveltuu hyvin kausaalisuuden havaitsemiseen, ja sen avulla voidaan tutkia vaikuttaako yksi tai useampi selittävä muuttuja selitettävään muuttujaan. Usean selittäjän lineaarisen regression avulla voidaan lisäksi arvioida selittävien muuttujien osuutta selitettävän muuttujan muutosten suuruuteen. (Allison, 1999, s. 1-5.)

8.5.2 Keskimääräinen marginaalivaikutus

Keskimääräisellä marginaalivaikutuksella voidaan regressiomallia hyödyntäen arvioida yksittäisen selittävän tekijän vaikutusta intervention tehoon. Regressioanalyysissä jokaiselle selittävälle muuttujalle lasketaan kerroin tilanteessa, jossa muut selittävät tekijät saavat nolla-arvonsa. Kun regressiomallissa on usean muuttujan välisiä vuorovaikutuksia tai sekä jatkuvia että diskreettejä muuttujia, yksittäisten muuttujien vaikutuksia on vaikeaa tulkita pelkästään regressiokertoimien perusteella. Keskimääräisen marginaalivaikutuksen avulla saadaan siis selville yksittäisen selittävän tekijän vaikutus lukitsemisaktiivisuuteen interventiossa, kun muiden selittävien tekijöiden vaikutukset keskiarvoistetaan. (Leeper, 2017.) Jokaisen regression yhteydessä on tarkasteltu kunkin regressiossa käytetyn selittävän muuttujan (faktorin) keskimääräistä marginaalivaikutusta lukitsemisaktiivisuuteen interventiossa käyttäjän aiemman lukitsemisaktiivisuuden eri tasoilla.

8.5.3 Datan rajaus ja muuttujien valinta analysointia varten

Regressioanalyysiä varten havaintoaineistosta valittiin sessiot, jotka olivat tapahtuneet 10 arkipäivän aikana ennen ja jälkeen ensimmäisen intervention. Yhteensä valittuja havaintoja oli siis 20 arkipäivän ajalta. Mahdollisen taustatrendin tutkimiseksi sessioiden päivämäärätiedon perusteella dataan lisättiin jokaiselle sessiolle päivänumeromuuttuja, joka oli juokseva numerointi regressiota varten valitun datan ensimmäisestä päivämäärästä lukien.

Intervention vaikutuksen tutkimiseksi dataan lisättiin myös muuttuja, joka sai arvon epätosi ennen interventiota ja intervention jälkeisissä sessioissa arvon tosi. Tätä hyödyntäen regressioanalyysin avulla oli mahdollista selvittää intervention vaikutuksen suuruus sessiokohtaiseen keskimääräiseen lukitsemisaktii-

visuuteen sekä vaikutuksen tilastollinen merkitsevyys. Kyseisen muuttujan regressiokerroin siis kuvasi lukitsemisaktiivisuuden muutoksen suuruutta intervention seurauksena.

Jokaiseen sessioon lisättiin myös tieto käyttäjän keskimääräisestä lukitsemisaktiivisuudesta esitarkkailujaksolla, minkä ansiosta regressioissa voitiin huomioida interventiota edeltäneen käyttäytymisen vaikutus intervention tehoon sekä sen yhteisvaikutus interventioviestien faktorien kanssa.

Lopuksi sessioihin liitettiin kokeen konfiguraatio eli käyttäjälle lähetetyn interventioviestin faktorien mukaiset muuttujien arvot sekä tieto siitä oliko käyttäjä ollut osa kontrolliryhmää. Suojelumotivaatiopohjaisen ja viitekehysvaikutukseen perustuvan intervention tehon vertailemiseksi dataan lisättiin muuttuja, joka indikoi oliko käyttäjälle lähetetty jokin suojelumotivaatioteoriapohjaisista interventioviesteistä. Kuvailun yksityiskohtaisuuden sekä uhkan kohdistumisen vaikutuksen tutkimiseksi dataan lisättiin näitä kuvaavat muuttujat, jotka saivat arvon 1, mikäli käyttäjälle lähetetyn interventioviestin konfiguraatiossa oli siinä käytetyn teorian vastaava faktori tasolla 1. Näiden muuttujien voidaan siis ajatella olleen yleistyksiä kummankin interventiotyypin faktoreista 2 ja 3.

Taulukkoon 10 on koottu regressiossa käytetyt selittävät muuttujat sekä esitetty niiden kuvaukset. Taulukossa 11 on esitetty muuttujien väliset korrelaatiot. Korrelaatiotaulukko vahvistaa oletuksen siitä, että aiempi keskimääräinen lukitsemisaktiivisuus (AvgLockRate.Pre) selittää suuren osan lukitsemisaktiivisuudesta (LRMean) myös intervention jälkeen.

TAULUKKO 10 Regressioanalyysissä ja korrelaatiotaulukossa käytetyt muuttujat ja niiden selitykset

Muuttuja	Kuvaus
LockRate	Session keskimääräinen lukitsemisaktiivisuus
LRMean	Ensimmäisen intervention jälkeen kahden viikon käyttäjäkohtainen keskiarvo lukitsemisaktiivisuudelle
is.After	Onko sessio intervention jälkeen (true) vai ennen (false)
AvgLockRate.pre	Keskimääräinen lukitsemisaktiivisuus esitarkkailujaksolla, jatkuva muuttuja
is.Control	Kuuluuko kontrolliin (true) vai ei (false)
DayNum	Juokseva numerointi tarkkailujakson alusta
is.PMT	Onko kyseessä suojelumotivaatioteoria (true) vai viitekehysvaikutus (false)
PMT.f1	Uhkan vakavuus ja todennäköisyys, tasot neutraali (0) ja korostettu / korkea (1)
PMT.f2	Uhkan relevanssi, tasot organisaatio (0) ja organisaatio + henkilökohtainen (1)
PMT.f3	Uhkan kuvailun yksityiskohtaisuus, matala (0) ja tarkka (1)
PMT.f4	Vastatoimen tehokkuus ja käyttäjän minäpystyvyys (yhdistetty efficacy), tasot neutraali (0) ja korostettu (1)
GF.f1	Viestin näkökulma, tasot positiivinen (0) ja negatiivinen (1)
GF.f2	Uhkan relevanssi, tasot organisaatio (0) ja organisaatio + henkilökohtainen (1)
GF.f3	Uhkan kuvailun yksityiskohtaisuus, matala (0) ja tarkka (1)
f.relevance	Uhkan relevanssi, tasot organisaatio (0) ja organisaatio + henkilökohtainen (1)
f.detail	Uhkan kuvailun yksityiskohtaisuus, matala (0) ja tarkka (1)

TAULUKKO 11 Muuttujien korrelaatiot

Muuttuja	n	M	SD	UserID	Grou-pID	LRMea n	Av-gLock-Rate.pre	is.Co ntrol	is.PMT	PMT.f1	PMT.f2	PMT.f3	PMT.f4	GF.f1	GF.f2	GF.f3	f.re-le-vance	f.de-tail
UserID	1962			1.00														
GroupID	1962			0.03	1.00													
LRMean	1437	2.04	2.20	-0.04	0.01	1.00												
AvgLock-Rate.pre	1353	1.86	2.01	-0.03	0.00	0.86***	1.00											
is.Control	1962	0.04	0.20	-0.02	-0.34***	0.01	0.02	1.00										
is.PMT	1881	0.66	0.47	0.00	-0.82***	-0.01	-0.02		1.00									
PMT.f1	1250	0.49	0.50	0.02	0.87***	0.03	-0.02			1.00								
PMT.f2	1250	0.49	0.50	-0.05	0.11***	-0.05	-0.05			0.00	1.00							
PMT.f3	1250	0.49	0.50	0.02	0.19***	-0.01	0.01			-0.03	-0.01	1.00						
PMT.f4	1250	0.50	0.50	0.03	0.44***	0.01	0.00			0.00	0.00	0.00	1.00					
GF.f1	631	0.49	0.50	-0.07	0.24***	-0.07	-0.07							1.00				
GF.f2	631	0.50	0.50	0.02	0.46***	-0.04	-0.04							0.03	1.00			
GF.f3	631	0.50	0.50	0.14***	0.87***	0.02	0.03							0.01	0.02	1.00		
f.relevance	1881	0.49	0.50	-0.03	0.11***	-0.04	-0.04		-0.01	0.00	1.00***	-0.01	0.00	0.03	1.00***	0.02	1.00	
f.detail	1881	0.49	0.50	0.06*	0.19***	0.00	0.02		-0.01	-0.03	-0.01	1.00***	0.00	0.01	0.02	1.00***	0.00	1.00

*** p < 0.001, ** p < 0.01, * p < 0.05

8.5.4 Intervention vaikutus kontrolliryhmään

Taulukossa 12 on esitetty usean selittäjän lineaarisen regressioanalyysin avulla lasketut regressiomallit, joissa yhdeksi selittäväksi muuttujaksi on otettu kontrolliryhmään kuuluminen (is.Control). Jäljempään malleista on sisällytetty selittäväksi muuttujaksi myös esitarkkailujakson lukitsemisaktiivisuus. Mallissa 2 havaintojen määrä on pienempi, koska kaikille käyttäjille ei ole voitu määrittää esitarkkailujakson keskimääräistä lukitsemiskäyttäytymistä (AvgLockRate.pre) luvussa 8.2 esitetyn mukaisesti. Selittävänä muuttujana käytettiin myös juoksevaa päivänumeroa (DayNum) regressioanalyysin aikaväliltä, jotta oltaisiin voitu havaita lukitsemisaktiivisuuden muutoksen ajallinen taustatrendi. Analyysijaksolla ei kuitenkaan havaittu tilastollisesti merkitsevää muutostrendiä työasemien lukitsemisessa. Mallin 1 havaittiin olevan selitysvoimaltaan varsin huono. Koska lisäksi haluttiin tutkia intervention vaikutuksen eroja erilaisten käyttäjien suhteen, esitarkkailujakson lukitsemisaktiivisuuden huomioinut malli 2 valittiin tarkempaan tarkasteluun. Koska malli 2 sisälsi muuttujien välisiä interaktioita, tulokset tulkittiin keskimääräisten marginaalivaikutusten avulla.

TAULUKKO 12 Intervention vaikutus session keskimääräiseen lukitsemisaktiivisuuteen yleisesti

Muuttuja	Malli 1	Malli 2
(Intercept)	1.93 ***	0.05
	(0.05)	(0.04)
is.After(true)	0.20	0.31 ***
	(0.14)	(0.09)
is.Control(true)	0.43 *	0.03
	(0.17)	(0.11)
DayNum	-0.00	-0.00
	(0.01)	(0.00)
is.After(true):is.Control(true)	-0.36	-0.21
	(0.22)	(0.14)
is.After(true):DayNum	0.00	-0.00
	(0.01)	(0.01)
AvgLockRate.pre		1.00 ***
		(0.01)
is.After(true):AvgLockRate.pre		-0.03 *
		(0.01)
R^2	0.002	0.623
Korjattu R^2	0.002	0.623
Havaintojen määrä	16369	15849

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 13 on esitettynä intervention keskimääräinen marginaalivaikutus kontrolliryhmään esitarkkailujakson lukitsemisaktiivisuuden eri arvoilla. Taulukosta voidaan havaita, että interventiolla ei ollut vaikutusta kontrolliryhmään millään esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden (AvgLockRate.pre) arvoilla. Taulukosta nähdään myös, että intervention vaikutus interventioviestin saaneiden käyttäjien (is.Control = false) osalta pieneni esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden kasvaessa. Keskimäärin yhden lukitsemisen työpäivän aikana tekevään henkilöön interventiolla havaittiin olleen noin 26 % positiivinen vaikutus, kun kolme lukitsemista session aikana tekevään henkilöön interventiolla havaittiin enää 7 % positiivinen vaikutus keskimääräiseen lukitsemisaktiivisuuteen. Suurin keskimääräinen marginaalivaikutus (0,28) havaittiin esitarkkailujaksolla työasemia aiemmin lukitsemattomilla käyttäjillä (AvgLockRate.pre = 0). Todella paljon esitarkkailujaksolla työasemia lukinneille käyttäjille (AvgLockRate.pre = 8) ei interventiolla havaittu olleen selvää vaikutusta.

TAULUKKO 13 Intervention keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen kontrolliryhmässä

AvgLockRate.pre	is.Control	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	false	0,28 (0,05)***	0,18 - 0,39
0	true	0,07 (0,15)	-0,22 - 0,36
1	false	0,26 (0,05)***	0,16 - 0,35
1	true	0,05 (0,15)	-0,24 - 0,33
3	false	0,20 (0,05)***	0,11 - 0,30
3	true	-0,01 (0,15)	-0,29 - 0,28
5	false	0,15 (0,06)*	0,03 - 0,27
5	true	-0,06 (0,15)	-0,35 - 0,24
8	false	0,07 (0,09)	-0,10 - 0,25
8	true	-0,14 (0,16)	-0,45 - 0,18

*** p < 0.001, ** p < 0.01, * p < 0.05

8.5.5 Suojelumotivaatioteorian ja viitekehyksen vaikutuksen vertailu

Taulukossa 14 on esitetty käytettyjen teorioiden vaikutuserojen vertailemiseksi tehdyn usean selittäjän lineaarisen regression tulokset. Malleihin ei sisällytetty kontrolliryhmää ilmaisevaa muuttujaa, vaan kontrolliryhmää koskevat havainnot poistettiin käsiteltävästä aineistosta. Tarkastelu tässä ja muissa seuraavaksi tulevissa alaluvuissa rajattiin vain intervention kohteena olleisiin henkilöihin. Mallin 1 havaittiin olevan selitysvoimaltaan varsin huono. Koska lisäksi haluttiin tutkia intervention vaikutuksen eroja erilaisten käyttäjien suhteen, esitarkkailujakson lukitsemisaktiivisuuden huomioinut malli 2 valittiin tarkempaan tarkasteluun. Koska malli 2 sisälsi muuttujien välisiä interaktioita, tulokset tulkittiin keskimääräisten marginaalivaikutusten avulla.

TAULUKKO 14 Suojelumotivaatioteorian ja viitekehysvaikutuksen vertailu regressiolla. Riippuvana muuttujana keskimääräinen lukitsemisaktiivisuus.

Muuttuja	Malli 1	Malli 2
(Intercept)	1.89 ***	0.04
	(0.05)	(0.04)
is.After(true)	0.25 ***	0.35 ***
	(0.07)	(0.06)
is.PMT(true)	0.03	0.02
	(0.06)	(0.05)
is.After(true):is.PMT(true)	-0.03	-0.14 *
	(0.09)	(0.07)
AvgLockRate.pre		1.00 ***
		(0.02)
is.After(true):AvgLockRate.pre		-0.06 **
		(0.02)
AvgLockRate.pre:is.PMT(true)		-0.01
		(0.02)
is.After(true):AvgLock-Rate.pre:is.PMT(true)		0.06 *
		(0.03)
R^2	0.002	0.617
Korjattu R^2	0.002	0.617
Havaintojen määrä	15811	15340

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 15 on esitetty pohjaviestin teorian faktorin (is.PMT) keskimääräiset marginaalivaikutukset interventiossa. Taulukosta voidaan havaita, että käytetyn teorian vaikutus riippuu keskimääräisen lukitsemisaktiivisuuden arvosta (AvgLockRate.pre). Viitekehysvaikutuksen viestit (is.PMT = false) olivat hieman tehokkaampia pienillä esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre $\leqslant$ 1). Esitarkkailujakson lukitsemisaktiivisuuden suuremmilla arvoilla (AvgLockRate.pre ≥ 5) suojelumotivaatioteorian viestit saattoivat olla hieman tehokkaampia.

TAULUKKO 15 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja käytetyn teorian funktiona

AvgLockRate.pre	is.PMT	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	false	0,35 (0,06)***	0,24 - 0,47
0	true	0,21 (0,04)***	0,13 - 0,29
1	false	0,29 (0,05)***	0,20 - 0,38
1	true	0,21 (0,03)***	0,14 - 0,27
3	false	0,17 (0,05)***	0,07 - 0,26
3	true	0,20 (0,04)***	0,13 - 0,27
5	false	0,04 (0,08)	-0,12 - 0,20
5	true	0,19 (0,06)**	0,07 - 0,30
8	false	-0,15 (0,14)	-0,42 - 0,12
8	true	0,17 (0,10)	-0,03 - 0,37

8.5.6 Suojelumotivaatioteorian faktoreiden vaikutus

Taulukossa 16 on esitetty suojelumotivaatioteorian faktoreiden usean selittäjän lineaarisen regression tulokset. Mallin 1 havaittiin olevan selitysvoimaltaan varsin huono. Koska lisäksi haluttiin tutkia intervention vaikutuksen eroja erilaisten käyttäjien suhteen, esitarkkailujakson lukitsemisaktiivisuuden huomioinut malli 2 valittiin tarkempaan tarkasteluun. Koska malli 2 sisälsi muuttujien välisiä interaktioita, tulokset tulkittiin keskimääräisten marginaalivaikutusten avulla jokaisen faktorin osalta erikseen.

TAULUKKO 16 Suojelumotivaatioteorian faktorien vaikutus keskimääräiseen lukitsemisaktiivisuuteen interventiossa

Muuttuja	Malli 1	Malli 2
(Intercept)	2.07 ***	0.05
	(0.08)	(0.07)
is.After(true)	0.08	-0.04
	(0.11)	(0.09)
PMT.f11	-0.15 *	-0.04
	(0.07)	(0.06)
PMT.f21	-0.27 ***	-0.01
	(0.07)	(0.06)
PMT.f31	0.11	0.04
	(0.07)	(0.06)
PMT.f41	-0.04	0.03
	(0.07)	(0.06)
is.After(true):PMT.f11	0.18	-0.03
	(0.10)	(0.09)
is.After(true):PMT.f21	0.08	0.22 *
	(0.10)	(0.09)
is.After(true):PMT.f31	-0.15	-0.01
	(0.10)	(0.09)
is.After(true):PMT.f41	0.16	0.29 ***
	(0.10)	(0.09)
AvgLockRate.pre		1.02 ***
		(0.03)
is.After(true):AvgLockRate.pre		0.08 *
		(0.04)
AvgLockRate.pre:PMT.f11		0.00
		(0.02)
AvgLockRate.pre:PMT.f21		-0.03
		(0.02)
AvgLockRate.pre:PMT.f31		-0.03
		(0.02)
AvgLockRate.pre:PMT.f41		-0.01
		(0.02)
is.After(true):AvgLockRate.pre:PMT.f11		0.10 **
		(0.03)
is.After(true):AvgLockRate.pre:PMT.f21		-0.10 **
		(0.03)
is.After(true):AvgLockRate.pre:PMT.f31		-0.03
		(0.03)
is.After(true):AvgLockRate.pre:PMT.f41		-0.13 ***
		(0.03)
R^2	0.005	0.615
Korjattu R^2	0.004	0.614
Havaintojen määrä	10498	10181

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 17 on esitetty suojelumotivaatioteorian uhkan vakavuuden ja todennäköisyyden faktorin (PMT.f1) keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen interventiossa. Pienillä esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre ≤ 1) kumpikin faktorin tasoista lisäsi lukitsemista lähes yhtä paljon. Uhkan vakavuuden ja todennäköisyyden korostaminen (PMT.f1 = 1) lisäsi lukitsemista myös esitarkkailujakson lukitsemisaktiivisuuden suuremmilla arvoilla (AvgLockRate.pre ≥ 3). Neutraalilla tasolla (PMT.f1 = 0) ei havaittu vaikutusta suuremmilla arvoilla. Korostetun tason vaikutus kasvoi esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden kasvaessa, kun taas neutraalin tason vaikutus pieneni.

TAULUKKO 17 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja uhkan vakavuuden ja todennäköisyyden faktorin funktiona

AvgLockRate.pre	PMT.f1	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,21 (0,06)***	0,10 - 0,33
0	1	0,19 (0,06)**	0,06 - 0,31
1	0	0,17 (0,05)***	0,07 - 0,26
1	1	0,24 (0,05)***	0,14 - 0,34
3	0	0,07 (0,05)	-0,03 - 0,17
3	1	0,35 (0,05)***	0,24 - 0,46
5	0	-0,02 (0,08)	-0,18 - 0,13
5	1	0,46 (0,09)***	0,28 - 0,63
8	0	-0,17 (0,13)	-0,43 - 0,10
8	1	0,62 (0,16)***	0,31 - 0,93

Taulukossa 18 on esitetty suojelumotivaatioteorian henkilökohtaisen relevanssin faktorin keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen interventiossa. Henkilökohtaisen relevanssin (PMT.f2 = 1) sisällyttäminen viesteihin lisäsi lukitsemista pienillä esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre ≤ 1) enemmän kuin pelkkä organisaatiokohdistus (PMT.f2 = 0). Suuremmilla esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre ≥ 3) pelkkä organisaatiokohdistus (PMT.f2 = 0) oli tehokkaampi. Esitarkkailujakson lukitsemisaktiivisuuden suurimmilla arvoilla (AvgLockRate.pre ≥ 5) faktorin henkilökohtaisen relevanssin (PMT.f2 = 1) sisältäneet viestit eivät näyttäneet vaikuttavan lukitsemiseen lainkaan. Faktorin tason 1 vaikutus pieneni esitarkkailujakson lukitsemisaktiivisuuden kasvaessa, kun taas tason 0 vaikutus kasvoi.

TAULUKKO 18 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja henkilökohtaisen relevanssin faktorin funktiona

AvgLockRate.pre	PMT.f2	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,10 (0,06)	-0,02 - 0,21
0	1	0,32 (0,06)***	0,19 - 0,44
1	0	0,15 (0,05)**	0,05 - 0,24
1	1	0,26 (0,05)***	0,16 - 0,36
3	0	0,24 (0,05)***	0,15 - 0,34
3	1	0,16 (0,05)**	0,05 - 0,26
5	0	0,34 (0,08)***	0,19 - 0,49
5	1	0,05 (0,09)	-0,13 - 0,23
8	0	0,48 (0,13)***	0,23 - 0,74
8	1	-0,11 (0,16)	-0,42 - 0,20

Taulukossa 19 on esitetty kuvailun tarkkuuden faktorin keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen interventiossa. Esitarkkailujakson lukitsemisaktiivisuuden kaikilla arvoilla kuvailun tarkkuuden molemmat tasot lisäsivät lukitsemista käytännössä lähes yhtä paljon. Tulosten perusteella näyttäisi, että matalan kuvailun tarkkuuden (PMT.f3 = 0) vaikutus kasvoi esitarkkailujakson lukitsemisaktiivisuuden kasvaessa. Korkealla kuvailun tarkkuudella (PMT.f3 = 1) vaikutus taas pieneni hieman esitarkkailujakson lukitsemisaktiivisuuden kasvaessa. Suurilla esitarkkailujakson lukitsemisen arvoilla (AvgLockRate.pre ≥ 5) matala kuvailun tarkkuus (PMT.f3 = 0) saattoi olla hieman parempi.

TAULUKKO 19 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja kuvailun tarkkuuden faktorin funktiona

AvgLockRate.pre	PMT.f3	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,20 (0,06)***	0,08 - 0,32
0	1	0,20 (0,06)**	0,08 - 0,32
1	0	0,22 (0,05)***	0,13 - 0,32
1	1	0,18 (0,05)***	0,09 - 0,28
3	0	0,25 (0,05)***	0,15 - 0,35
3	1	0,15 (0,05)**	0,05 - 0,25
5	0	0,29 (0,08)***	0,12 - 0,45
5	1	0,12 (0,08)	-0,04 - 0,28
8	0	0,34 (0,15)*	0,05 - 0,62
8	1	0,07 (0,15)	-0,21 - 0,36

Taulukossa 20 on esitetty suojelumotivaatioteorian vastatoimen tehokkuuden ja minäpystyvyyden korostamisen faktorin (PMT.f4) keskimääräinen marginaali-

vaikutus interventiossa. Tulosten perusteella vastatoimen tehokkuuden ja minäpystyvyyden korostamisen (PMT.f4 = 1) vaikutus pieneni esitarkkailujakson lukitsemisaktiivisuuden kasvaessa, kun taas neutraalin tason (PMT.f4 = 0) vaikutus kasvoi. Esitarkkailujaksolla työasemiaan lukitsemattomien (AvgLockRate.pre = 0) joukossa korostettu taso oli selvästi tehokkaampi ja sitä suuremmilla esitarkkailujakson lukitsemisen arvoilla neutraali taso oli tehokkaampi.

TAULUKKO 20 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja vastatoimen tehokkuuden ja minäpystyvyyden faktorin funktiona

AvgLockRate.pre	PMT.f4	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,05 (0,06)	-0,08 - 0,17
0	1	0,33 (0,06)***	0,22 - 0,45
1	0	0,12 (0,05)*	0,02 - 0,22
1	1	0,28 (0,05)***	0,18 - 0,37
3	0	0,25 (0,05)***	0,15 - 0,36
3	1	0,16 (0,05)**	0,06 - 0,25
5	0	0,39 (0,09)***	0,22 - 0,56
5	1	0,04 (0,08)	-0,12 - 0,20
8	0	0,59 (0,15)***	0,30 - 0,89
8	1	-0,14 (0,14)	-0,41 - 0,13

8.5.7 Viitekehysvaikutuksen faktorien vaikutus

Taulukossa 21 on esitetty viitekehysvaikutuksen faktorien usean selittäjän lineaarisen regression tulokset. Mallin 1 havaittiin jälleen olevan selitysvoimaltaan varsin huono. Koska lisäksi haluttiin tutkia intervention vaikutuksen eroja erilaisten käyttäjien suhteen, esitarkkailujakson lukitsemisaktiivisuuden huomioinut malli 2 valittiin tarkempaan tarkasteluun. Koska malli 2 sisälsi muuttujien välisiä interaktioita, tulokset tulkittiin keskimääräisten marginaalivaikutusten avulla jokaisen faktorin osalta erikseen.

TAULUKKO 21 Viitekehysvaikutuksen faktorien vaikutus keskimääräiseen lukitsemisaktiivisuuteen interventiossa

Muuttuja	Malli 1	Malli 2
(Intercept)	2.06 ***	0.03
	(0.10)	(0.08)
is.After(true)	0.23	0.55 ***
	(0.13)	(0.11)
GF.f11	-0.32 **	0.02
	(0.10)	(0.08)
GF.f21	-0.02	0.00
	(0.10)	(0.08)
GF.f31	0.00	-0.01
	(0.10)	(0.08)
is.After(true):GF.f11	-0.14	-0.14
	(0.14)	(0.12)
is.After(true):GF.f21	0.03	-0.19
	(0.14)	(0.12)
is.After(true):GF.f31	0.13	-0.02
	(0.14)	(0.12)
AvgLockRate.pre		1.02 ***
		(0.03)
is.After(true):AvgLockRate.pre		-0.16 ***
		(0.04)
AvgLockRate.pre:GF.f11		-0.05
		(0.03)
AvgLockRate.pre:GF.f21		-0.03
		(0.03)
AvgLockRate.pre:GF.f31		0.02
		(0.03)
is.After(true):AvgLockRate.pre:GF.f11		0.00
		(0.04)
is.After(true):AvgLockRate.pre:GF.f21		0.12 **
		(0.04)
is.After(true):AvgLockRate.pre:GF.f31		0.05
		(0.04)
R^2	0.009	0.634
Korjattu R^2	0.007	0.633
Havaintojen määrä	5313	5159

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 22 on esitetty viitekehysvaikutuksen näkökulman (GF.f1) keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen interventiossa. Lukitsemisesta saatavan edun näkökulma (GF.f1 = 0) lisäsi lukitsemista esitarkkailujakson

lukitsemisaktiivisuuden pienillä arvoilla (AvgLockRate.pre ≤ 3) enemmän kuin lukitsemisen laiminlyönnistä koituvaa haittaa korostava näkökulma (GF.f1 = 1). Faktorin molemmilla tasoilla vaikutus pieneni esitarkkailujakson lukitsemisaktiivisuuden kasvaessa. Suurilla esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre ≥ 5) kummallakaan faktorin tasolla ei ollut vaikutusta lukitsemisaktiivisuuteen.

TAULUKKO 22 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja viitekehysvaikutuksen näkökulman faktorin funktiona

AvgLockRate.pre	GF.f1	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,44 (0,08)***	0,28 - 0,60
0	1	0,30 (0,08)***	0,15 - 0,46
1	0	0,37 (0,07)***	0,24 - 0,50
1	1	0,23 (0,07)***	0,10 - 0,36
3	0	0,22 (0,07)***	0,09 - 0,35
3	1	0,09 (0,07)	-0,06 - 0,23
5	0	0,07 (0,10)	-0,13 - 0,28
5	1	-0,06 (0,12)	-0,29 - 0,17
8	0	-0,15 (0,18)	-0,50 - 0,20
8	1	-0,28 (0,20)	-0,68 - 0,12

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 23 on esitetty viitekehysvaikutuksen henkilökohtaisen relevanssin faktorin keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen interventiossa. Pelkkä organisaatiokohdistus (GF.f2 = 0) lisäsi lukitsemista esitarkkailujaksolla aiemmin työasemaa lukitsemattomilla käyttäjillä (AvgLockRate.pre = 0) enemmän kuin henkilökohtaisen relevanssin taso (GF.f1 = 1). Pienellä esitarkkailujakson lukitsemisaktiivisuudella (AvgLockRate.pre = 1) kumpikin faktorin taso lisäsi lukitsemista yhtä paljon. Suuremmilla esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre ≥ 3) henkilökohtaisen relevanssin sisällyttäminen viesteihin (GF.f2 = 1) oli tehokkaampi. Molemmilla faktorin tasoilla vaikutus heikkeni esitarkkailujakson lukitsemisaktiivisuuden kasvaessa. Suurella esitarkkailujakson lukitsemisaktiivisuudella (AvgLockRate.pre = 8) pelkkä organisaatiokohdistus (GF.f2 = 0) näytti jopa vähentävän lukitsemista. Tämän kuitenkin arveltiin aiheutuvan siitä, että suurilla esitarkkailujakson lukitsemisaktiivisuuksilla malli ei ole välttämättä tarkka pienen havaintomäärän vuoksi.

TAULUKKO 23 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja henkilökohtaisen relevanssin faktorin funktiona

AvgLockRate.pre	GF.f2	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,47 (0,08)***	0,30 - 0,63
0	1	0,28 (0,08)***	0,12 - 0,44
1	0	0,33 (0,07)***	0,20 - 0,46
1	1	0,27 (0,07)***	0,14 - 0,40
3	0	0,06 (0,07)	-0,07 - 0,20
3	1	0,24 (0,07)***	0,11 - 0,38
5	0	-0,20 (0,11)	-0,43 - 0,02
5	1	0,22 (0,11)*	0,00 - 0,43
8	0	-0,61 (0,20)**	-1,00 – (-0,22)
8	1	0,18 (0,18)	-0,18 - 0,54

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 24 on esitetty kuvailun tarkkuuden faktorin keskimääräinen marginaalivaikutus lukitsemisaktiivisuuteen interventiossa. Esitarkkailujakson lukitsemisaktiivisuuden kaikilla arvoilla kuvailun tarkkuuden molemmat tasot vaikuttivat lukitsemisaktiivisuuteen käytännössä lähes yhtä paljon. Kummankin tason vaikutus pieneni lukitsemisaktiivisuuden kasvaessa säilyen positiivisena esitarkkailujakson alemmilla lukitsemisaktiivisuuksilla (AvgLockRate.pre ≤ 3). Suurilla esitarkkailujakson lukitsemisen arvoilla (AvgLockRate.pre ≥ 5) korkea kuvailun tarkkuus (GF.f3 = 1) saattoi olla hieman parempi. Suurella esitarkkailujakson lukitsemisaktiivisuudella (AvgLockRate.pre = 8) kuvailun matala tarkkuus (GF.f3 = 0) näytti jopa vähentävän lukitsemista. Tämänkin arveltiin aiheutuvan siitä, että suurilla esitarkkailujakson lukitsemisaktiivisuuksilla malli ei ole välttämättä tarkka pienen havaintomäärän vuoksi.

TAULUKKO 24 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja kuvailun tarkkuuden faktorin funktiona

AvgLockRate.pre	GF.f3	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,38 (0,08)***	0,23 - 0,54
0	1	0,36 (0,08)***	0,20 - 0,52
1	0	0,28 (0,07)***	0,16 - 0,41
1	1	0,32 (0,07)***	0,19 - 0,45
3	0	0,09 (0,07)	-0,05 - 0,22
3	1	0,22 (0,07)**	0,09 - 0,36
5	0	-0,11 (0,11)	-0,33 - 0,10
5	1	0,13 (0,11)	-0,09 - 0,35
8	0	-0,41 (0,19)*	-0,78 – (-0,04)
8	1	-0,01 (0,19)	-0,39 - 0,37

*** p < 0.001, ** p < 0.01, * p < 0.05

8.5.8 Kuvailun tarkkuuden ja viestin henkilökohtaisen relevanssin vaikutus

Regression avulla tarkasteltiin myös kuvailun tarkkuuden ja viestin henkilökohtaisen relevanssin vaikutusta kummallekin teorialle yhdistettyinä faktoreina (f.relevance ja f.detail). Relevanssissa ja kuvailun tarkkuudessa oli pyritty molempien pohjateorioiden mukaisissa interventioviesteissä yhdenmukaisuuteen, mutta pieniä eroja muotoiluissa jouduttiin tekemään, jotta viestit pysyivät käytetyn teorian ja muiden faktorien tasojen mukaisina.

Taulukossa 25 on esitetty usean selittäjän lineaarisen regressioanalyysin tulokset, kun intervention vaikutusta selittävinä muuttujina käytettiin yhdistettyjä henkilökohtaisen relevanssin ja kuvailun tarkkuuden faktoreita. Mallien 4, 5 ja 6 selitysvoimassa ei ollut eroja. Koska haluttiin tutkia intervention vaikutuksen eroja erilaisten käyttäjien suhteen, esitarkkailujakson lukitsemisaktiivisuuden ja molemmat yhdistyt faktorit huomioinut malli 6 valittiin tarkempaan tarkasteluun. Koska malli 6 sisälsi muuttujien välisiä interaktioita, tulokset tulkittiin keskimääräisten marginaalivaikutusten avulla.

TAULUKKO 25 Yhdistettyjen faktorien kuvailun tarkkuus ja henkilökohtainen relevanssi vaikutus keskimääräiseen lukitsemisaktiivisuuteen interventiossa

Muuttuja	Malli 1	Malli 2	Malli 3	Malli 4	Malli 5	Malli 6
(Intercept)	2.00 ***	1.96 ***	1.87 ***	0.05	0.04	0.05
	(0.04)	(0.05)	(0.04)	(0.04)	(0.04)	(0.04)
is.After(true)	0.19 ***	0.22 **	0.26 ***	0.22 ***	0.27 ***	0.23 ***
	(0.06)	(0.07)	(0.06)	(0.05)	(0.05)	(0.06)
f.relevance1	-0.20 ***	-0.20 ***		-0.01		-0.01
	(0.06)	(0.06)		(0.05)		(0.05)
is.After(true):f.relevance1	0.07	0.07		0.08		0.08
	(0.08)	(0.08)		(0.07)		(0.07)
f.detail1		0.08	0.08		0.02	0.02
		(0.06)	(0.06)		(0.05)	(0.05)
is.After(true):f.detail1		-0.06	-0.06		-0.02	-0.03
		(0.08)	(0.08)		(0.07)	(0.07)
AvgLockRate.pre				1.00 ***	1.00 ***	1.01 ***
				(0.01)	(0.01)	(0.02)
is.After(true):AvgLockRate.pre				-0.02	-0.03	-0.02
				(0.02)	(0.02)	(0.02)
AvgLockRate.pre:f.relevance1				-0.03		-0.03
				(0.02)		(0.02)
is.After(true):AvgLock-Rate.pre:f.relevance1				-0.02		-0.02
				(0.03)		(0.03)
AvgLockRate.pre:f.detail1					-0.01	-0.01
					(0.02)	(0.02)
is.After(true):AvgLock-Rate.pre:f.detail1					0.00	0.01
					(0.03)	(0.03)
R^2	0.003	0.002	0.003	0.617	0.617	0.617
Korjattu R^2	0.003	0.002	0.003	0.617	0.617	0.617
Havaintojen määrä	15811	15811	15811	15340	15340	15340

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 26 on esitetty yhdistetyn henkilökohtaisen relevanssin faktorin (f.relevance) keskimääräiset marginaalivaikutukset interventiossa. Henkilökohtaisen relevanssin sisällyttäminen (f.relevance = 1) viesteihin saattoi tulosten perusteella olla hieman tehokkaampaa esitarkkailujakson lukitsemisaktiivisuuden pienimmillä arvolla (AvgLockRate.pre ≤ 1) kuin pelkkä organisaatiokohdistus (f.relevance = 0). Tätä suuremmilla esitarkkailujakson lukitsemisaktiivisuuden arvoilla (AvgLockRate.pre ≥ 3) faktorin molemmat tasot olivat yhtä tehokkaita ja teho heikkeni esitarkkailujakson lukitsemisaktiivisuuden kasvaessa.

TAULUKKO 26 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja yhdistetyn henkilökohtaisen relevanssin faktorin funktiona

AvgLockRate.pre	f.relevance	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,22 (0,05)***	0,12 – 0,31
0	1	0,30 (0,05)***	0,20 – 0,40
1	0	0,20 (0,04)***	0,13 – 0,28
1	1	0,27 (0,04)***	0,19 – 0,35
3	0	0,17 (0,04)***	0,09 – 0,25
3	1	0,20 (0,04)***	0,12 – 0,29
5	0	0,13 (0,06)*	0,01 – 0,26
5	1	0,14 (0,07)*	0,00 – 0,27
8	0	0,08 (0,11)	-0,13 – 0,30
8	1	0,04 (0,12)	-0,20 – 0,28

*** p < 0.001, ** p < 0.01, * p < 0.05

Taulukossa 27 on esitetty yhdistetyn kuvailun tarkkuuden faktorin keskimääräiset marginaalivaikutukset interventiossa. Faktorin molemmat tasot havaittiin kutakuinkin yhtä tehokkaiksi tehon heikentyessä esitarkkailujakson lukitsemisaktiivisuuden kasvaessa.

TAULUKKO 27 Intervention vaikutus lukitsemisaktiivisuuteen esitarkkailujakson keskimääräisen lukitusaktiivisuuden ja yhdistetyn kuvailun tarkkuuden faktorin funktiona

AvgLockRate.pre	f.detail	Keskimääräinen marginaalivaikutus	95% luottamusväli
0	0	0,27 (0,05)***	0,18 - 0,37
0	1	0,24 (0,05)***	0,15 - 0,34
1	0	0,25 (0,04)***	0,17 - 0,32
1	1	0,22 (0,04)***	0,15 - 0,30
3	0	0,19 (0,04)***	0,11 - 0,27
3	1	0,18 (0,04)***	0,10 - 0,26
5	0	0,14 (0,07)*	0,01 - 0,27
5	1	0,13 (0,07)*	0,01 - 0,26
8	0	0,06 (0,11)	-0,17 - 0,28
8	1	0,07 (0,11)	-0,15 - 0,29

*** p < 0.001, ** p < 0.01, * p < 0.05

9 YHTEENVETO

Tässä tutkielmassa tutkittiin pitkittäisellä kenttätutkimuksella käyttäjien lukitsemiskäyttäytymiseen vaikuttamista toistuvilla interventioilla. Tutkimus toteutettiin oikeassa organisaatiossa ja tutkimuksen havaintoaineisto muodostui käyttäjien todellisesta lukitsemiskäyttäytymisestä. Tutkimusongelma määritettiin seuraavasti: ”Miten toistettu sähköposti-interventio vaikuttaa organisaation henkilökunnan todelliseen lukitsemiskäyttäytymiseen?”.

Tehdyn tutkimuksen perusteella voitiin vastata tutkimusongelmaan ja sitä tarkentaviin tutkimuskysymyksiin:

Kysymys 1: Voidaanko sähköposti-interventiolla lisätä työasemien lukitsemista ja onko vaikutus pysyvä?

Kysymys 2: Onko sähköposti-intervention toistamisesta hyötyä?

Kysymys 3: Eroaako suojelumotivaatioteoriaan pohjautuvan intervention teho viitekehysvaikutukseen perustuvan intervention tehosta?

Kysymys 4: Miten suojelumotivaatioteorian mukaisen uhkan vakavuuden ja todennäköisyyden sekä vastatoimen tehokkuuden ja minäpystyvyyden korostaminen vaikuttaa lukitsemiskäyttäytymiseen interventiossa?

Kysymys 5: Miten viestin viitekehyksen valinta vaikuttaa työasemien lukitsemiseen interventiossa?

Kysymys 6: Miten henkilökohtaisen relevanssin korostaminen tai kuvailun yksityiskohtaisuuden lisääminen vaikuttaa työasemien lukitsemiseen interventiossa?

Tutkimuksen havaintojakson aikana työasemien lukitseminen lisääntyi selvästi. Yksittäisen session lukittunaoloajan mediaani kasvoi 45 minuuttia. Myös yhdessä sessiossa tehtyjen lukitusten kappalemäärän mediaani kasvoi yhdestä kahteen. Täysin lukitsemattomien sessioiden suhteellinen osuus kaikista laski noin 20 prosenttiyksikköä. Havaintojakson aikana suurin osa käyttäjistä lisäsi työasemien lukitsemista tai vähintään säilytti saman lukitsemistason. Interventiolla voitiin siis lisätä työasemien lukitsemista. Kahden ensimmäisen intervention yhteenlaskettu lyhyen aikavälin kasvu lukitsemisaktiivisuudessa oli 30%. Tutkimuksessa ei havaittu viitteitä siitä, että intervention vaikutus olisi ollut väliaikaista. Intervention jokaisesta toistosta havaittiin olevan hyötyä vähintään organisaation käyttäjien jonkin osajoukon kannalta. (Kysymykset 1 ja 2).

Ensimmäisessä interventiossa viitekehysvaikutukseen perustuneiden viestien tehon havaittiin olevan hieman parempi kuin suojelumotivaatioteoriaan

pohjautuneiden viestien, kun tarkasteltiin esitarkkailujaksolla vähemmän työasemia lukinneita käyttäjiä. (Kysymys 3)

Suojelumotivaatioteorian uhkan vakavuuden ja todennäköisyyden faktorin tasojen havaittiin olevan yhtä tehokkaita, kun esitarkkailujakson keskimääräinen lukitsemisaktiivisuus oli yksi tai vähemmän päivässä. Vakavuuden ja todennäköisyyden korostaminen kuitenkin oli tehokkaampaa, kun esitarkkailujakson lukitsemisaktiivisuus oli kolme tai enemmän. Neutraalilla tasolla ei ollut enää vaikutusta esitarkkailujakson lukitsemisaktiivisuuden ollessa kolme tai enemmän. Vastatoimen tehokkuuden ja käyttäjän minäpystyvyyden korostaminen oli tehokkaampi esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden ollessa yksi tai vähemmän. Esitarkkailujakson lukitsemisaktiivisuuden arvolla kolme tai enemmän neutraali taso oli tehokkaampi. (Kysymys 4)

Viitekehysvaikutuksen näkökulmista saadun hyödyn korostaminen oli tehokkaampi käyttäjillä, joiden esitarkkailujakson keskimääräinen lukitsemisaktiivisuus oli kolme tai alle. Esitarkkailujaksolla keskimäärin yli kolme lukitsemista päivässä tehneille käyttäjille molemmat teoriat olivat yhtä tehokkaita ja esitarkkailujakson viiden päivittäisen lukitsemisen kohdalla kummallakaan näkökulmalla ei ollut enää vaikutusta. (Kysymys 5)

Suojelumotivaatioteorian viesteissä henkilökohtaisen relevanssin korostaminen oli tehokkaampaa käyttäjille, joilla esitarkkailujakson lukitsemisaktiivisuus oli yksi tai vähemmän. Esitarkkailujaksolla kolme lukitusta päivässä tai enemmän tehneillä pelkkä organisaatiokohdistus oli tehokkaampi. Henkilökohtaisen relevanssin korostamisen vaikutus heikkeni ja organisaatiokohdistuksen vaikutus puolestaan kasvoi esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden kasvaessa. Henkilökohtaisen relevanssin korostamisella ei ollut enää vaikutusta esitarkkailujakson lukitsemisaktiivisuuden arvoilla viisi tai enemmän. Kuvailun tarkkuudella ei näyttänyt suojelumotivaatioteorian viesteissä olevan juurikaan merkitystä ja molemmat faktorin tasot olivat kutakuinkin yhtä tehokkaita. Esitarkkailujaksolla keskimäärin viisi kertaa päivässä tai useammin lukinneiden joukossa matala kuvailun tarkkuus saattoi olla hieman tehokkaampi.

Viitekehysvaikutuksen viesteissä organisaatiokohdistus oli tehokkaampi käyttäjille, jotka eivät esitarkkailujaksolla olleet lukinneet työasemaa kertaakaan. Esitarkkailujaksolla keskimäärin kerran päivässä lukinneilla henkilökohtaisen relevanssin korostaminen sekä pelkkä organisaatiokohdistus olivat kummatkin yhtä tehokkaita. Kolme tai enemmän lukituksia esitarkkailujaksolla tehneille käyttäjille henkilökohtaisen relevanssin korostaminen oli tehokkaampaa. Molempien tasojen vaikutus heikkeni esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden kasvaessa. Keskimääräisen lukitsemisaktiivisuuden ollessa kahdeksan havaittiin lukitsemisaktiivisuutta heikentävä vaikutus. Havainnon arveltiin kuitenkin aiheutuvan lähinnä regression lineaarisuudesta sekä havaintoaineiston painottumisesta vähemmän lukinneisiin käyttäjiin. Viitekehysvaikutuksen viesteissä kuvailun tarkkuus oli sekä matalalla että tarkalla tasolla yhtä tehokas ja vaikutus heikkeni keskimääräisen lukitsemisaktiivisuuden kasvaessa.

Henkilökohtaisen relevanssin vaikutuksen havaittiin siis riippuneen käytetystä pohjaviestistä, kun taas kuvailun tarkkuuden vaikutus oli kummankin teoriapohjan osalta samanlainen. Viestejä muotoiltaessa faktoreiden tasoihin liittyneet ilmaisut oli pyritty pitämään mahdollisimman yhtenäisenä, mutta käytännössä käytetyt ilmaisut eivät kuitenkaan olleet täysin samanlaisia pohjaviestien ja teorioiden erojen vuoksi. Tämä saattoi osaltaan vaikuttaa teorioiden välillä havaittuihin eroihin henkilökohtaisen relevanssin vaikutuksessa. Tarkasteltaessa yhdistettyä henkilökohtaisen relevanssin faktoria havaittiin, että henkilökohtaisen relevanssin korostaminen oli tehokkaampaa esitarkkailujakson lukitsemisaktiivisuuden ollessa yksi tai vähemmän. Kolme tai enemmän lukitsevilla molemmat tasot olivat lähes yhtä tehokkaita ja kummankin tason vaikutus heikkeni esitarkkailujakson lukitsemisaktiivisuuden kasvaessa. Saatuihin tuloksiin vaikutti osaltaan se, että suojelumotivaatiopohjaisen viestin saaneita käyttäjiä oli kokonaisuudessaan enemmän, joten suojelumotivaatioteorian henkilökohtaisen relevanssin faktorin painoarvo oli yhdistetyn faktorin tuloksissa suurempi. Yhdistetyn kuvailun tarkkuuden faktorin vaikutus oli molemmilla tasoilla sama heikentyen esitarkkailujakson lukitsemisaktiivisuuden kasvaessa. (Kysymys 6)

Suojelumotivaatioteorian aiemman tutkimuksen meta-analyysissä (Floyd ym., 2000) minäpystyvyys on havaittu merkittävimmäksi suojelumotivaatiota selittäväksi tekijäksi. Tässä tutkimuksessa minäpystyvyyden korostamisen havaittiin olleen tehokasta vain aiemmin vähän työasemia lukinneille käyttäjille, kun taas minäpystyvyyden kannalta neutraalit viestit havaittiin tehokkaammiksi enemmän työasemiaan lukinneille käyttäjille. Nyt saadut tulokset eivät siis anna tukea minäpystyvyydelle tärkeimpänä motivoivana tekijänä, kun tarkastellaan todellista käyttäytymistä työasemien lukitsemisen kontekstissa. Uhkan vakavuuden ja todennäköisyyden korostamisen havaittiin olevan tehokasta aiemmasta lukitsemisesta riippumatta. Saatuja tuloksia aiempiin tutkimuksiin verrattaessa on syytä huomata, että tässä tutkimuksessa selitettävänä muuttujana oli todellinen käyttäytyminen, kun taas valtaosa aiemmasta tutkimuksesta on keskittynyt käyttäytymisen aikeen tutkimiseen. Lisäys käyttäytymisen aikeessa ei aina lisää todellista käyttäytymistä (Webb & Sheeran, 2006).

Henkilökohtaisen relevanssin mahdollinen puuttuminen tietoturvauhkien kontekstissa on nähty tekijänä, joka pitäisi huomioida, jos tietoturvakäyttäytymiseen halutaan vaikuttaa tehokkaasti. Tässä tutkimuksessa henkilökohtaisen relevanssin sisällyttäminen viesteihin tehosti intervention vaikutusta suojelumotivaatioteorian osalta aiemmin vähemmän lukinneille ja viitekehysvaikutuksen osalta taas aiemmin enemmän lukinneille käyttäjille. Yhdistettynä faktorina henkilökohtaisen relevanssin korostaminen oli mahdollisesti hieman tehokkaampaa vain aiemmin vähän lukinneille. Saadut tulokset eivät siis anna tukea sille, että henkilökohtaisen relevanssin korostamisella saataisiin merkittävästi tehostettua tietoturvakäyttäytymiseen vaikuttamista. Esimerkiksi suojelumotivaatioteorian osalta saadut tulokset indikoivat paljon aiemmin lukinneiden kohdalla päinvastaista.

Viitekehysvaikutuksen tutkimuksen meta-analyysissä (Levin ym., 1998) tavoitekehyksen osalta todetaan negatiivisesti kehystetyn, haittoja korostavan

viestin olevan yleensä tehokkaampi. Tutkimuksissa, joissa asetelma oli tavoitekehyksen mukainen, oli kuitenkin paljon vaihtelua ja systemaattisen tutkimuksen tarvetta korostetaan. Niin ikään tietoturvatutkimuksessa tulokset ovat vaihtelevia ja tutkimusta on tehty vähäisesti. Tässä tutkimuksessa tehokkaammaksi havaittu positiivinen viitekehys havaittiin tehokkaammaksi myös Anderson & Agarwal (2010) tietoturvatutkimuksessa. Toisessa molemmat kehykset sisältäneessä tietoturvatutkimuksessa viitekehysten välillä taas ei havaittu eroa (Barlow ym., 2013). Huomioitavaa on, että aiemmassa tietoturvatutkimuksessa on tutkittu viestin vaikutusta aikeeseen ja tässä tutkimuksessa selitettävänä muuttujana oli todellinen käyttäytyminen. Tutkimustulos on myös sikäli mielenkiintoinen, että aiemmassa tutkimuksessa havaittu negatiivisen viitekehyksen tehokkaampi vaikutus ei tässä tutkimuksessa saanut vahvistusta. Negatiivisen viitekehyksen tehokkuuden hypoteesiin nojaten esimerkiksi Shropshire ym. (2010) tutkimus ei huomioinut positiivista viitekehystä lainkaan, vaan tutkimuksessa tutkittiin ainoastaan negatiivisen viitekehyksen vaikutusta ennaltaehkäisevän (preventiivinen) ja havaitsevan (detektiivinen) tietoturvateknologian käyttöönottoon. Tässä tutkielmassa esitellyn tutkimuksen havaintojen perusteella viitekehysvaikutuksen tietoturvatutkimuksessa on syytä huomioida myös positiivinen kehys.

Tässä tutkimuksessa havaittiin, että intervention vaikutus pieneni esitarkkailujakson keskimääräisen lukitsemisaktiivisuuden kasvaessa. Tämän arveltiin johtuvan siitä, että paljon lukitsevat käyttäjät lukitsevat työasemansa lähes aina poistuessaan työasemalta eikä heillä näin ollen ole juuri varaa parantaa suoritustaan. Suurin muutos lukitsemisaktiivisuudessa havaittiin alle kolme lukitusta tekevillä käyttäjillä, joilla taas oli todennäköisesti enemmän parantamisen varaa lukitsemisessaan.

Seuraavissa alaluvuissa tarkastellaan kokeen reliabiliteettia ja validiteettia sekä tulosten merkitystä käytännölle ja teorialle. Lopuksi esitetään joitain jatkotutkimusideoita.

9.1 Kokeen reliabiliteetti ja validiteetti

Mittauksen reliabiliteetilla tarkoitetaan sitä, että saadut mittaustulokset eivät ole sattumanvaraisia vaan samanlaisissa olosuhteissa saadaan aina samanlaiset tulokset. Tässä tutkimuksessa lukitsemista mitattiin keräämällä suoraan työasemien teknisistä tapahtumalokeista lukitsemiseen liittyneitä tietoja, jotka itsessään ovat täysin luotettavia. Jokainen havaittu lukitseminen siis vastasi todellista työaseman lukittumistapahtumaa. Datankeruujärjestelmään sisällytettiin varmistuksia, joiden avulla voitiin seurata, ettei työasemien raportoimissa datoissa ollut ajallisesti katkoja. On kuitenkin todennäköistä, että pieni osa kokeen aikana tehdyistä lukitsemisista jäi huomaamatta sellaisten teknisten syiden vuoksi, jotka estivät datankeruukomponentin toiminnan yksittäisissä työasemissa. Data saatiin kuitenkin kerättyä valtaosalta aktiivisessa käytössä olleista työasemista, joten

tällä ei tutkimuksen tekijöiden parhaan arvion mukaan ollut merkittävää vaikutusta mittauksen reliabiliteettiin.

Mittauksen validiteetti voidaan jakaa ainakin sisäiseen ja ulkoiseen validiteettiin. Sisäinen validius tarkoittaa sitä, että kokeessa saadut tulokset johtuvat juuri niistä tekijöistä, joista tutkija olettaa niiden johtuvan. Tämän tutkimuksen kannalta keskeistä on siis, että havaittu muutos lukitsemisaktiivisuudessa todella oli intervention aiheuttama eikä johtunut esimerkiksi kokeen ulkopuolisesta, tuntemattomaksi jääneestä tekijästä tai ollut puhtaasti sattumaa. Tutkimuksen koeasetelmaan sisällytettiin kontrolliryhmä, jolle ei lähetetty yhtään interventioviesteistä. Tämän tarkoituksena oli sulkea pois kokeen ulkopuolisten tekijöiden vaikutuksen mahdollisuus. Kontrolliryhmän lukitsemiskäyttäytymisessä ei havaittu äkillisiä muutoksia, jollaisia taas intervention saaneiden käyttäjien lukitsemiskäyttäytymisessä havaittiin interventioiden yhteydessä. Regressioanalyysin tulosten perusteella voitiin taas todeta olevan äärimmäisen epätodennäköistä, että lukitsemisaktiivisuuden muutos interventiossa olisi ollut sattumaa. Lisäksi tutkimuksen salassapidolla varmistettiin, ettei tieto tutkimuksesta päässyt vaikuttamaan organisaation henkilökunnan lukitsemiskäyttäytymiseen.

Tämän tutkimuksen sisäisen validiteetin kannalta eräs heikkous oli, ettei tutkimusasetelmassa ollut mahdollista tietää, ketkä käyttäjistä todellisuudessa lukivat saamansa interventioviestin, luettiinko viesti osittain vai kokonaisuudessaan ja tapahtuiko viestin lukeminen heti lähetyksen jälkeen vai myöhemmin. Tämä saattoi vaikuttaa saatuihin tuloksiin esimerkiksi pienentämällä intervention vaikutusta tai vaikkapa vinouttamalla otosta. Voidaan pitää mahdollisena, että esimerkiksi luonteeltaan huolelliset käyttäjät lukivat todennäköisemmin viestin kokonaan, jolloin interventiossa havaitut tehoerot faktorien vaikutuksissa olisivat perustuneet pääasiassa näihin käyttäjiin. Toiset käyttäjät saattoivat esimerkiksi lukea viestistä pelkän otsikon (engl. subject), jota ei manipuloitu viestin faktorikonfiguraation perusteella. Tällöin heidän käyttäytymisessä havaitut muutokset eivät olisi voineet aiheutua tietystä faktorin tasosta tai faktorin tasojen yhdistelmästä. Otosta saattoi osaltaan vinouttaa myös se, että analyysin yksinkertaistamiseksi tarkasteltavaksi valittiin vain yhden työpäivän kestäneet sessiot. Näin saatettiin rajata tutkimuksen ulkopuolelle käyttäjiä, jotka eivät kirjautuneet työasemaltaan ulos työpäivän päätteeksi vaan jättivät työasemansa lukituksi. On lisäksi mahdollista, että käyttäjät puhuivat keskenään saamistaan viesteistä tai niiden sisällöstä, mikä taas saattoi olla vaikuttava, kontrolloimaton tekijä kokeessa.

Toinen sisäistä validiutta heikentävä asia erityisesti pidemmän aikavälin muutosta tarkasteltaessa oli se, ettei kerätyn datan perusteella ollut mahdollista tunnistaa kaikkia automaattisia työaseman lukittumisia, jotka tapahtuivat tietyn aikaviiveen jälkeen. Automaattisen lukittumisen aikaviive oli organisaation työasemilla käyttäjien itse asetettavissa. Lisäksi tutkimuksen aikana organisaatiossa oli menossa työasemien päivittäminen uuteen käyttöjärjestelmäversioon, jonka yhteydessä työaseman automaattisen lukittumisen aikaviive saattoi lyhentyä. Tämän arveltiin aiheuttaneen ainakin osan havaitusta pidemmän aikavälin kas-

vusta päivittäisissä lukitusten määrissä. Lyhyemmän aikavälin äkillisissä muutoksissa automaattisten lukitusten osuuden arveltiin kuitenkin olevan hyvin pieni, sillä käyttöjärjestelmäpäivityksiä tehtiin tasaisesti työasema kerrallaan koko tutkimuksen ajan.

Ulkoinen validiteetti vaikuttaa siihen, kuinka hyvin tutkimuksessa saadut tulokset ovat yleistettävissä. Tämän tutkimuksen vahvuutena oli intervention saaneiden henkilöiden suuri määrä sekä pitkä tarkkailujakso. Organisaation henkilökunnan työtehtävät ja siten työaseman käyttötavat olivat vaihtelevia, joten tutkimus kattoi suuren määrän erilaisia tapauksia. Lisäksi tutkimusta tehdessä pyrittiin huomioimaan kaikessa, ettei kokeessa käytetty asetelma poikkeaisi organisaation normaalista toiminnasta. Tutkimus toteutettiin kuitenkin vain yhdessä organisaatiossa, jolloin saadut tulokset voivat olla jossain määrin sidoksissa kyseisen organisaation organisaatiokulttuurin, työasemaympäristön sekä toimialan kontekstiin.

9.2 Tulosten merkitys

Tässä luvussa pohditaan saatujen tulosten merkitystä tutkimuksen ja käytännön kannalta.

9.2.1 Tutkimukselle

Tässä tutkielmassa esitetty tutkimus vastaa aiemman tutkimuksen puutteisiin koeasetelmalla, jossa todellista käyttäytymistä tarkkaillaan oikeassa organisaatiossa pitkällä ajanjaksolla. Koska tutkimuksessa interventioviestien sisältöä manipuloitiin eri faktorien osalta, saatiin myös tietoa valittujen faktorien vaikutuksesta käyttäytymiseen. Suojelumotivaatioteorian tutkimuksen kannalta mielenkiintoinen havainto oli, että uhkan vakavuuden ja todennäköisyyden korostaminen eli uhka-arvioon vaikuttaminen oli tehokkaampaa kuin minäpystyvyyden ja vastatoimen tehokkuuden korostaminen eli selviytymisarvioon vaikuttaminen. Lisäksi tutkimuksessa havaittiin, ettei tietoturvauhkalla tarvitse välttämättä olla suoraa henkilökohtaista relevanssia, jotta käyttäjät ryhtyisivät toimiin siltä suojautumiseksi.

Viitekehysvaikutuksen osalta tämä tutkimus lukeutuu harvoihin tietojärjestelmätieteessä tehtyihin tietoturvatutkimuksiin, joissa viitekehysvaikutusta on tutkittu sekä negatiivisen että positiivisen kehyksen osalta. Kyseessä on myös ainoa oikeassa organisaatiossa tapahtuvaa todellisen käyttäytymisen muutosta mitannut tutkimus, jossa hyödynnettiin viitekehysvaikutusta. Tämä tutkimus osoittaa, että myös muiden teorioiden, kuten viitekehysvaikutuksen tutkiminen tietoturvakontekstissa on tarpeellista ja positiivinen vaikutus organisaation tietoturvaan voi lisäksi olla merkittävämpi kuin esimerkiksi paljon hyödynnetyllä suojelumotivaatioteorialla.

Tutkimus osoittaa lisäksi, että tietoturvatutkimusta on mahdollista tehdä myös todellista käyttäytymistä havainnoimalla, ja että tämän kaltaisen tutkimuksen avulla voidaan saada arvokasta tietoa selittävien muuttujien vaikutuksista. Koeasetelma ja tutkimuksen toteutus pyrittiin kuvailemaan tarkkuudella, joka mahdollistaa kokeen toistamisen ja toimii myös apuna uusien todellista käyttäytymistä tutkivien kokeiden suunnittelussa esimerkiksi datankeruun osalta.

9.2.2 Käytännölle

Tutkimuksessa havaittiin kokeellisesti sähköpostiviestin olevan tehokas keino lisätä käyttäjien lukitsemisaktiivisuutta. Myös viestin toistamisen havaittiin olevan hyödyllistä, sillä jokainen toisto lisäsi työasemien lukitsemista interventiota edeltäneeseen tasoon verrattuna. Koska sähköpostiviestin lähettämisen yksikkökustannus on häviävän pieni, voidaan sähköpostiviestintää pitää hyödyllisenä osana organisaation tietoturvan hallintaa. Tutkimuksessa havaittiin lisäksi, että intervention kokonaisvaikutus sekä viestin eri piirteiden korostamisen vaikutus riippuu käyttäjien aiemmasta lukitsemisaktiivisuudesta. Tehokkaan intervention toteuttamiseksi voikin olla siis hyödyllistä kerätä etukäteen tietoa käyttäjien nykyisestä käyttäytymisestä ja mukauttaa kunkin käyttäjän saama viesti kerätyn tiedon perusteella. Näin intervention vaikutus kokonaisuudessaan voidaan pyrkiä maksimoimaan.

Tämän tutkimuksen yksi merkittävistä kontribuutioista oli havainto positiivisen kehystämisen, eli toiminnasta saatavan hyötyjen korostamisen, tehokkuudesta keinona vaikuttaa lukitsemisaktiivisuuteen. Tehokkaan tietoturvaviestinnän ei tarvitse siis välttämättä olla uhkakuvia herättävää pelottelua, vaan se voi olla myös positiivista toiminnan etujen korostamista.

9.3 Jatkotutkimusideoita

Tutkielman laajuus asetti rajoitteita aineiston analyysille. Tutkimuksessa kerätystä aineistosta ei tarkasteltu tässä tutkielmassa interventioiden kumulatiivista vaikutusta tai faktoreiden tarkempia yhteisvaikutuksia. Kerättyä aineistoa hyödyntäen olisikin mahdollista tutkia lukitsemiskäyttäytymistä ja interventioiden vaikutusta käyttäytymiseen syvemmällä tasolla. Lisäksi kokeen toistaminen toisessa organisaatiossa voisi antaa arvokasta tietoa siitä, kuinka hyvin nyt tehdyn tutkimuksen tulokset ovat yleistettävissä muihin organisaatioihin.

Yhteistyö tutkijoiden ja organisaation IT-osaston välillä mahdollistaa monipuolisesti erilaisten todellista käyttäytymistä havainnoivien tutkimusten toteuttamisen. Keskeistä tällaisia tutkimuksia suunniteltaessa on ymmärtää, minkälaista dataa organisaation tietojärjestelmistä on mahdollista saada ja miten tätä dataa voidaan hyödyntää tietoturvakäyttäytymisen mittaamiseen. Tutkimuksen kannalta mielenkiintoista objektiivista dataa tuottavia tietojärjestelmiä voisivat

työasemien lisäksi olla esimerkiksi sähköpostijärjestelmä, työasemien, mobiililaitteiden ja käyttäjätunnusten hallintajärjestelmät, palveluhallinnanjärjestelmät ja tietoverkon laitteet. Hyödyntämällä organisaation olemassa olevia tietojärjestelmiä voitaisiin tietoturvatutkimuksen painopistettä siirtää käyttäytymisen aikeen kyselemisestä todellisen käyttäytymisen havainnointiin.

LÄHTEET

Allison, P. D. (1999). Multiple Regression: A Primer. Pine Forge Press.

Anderson, & Agarwal. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly, 34(3), 613. https://doi.org/10.2307/25750694

Andress, J. (2014). What is Information Security? Teoksessa The basics of Information security: Undestanding the fundamentals of InfoSec in Theory and Practice (ss. 1–22). Syngress.

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? Proceedings of the International Conference on Cyber Security for Sustainable Society, 118–131.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security, 39(PART B), 145–159. https://doi.org/10.1016/j.cose.2013.05.006

Beautement, A., Sasse, M., & Wonham, M. (2009). The compliance budget: Managing security behaviour in organisations. Proceedings of the 2008 Workshop on New Security Paradigms, 47–58. https://doi.org/10.1145/1595676.1595684

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Quarterly, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32(JUNE), 90–101. https://doi.org/10.1016/j.cose.2012.09.010

D 'arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1). https://doi.org/10.1287/isre.1070.0160

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Elliott, J., Holland, J., & Thomson, R. (2012). Longitudinal and Panel Studies. Teoksessa The SAGE Handbook of Social Rsearch Methods (ss. 228–248). Sage Publications Ltd. https://doi.org/10.4135/9781446212165

Fehr, B., & Russell, J. A. (1984). Concept of emotion viewed from a prototype perspective. Journal of Experimental Psychology: General, 113(3), 464–486. https://doi.org/10.1037/0096-3445.113.3.464

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Gross, C. (2017). Field Experiments. Teoksessa The SAGE Encyclopedia of

Communication Research Methods (ss. 561–563). https://doi.org/10.4135/9781483381411

Hibbert, S., Smith, A., Davies, A., & Ireland, F. (2007). Guilt appeals: Persuasion knowledge and charitable giving. Psychology and Marketing, 24(8), 723–742. https://doi.org/10.1002/mar.20181

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? Computers & Security, 21(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and Persuasion: Psychological Studies of Opinion Change. Yale University Press.

Janis, I. L. (1967). Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research. Advances in Experimental Social Psychology, 3, 166–224. https://doi.org/10.1016/S0065-2601(08)60344-5

Janis, I. L., & Feshbach, S. (1953). Effects of fear-arousing communications. Journal of Abnormal and Social Psychology, 48(1), 78–92. https://doi.org/10.1037/h0060732

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). an Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats To the Human Asset Through Sanctioning Rhetoric 1. MIS Quarterly, 39(1), 113–134. https://doi.org/https://doi.org/10.25300/misq/2015/39.1.06

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. Econometrica (pre-1986), 47(2), 263.

King, M. F., & Bruner, G. C. (2000). Social desirability bias: A neglected aspect of validity testing. Psychology and Marketing, 17(2), 79–103. https://doi.org/10.1002/(SICI)1520-6793(200002)17:2<79::AID-MAR2>3.0.CO;2-0

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597–607. https://doi.org/10.1016/j.im.2003.08.001

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. Teoksessa Proceedings of the Annual Hawaii International Conference on System Sciences (ss. 2978–2987). https://doi.org/10.1109/HICSS.2013.192

Leeper, T. J. (2017). margins: Marginal Effects for Model Objects. Noudettu 19. huhtikuuta 2018, osoitteesta https://github.com/leeper/margins

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. Advances in Experimental Social Psychology, 5(C), 119–186. https://doi.org/10.1016/S0065-2601(08)60091-X

Levin, I. P., & Gaeth, G. J. (1988). How Consumers are Affected by the Framing of Attribute Information Before and After Consuming the Product. Journal of Consumer Research, 15(3), 374. https://doi.org/10.1086/209174

Levin, I. P., Schneider, S., & Gaeth, G. (1998). All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects. Organizational behavior and human decision processes, 76(2), 149–188.

https://doi.org/10.1006/obhd.1998.2804

Levin, I. P., Schnittjer, S. K., & Thee, S. L. (1988). Information framing effects in social and personal decisions. Journal of Experimental Social Psychology, 24(6), 520–529. https://doi.org/10.1016/0022-1031(88)90050-9

McGlothlin, W. H. (1956). Stability of Choices among Uncertain Alternatives. The American Journal of Psychology, 69(4), 604. https://doi.org/10.2307/1419083

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems, 34(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Meyerowitz, B. E., & Chaiken, S. (1987). The effect of message framing on breast self-examination attitudes, intentions, and behavior. Journal of personality and social psychology, 52(3), 500–510. https://doi.org/10.1037/0022-3514.52.3.500

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

O'Leary, J. G. (2014). Building and Maintaining an Effective Security Awareness Program. Teoksessa Information Security Fundamentals (2. p., ss. 109–145). Auerbach Publications.

Peltier, T. R. (2014). Information Security Fundamentals. Teoksessa Information Security Fundamentals (2. p.). Auerbach Publications.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers and Security, 31(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. Journal of Homeland Security and Emergency Management, 11(4), 489–510. https://doi.org/10.1515/jhsem-2014-0035

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. Journal of Management, 12(4), 531–544. https://doi.org/10.1177/014920638601200408

R Core Team. (2013). R: A Language and Environment for Statistical Computing. Noudettu 20. elokuuta 2004, osoitteesta http://www.r-project.org/

Rogers, R. W. (1975). A Protection Motivation Theory Of Fear Appeals And Attitude Change. Journal of Psychology: Interdisciplinary and Applied, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitute Change: A Revised Theory of Porotection Motivation. Social Psychophysiology: A Sourcebook. https://doi.org/10.1093/deafed/ent031

Rosemann, M., & Vessey, I. (2008). Toward improving the relevance of information systems research to practice: The role of applicability checks. Mis Quarterly, 32(1), 1–22. https://doi.org/10.2307/25148826

Rothman, A. J., Bartels, R. D., Wlaschin, J., & Salovey, P. (2006). The Strategic Use of Gain- and Loss-Framed Messages to Promote Healthy Behavior: How Theory Can Inform Practice. Journal of Communication, 56, 202–220.

https://doi.org/10.1111/j.1460-2466.2006.00290.x

Rothman, A. J., & Salovey, P. (1997). Shaping perceptions to motivate healthy behavior: the role of message framing. Psychological Bulletin, 121(1), 3–19. https://doi.org/10.1037/0033-2909.121.1.3

Ruiter, R. A. C., Kessels, L. T. E., Peters, G. J. Y., & Kok, G. (2014). Sixty years of fear appeal research: current state of the evidence. International journal of psychology : Journal international de psychologie, 49(2), 63–70. https://doi.org/10.1002/ijop.12042

Schutt, R. K. (2011). Investigating the Social World: The Process and Practice of Research (7. p.). Sage Publications.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2005). Experiments and generalized causal inference. Experimental and quasi-experimental designs for generalized causal inference, 100(470), 1–81. https://doi.org/10.1198/jasa.2005.s22

Shropshire, J. D., Warkentin, M., & Johnston, A. C. (2010). Impact of Negative Message Framing on Security Adoption. Journal of Computer Information Systems, 51(1), 41–52.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International Journal of Information Security and Privacy, 9(1), 26–46. https://doi.org/10.4018/IJISP.2015010102

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers and Security. https://doi.org/10.1016/j.cose.2004.07.001

Stiff, J. B., & Mongeau, P. A. (2003). Persuasive Message Characteristics: Emotional Appeals. Teoksessa Persuasive Communication (2nd Editio, ss. 145–164). New York: The Guilford Press.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. Science, 211(4481), 453–458. https://doi.org/10.1126/science.7455683

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49, 190–198. https://doi.org/10.1016/j.im.2012.04.002

Verizon Enterprise. (2018). 2018 Data Breach Investigations Report.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. Decision Support Systems. https://doi.org/http://dx.doi.org/10.1016/j.dss.2016.09.013

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. Psychological bulletin, 132(2), 249–268. https://doi.org/10.1037/0033-2909.132.2.249

Whitman, M. E., & Mattord, H. J. (2011). Implementing Information Security. Teoksessa Principles of Information Security (4. p., ss. 433–469). Cengage Learning.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs. https://doi.org/10.1080/03637759209376276

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yhteiskuntatieteellinen tietoarkisto. (2018). Aineistonhallinnan käsikirja [verkkojulkaisu]. Noudettu 15. toukokuuta 2018, osoitteesta http://www.fsd.uta.fi/aineistonhallinta/fi/

LIITE 1 SUOJELUMOTIVAATIOTEORIAAN POHJAUTUVAT INTERVENTIOVIESTIT

Faktorikonfiguraatio (2^4 faktorikoeasetelma)

#	Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1	0 = Neutraali	0 = Organisaatio	0 = Matala	0 = Neutraali
2	0 = Neutraali	1 = Organisaatio + henkilökohtainen	0 = Matala	0 = Neutraali
3	0 = Neutraali	0 = Organisaatio	1 = Tarkka	0 = Neutraali
4	0 = Neutraali	1 = Organisaatio + henkilökohtainen	1 = Tarkka	0 = Neutraali
5	0 = Neutraali	0 = Organisaatio	0 = Matala	1 = Korostettu
6	0 = Neutraali	1 = Organisaatio + henkilökohtainen	0 = Matala	1 = Korostettu
7	0 = Neutraali	0 = Organisaatio	1 = Tarkka	1 = Korostettu
8	0 = Neutraali	1 = Organisaatio + henkilökohtainen	1 = Tarkka	1 = Korostettu
9	1 = Korkea	0 = Organisaatio	0 = Matala	0 = Neutraali
10	1 = Korkea	1 = Organisaatio + henkilökohtainen	0 = Matala	0 = Neutraali
11	1 = Korkea	0 = Organisaatio	1 = Tarkka	0 = Neutraali
12	1 = Korkea	1 = Organisaatio + henkilökohtainen	1 = Tarkka	0 = Neutraali
13	1 = Korkea	0 = Organisaatio	0 = Matala	1 = Korostettu
14	1 = Korkea	1 = Organisaatio + henkilökohtainen	0 = Matala	1 = Korostettu
15	1 = Korkea	0 = Organisaatio	1 = Tarkka	1 = Korostettu
16	1 = Korkea	1 = Organisaatio + henkilökohtainen	1 = Tarkka	1 = Korostettu

Faktorien selitykset

Uhkan taso ~ Kuinka vakavaksi ja todennäköiseksi uhka kuvaillaan.
Uhkan kohdistuminen ~ Uhkan kohdistumisen painottaminen viestissä
Kuvailun tarkkuus ~ Kuinka yksityiskohtaisesti uhkan seuraamukset kuvaillaan
Pystyvyys ~ Korostetaanko ehdotetun vastatoimen tehokkuutta ja käyttäjän minäpystyvyyttä toimen suorittamiseksi

Interventioryhmä #1

Uhkan taso	Uhkan kohdistu-minen	Kuvailun tark-kuus	Pystyvyys
0 = Neutraali	0 = Organisaatio	0 = Matala	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization>. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L.

To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #2

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	1 = Organisaatio + Henkilökohtainen	0 = Matala	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization> as well as your own information security. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #3

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	0 = Organisaatio	1 = Tarkka	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi tiedostot, verkkolevyt, sähköposti ja kalenteri. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö saattaa päästä myös SAP:n ja <sisäinen verkkopalvelu> kaltaisiin selaimilla käytettäviin palveluihin.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization>. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password. These can include files, network folders, email, and calendars. With the user account information remembered by web browsers the intruder could also gain access to web-based services such as SAP and <internal web service>.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #4

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	1 = Organisaatio + Henkilökohtainen	1 = Tarkka	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi työtiedostot ja henkilökohtaiset tiedostosi, kotihakemistosi, verkkolevyt sekä sähköpostisi ja kalenterisi. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö saattaa päästä myös SAP:n, <sisäinen verkkopalvelu>, Gmailin ja Facebookin kaltaisiin selaimilla käytettäviin palveluihin.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization> as well as your own information security. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password. These can include your work and personal files, your home directory and network folders, and your email and calendars. With the user account information remembered by web browsers the intruder could also gain access to web-based services such as SAP, <internal web service>, Gmail and Facebook.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L.

To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #5

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	0 = Organisaatio	0 = Matala	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization>. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #6

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	1 = Organisaatio + Henkilökohtainen	0 = Matala	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin

sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization> as well as your own information security. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #7

Uhkan taso	Uhkan kohdistu-minen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	0 = Organisaatio	1 = Tarkka	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi tiedostot, verkkolevyt, sähköposti ja kalenteri. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö saattaa päästä myös SAP:n ja <sisäinen verkkopalvelu> kaltaisiin selaimilla käytettäviin palveluihin.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization>. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password. These can include files, network folders, email, and calendars. With

the user account information remembered by web browsers the intruder could also gain access to web-based services such as SAP and <internal web service>.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #8

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
0 = Neutraali	1 = Organisaatio + Henkilökohtainen	1 = Tarkka	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema voi olla tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, saatat vaarantaa <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa voisi halutessaan käyttää auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö voisi päästä käsiksi tunnuksellasi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi työtiedostot ja henkilökohtaiset tiedostosi, kotihakemistosi, verkkolevyt sekä sähköpostisi ja kalenterisi. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö saattaa päästä myös SAP:n, <sisäinen verkkopalvelu>, Gmailin ja Facebookin kaltaisiin selaimilla käytettäviin palveluihin.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä

CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation may pose a security risk

If you leave your workstation unsupervised and logged in with your user account, you may compromise the information security of the <organization> as well as your own information security. While you are away, anyone could gain access to your workstation and use it with your identity. This way an unauthorized person could use your user account to access all services and resources that do not ask for your password. These can include your work and personal files, your home directory and network folders, and your email and calendars. With the user account information remembered by web browsers the intruder could also gain access to web-based services such as SAP, <internal web service>, Gmail and Facebook.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #9

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	0 = Organisaatio	0 = Matala	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization>. While you are away, anyone can gain direct access to your workstation and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #10

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	1 = Organisaatio + Henkilökohtainen	0 = Matala	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization> as well as your own information security. While you are away, anyone can gain direct access to your workstation

and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #11

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	0 = Organisaatio	1 = Tarkka	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi tiedostot, verkkolevyt, sähköposti ja kalenteri. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö pääsee myös SAP:n ja <sisäinen verkkopalvelu> kaltaisiin selaimilla käytettäviin palveluihin.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization>. While you are away, anyone can gain direct access to your workstation and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password. These can include files, network folders, email, and calendars. With the user account information remembered by web browsers the intruder is able to access web-based services such as SAP and <internal web service>.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #12

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	1 = Organisaatio + Henkilökohtainen	1 = Tarkka	0 = Neutraali

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi työtiedostot ja henkilökohtaiset tiedostosi, kotihakemistosi, verkkolevyt sekä sähköpostisi ja kalenterisi. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö pääsee myös SAP:n, <sisäinen verkkopalvelu>, Gmailin ja Facebookin kaltaisiin selaimilla käytettäviin palveluihin.

Estät työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Voit lukita Windows-työaseman seuraavasti: paina näppäinyhdistelmää CTRL + ALT + DEL ja valitse "Lock" (Lukitse). Vaihtoehtoisesti voit käyttää näppäinyhdistelmää Windows-lippu + L. Palauttuasi jatkat työskentelyä kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization> as well as your own information security. While you are away, anyone can gain direct access to your workstation and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password. These can include your work and personal files, your home directory and network folders, and your email and calendars. With the user account information remembered by web browsers the intruder is able to access web-based services such as SAP, <internal web service>, Gmail and Facebook.

You can prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. To lock a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To resume work, log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #13

Uhkan taso	Uhkan kohdistu-minen	Kuvailun tark-kuus	Pystyvyys
1 = Korkea	0 = Organisaatio	0 = Matala	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization>. While you are away, anyone can gain direct access to your workstation and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #14

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	1 = Organisaatio + Henkilökohtainen	0 = Matala	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä

CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization> as well as your own information security. While you are away, anyone can gain direct access to your workstation and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #15

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	0 = Organisaatio	1 = Tarkka	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi tiedostot, verkkolevyt, sähköposti ja kalenteri. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö pääsee myös SAP:n ja <sisäinen verkkopalvelu> kaltaisiin selaimilla käytettäviin palveluihin.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization>. While you are away, anyone can gain direct access to your workstation and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password. These can include files, network folders, email, and calendars. With the user account information remembered by web browsers the intruder is able to access web-based services such as SAP and <internal web service>.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:

<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #16

Uhkan taso	Uhkan kohdistuminen	Kuvailun tarkkuus	Pystyvyys
1 = Korkea	1 = Organisaatio + Henkilökohtainen	1 = Tarkka	1 = Korostettu

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 10.5.2017 | Internal bulletin 10 May 2017

Lukitsematon työasema on vakava tietoturvariski

Jos poistut työpisteeltäsi työpäivän aikana ja jätät työasemasi auki omalla tunnuksellasi ilman valvontaa, vaarannat vakavasti <organisaation> tietoturvan lisäksi myös oman tietoturvasi. Sinun poissa ollessasi kuka tahansa pystyy vapaasti käyttämään auki jättämääsi työasemaa sinun nimissäsi. Näin ulkopuolinen henkilö pääsee tunnuksellasi suoraan käsiksi kaikkiin sellaisiin palveluihin ja resursseihin, joita avattaessa ei kysytä salasanaa. Näitä ovat esimerkiksi työtiedostot ja henkilökohtaiset tiedostosi, kotihakemistosi, verkkolevyt sekä sähköpostisi ja kalenterisi. Internet-selaimen muistamien tunnusten avulla ulkopuolinen henkilö pääsee myös SAP:n, <sisäinen verkkopalvelu>, Gmailin ja Facebookin kaltaisiin selaimilla käytettäviin palveluihin.

Estät tehokkaasti työasemasi luvattoman käytön, kun lukitset työasemasi aina sen luota poistuessasi. Lukitseminen on nopeaa ja helppoa: Windows-työasemalla paina näppäimiä CTRL + ALT + DEL ja valitse Lock (Lukitse). Lukitseminen onnistuu kätevästi myös näppäinyhdistelmällä Windows-lippu + L. Palattuasi jatkat työskentelyä suoraan siitä mihin jäit kirjautumalla sisään omalla salasanallasi.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

An unlocked workstation poses a serious security risk

If you leave your workstation unsupervised and logged in with your user account, you severely compromise the information security of the <organization> as well as your own information security. While you are away, anyone can gain direct access to your workstation

and use it with your identity. This way an unauthorized person can freely use your user account to access all services and resources that do not ask for your password. These can include your work and personal files, your home directory and network folders, and your email and calendars. With the user account information remembered by web browsers the intruder is able to access web-based services such as SAP, <internal web service>, Gmail and Facebook.

You can efficiently prevent unauthorized access by locking your workstation whenever you leave it unsupervised during the workday. Locking your workstation is fast and easy: On a Windows workstation, press CTRL + ALT + DEL and select "Lock". Alternatively, you can use the keyboard shortcut Windows key + L. To continue working right where you left off, simply log back in with your password.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For more detailed instructions and information about other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

LIITE 2 VIITEKEHYSVAIKUTUS-POHJAISET INTERVENTIOVIESTIT

Faktorikonfiguraatio (2^3 faktorikoeasetelma)

#	Tyyppi	Kohdistus	Yksityiskohtaisuus
17	0 = Positiivinen kehys	0 = Organisaatio	0 = Matala
18	1 = Negatiivinen kehys	0 = Organisaatio	0 = Matala
19	0 = Positiivinen kehys	1 = Organisaatio + Henkilökohtainen	0 = Matala
20	1 = Negatiivinen kehys	1 = Organisaatio + Henkilökohtainen	0 = Matala
21	1 = Positiivinen kehys	0 = Organisaatio	1 = Tarkka
22	1 = Negatiivinen kehys	0 = Organisaatio	1 = Tarkka
23	1 = Positiivinen kehys	1 = Organisaatio + Henkilökohtainen	1 = Tarkka
24	1 = Negatiivinen kehys	1 = Organisaatio + Henkilökohtainen	1 = Tarkka

Faktorien kuvaus

Tyyppi ~ Viitekehysteorian mukainen positiivinen tai negatiivinen kehys
Uhkan kohdistuminen ~ Kohdistumisen painottaminen viestissä
Kuvailun tarkkuus ~ Kuinka yksityiskohtaisesti viestissä kuvaillaan seurauksia

Interventioryhmä #17

Tyyppi	Kohdistus	Yksityiskohtaisuus
0 = Positiivinen kehys	0 = Organisaatio	0 = Matala

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsemalla työaseman parannat tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Kun lukitset työaseman, kukaan ei voi poissa ollessasi käyttää työasemaa sinun tunnuksellasi ja näin toimimalla parannat <organisaation> tietoturvaa. Lukitsemalla säännöllisesti työasemasi varmistat, että työasemaasi ei väärinkäytetä ja työasemasi on turvassa ulkopuolisilta poissa ollessasi.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Locking your workstation enhances information security

Remember to lock your workstation every time you leave your desk. When the workstation is locked, no one can use it through your user account while you are away. This will improve the <organization>'s information security. By locking your workstation regularly, you can protect it from unauthorized access.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #18

Tyyppi	Kohdistus	Yksityiskohtaisuus
1 = Negatiivinen kehys	0 = Organisaatio	0 = Matala

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsematon työasema heikentää tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Jättäessäsi työasemasi lukitsematta, ulkopuoliset voivat käyttää halutessaan työasemaa sinun tunnuksellasi ja siten vaarannat <organisaation> tietoturvan. Lukitsematon työasema on aina tietoturvariski ja mahdollistaa työaseman väärinkäytön.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Unlocked workstation compromises information security

Remember to lock your workstation every time you leave your desk. When the workstation is left unlocked, anyone can use it through your user account. This compromises the <organization>'s information security. An unlocked workstation is always a risk and enables unauthorized access to the workstation.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #19

Tyyppi	Kohdistus	Yksityiskohtaisuus
0 = Positiivinen kehys	1 = Organisaatio + Henkilökohtainen	0 = Matala

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsemalla työaseman parannat tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Kun lukitset työaseman, kukaan ei voi poissa ollessasi käyttää työasemaa sinun tunnuksellasi ja näin toimimalla parannat <organisaation> tietoturvan lisäksi omaa tietoturvaasi. Lukitsemalla säännöllisesti työasemasi varmistat, että työasemaasi ei väärinkäytetä ja työasemasi on turvassa ulkopuolisilta poissa ollessasi.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin

sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Locking your workstation enhances information security

Remember to lock your workstation every time you leave your desk. When the workstation is locked, no one can use it through your user account while you are away. This will improve the <organization>'s information security as well as your own information security. By locking your workstation regularly, you can protect it from unauthorized access.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #20

Tyyppi	Kohdistus	Yksityiskohtaisuus
1 = Negatiivinen kehys	1 = Organisaatio + Henkilökohtainen	0 = Matala

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsematon työasema heikentää tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Jättäessäsi työasemasi lukitsematta, ulkopuoliset voivat käyttää halutessaan työasemaa sinun tunnuksellasi ja siten vaarannat <organisaation> tietoturvan lisäksi oman tietoturvasi. Lukitsematon työasema on aina tietoturvariski ja mahdollistaa työaseman väärinkäytön.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Unlocked workstation compromises information security

Remember to lock your workstation every time you leave your desk. When the workstation is left unlocked, anyone can use it through your user account. This compromises the <organization>'s information security as well as your own information security. An unlocked workstation is always a risk and enables unauthorized access to the workstation.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #21

Tyyppi	Kohdistus	Yksityiskohtaisuus
0 = Positiivinen kehys	0 = Organisaatio	1 = Tarkka

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsemalla työaseman parannat tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Kun lukitset työaseman, kukaan ei voi poissa ollessasi käyttää työasemaa sinun tunnuksellasi ja näin toimimalla parannat <organisaation> tietoturvaa. Lukitsemalla työasemasi suojaat työtiedostot, sähköpostin, ryhmähakemistot (S-asema) sekä muut <organisaation> palvelut ja resurssit väärinkäytöltä. Myös työaseman internet-selaimen muistamat tunnukset ja salasanat ovat turvassa, kun työasema on lukittu. Lukitsemalla siis estät ulkopuolisilta pääsyn selaimella käytettäviin palveluihin kuten <sisäinen verkkopalvelu> tai SAP. Lukitsemalla säännöllisesti työasemasi varmistat, että työasemaasi ei väärinkäytetä ja työasemasi on turvassa ulkopuolisilta poissa ollessasi.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Locking your workstation enhances information security

Remember to lock your workstation every time you leave your desk. When the workstation is locked, no one can use it through your user account while you are away. This will improve the <organization>'s information security. Locking the workstation will protect your work files, e-mail account, shared directories (the S drive) and other <organization> services and resources from abuse. In addition, login information remembered by web browsers will be kept safe when the workstation is locked, preventing others from accessing web-based services such as <internal web service> and SAP. By locking your workstation regularly, you can protect it from unauthorized access.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #22

Tyyppi	Kohdistus	Yksityiskohtaisuus
1 = Negatiivinen kehys	0 = Organisaatio	1 = Tarkka

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsematon työasema heikentää tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Jättäessäsi työasemasi lukitsematta, ulkopuoliset voivat käyttää halutessaan työasemaa sinun tunnuksellasi ja siten vaarannat <organisaation> tietoturvan. Lukitsemattomalta työasemalta kuka tahansa voi käyttää työtiedostoja, sähköpostia, ryhmähakemistoja (S-asema) sekä muita <organisaation> palveluita ja resursseja poissa ollessasi. Myös internet-selaimen muistamia tunnuksia ja salasanoja voidaan tietämättäsi käyttää lukitsemattomalla työasemalla. Selaimella ulkopuolinen voi päästä palveluihin kuten <sisäinen verkkopalvelu> tai SAP.Lukitsematon työasema on aina tietoturvariski ja mahdollistaa työaseman väärinkäytön.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Unlocked workstation compromises information security

Remember to lock your workstation every time you leave your desk. When the workstation is left unlocked, anyone can use it through your user account. This compromises the <organization>'s information security. From an unlocked workstation, anyone can use your work files, e-mail account, shared directories (the S drive) and other <organization> services and resources while you are away. Web browsers are also vulnerable to abuse as they may remember login information to various web-based services such as <internal web

service> and SAP. An unlocked workstation is always a risk and enables unauthorized access to the workstation.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #23

Tyyppi	Kohdistus	Yksityiskohtaisuus
0 = Positiivinen kehys	1 = Organisaatio + Henkilökohtainen	1 = Tarkka

---

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsemalla työaseman parannat tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Kun lukitset työaseman, kukaan ei voi poissa ollessasi käyttää työasemaa sinun tunnuksellasi ja näin toimimalla parannat <organisaation> tietoturvan lisäksi omaa tietoturvaasi. Lukitsemalla työasemasi suojaat kotihakemistosi (<levykirjain>), sähköpostisi, kalenterisi sekä muut <organisaation> palvelut ja resurssit väärinkäytöltä. Myös työaseman internet-selaimen muistamat tunnukset ja salasanat ovat turvassa, kun työasema on lukittu. Lukitsemalla siis estät ulkopuolisilta pääsyn selaimella käytettäviin palveluihin kuten Facebook, Gmail, <sisäinen verkkopalvelu> tai SAP. Lukitsemalla säännöllisesti työasemasi varmistat, että työasemaasi ei väärinkäytetä ja työasemasi on turvassa ulkopuolisilta poissa ollessasi.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Locking your workstation enhances information security

Remember to lock your workstation every time you leave your desk. When the workstation is locked, no one can use it through your user account while you are away. This will improve the <organization>'s information security as well as your own information security. Locking the workstation will protect your home directory (<drive letter>), e-mail account, calendar and other <organization> services and resources from abuse. In addition, login information remembered by web browsers will be kept safe when the workstation is locked, preventing others from accessing web-based services such as Facebook, Gmail, <internal web service> and SAP. By locking your workstation regularly, you can protect it from unauthorized access.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>

Interventioryhmä #24

Tyyppi	Kohdistus	Yksityiskohtaisuus
1 = Negatiivinen kehys	1 = Organisaatio + Henkilökohtainen	1 = Tarkka

OTSIKKO: [organisaatiotunniste] Älä jätä työasemaasi lukitsematta | Do not leave your workstation unlocked

---

Sisäinen tiedote 25.10.2017 | Internal bulletin 25 October 2017

Lukitsematon työasema heikentää tietoturvaa

Muista lukita työasemasi aina poistuessasi työpisteeltäsi. Jättäessäsi työasemasi lukitsematta, ulkopuoliset voivat käyttää halutessaan työasemaa sinun tunnuksellasi ja siten vaarannat <organisaation> tietoturvan lisäksi oman tietoturvasi. Lukitsemattomalta työasemalta kuka tahansa voi käyttää kotihakemistoasi (<levykirjain>), sähköpostiasi, kalenteriasi sekä muita <organisaation> palveluita ja resursseja poissa ollessasi. Myös internet-selaimen muistamia tunnuksia ja salasanoja voidaan tietämättäsi käyttää lukitsemattomalla työasemalla. Selaimella ulkopuolinen voi päästä palveluihin kuten Facebook, Gmail, <sisäinen verkkopalvelu> tai SAP. Lukitsematon työasema on aina tietoturvariski ja mahdollistaa työaseman väärinkäytön.

Työaseman lukitseminen tarkoittaa työaseman sulkemista niin, että käytön jatkaminen vaatii salasanaa. Annettuasi salasanasi työpöytä aukeaa samaan kohtaan, kuin mihin aiemmin sen jätit. Työasema kannattaa lukita aina, kun poistut työpisteeltä esimerkiksi syömään, kahville, tulostamaan tai muille asioille työpäivän aikana.

Lukitset työasemasi (Windows-työasemalla) näppäinyhdistelmällä CTRL + ALT + DEL ja sen jälkeen valitsemalla avautuvasta valikosta Lock (Lukitse). Vaihtoehtoisesti voit lukita työasemasi näppäinyhdistelmällä Windows-lippu + L.

Työpäivän päätteeksi työasemalta kannattaa pelkän lukitsemisen sijaan kirjautua ulos.

Tarkemmat ohjeet sekä tietoa muiden käyttöjärjestelmien lukitustoiminnosta löydät:
<linkki ohjeisiin kuinka työasema lukitaan>

Lisätietoja:
<Yhteystiedot>

--

Unlocked workstation compromises information security

Remember to lock your workstation every time you leave your desk. When the workstation is left unlocked, anyone can use it through your user account. This compromises the <organization>'s information security as well as your own information security. From an unlocked workstation, anyone can use your home directory (<drive letter>), e-mail account, calendar and other <organization> services and resources while you are away. Web browsers are also vulnerable to abuse as they may remember login information to various web-based services such as Facebook, Gmail, <internal web service> and SAP. An unlocked workstation is always a risk and enables unauthorized access to the workstation.

After the workstation is locked it cannot be used without your password. All programs will be left open and running in the background, and the desktop will open wherever you left

off when you log back in. Your workstation should always be locked when you leave the desk, whether it's for lunch, coffee, to print something, or to run other errands.

You can lock your Windows workstation by pressing CTRL + ALT + DEL and choosing Lock. Alternatively, you can use the keyboard shortcut Windows key + L.

When your workday ends, it is recommended that you log off instead of merely locking the workstation.

For detailed instructions and information on other operating systems:
<link to instructions on how to lock workstation>

Further information:
<Contact information>