VAASAN YLIOPISTO

TEKNIIKAN JA INNOVAATIOJOHTAMISEN YKSIKKÖ

TIETOJÄRJESTELMÄTIEDE

TIETOJENKALASTELUSIMULAATIONA JÄRJESTETYN KOULUTUKSEN VAIKUTUS TYÖNTEKIJÖIDEN KYKYYN TUNNISTAA SÄHKÖPOSTIN KAUTTA TULEVIA TIETOJENKALASTELUVIESTEJÄ

Perttu Toikkanen

Tietojärjestelmätieteen

Pro gradu –tutkielma

VAASA 2020

SISÄLLYSLUETTELO **sivu**

1 JOHDANTO 5

2 TIETOTURVA 7

2.1 Yrityksen tietoturva 7

2.2 Turvallisuus ja tietojenkalastelurikosten vastainen työ 10

2.3 Petoksiin ja tietomurtoihin liittyvä lainsäädäntö 11

2.4 Tietoturvapolitiikka ja -kulttuuri 12

2.5 Tietojenkalastelu 14

3 HENKILÖSTÖN TIETOTURVAKÄYTTÄYTYMINEN JA SEN PARANTAMINEN KOULUTUKSEN AVULLA 21

3.1 Tietoturvakäyttäytyminen ja sen parantaminen 21

3.2 Koulutuksen merkitys tietoturvakäyttäytymisen parantamisessa 27

4 TUTKIMUKSEN HYPOTEESIT JA KOEASETELMA 33

5 AINEISTO, TOTEUTUS JA MENETELMÄT 35

6 KOULUTUSSOVELLUS 38

6.1 Järjestelmän implementointi 38

6.2 Tietojenkalastelusimulaation toimintaperiaate ja koulutuksen toteutus 40

7 TULOKSET 44

7.1 Yleistä tuloksista 44

7.2 Ensimmäiseen hypoteesiin liittyvät tulokset 45

7.3 Toiseen hypoteesiin liittyvät tulokset 52

8 DISKUSSIO JA YHTEENVETO 59

LÄHDELUETTELO 63

LIITTEET

LIITE 1. Wilcoxin testin tulokset

LIITE 2. Ote aineistosta

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Perttu Toikkanen
Tutkielman nimi: Tietojenkalastelusimulaationa järjestetyn koulutuksen vaikutus työntekijöiden kykyyn tunnistaa sähköpostin kautta tulevia tietojenkalasteluviestejä
Ohjaajan nimi: Tero Vartiainen
Tutkinto: Kauppatieteiden maisteri
Ohjelma: Tietojärjestelmätiede
Pääaine: Tietotekniikka
Opintojen aloitusvuosi: 2012
Tutkielman valmistumisvuosi: 2020 **Sivumäärä**: 74

TIIVISTELMÄ:

Tietojenkalastelu (engl. phishing) on maailmanlaajuisesti mittava uhka. Tietojenkalastelu tapahtuu usein sähköpostin välityksellä. Tietojenkalastelua vastaan taisteltaessa voidaan käyttää erilaisia teknologisia ratkaisuja. Se ei kuitenkaan yksin riitä, sillä ihminen eli käyttäjä on aina tietoturvan heikoin lenkki. Ihmisiä on näin ollen koulutettava tunnistamaan tietojenkalasteluun käytettäviä haitallisia sähköpostiviestejä. Tässä tutkimuksessa selvitettiin, kuinka suuri vaikutus koulutuksella on työntekijöiden kykyyn havaita sähköpostitse leviäviä tietojenkalasteluviestejä.

Tutkimuksen teoreettisessa viitekehyksessä paneudutaan tietoturvan ja tietojenkäsittelyn käsitteisiin ja niistä tehtyihin tutkimuksiin. Tietoturvakäyttäytyminen ja sen parantaminen on tutkimuksen kannalta keskeinen asia. Nimenomaan koulutuksen merkitys on tässä keskiössä.

Tutkimuksessa tutkittiin tietoturvakoulutusjärjestelmän tehokkuutta. Kyseisen sovelluksen avulla asiakasyritysten työntekijöille lähetetään tekaistuja kalasteluviestejä sähköpostitse. Koulutussovelluksessa syntynyttä dataa käytettiin tutkimuksessa aineistona.

Henkilöiden sähköpostiin tulevat haitalliset viestit tai linkit voivat olla vaikeasti havaittavissa monestakin eri syystä. Tutkimuksessa saatiin vahva näyttö siitä, että tietojenkalastelusimulaationa järjestetyllä koulutuksella oli suuri vaikutus yrityksen työntekijöiden kykyyn tunnistaa haitallisia sähköposteja. Koulutuksen jatkuessa työntekijöiden kyky tunnistaa kalasteluviestejä parani selvästi.

AVAINSANAT: tietoturva, tietojenkalasteluviestit, tietojenkalastelusimulaatio, koulutus

UNIVERSITY OF VASA
Faculty of technology
Author: Perttu Toikkanen
Topic of the Master's Thesis: Affect of simulated phishing training on employees ability to recognize malicious emails
Instructor: Tero Vartiainen
Degree: Master of Science in Economics and Business Administration
Major: Computer Science
Degree Programme: Information Systems
Year of Entering the University: 2012
Year of Completing the Master's Thesis: 2020 **Pages**: 74

ABSTRACT:

Phishing is a major threat worldwide. Phishing often happens via email. In the fight against phishing, a variety of technological solutions can be used. However, that alone is not enough, as the human being, i.e. the user, is always the weakest link in security. Therefore, people need to be trained to identify malicious e-mails used for phishing. This study examined the impact of training on employees' ability to detect phishing messages spread by e-mail.

The theoretical framework of the research focuses on the concepts of information security and data processing and the research conducted on them. Behavior towards data security and its improvement is central to this research. More specifically the importance of training and education is in the focus.

An information security training system was used in the study. This training application, which effectiveness was studied in the study, is in use in many companies. The application is used to send fake phishing messages by e-mail to employees of companies that are using the training application. Data generated by the training application was used as data for the study.

Malicious messages or links to individuals' emails can be difficult to detect for a variety of reasons. The study provided strong evidence that simulatied phishing training had a major impact on the ability of a company's employees to identify malicious emails. As the training continued, the ability of employees to recognize phishing messages clearly improved.

KEYWORDS: information security, phishing messages, phishing simulation, training

1 JOHDANTO

Tämän tutkielman aiheena on tietojenkalastelusimulaationa järjestetyn koulutuksen vaikutus yritysten kykyyn ehkäistä tietoturvauhkia. Tutkielmassa tullaan selvittämään, kuinka suuri vaikutus koulutuksella on työntekijöiden kykyyn havaita sähköpostitse leviäviä tietojenkalasteluviestejä.

Tietojenkalastelusimulaatiolla tarkoitetaan tässä tutkielmassa koulutusta, jossa käytetään koulutusmenetelmänä tekaistuja kalasteluviestejä. Nämä viestit simuloivat aitoja kalasteluviestejä, jotka ovat kuitenkin käyttäjälle turvallisia. Koulutukseen osallistuville henkilöille lähetetään simuloituja uhkia noin kerran viikossa. Heidän tehtävänsä on oppia tunnistamaan epäilyttävät sähköpostiviestit.

Tietoturvallisuuden suurin uhka on monien tutkimusten mukaan käyttäjä itse. Uhkaa vastaan pyritään suojautumaan koulutuksella. Sen avulla pyritään vaikuttamaan käyttäjän tekemiin valintoihin siten, että tietoturvallisuus paranee. Toimintatavat ja asenteet, joita työntekijä saattaa kohdata jokapäiväisissä tilanteissa vaativat huolellista paneutumista. Käyttäjiä on neuvottava ja ohjattava tietoturvallisuudesta. Tietoturvallisuuskoulutusta on järjestettävä henkilöstölle säännöllisesti. Henkilöstöön liittyvien tietoturvariskien lisäksi päivitetään tietenkin virustorjuntaa ja huolehditaan palomuurista.

Tietoyhteiskunnan kehittyminen ja tietoverkot ovat lisänneet tietoturvallisuuden merkitystä. Tietoturvallisuus on nykyisin kaikissa yrityksissä keskeinen asia. Yrityksillä on paljon luottamuksellista tietoa, joka on suojattava ulkopuolisilta. Henkilöstö muodostaa merkittävän tietoturvariskin yrityksille (Hu, Dinev, Hart & Cooke 2012).

Kyberturvallisuuskeskuksen (2020a: 24-25) mukaan hyvä turvallisuuskulttuuri on edellytys sille, että henkilöstö sitoutuu kyberturvallisuuteen.

Yrityksen työntekijöiden kyky noudattaa organisaation tietoturvakäytäntöjä on yleisesti tunnistettu haaste ja uhka tietoturvan kannalta (Karjalainen 2011). Tietoturvan kehittyessä rikollisten mahdollisuudet päästä käsiksi arkaan tietoon tai tietojärjestelmiin ovat vaikeutuneet huomattavasti. Teknisten ratkaisujen parannuttua tietoturva-aukkoja on vaikea löytää. Sen sijaan tietojenkalastelu ja ihmisten huolimattomuus on suuri uhka. Yksittäisillä henkilöillä ja yrityksen työntekijöillä on pääsy moniin järjestelmiin, jotka sisältävät arvokasta tietoa. Käyttäjätunnukset ja salasanat suojaavat yleensä näitä

järjestelmiä. Ne ovat yksittäisen työntekijöiden hallussa ikään kuin avaimet lukittuun oveen. Tietojenkalastelussa käytetään erilaisia manipuloinnin keinoja, joilla pyritään siihen, että käyttäjä luovuttaa kyseiset avaimet hyökkäyksen tekijälle. Yritysten henkilöstö voi kohdata erilaisia tietoturvauhkia. Vääränlaisen linkin tai liitetiedoston avaaminen on vain yksi näistä.

Yritysten tietoturvaa ja tietoturvakoulutusta on tutkittu aikaisemmin paljon, mutta tietoturvakoulutuksen vaikutuksia on haastava tutkia, sillä se vaatii varsin paljon aikaa. Tässä tutkimuksessa pyritään löytämään osittaisia vastauksia koulutuksen tuloksiin, ja siihen voiko tietojenkalastelusimulaatiolla vaikuttaa yrityksen tietoturvan tasoon. Tutkimus tullaan rajaamaan ainoastaan sähköpostitse tapahtuvaan tietojenkalasteluun.

Tutkielmaan valittiin edellä olevien lähtökohtien pohjalta seuraava tutkimuskysymys:

Miten paljon tietojenkalastelusimulaationa järjestetty koulutus vaikuttaa henkilöstön kykyyn tunnistaa haitallisia sähköposteja?

Tutkimuksen teoriaosassa määritellään tietoturvan käsite ja perehdytään aikaisempiin tutkimuksiin yritysten tietoturvasta sekä tietoturvapolitiikasta ja -kulttuurista. Tämän tutkimuksen kannalta keskeinen käsite on tietojenkalastelu. Tähän käsitteeseen ja siihen liittyviin tutkimuksiin tutustutaan seuraavaksi. Teoriaosassa paneudutaan vielä myös tietoturvakäyttäytymiseen ja sen parantamiseen koulutuksen avulla.

Teoriaosan jälkeen alkaa tutustuminen oman tutkimuksen hypoteeseihin ja koeasetelmaan sekä sen jälkeen aineiston hankkimiseen liittyviin asioihin. Tutkimuksen toteutus ja menetelmät käydään läpi seuraavaksi. Tutkimuksen kannalta keskeinen asia on koulutussovellus ja siihen liittyvät asiat käsitellään huolellisesti. Tutkimuksesta saatuja tuloksia kuvaillaan ja niiden merkitystä pohditaan. Lopuksi käydään läpi mahdollisten jatkotutkimusten aiheita.

2 TIETOTURVA

2.1 Yrityksen tietoturva

Tietoturvalla (eng. infomation security) ja tietoturvallisuudella (eng. data security) tarkoitetaan samaa asiaa. Yleinen suomalainen asiasanasto (2019) suosittelee käyttämään termiä tietoturva.

Tietoturva määritellään Tietotekniikan liiton ja Ilmari Pietarisen (2008: 340) mukaan:

> Tavoitetilaksi, jossa tiedot, tietojärjestelmät ja palvelut suojataan asianmukaisesti siten, että uhat, jotka kohdistuvat tietojen, tietojärjestelmien ja palvelujen käytettävyyteen, eheyteen ja luottamuksellisuuteen, eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille. (Tietotekniikan liitto ym. 2008: 340.)

Valtiovarainministeriö ja Viestintävirasto käyttävät julkaisuissaan edellä mainittua määritelmää. Kyseisen määritelmän mukaan tietoturvalla tarkoitetaan myös lainsäädäntöä ja muita normeja sekä toimenpiteitä, joilla pyritään varmistamaan tietoturva normaali- ja poikkeusoloissa.

Tietoturva määritellään Sanastokeskuksen (2015) mukaan ”järjestelyiksi, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus”. Käytettävyydellä tarkoitetaan määritelmässä sitä, että tieto on saatavilla halutuille henkilöille haluttuna aikana nopeasti ja oikeassa muodossa. Eheydellä puolestaan tarkoitetaan sitä, että tieto on paikkansapitävää ja virheetöntä. Se, että tietoon pääsevät käsiksi vain ne, joilla siihen on oikeus, on luottamuksellisuutta.

Leppäsen (2006: 285) mukaan tietoturva käsitetään helposti liian laajana. Sen ei pitäisi olla teknologiayrityksissä turvallisuusjohtamisen synonyymi.

Jarno Limnéll, Klaus Majewski ja Mirva Salminen (2014: 241) määrittelevät kirjassaan Kyberturvallisuus, tietoturvan seuraavalla tavalla:

> Tiedon suojaaminen ja sen käytön turvaaminen. Vaikka tietoturva yhdistetään yleensä vain sähköisen tiedon salaamiseen tai julkaisemiseen, siihen käsiksi pääsyyn ja sen käsittelemiseen, säilömiseen, kopioimiseen ja siirtämiseen, koskee se yhtä lailla myös fyysisessä muodossa olevaa tietoa. Laajimmillaan tietoturvalla

> voidaan tarkoittaa minkä tahansa tiedon asianmukaista käsittelyä. (Limnéll ym. 2014: 241.)

Kyberturvallisuuskeskuksen (2020a: 4) mukaan kyberturvallisuudella viitataan turvallisuushaasteisiin, joita yhteiskunta ja organisaatiot kohtaavat. Kyberturvallisuudella voidaan tarkoittaa myös niitä toimenpiteitä, joilla kyberuhkiin varaudutaan. Varautuminen on tärkeää, sillä kyberuhilla voi olla vakavia haittoja organisaatiolle.

Termejä tietoturvallisuus ja kyberturvallisuus käytetään usein ristiin. Molemmissa on kyse datan suojaamisesta sekä tietojärjestelmien toiminnan varmistamisesta. Toiminnan tavoitteilla on kuitenkin selvä ero. Tietoturva pyrkii tietojen, tiedostojen ja yksittäisten koneiden suojaamiseen. Tietoturvan avulla suojataan sekä omaa että perheen ja työnantajan toimintaa. Tietoturvan uhkakuvat liittyvät vahinkoihin (laite putoaa, poistamme vahingossa tärkeän tiedoston tms.) tai nettirikollisten tekoihin (urkitaan salasanoja, varastetaan laitteita, murtaudutaan yrityksen verkkoon). Kyberturvallisuus tarkoittaa tietoturvan ulottamista yhteiskunnan peruspalveluihin. (Järvinen 2018: 14-15.)

Työntekijänä yksilöön voi kohdistua tiedon kalastelua tai vakoiluyrityksiä, joiden tavoitteena on varastaa yrityssalaisuuksia tai muuta tärkeää tietoa. Yrityksen jokaisen työntekijän olisi osattava olla valppaana ja heidän kaikkien olisi hallittava turvallisuuden perustaidot, jotta yritykselle ei muodostuisi turvallisuusriskiä. Työntekijä pääsee pitkälle jo sillä, että tiedostaa yleisimmät riskit, hallitsee perusperiaatteet ja käyttää tervettä järkeä. Kirjassa mainitaan seuraavia riskejä: varmuuskopiointi, riittävän vahvat salasanat, eri salasanat eri palveluihin ja näiden vaihtaminen riittävän usein, epäilyttävien sähköpostilinkkien ja liitteiden avaamatta jättäminen, tuntemattomien muistitikkujen tai muiden laitteiden kokeilematta jättäminen, ohjelmistopäivitykset, sähköpostihuijaukset ym. Tällaiset perusasiat olisi laitettava kuntoon. (Limnéll ym. 2014: 49-52.)

Yrityksen tietoturvan kohde on yrityksen tietopääoma. Siihen sisältyvät erilaiset aineettomat oikeudet, kuten esimerkiksi tavaramerkit, patentit ja kehitysprosessit. Siihen sisältyvät myös erilaiset tietokannat, sopimuksiin liittyvät asiat sekä asiakas- ja yhteystiedot. Tietoturvan tavoitteena on se, että tiedon säilyminen, saatavuus ja luottamuksellisuus voidaan turvata. (Limnéll ym. 2014: 55.)

Perinteinen jaottelu, jossa IT-osasto on ollut oma kokonaisuutensa, on jäänyt ajastaan jälkeen. Turvallisuus ei myöskään saisi olla muutaman työntekijän osaamisen varassa. Joissain tilanteissa on taloudellisten säästöjen saamiseksi turvallisuuteen liittyviä asioita

ulkoistettu. Nykyajan turvallisuusajattelun mukaan kyberturvallisuus on nostettava strategisen tason kysymykseksi. Sen on oltava osa kaikkea muuta toimintaa ja näihin haasteisiin vastaaminen vaatii kokonaisnäkemystä yrityksen toiminnasta. Muutoksia ja vaaroja on vaikea havaita. Jos teknologia toimii, se voidaan unohtaa. Jos toiminta häiriintyy tai katkeaa, on yleensä jo liian myöhäistä. Automaation uskotaan tuottavan turvallisuutta, mutta todellisuudessa asia on monimutkaisempi. Uudenlaisia haavoittuvuuksia syntyy läpi liiketoimintaprosessin. Kyberturvallisuudella varmistetaan, että automatisoidut prosessit toimivat ja ettei mikään ulkopuolinen toimija pääse häiritsemään, väärinkäyttämään tai keskeyttämään niitä. Toimintavarmuus on yrityksille tärkeää. Kyberturvallisuuden avulla toimintatapoja voidaan kehittää ja tehostaa. Haavoittuvuuksia ja haittoja syntyy, kun verkottuminen on tiivistä. Vaikutukset voivat olla vakavia. Tulevaisuuden varmistamiseksi on pidettävä turvallisuudesta huolta. Yrityksissä tulisi olla yhteisiä standardeja, kontrolleja, käytäntöjä, raportointia ja häiriönhallintaa. Kyberturvallisuuden kysymysten tulisi olla johtamistoiminnassa keskeinen osa-alue. (Limnéll ym. 2014: 55-58.)

Työntekijän tietoturvatietoisuuden merkitys on yrityksissä suuri. Pelkästään teknisillä ratkaisuilla ei pystytä ratkaisemaan tietoturvan uhkia. Roy Sarkarin (2010) mukaan yritysten tulisi määritellä sisältä tulevat uhat ensimmäiseksi. Olisi arvioitava teknistä toteutusta, tietoturvajärjestelyjä sekä ihmisen käyttäytymistä. Colwillin (2009) tutkimuksen mukaan tietoturvakysymyksissä tulisi huomioida erityisesti työntekijät ja yrityksen sisällä olevat tahot. Teknisissä ratkaisuissa olisi huomioitava ihmisen käyttäytyminen. Tietoturvatietoisuuden lisääminen ja tietoturvakoulutus ovat keskeisessä roolissa yritysten tietoturvaa rakennettaessa.

Computer Crime and Security Survey -tutkimuksessa (2009), jonka Computer Security Institute teki, selvisi, että työntekijän tahattomasta toiminnasta aiheutuvat tietoturvahaitat ovat yleisempiä kuin tahallisesta toiminnasta aiheutuvat haitat.

Työntekijöiden olisi saatava tietää toimintatapojen perimmäiset syyt. Tietoturvasäännöstön laatiminen on tärkeä osa luotettavaa yritysympäristöä. Helsingin seudun kauppakamari ym. (2008: 72) pitävät tärkeänä sitä, että säännöstö olisi lyhyt, selkeä ja käytännönläheinen. Kaikkein tärkein asia on kuitenkin se, että yritysjohto sitoutuu tietoturvakulttuuriin ja antaa sen näkyä yrityksen työntekijöille.

2.2 Turvallisuus ja tietojenkalastelurikosten vastainen työ

Kriminologian ja oikeuspolitiikan instituutti seuraa rikollisuustilannetta ja julkaisee Rikollisuustilanne - katsauksia. Kyberrikollisuudella tarkoitetaan näissä katsauksissa verkossa tapahtuvaa ja verkkovälitteistä rikollisuutta, joka jakautuu tietotekniikkaan kohdistuviin rikoksiin ja tietokoneavusteisiin rikoksiin. Kaikki viranomaisten tietoon tulleet teot, jotka kuuluvat tietomurtojen (tietomurto, tietomurron yritys, törkeä tietomurto, törkeän tietomurron yritys ja suojauksen purkujärjestelmärikos) alaisuuteen, ovat olleet kasvusuuntaisia vuodesta 2014 lähtien. Haittaohjelmat, kuten esimerkiksi tietokonevirukset, olivat yleisin verkkorikosten muoto. Yrityksiin kohdistuvista tietomurroista on katsauksen mukaan niukasti tilastointia tai tietolähteitä, sillä niistä ei läheskään aina raportoida yrityksen ulkopuolelle tai viranomaisille. Vuoden 2018 yritysuhritutkimuksen mukaan 6 prosenttia majoitus- ja ravintola-alan yrityksistä ja 7 prosenttia kaupan alan yrityksistä raportoi hyökkäyksistä tietojärjestelmiä kohtaan. (Danielsson 2019.)

Kauppakamarit pyrkivät kehittämään suomalaisten yritysten toimintaedellytyksiä. Ne ovat vuodesta 2005 lähtien kartoittaneet yritysjohtajilta saatujen tietojen perusteella yritysten turvallisuustilannetta. Viimeisin selvitys on tehty vuonna 2017. Sen mukaan riskienhallintaan pitää panostaa, sillä rikosriskit ovat kasvussa. Osa väärinkäytöksistä ja rikoksista kohdistuu tietoon. Tällaisia riskejä saattoivat olla esimerkiksi tietoturvaan murtautuminen, hakkeroinnin yrittäminen tai luvaton kopiointi. Myös identiteettikaappauksia tai kyberhyökkäyksiä sekä palvelunestohyökkäyksiä esiintyi. Näitä turvallisuusriskejä ilmoitti kokeneensa 43 % selvitykseen vastanneista yrityksistä. Riskien arveltiin lisääntyneen paljon tai jonkin verran. Toteutuneita riskejä oli sitä enemmän mitä isommasta firmasta oli kysymys. Tästä toiminnasta on yrityksille taloudellista ja muutakin haittaa. Kauppakamarin mukaan tarvitaan lisää panostusta ongelmien torjumiseksi. Osa yrityksistä ei tunnista riskien olemassaoloa, eikä niin ollen osaa varautua niihin. Osa yrityksistä kaipaa viranomaisilta ja muista lähteistä lisää tietoa aiheesta. (Kauppakamari 2017.)

Liikenne- ja viestintäviraston kyberturvallisuuskeskus antaa ohjeita siitä, miten tulisi toimia, jos havaitsee tietoturvapoikkeaman. Siitä olisi hyvä ilmoittaa sekä viranomaisille että IT-tuelle. Ilmoitus kannatta tehdä useammalle toimijalle, sillä viranomaiset eivät voi vaihtaa tietoja keskenään ilman ilmoittajan lupaa. Ilmoittamisen lisäksi tarvitaan lähes

aina myös käytännön toimienpiteitä. Tilanteet ovat erilaisia ja niiden käsittelyyn ei ole olemassa yhtä toimintamallia. (Kyberturvallisuuskeskus 2020b.)

Kalasteluviestiä on usein vaikea havaita. Selaimen kohdeosoite kannattaa tarkastaa. Sitä katsomalla voi huomata, että linkki on ohjaa tietojenkalastelusivulle aidon kirjautumissivun sijaan. Kyberturvallisuuskeskus suosittaa ottamaan käyttöön kaksivaiheisen kirjautumisen, jossa tavallisen salasanan lisäksi kirjautuminen pitää vahvistaa myös jollakin toisella keinolla, esimerkiksi toiseen päätelaitteeseen tulevan kertakäyttökoodin avulla. (Kyberturvallisuuskeskus 2017.)

Yritykset ilmoittavat tietoturvallisuusloukkauksista Kyberturvallisuuskeskukselle. Niiden avulla Kyberturvallisuuskeskus tiedottaa tilanteesta parantaakseen turvallisuutta. Sama taho auttaa uhkien torjunnassa viranomaisia ja tietoturvayhteisöä. Kyberturvallisuuskeskus tekee yhteistyötä Microsoftin kanssa kootessaan uhan havainnointi- ja torjuntakeinoja koskevia ohjeita. (Kyberturvallisuuskeskus 2018b.)

2.3 Petoksiin ja tietomurtoihin liittyvä lainsäädäntö

Yrityksiin kohdistuvista väärinkäytöksistä osa täyttää rikoksen tunnusmerkit. Turvallisuustilanne on Kauppakamarin (2018a) mukaan Suomessa heikentynyt. Erityisesti suuret yritykset joutuvat rikollisuuden kohteiksi.

Rikoslainsäädännössä puhutaan seuraavanlaisista rikoksista: petos, identiteettivarkaus, kiristys, tietomurto ja markkinointirikos.

Jos teko ei ole rangaistava, poliisi tai syyttäjä eivät tartu ongelmaan. Silloin haitat jäävät yritysten yksin kannettaviksi.

Suomen rikoslain (Rikoslaki 19.12.1889/39) 36 luvun 1 pykälässä petoksesta säädetään seuraavasti:

> Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava petoksesta *sakkoon* tai *vankeuteen* enintään kahdeksi vuodeksi.

> Petoksesta tuomitaan myös se, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa.
>
> Yritys on rangaistava. (Rikoslaki 19.12.1889/39.)

Petos voi olla törkeä tai lievä.

Lievässä petoksessa tavoiteltu hyöty ja aiheutettu vahinko ovat kokonaisuutena arvosteltuna vähäisiä. Siitä tuomitaan sakkorangaistus. Lievän petoksen yritystä ei ole rikoslaissa säädetty rangaistavaksi. (Rikoslaki 19.12.1889/36 3 §.)

Törkeässä petoksessa tavoitellaan huomattavaa hyötyä, aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa, rikos tehdään käyttämällä hyväksi vastuulliseen asemaan perustuvaa erityistä luottamusta tai rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa. (Rikoslaki 19.12.1889/36 2 §.) Rahallista summaa, milloin törkeän petoksen raja ylittyy, ei ole määritelty. Käytännössä kyseessä on tuhansien eurojen varallisuusetu. Törkeän petoksen kohdalla huomattavana hyötynä on pidetty tuhansien eurojen varallisuusetua (Nuutila, Mahanen 2009: 990). Törkeästä petoksesta tuomitaan vankeuteen.

Tietomurroista säädetään Rikoslain tieto- ja viestintärikoksia käsittelevässä luvussa 38, 8 §:ssä seuraavasti:

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (Rikoslaki 19.12.1889/38.)

2.4 Tietoturvapolitiikka ja -kulttuuri

Limnéll ym. (2014) määrittelevät tietoturvapolitiikan seuraavasti:

> Tietoturvapolitiikka on johdon tahtotila siitä, miten organisaatiossa toteutetaan tietoturvaa siten, että se ei estä liiketoimintaa vaan tukee sitä. Organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Yrityksissä on valtavasti luottamuksellista tietoa, joka on suojattava ulkopuolisilta. Näiden tietojen turvaaminen on monelta osin ihmisten ja työntekijöiden yhteinen tehtävä. Kaikissa yrityksissä vallitsee oma kulttuuri, joka määrittelee yrityksen toimintatapoja. Yksi osa yrityskulttuuria on tietoturvakulttuuri. Tietoturvakulttuureita on yhtä monia kuin yrityksiä, ja niitä määrittelee esimerkiksi yrityksen koko ja toimiala. Minkä tahansa kulttuurin tavoin tietoturvan merkitys ja taso määräytyy yksittäisten henkilöiden tavasta toimia yhdessä. Toisin kuin työntekijän osaaminen omassa työtehtävässä, tietoturvan osalta ei voida olettaa tiettyä osaamistasoa. Koska tietoturva ei ole yksittäisen ihmisen tai järjestelmän hallittavissa, on olennaista, että osaamista kehitetään jatkuvasti ja vastuu jakautuu koko organisaation kesken. (Van Niekerk & Von Solms 2010: 476-486.)

Tietoturvasuunnittelun eräänä tavoitteena on luoda organisaatiolle toimiva tietoturvapolitiikka (eng. Information Security Policy). Se muodostuu käytännöistä, joiden avulla haluttu turvallisuuden taso saavutetaan. Tietoturvapolitiikka ohjaa organisaation tietoturvakäytäntöjä ja tietoturvallisuusprosesseja. Tietoturvasuunnitelmassa kuvataan menetelmiä ja teknisiä ratkaisuja. Se voidaan luokitella joko luottamukselliseksi tai salaiseksi. Tietoturvasuunnitelmasta muodostetaan usein erillinen ohje tietojärjestelmän käyttäjiä varten. Se voi muodostua pelkäksi ohjesäännön kaltaiseksi asiakirjaksi. Käytännön kokemukset ovat osoittaneet, etteivät tällaiset dokumentit motivoi tietojärjestelmän käyttäjiä noudattamaan annettuja ohjeita tai määräyksiä. (Hakala, Vainio & Vuorinen 2006: 7-10.)

Moderni tietoturvasuunnittelu perustuu Hakalan ym. (2006: 17-18) mukaan liiketoimintaturvallisuuteen ja kokonaisturvallisuuspolitiikkaan, joka määrittelee tietoturvan tavoitteet. Liian jäykät turvallisuusmääräykset voivat heidän mukaansa vaikeuttaa liiketoimintaa. Tarvitaan tasapainoilua tietoturvan sekä tietojärjestelmien joustavuuden ja palvelutason välillä. Uusi tietoturvasuunnitelma pyritään tekemään tiimi- ja projektityönä. Se laaditaan tietoturvapolitiikassa asetettujen suuntaviivojen pohjalta. Suunnitelma sisältää käytänteet, työmenetelmät ja tekniset ratkaisut. Tietoturvasuunnitelma on näin ollen luottamuksellinen. Se laaditaan keskipitkälle aikavälille ja sitä päivitetään tarvittaessa.

Kyberstrategia vaatii johdon sitoutumista. Yrityksen strategisella tasolla ei ole kaikkea vaadittavaa ymmärrystä asiaan liittyvistä haasteista. Olisikin tärkeätä, että strategiaprosessin toteuttamisessa oltaisiin vuorovaikutuksessa koko yrityksen tasolla. Näin kaikkien osaaminen saadaan käytettyä hyödyksi. (Limnéll ym. 2014: 157-158).

Kyberstrategian ideana on ajattelutavan muutos. Muita kyberstrategian tuloksia ovat muiden muassa reaaliaikainen tilannetietoisuus ja edistyneisiin uhkiin varautuminen. Uhat ovat entistä hienostuneempia ja vaativat moninaisuudessaan uudenlaista ajattelua. Keskitetty turvallisuusjohtaminen mahdollistaa nopeat päivitykset ja parannusten tekemisen. Kyberturvallisuus vaatii rahaa, aikaa ja tietotaitoa. Tietotaito ei ole kiinni työntekijöiden määrästä vaan näiden laadullisesta osaamisesta. Resurssien käytön optimoinnissa tulee keskittyä yksinkertaisuuteen ja toimintakulujen kurissa pitämiseen. (Limnéll ym. 2014: 223-226.)

Kyberturvallisuuskeskuksen (2020a: 3, 24) mukaan yrityksen hallituksella on vastuu siitä, että kyberturvallisuus on hoidettu hyvin. Näin suojataan yrityksen toimintakykyä ja edistetään yrityksen etua. Avoimuus turvallisuuspoikkeamien raportoinnissa on tärkeää.

Organisaation kyberturvallisuustoimenpiteet ja –investoinnit määritetään uhka-arvioiden perusteella. Arvioinnissa määritellään uhkien vaikutuksia ja todennäköisyyksiä, sekä määritellään, millaisia riskejä organisaatio on valmis sietämään. (Kyberturvallisuuskeskus 2020a: 18-20.)

2.5 Tietojenkalastelu

Kyberuhkia on erilaisia. Ne voivat olla esimerkiksi haittaohjelmia tai palvelunestohyökkäyksiä. Tässä tutkielmassa keskitytään kuitenkin vain sähköpostitse tapahtuvaan tietojenkalasteluun.

Termi “phishing” tulee alun perin analogiasta, jossa varhaiset kyberrikolliset käyttivät sähköposteja koukkuina ”kalastettaessa” salasanoja ja saadakseen taloudellisia tietoja internetkäyttäjien “merestä”. ”Ph”:n käyttö terminologiassa on osittain hävinnyt ajan saatossa, mutta liittyy todennäköisesti suosittuihin hakkereiden nimeämiskäytäntöihin, kuten ”phreakeihin”, jotka olivat mukana “phreakamassa” eli hakkeroimassa puhelinjärjestelmiin. (Ollmann 2007: 3.)

Termi phishing otettiin käyttöön laajemmin käyttöön vuonna 1996 hakkereiden toimesta, jotka varastivat America Online (AOL) -tilejä huijaamalla salasanoja hyväuskoisilta AOL internet-palveluntarjoajan käyttäjiltä. Hakkeroituja tilejä ruvettiin kutsumaan phishiksi, ja vuoteen 1997 mennessä phish-tuotteilla tehtiin aktiivisesti kauppaa hakkereiden välillä sähköisen valuutan muodossa. On tutkittuja tapauksia, joissa hakkerit rutiininomaisesti vaihtoivat toimivia AOL-phisejä hakkerointiohjelmistoihin tai varastettuihin sovelluksiin ja peleihin. (Kay 2004; Ollmann 2007: 3.)

Ajan myötä phishing-hyökkäyksen määritelmä on hämärtynyt ja laajentunut. Termi kattaa käyttäjätilitietojen hankkimisen lisäksi myös pääsyn henkilökohtaisiin ja taloudellisiin tietoihin. Alun perin käyttäjien huijaaminen saamalla heidät vastaamaan sähköpostiviesteihin salasanojen ja luottokorttitietojen hankkimiseksi, on nykyään laajentunut myös mm. väärennettyihin verkkosivustoihin ja haittaohjelmiin. Ne tallentavat salasanoja ja ottavat kuvankaappauksia. (Ollmann 2007: 3.)

Tietoturvallisuuden tarve on kasvanut, kun teknologian määrä yhteiskunnassamme on kasvanut. Kyberrikolliset ovat jo pitkään käyttäneet erilaisia tekniikoita luvattoman pääsyn saamiseksi järjestelmiin. Vuosien saatossa kyberrikolliset ovat kuitenkin siirtyneet hyökkäämään koneiden ja järjestelmien sijaan turvallisuuden ketjun heikoimpaan lenkkiin, ihmisiin. (Heartfield & Loukas 2015: 1.)

Verkkourkinta eli tietojenkalastelu (eng. phishing) on yleistynyt tietoturvauhka. Tietojenkalastelu ei ole ilmiönä uusi, mutta sitä on ollut vauhdittamassa internetin ja sähköpostin käytön yleistyminen. Kalastelun tavoitteena on yleensä saada käyttäjä jakamaan luottamuksellista tietoa, kuten käyttäjätunnuksia, henkilötietoja ja salasanoja. Useimmiten hyökkääjä pyrkii saamaan kalastelun avulla tietoa, joka on hyödynnettävissä taloudellisen voiton saavuttamiseksi. Tietojenkalastelussa käytetään yleensä sosiaalisen manipuloinnin tekniikoita, jotka perustuvat henkilöiden hyväuskoisuuteen. Vastaanottajalle pyritään kalasteluviesteissä luomaan uteliaisuutta, pelkoa tai kiireen tuntua. (Hadnagy & Fincher 2015.)

Tietojenkalastelun seurauksena voidaan Kyberturvallisuuskeskuksen mukaan (2020a: 4-6) esimerkiksi harhauttaa organisaation taloushallintoa maksamaan väärennettyjä laskuja tai yrityssalaisuuksia voidaan vakoilla varastettuja käyttäjätunnuksia käyttämällä.

Englantilainen tietoturvayhtiö Sophos on teettänyt kyselyn länsieurooppalaisille IT-johtajille. Siinä kyselyssä yli puolet lähes tuhannesta IT-johtajasta totesi yrityksensä törmänneen tilanteeseen, jossa työntekijät olivat toimineet ei-toivottujen sähköpostien ja niissä olevien linkkien kanssa väärin. Tutkimuksen mukaan suuremmat yritykset joutuvat pieniä yrityksiä todennäköisemmin tietojenkalasteluansoihin. Pienissä yrityksissä henkilökunta saa vähemmän koulutusta tietoturvauhkiin liittyen, mutta silti suuremmat yritykset joutuvat useammin ansojen kohteiksi. Todennäköisesti rikostentekijät tavoittelevat suurempia voittoja ja kohdistavat näin ollen toimintansa kookkaampiin organisaatioihin. (Computer Weekly 2019; Information Age 2019.)

Kyberturvallisuuskeskuksen julkaisun mukaan (2020a: 4-6) tietojenkalastelu on erityisen yleistä Microsoft Office 365 -ympäristössä. Kyberturvallisuuskeskus varoittaa huijausviesteistä useasti. Monet huijauksista ovat hyvin suunniteltuja ja vaikeita havaita huijauksiksi. Julkaisussa on seuraavanlainen esimerkki Office 365 huijausviestistä ja siihen liittyvästä tapahtumaketjusta:

1. Rikollinen lähettää tietojenkalasteluviestin sähköpostitse.

2. Vastaanottaja lukee viestin ja klikkaa siinä olevaa linkkiä.

3. Linkin päässä onkin tietojenkalastelusivu, joka pyytää syöttämään käyttäjätunnuksen ja salasanan.

4. Kalastelusivulle syötetyt tunnukset menevätkin rikollisen tietoon.

5. Haltuunsa saamilla tunnuksilla rikollinen pääsee seuraamaan yrityksen sisäistä liikennettä.

6. Nyt rikollinen pääsee lukemaan esim. laskutusliikennettä.

7. ”Anteeksi, edellinen lasku oli väärä. TÄSSÄ on oikea lasku.”, kirjoittaa rikollinen ja korjaa potin taskuunsa. (Kyberturvallisuuskeskus 2020a: 4.)

Sosiaalinen manipulointi (eng. social engineering) on toimintaa, jossa henkilöä pyritään vakuuttamaan vapaaehtoisesti ja/tai tietämättä antamaan luottamuksellisia tai yksityisiä tietoja tuotteesta tai palvelusta (Gragg 2003:4). Sosiaalisen manipuloinnin hyökkäykset

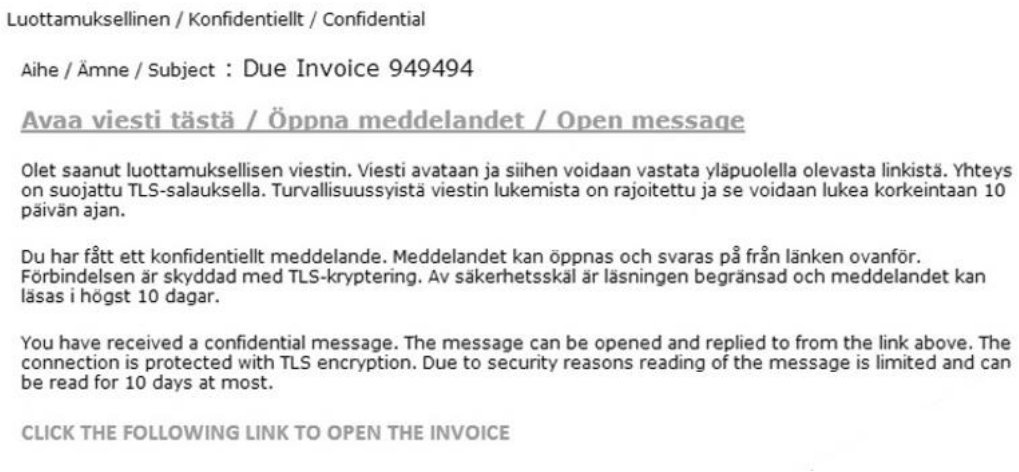
eivät ole mitään uutta, mutta kyberrikollisten tarvitessa enemmän ja enemmän teknistä osaamista, monet ovat palanneet takaisin sosiaaliseen manipulointiin (Twitchell 2006:1).

Sosiaalisen manipuloinnin hyökkäyksiä on useita, mukaan lukien houkuttelu, vakuuttelu, käänteispsykologia, roskapostit, ja puhelinsoitot. Kaikki sosiaalisen manipuloinnin hyökkäykset eivät vaadi kehittynyttä teknistä osaamista, mutta yhteisenä tekijänä kaikkiin liittyy inhimillisen virheen hyväksi käyttäminen (Sumner & Yuan 2019: 72). Yksi yleisimmistä sosiaalisen manipuloinnin hyökkäyksistä on tietojenkalastelu, johon myös tässä tutkielmassa keskitytään.

Ongelma sosiaalisen manipuloinnin avulla tehdyissä sähköpostihyökkäyksissä on se, että niiden tunnistaminen koneellisesti ja sitä kautta suodattaminen ei yksin riitä. Osa hyökkäyksistä päätyy aina käyttäjien sähköpostiin, jolloin niiden tunnistaminen on olennaista, jotta kalastetulta vältytään. Tästä syystä on tärkeää kouluttaa ihmiset tunnistamaan nämä hyökkäykset. (Hadnagy & Fincher 2015: 31.)

Tietojenkalastelun yhteydessä tekijät yrittävät suostutella uhreja yksityisen tai luottamuksellisen tiedon paljastamiseen rakentamalla viestit niin, että huomio kiinnittyy tiettyihin kohtiin viestissä. He välttävät yksityiskohtia, jotka johtaisivat harhan havaitsemiseen (Harrison, Svetieva & Vishwanath 2016: 267). Tietojenkalastelusähköpostien viesti on yleensä lyhyt ja luottaa tyypillisesti kiireellisiin termeihin, kuten “varoitus” tai “määräaika”. Ne esiintyvät yhdessä lauseiden, kuten “tilin välitön sulkeminen” tai “lunastamaton veronpalautus”, kanssa. Tietojenkalastelijat yrittävät näiden termien avulla korostaa tunnepitoisia reaktioita ja saada käyttäjät toimimaan nopeasti ohittamalla rationaalisemmat päätöksentekoprosessit ja jättämättä huomiotta esimerkiksi mistä osoitteesta viesti on lähetetty. Tietojenkalasteluviestien pelkoa herättävä sisältö voi vaikuttaa myös muuhun tapaan, jolla käyttäjät käsittelevät sähköpostia. Sisältö voi lisätä heidän todennäköisyyttään jättää huomioimatta viestin osat, jotka osoittavat sen vilpillisen luonteen (Vishwanath, Herath, Chen, Wang & Rao 2011).

Kuvassa 1 esitetään Kauppakamarin (2018b) mainitsema esimerkki ns. turvapostin näköisestä tietojenkalasteluviestistä. Esimerkkiviestin tarkoitus on herättää luottamusta ja sen avulla saada käyttäjä avaamaan viestissä oleva linkki. Tämän kalasteluviesti on erityisen hyvin tehty ja siinä käytetty suomen kieli on hyvää.


Luottamuksellinen / Konfidentiellt / Confidential

Aihe / Ämne / Subject : Due Invoice 949494

Avaa viesti tästä / Öppna meddelandet / Open message

Olet saanut luottamuksellisen viestin. Viesti avataan ja siihen voidaan vastata yläpuolella olevasta linkistä. Yhteys on suojattu TLS-salauksella. Turvallisuussyistä viestin lukemista on rajoitettu ja se voidaan lukea korkeintaan 10 päivän ajan.

Du har fått ett konfidentiellt meddelande. Meddelandet kan öppnas och svaras på från länken ovanför. Förbindelsen är skyddad med TLS-kryptering. Av säkerhetsskäl är läsningen begränsad och meddelandet kan läsas i högst 10 dagar.

You have received a confidential message. The message can be opened and replied to from the link above. The connection is protected with TLS encryption. Due to security reasons reading of the message is limited and can be read for 10 days at most.

CLICK THE FOLLOWING LINK TO OPEN THE INVOICE

Kuva 1. Turvapostin näköinen sähköpostiviesti (Kauppakamari 2018b.)

Vaikka monet tietojenkalastajat yrittävät yllyttää pelolla (esimerkiksi uhkakuvat pankkitilin sulkeutumisesta), toiset yrittävät vakuuttaa uhreja luomalla palkkiopohjaisia viestejä, joissa tiedonkalastaja tarjoaa jotain arvokasta käyttäjille, kuten tavaroita tai rahaa. Yhtenä tunnetuimmista esimerkeistä tähän kuuluu nigerialaiskirjeet, joihin perustuu lupaus houkuttelevasta palkinnosta. Tämä suosittu huijaus provosoi käyttäjiä kertomaan henkilökohtaisia tietoja ja pankkitietojaan lupaamalla merkittävän palkkion vastineeksi avusta suuren rahasumman siirtämisessä Nigeriasta. (Harrison, Svetieva & Vishwanath 2016: 267-268.)

Sen lisäksi, että tietojenkalasteluviestien kielellisessä rakenteessa on eroavaisuuksia, löytyy eroavaisuuksia myös ns. hyökkäysmalleissa. Prem ja Reddy (2019: 1447) ovat luokitelleet kolme yleistä phishing hyökkäysmallia seuraavasti:

Spear phishing: Tiedonkalastusviestit pyritään suuntaamaan tiettyihin ihmisryhmiin tai yrityksiin, jotta viestit olisivat paremmin kohdennettuja. Tiedonurkkijat käyttävät usein jotain saatavilla olevia tietoja tai tilastoja, joiden avulla onnistumisen todennäköisyys olisi parempi.

Whaling: Niin sanotussa “valaanpyynnissä” tiedonkalastusviestit suunnataan etenkin yritysten ja muiden näkyvien tai tärkeiden elinten ylimmässä johdossa sijaitseville henkilöille. Viestit tuotetaan usein niin, että ne on kohdennettu tärkeässä asemassa olevan henkilön työrooliin liittyen ja sisältävät esimerkiksi asiakasreklamaatiota tai haasteita oikeudenkäyntiin.

Clone phishing: Tiedonkalastusviestissä pyritään kloonaamaan oikeaa, aiemmin lähetettyä sähköpostia, jossa mahdolliset vastaanottajatiedot, liitetiedostot ja linkit on saatu muistuttamaan identtistä versiota aidosta sähköpostista. Kloonatussa sähköpostissa mahdolliset liitetiedostot tai linkit on muutettu vahingollisiksi ja sähköpostin lähettäjäksi on asetettu sähköpostiosoite, joka muistuttaa alkuperäistä lähettäjää. (Prem & Reddy 2019.)

Kalastelun tavoitteena on yleensä saada käyttäjä jakamaan luottamuksellista tietoa, kuten käyttäjätunnuksia, henkilötietoja ja salasanoja. Useimmiten hyökkääjä pyrkii saamaan kalastelun avulla tietoa, joka on hyödynnettävissä taloudellisen voiton saavuttamiseksi (Hadnagy & Fincher 2015). Ollmann (2007: 8) kuitenkin kirjoittaa, että motivaatiot ja taloudelliset edut ovat muuttuneet ajan myötä ja kehittyvät jatkossakin. Ollmann määrittelee, että tietojenkalasteluhuijausten yleisin tarkoitus on:

- Sisäänkirjautumistietojen kaappaaminen: Verkkopalveluihin, kuten sähköpostiin ja verkkokauppaan, pääsyä varten. Pörssikauppojen lisääntymisestä verkossa on seurannut se, että asiakkaan kaupankäyntitiedot tarjoavat helpon tavan kansainvälisille rahansiirroille.

- Pankkitietojen varastaminen: Verkkopankkien kirjautumistunnusten avulla tiedonurkkijalla on helppo pääsy valmiisiin siirrettäviin varoihin.

- Luottokorttitiedot: Luottokortin numerolla, voimassaolon päättymis- ja myöntämispäivällä, kortinhaltijan nimellä ja luottokortin validointinumerolla (CCV) on välitön arvo useimmille rikollisille.

- Osoite- ja muiden henkilökohtaisten tietojen kaappaaminen: Kaikki henkilökohtaiset tiedot, etenkin osoitetiedot, ovat helposti myytävissä ja niille löytyy jatkuvasti kysyntää mm. suoramarkkinointiyrityksissä.

- Liikesalaisuuksien ja luottamuksellisten asiakirjojen varastaminen: Kohdennettujen viestien avulla, eli spear phishingillä, pyritään teolliseen vakoiluun ja niiden avulla hankkitaan luottamuksellisia tietoja tietyistä yrityksistä.

- Bottien ja DDoS-agenttien jakaminen: Kyberrikolliset käyttävät tietokalasteluhuijauksia asentaakseen erityisiä botteja ja DDoS-agentteja tietokoneisiin saadakseen pääsyn niiden verkkoihin. Tällä tavoin tartutettuja tietokoneita ja verkkoja voidaan myöhemmin myös vuokrata muille rikollisille.

- Hyökkäyksen levittäminen: Yhdistelemällä tietojenkalastusta ja bottien asennuksia rikolliset voivat käyttää yhtä yrityksen uhria "hyppypisteenä" myös tulevia hyökkäyksiä varten samassa yrityksessä.

3 HENKILÖSTÖN TIETOTURVAKÄYTTÄYTYMINEN JA SEN PARANTAMINEN KOULUTUKSEN AVULLA

3.1 Tietoturvakäyttäytyminen ja sen parantaminen

Tekniset tietoturvaratkaisut eivät yrityksissä riitä, sillä tietoturvan pettäminen on usein seurausta ihmisen toiminnasta. Tutkimuksen mukaan jopa 35% tietoturvaan liittyvistä virheistä on ihmisen aiheuttamia (Alaskar, Vodanovich & Shen 2015: 4242).

Tietojenkalastelussa ihmiset saadaan käyttäytymään epärationaalisesti. Siinä käytetään hyväksi tunteita, kiireen tuntua ja luottamusta.

Tietojenkalastajat pyrkivät ymmärtämään, miten ihmisen päätöksenteko toimii. Päätöksenteon taustalla ei aina ole tietoa. Hyökkääjät pyrkivät usein vaikuttamaan ihmisten tunteisiin. Jos tunnereaktio on vahva, voi päätöksentekoprosessi heikentyä ja tietojenkalastelu onnistua (Hadnagy & Fincher 2015).

Usein hyökkääjä kerää ensin uhrista tietoja, joiden avulla hän synnyttää luottamuksen. Personoitu viesti vakuuttaa ihmiseen ja näin kalastelun uhri saadaan toimimaan kuten hyökkääjä haluaa (Speed, Nykamp, Heisner, Anderson & Nampalli 2014).

Viesteille on usein tyypillistä se, että kohteelle luodaan kiireen tuntua. Viesti tuntuu henkilöstä tärkeältä ja asia on kiireellinen. Tällöin hän ei toimi järkevällä tavalla vaan juuri niin kuin tietojenkalastelija haluaa (Hong 2012).

Hadnagy ja Fincher (2015) korostavat, että turvallisesti toimiakseen, päätöksen taustalla pitäisi aina olla riittävästi tietoa ja asia pitäisi ymmärtää ennen toimimista. He korostavat myös sitä, että virheistä on mahdollisuus oppia.

Chaudharyn (2016) mukaan iällä, sukupuolella, kulttuurilla ja aikaisemmalla kokemuksella voi olla vaikutusta siihen, miten tietojenkalastelu onnistuu. Naiset joutuvat miehiä useammin kalastelun uhreiksi. Samoin nuoremmat ihmiset ja ne, joilla on vähemmän teknologista kokemusta (Jagatic, Johnson, Jakobsson & Menczer 2007). Sellainen koulutus, jossa on harjoiteltu tunnistamaan tietojenkalasteluviestejä auttaa suojautumaan kalastelulta (Downs, Holbrook & Cranor 2007). Pattinsonin, Jerramin,

Parsonsin, McCormacin ja Butavicius (2012) mukaan sellaiset henkilöt tunnistavat kalasteluviestejä paremmin, jotka ovat olleet lähiaikoina aiheen kanssa tekemisessä.

Tietynlaiset taustat ja kulttuurit saavat ihmiset toimimaan sähköpostissa huolellisemmin kuin toiset (Chaudhary 2016). Myös aikaisemmat kokemukset tietojenkalastelusta vaikuttavat todennäköisesti siihen, että ihminen toimii huolellisemmin (Vishwanath ym. 2011).

Stanton, Stam, Mastrangelo ja Jolton (2005) ovat tarkastelleet tietoturvakäyttäytymistä kahden dimension kautta. Toinen liittyy käyttäjän taitotasoon ja toinen toiminnan tarkoituksellisuuteen tai tahattomuuteen.

Tietoturvakäyttäytymisen seuraukset voivat Ryanin ja Decin mukaan olla konkreettisia, kuten palkinto tai rangaistus, tai normeihin liittyviä, kuten hyväksyntä tai paheksunta (Ryan & Deci: 2000).

Henkilökunnan tietoturvakäyttäytymisellä on suuri merkitys yritysten tietoturvan parantamisessa. Hyvään tietoturvakäyttäytymiseen pyrittäessä, keskeiseksi asiaksi nousee henkilöstön motivointi. Heillä on oltava halu noudattaa määräyksiä sekä tiedot, taidot ja tietoisuus tietoturvaan liittyvistä asioista. Tietoturvakäyttäytymisestä puhuttaessa täytyy huomioida konteksti. Ihmisten käyttäytyminen on erilaista kontekstista riippuen. Tässä tutkielmassa ei käsitellä kotikäyttäjän tietoturvakäyttäytymistä, vaan keskitytään vain yritys- ja organisaatiokonteksteihin. Tietoturvakäyttäytyminen voi olla yritykselle uhka, mutta sen vaikutus voi olla myös positiivinen, esimerkiksi tietoturvaan liittyvien puutteiden havaitseminen.

Useimmiten turvallisuustutkimus keskittyy informaatioteknologian resurssien väärinkäyttöön, vaikka Moodyn (2011: 19) mukaan pitäisi selvittää sitä, miksi ihmiset jättävät toiminnassaan tarkoituksella huomioimatta tietoturvan. Hänen mukaansa tietoturvatutkimuksessa ei ole pyritty selittämään motivaation osuutta. Moody tutki tietoturvaohjeiden laiminlyönnin syitä.

Nurmi ja Salmela-Aro (2005: 12) korostavat sisäsyntyisen motivaation merkitystä. Sisäisessä motivaatiossa henkilö on aidosti kiinnostunut opittavasta asiasta ja hän saa siitä tyydytystä. Toiminta on ulkosyntyistä motivaatiota tehokkaampaa, eikä ulkoista palkkiota tarvita. Motivaatiota tutkitaan modernissa motivaatioteoriassa ihmisen

tavoitteiden näkökulmasta. Aluksi kartoitetaan ihmisen tavoitteet, pyrkimykset ja hankkeet, ja sitten tutkitaan millainen on ihmisen arvio omista mahdollisuuksistaan toteuttaa ne ja vaikuttaa niihin. Tavoitellaan sitä, että ihminen arvioi toimintansa tärkeyden ja pohtii sen herättämiä tunteita. (Nurmi ym. 2005: 19–20, 23.)

Ruohotien (1998: 50) mukaan motivaation perustana ovat tarpeet sekä niistä muotoutuvat arvot ja motiivit. Ne muuttuvat tavoitteiden ja aikomusten kautta toiminnaksi. Lopulta päädytään seurauksiin ja saadaan toiminnasta palkkiota sekä tyytyväisyyttä. Monet muutkin tutkijat Maslowista lähtien korostavat tarpeiden vaikutusta ihmisen käyttäytymisessä. Oppimisen edellytyksenä on se, että yksilöiden perustarpeiden tulee olla kunnossa.

Keskustelun, muistilistojen ja Internetpohjaisten ohjeiden vaikutuksia ihmisen tietoturvakäyttäytymiseen ovat tutkineet Cox, Connolly ja Currall (2001). Heidän mukaansa ihmisen käyttäytyminen on keskeinen ja kriittinen tekijä tietoturvalle ja kaikki kolme tekijää (keskustelu, muistilistat ja Internet-pohjaiset ohjeet) ovat merkityksellisiä tietoturvatietoisuuden parantamiseksi.

Tietoturvakäyttäytymiseen vaikuttavat monet eri tekijät. Osa niistä on sisäsyntyisiä, kuten toiminnan koetut vaikutukset, henkilökohtainen osaaminen, halu noudattaa määräyksiä ja tietoisuus niistä (Herath & Rao 2009). Herath ja Rao kehittivät tutkimuksessaan teorian, jossa rangaistuksella oli kannustava vaikutus. Lisäksi työntekijän tehokasta toimintaa huomioitiin. Tutkimuksen mukaan tietoturvakäyttäytymiseen voidaan vaikuttaa sekä sisäisen että ulkoisen motivoinnin avulla. Sisäisessä motivoinnissa tärkeää on työntekijän tehokkaan toiminnan huomioiminen. Herathin ja Raon mukaan työntekijöitä motivoi tieto siitä, että kiinni jäämisestä seuraa rangaistus. Tosin rangaistuksen ankaruus aiheutti negatiivisen vaikutuksen tietoturvakäyttäytymiseen.

Motivoituminen vaatii tavoitteita. Niermeyer ja Seyffer (2004: 38-62) kirjoittavat siitä, että kunkin työntekijän pitäisi päättää tavoitteisiin pyrkimisestä henkilökohtaisesti. Tavoitteiden tulisi olla realistisia, haastavia, houkuttelevia, mitattavia ja niillä olisi oltava henkilökohtainen merkitys. Johtohenkilöstön olisi välttämätöntä kuitenkin motivoida työntekijöitä. Motivoitaessa tavoitteet muotoillaan haasteellisiksi, työntekijän itseluottamusta vahvistetaan ja hänen kehitystään tuetaan, tarjotaan liikkumavaraa ja

annetaan palautetta rakentavasti. Itseluottamuksen määrällä on selkeä vaikutus motivaatioon.

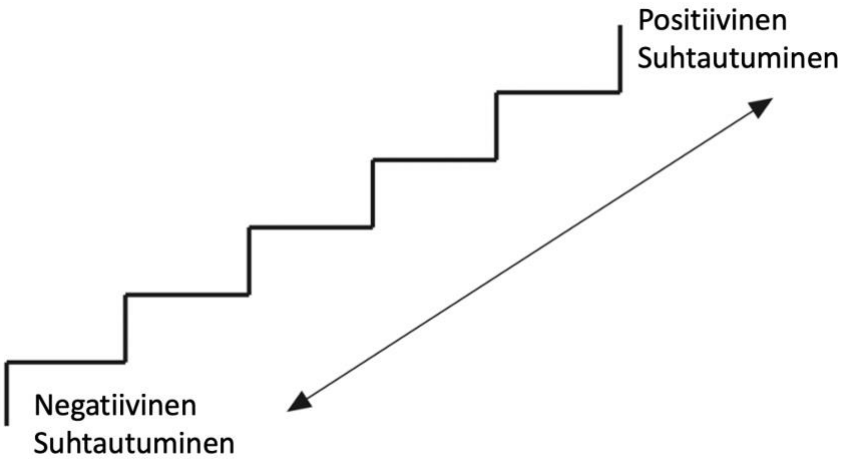
Ku, Chang ja Yen (2009) tutkivat tietoturvan hallintajärjestelmän (ISMS) käyttöä erityisesti Taiwanissa. Tutkimuksen tuloksien mukaan hallintajärjestelmän käyttöönotossa tärkeitä motivaatiotekijöitä ovat onnistuneet kokemukset aiemmilta ajoilta ja ohjeiden ymmärtämisen taso, dokumenttien taso ja niiden saatavuus sekä organisaation oppiminen ja organisaatiokulttuuri, mukaan lukien ylimmän johdon tuki sekä koulutus.

Tietoturvakäyttäytymistä voidaan pyrkiä parantamaan erilaisin toimin. Lähes kaikissa niissä on keskiössä henkilön oma motivaatio. Työntekijän tietoisuuden lisääminen on tärkeää (Siponen 2000). Toinen merkittävä asia on yrityksen hyvä tietoturvapolitiikka (Höne & Eloff 2002). Näihin molempiin liittyy olennaisesti tietoturvakoulutus. Höne ja Eloff (2002) ovat tutkimuksensa perusteella sitä mieltä, että ohjeistukset sisältävät usein vaikeasti ymmärrettäviä termejä ja ne kirjoitetaan liian teknisestä näkökulmasta.

Tietoturvatietoisuus lisääntyy, kun otetaan käyttäjät mukaan tietoturvan riskienhallintaan. Samalla yhdistetään tietoturvariskien hallinta liiketoimintaympäristöön. Spearsin ja Barkin (2010) mukaan näin saavutetaan parempia tuloksia. Käyttäjiltä saadaan tietoja, joiden perusteella voidaan kehittää tehokkaampia tietoturvatoimintoja. Lisäksi käyttäjät sitoutuvat suojelemaan liiketoiminnalle merkittäviä tietoja.

Tietoturvakoulutusta kehittäessä täytyy muistaa, että henkilöstön lähtötaso ja suhtautuminen koulutukseen on hyvin erilaista. Siponen (2000) esittää tutkimuksessaan mallin siitä, miten henkilöstö suhtautuu tietoisuutta lisäävään koulutukseen. Kuvassa 2. nähty malli esittää miten käyttäjä reagoi koulutukseen liittyviin aktiviteetteihin. Mallin

mukaan käyttäjiä tulee johdattaa askel kerrallaan kohti positiivista reaktioita, eikä siihen ole oikotietä. (Siponen 2000: 34-35.)



Kuva 2. Koulutettavien suhtautuminen tietoisuutta lisäävään koulutukseen. (Siponen 2000.)

Iiro-Antti Räikkönen (2017) tutki teemahaastattelujen avulla työntekijöiden tietoturvakäytänteitä sekä motivaation merkitystä siinä. Hänen mukaansa oppiminen, tietoturvatietoisuus sekä työpaikan kulttuuri ovat keskeisiä tekijöitä henkilön tietoturvakäytänteissä. Myös riskien ymmärtämisellä ja oman toiminnan merkityksen ymmärtämisellä on vaikutusta.

Teknologioiden ja työkalujen lisäksi olisi tärkeää, että ihmisillä olisi hyvät taidot oikeiden ja turvallisten ratkaisujen tekemiseksi. Chaudharyn (2016) mukaan urkintaa torjuvien sovellusten lisäksi olisi tärkeä kouluttaa ihmisiä tiedon urkinnasta ja hakkeroinnista. Monet toimenpiteet toimivat heikosti, sillä ne eivät huomioi riittävästi uusia sosiaalisen hakkeroinnin ja tiedon urkinnan menetelmiä. Olisikin tärkeä suunnitella opetusta tulevaisuuden tietoturvatarpeita varten ja koulutuksessa tulisi huomioida ihmisten oppimistavat ja ajattelumallit. (Chaudhary 2016.)

Ying Li (2015) on tutkinut sitä, miten tietoturvakäyttäytyminen vaihtelee eri konteksteissa. Tietokoneen käyttäjä toimii eri tavalla organisaatioympäristössä ja henkilökohtaisen tietokoneen käytön yhteydessä. Näin ollen tietoturvakäyttäytymistä tutkittaessa on hänen mukaansa tärkeätä huomioida konteksti.

Petri Puhakainen (2006) on tutkinut tietoturvakäyttäytymistä ja keinoja sen muuttamiseksi. Hänen mukaansa oma henkilöstö on yrityksen suurin tietoturvauhka. Laiminlyöntejä tapahtuu jatkuvasti. Yrityksen johto sitoutuu huonosti tietoturvasäännöstöön ja sen käyttöä ei motivoida riittävästi. Lisäksi koulutus suunnitellaan ja toteutetaan huonosti. Puhakaisen mukaan tietoturvatoimenpiteet painottuvat liian paljon tekniikkaan. Henkilöstön asenteeseen vaikuttaminen olisi tärkeää. Mielipidevaikuttajien käytännön osallistuminen toimintaan vaikuttaa yleiseen asenteeseen. Käyttäjien mukanaolo tietoturvapolitiikan luomisessa auttaa heitä myöhemmin hyväksymään tietoturvallisuuteen liittyviä toimia. Työntekijöiden tulisi saada tietoturvaan liittyvää koulutusta yrityksen tietoturvapolitiikan mukaisesti ja uusien työntekijöiden perehdyttämiseen tulisi kiinnittää huomiota.

Pelkkä motivaatio ei yksin vaikuta työntekijän toiminnan laatuun ja määrään. Siihen vaikuttavat myös työntekijän halu ja kyky käyttää osaamistaan työnantajan hyväksi. (Vartiainen ja Nurmela 2005: 190) Työympäristön esteet ja tuki ovat myös keskeisessä roolissa. Thomson ja von Solms (2005) esittävät, että yrityskulttuuriin on syytä vaikuttaa yrityksen johdon taholta, jotta jokapäiväinen tietoturvakulttuuri saadaan hyvälle tasolle. Vartiainen ym. (2005: 196-197) kirjoittava vielä, että vuorovaikutusrakenteilla pystytään lisäämään työntekijän sisäistä motivaatiota. Tärkeintä on saada organisaatiolta, johdolta tai esimieheltä palautetta. Toiminnan suuntaamiseen ja ylläpitoon vaikuttavat ulkoiset palkkiot. Myyry, Siponen, Pahnila, Vartiainen ja Vance (2009) toteavat, että vaikka työntekijät tietävät tietoturvaohjeista, he eivät noudata niitä.

Tietoturvakäyttäytymiseen liittyy tietoturvauhkien ja niiden vaikutusten ymmärtäminen. Liang ja Xue (2010) tutkimuksessa tutkittiin tietokonekäyttäjien pyrkimyksiä välttää tietoturvauhkia. Uhkien välttämiseen liittyy motivaatio, ymmärrys uhasta, suojauksen tehokkuus ja mahdollisuus vaikuttaa itse tilanteeseen. Jos henkilöllä on ymmärrys mahdollisesta uhasta, he pyrkivät havainnoimaan sitä. Tämän tutkimuksen mukaan suojauksen tehostaminen vähentää motivaatiota välttää uhkan toteutumista.

3.2 Koulutuksen merkitys tietoturvakäyttäytymisen parantamisessa

Nykyisissä työtehtävissä työntekijöiltä vaaditaan jatkuvaa oppimista. Uusien tietojen ja taitojen oppiminen on jatkuva prosessi. Tietoturvaohjeiden omaksuminen on yksi esimerkki tällaisesta oppimisesta.

Puolimatkan (2002: 85) mukaan oppija on yksilö, joka ajattelee, ymmärtää ja noudattaa sääntöjä. Oppiminen vaikuttaa hänen maailmankuvaansa. Oppimisessa voi olla monta kerrosta ja sen vaikutukset voivat olla pitkävaikutteisia. Lisäksi oppiminen vaikuttaa myös henkilön motivaatioon.

Oppimisprosessissa on Ruohotien (1998: 77, 132-133) mukaan seuraavat kolme vaihetta: toimintaan sitoutuminen, toiminnan kontrollointi ja sen itsereflektointi. Viimeksi mainitussa tarkastellaan oppimiskokemuksia ja arvioidaan niiden merkitystä.

Laaksosen, Nevasalon ja Tomulan (2006: 254-255) mukaan tietoturvakoulutuksen tavoitteena on suojata yrityksen tieto kustannustehokkaasti ja tarkoituksenmukaisesti. Heidän mukaansa työntekijöiden motivaatiolla on suuri vaikutus koulutuksen tehokkuuteen. Koulutuksessa pitäisi kiinnittää huomiota siihen, että jokainen työntekijä ymmärtää omaan työhönsä liittyvät riskit ja osaa minimoida ne. Tietoturvatoiminnan organisoimisessa ja työntekijöiden kouluttamisessa tehdään yritysten tietoturvan kehittämisen suurimmat virheet.

Tietojenkalastelua voidaan välttää kouluttamalla ihmisiä. Parmarin (2012) mukaan erityisesti yritysten kannattaisi kouluttaa työntekijöitään tietojenkalastelua vastaan. Koulutuksen haasteena on se, että ihmiset luulevat osaavansa tunnistaa kalasteluviestit (Hong 2012).

Tietojenkalastelussa käytettävien viestien sisällöt ovat samantapaisia ja näin ollen ne on mahdollista oppia tunnistamaan. (Robila & Ragucci 2006). Koulutuksen avulla voidaan opettaa ihmisiä tunnistamaan näitä sähköpostiviestejä (Almomani, Gupta, Atawneh, Meulenberg & Almomani 2013). Internetissä on runsaasti ilmaista materiaalia, joiden avulla tietojenkalastelun riskeihin voi tutustua ja uhkiin voi oppia varautumaan. Monien valtioiden ja erilaisten organisaatioiden sekä tietoturvayritysten kautta löytyy materiaalia ja koulutuspalveluista tietojenkalasteluun liittyvistä riskeistä. (Almomani ym. 2013).

Koulutuksessa voidaan myös käyttää apuna simuloituja tietojenkalastelu -yrityksiä. Tällainen koulutus on osoittautunut tehokkaaksi ja hyväksi. Henkilöt saavat koulutuksessa palautetta siitä, miten he ovat toimineet tietojenkalasteluviestin saatuaan (Jansson & von Solms 2013). PhishGuru on yksi niistä järjestelmistä, jotka toimivat simuloiden aitoja kalasteluviestejä. Järjestelmä lähettää henkilölle ilmoituksen, jos hän on klikannut viestissä olevaa linkkiä. Henkilölle myös kerrotaan miten kalasteluviestin olisi voinut tunnistaa (Kumaraguru, Cranshaw, Acquisti, Cranor, Hong, Blair & Pham, 2009). Monet organisaatiot ovat kehittäneet omia menetelmiään henkilöstön kouluttamiseen, jotta uhkia voitaisiin vähentää.

Koulutuksessa voidaan käyttää myös erilaisia sovelluksia ja pelejä. Tällainen on esimerkiksi Anti-Phoching Phil -peli. Peli opettaa pelaajaa tunnistamaan tietojenkalasteluviestien ominaisuuksia. Tutkimuksen (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge 2007) mukaan pelaamalla saatiin parempia tuloksia kuin aiheeseen liittyvää materiaalia lukemalla.

Almomani ym. (2013) kirjoittavat, että paras tulos koulutuksessa saadaan eri keinoja yhdistämällä. Materiaaleja opiskelemalla oppii teoriaa. Sovelluksia ja pelejä käyttämällä oppi käytännössä sen, millaisiin viesteihin kannattaa suhtautua epäluuloisesti.

Kalasteluun käytettävät viestit kehittyvät jatkuvasti. Hyvän koulutuksen avulla voi oppia suojautumaan uhilta. Tietojenkalastelua ei kohdisteta järjestelmiä, vaan ihmisiä kohtaan. Virheen tulee yleensä ihminen, ei järjestelmä (Chaudhry, Chaudhry & Rittenhouse, 2016).

Kasvatustieteen maisteri Mari Karjalainen (2011) tutki Oulun Tietojenkäsittelytieteiden laitokselle tekemässään väitöskirjassa työntekijöiden tietoturvakäyttäytymisen parantamista. Hänen mukaansa työntekijät noudattavat huonosti tietoturvallisuusohjeita. Väitöskirjassa tutkittiin sitä, miten tehokkaita tietoturvakoulutuksia tulisi suunnitella ja toteuttaa. Väitöskirjan mukaan tietoturva-ajatteluun liittyvät tietoturvauhkien ymmärtäminen sekä tiedon arvossa pitäminen ja oman vastuun tiedostaminen. Työntekijöillä on myös sellaisia asenteita, jotka vaikuttavat tietoturvaan, vaikka eivät siihen suoranaisesti liitykään.

Koulutuksen kehittäminen on Karjalaisen (2011) mukaan tarpeellista, koska tietoturvaan liittyvä välinpitämättömyys on lisääntynyt ja sitä seuranneet kustannukset ovat olleet

kovassa kasvussa. Väitöskirjassa esitetään tietoturvakoulutuksessa huomioon otettavia tekijöitä.

Karjalainen (2011: 49-62) esittelee väitöskirjassaan tietoturvakoulutuksen järjestämisen pedagogisia vaatimuksia. Hänen mukaansa koulutuksessa olisi huomioitava työmuistin kognitiivinen kuormitus ja oppijan aiemmat tiedot. Järjestelmällistä kognitiivisen tiedon käsittelyä tulisi käyttää. Lisäksi koulutuksen sisällön tulisi olla yhteisökeskeistä ja sen olisi perustuttava kollektiivisiin kokemuksiin ja koulutettavien näkökulmiin. Opetusmenetelmien tulisi keskittyä kollektiivisen tiedon kriittiseen tarkasteluun ja kokemusten kautta tapahtuvaan aitoon ongelmanratkaisuun. Yhteisöllisen oppimisen tekniikoita olisi hyvä käyttää, jotta voitaisiin tuottaa kollektiivista osaamista.

Karjalaisen (2011) väitöskirjassa on kehitetty metateoria tietoturvakoulutuksen suunnittelua varten. Tutkimuksen mukaan tietoturvakoulutus eroaa normaalista koulutuksesta, ja se vaatii laajemman teoreettisen pohjan, jotta tutkimusta voidaan kehittää. Tutkijoiden kehittämän teorian mukaan koulutuksen tulisi sisältää neljä vaihetta; konkreettiset kokemukset, reflektoiva havainnointi, abstraktien käsitteiden muodostaminen ja aktiivinen kokeilu.

Motivaatiolla on suuri merkitys kaikessa ihmisen toiminnassa. Niina Kinnunen (2015) on tutkinut motivaation merkitystä tietoturvaohjeistuksen noudattamisessa. Hänen mukaansa erilaisten tietoturvaohjeistajien ja –ohjeistusten määrä on liian suuri. Tulisi pyrkiä noudattamaan yleisesti hyväksyttyjä tietoturvastandardeja ja -käytänteitä ja yritysten työntekijät tulisi saada ymmärtämään miksi kunkin kriteerin noudattaminen on tärkeää. Perusteet tulisi kertoa työntekijälle siten, että hän ymmärtää mitä konkreettisia vaikutuksia on sillä, jos työntekijä jättää noudattamatta ohjeita. Näin työntekijä motivoituu paremmin noudattamaan annettuja ohjeita. Noudattamisen syitä voi perustella joko sisäisesti (tunne valinnanmahdollisuudesta, tunne omasta osaamisesta, tunne noudattamisen merkityksellisyydestä, tunne tietoturvan toteutumisen edistymisestä) tai ulkoisesti motivoivilla (toisen henkilön tai tilanteen vaatimus) tekijöillä. Tietoturvan toteutumisesta olisi Kinnusen mukaan tärkeää antaa palautetta ja yritysjohdon tulisi selkeästi vaatia tietoturvakriteerien noudattamista. Vaatimus tulisi perustella selkeästi ja työntekijän tulisi ymmärtää noudattamatta jättämisestä aiheutuva vaikutus. Tutkimus suosittelee, että tietoturvakäytänteet sisällytettäisiin työhöntuloperehdytykseen. Hyvä tietoturvakulttuuri ja kollegojen esimerkki sekä uusista tietoturvakäytänteistä tiedottaminen on Kinnusen mukaan tärkeää. Työntekijöille tulee tarjota koulutusta ja

heidät pitää saada ymmärtämään, miksi kriteerin noudattaminen yrityksessä on tärkeää ja miksi noudattamista vaaditaan. Kehittämisen ja ohjauksen tulisi olla tietoturva-asioissa jatkuvaa ja kokonaisvaltaista. Kinnusen tutkimustulosten mukaan merkittävä motivaation lähde työntekijällä on oma usko tietoturvan toteuttamisen tärkeydestä. Toisen henkilön tai olosuhteiden aiheuttama vaatimus voivat myös olla tietoturvan noudattamisen taustalla. (Kinnunen 2015: 167-168.)

Nykänen (2011: 14) tutki tietoturvakoulutuksen vaikutusta yksilön ja organisaation tietoturvakäyttäytymiseen. Sitä on hänen mukaansa tutkittu hyvin vähän. Tulosten mukaan koulutuksessa tulee pyrkiä vaikuttamaan yksilön tapoihin ja käyttäytymiseen sekä yksilön oman toiminnan seurausten vastuuttamiseen.

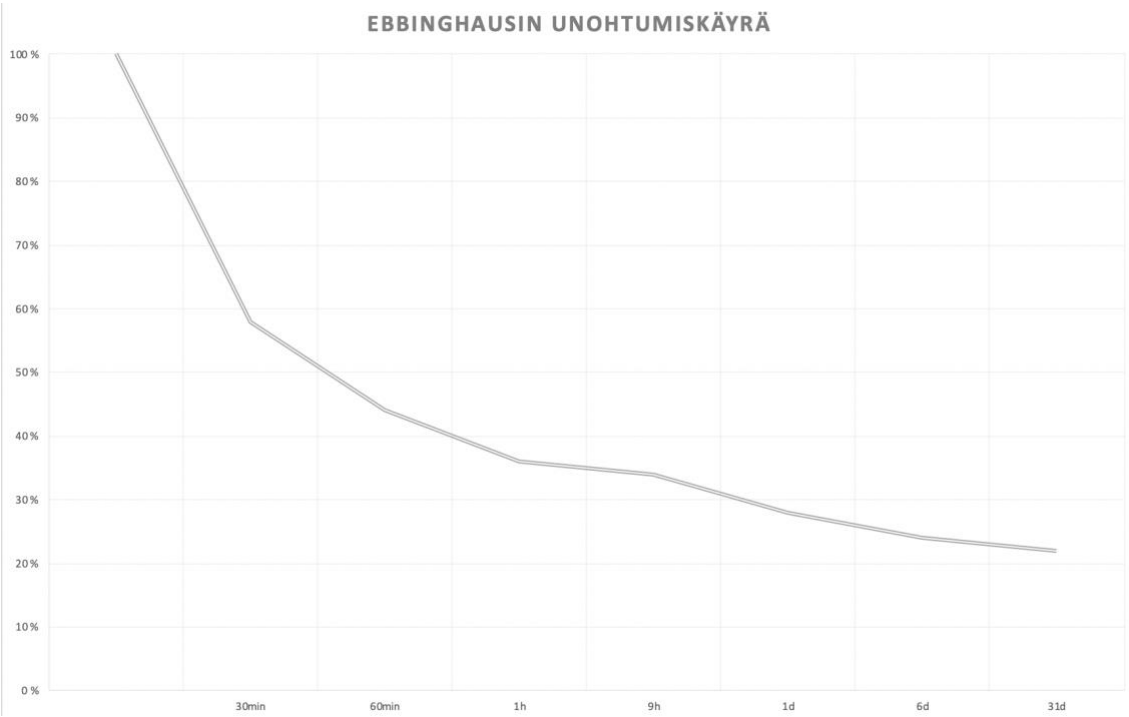
Internet-pohjaisten järjestelmien käyttö ja sovellukset sekä työaseman käyttö työhön liittymättömiin tarpeisiin, ovat tuoneet yrityksen arkipäivään haasteita, joissa tietoturvakäyttäytyminen on merkittävässä asemassa. Kari Nykänen (2011) tutki väitöskirjassaan tietoturvakoulutuksen vaikutusta yksilön työhön liittymättömän Internet-käyttäytymisen muuttamiseen. Nykäsen tutkimuksen mukaan olisi tärkeätä, että yksilöt ottaisivat enemmän vastuuta toiminnastaan, jotta toivottava muutos tietoturvakäyttäytymisessä tapahtuisi. Nykänen pitää tärkeänä, että jotta tietoja ja taitoja voidaan soveltaa eri ympäristöissä, ne täytyy sitoa laajempaan kokonaisuuteen. Näin koulutettavat asiayhteydet aikaansaavat oppijalle syvällisemmän ja vaikuttavamman oppimiskokemuksen. Nykäsen mukaan ihmiselle riittää yksinkertainen selitys tietoturvallisista tavoista toimia. (Nykänen 2011: 275.)

Tiedot on mahdollista oppia nopeasti, mutta ne myös unohtuvat nopeasti. Taitojen oppiminen tapahtuu hitaammin, mutta kun ne on oppinut, ne säilyvät pidempään. Oppiminen voi olla induktiivista, jolloin edetään yksityiskohtaisesta tiedonkäsittelystä yleisiin lainalaisuuksiin päin. Deduktiivisessa tiedonkäsittelyssä edetään päinvastoin eli ensin käsitellään yleisiä periaatteita ja niistä edetään yksityiskohtiin. Uutta asiaa oppivalle induktiivinen tapa on parempi. Deduktiivisesti voi edetä, jos oppijalla on jo ennestään tietoa asiasta. (Bannert 2002; Pollock, Chandler & Sweller 2002.)

Tietoturvakoulutuksen toteuttamisessa toimivat kaikki oppimiseen liittyvät lainalaisuudet. Siinä tulee huomioida mm. ihmisen aikaisempi tietotaito, motivaatio, erilaiset oppimistyylit sekä opitun siirtäminen käytäntöön. Oppijan oma aktiivisuus oppimisprosessissa on tärkeä. Hän muokkaa saamansa tiedon aikaisempia kokemuksiaan

apuna käyttäen. Kasvatustieteessä puhutaan konstruktiivisesta oppimisnäkemyksestä. (Tynjälä 1999.)

Koulutusta järjestettäessä on hyvä huomioida myös se, että ihminen oppii hyvin tekemisen kautta. Ebbinghausin määrittelemän unohtamiskäyrän (eng. forgetting curve) mukaan kuuntelemalla opituista uusista asioista melkein 60 prosenttia unohtuu jo ensimmäisen tunnin aikana. Unohtamiskäyrä on esitettynä kuvassa 3. (Schimanke, Mertens & Vornberger 2013: 3.)



Kuva 3. Ebbinghausin unohtumiskäyrä. (Schimanke ym. 2013.)

Simuloitua tietojenkalastelukoulutusta on tutkittu myös aikaisemmin. Korealainen tutkimustyhmä on suorittanut empiirisen kokeen, jossa valitulle ryhmälle lähetetään simuloituja kalasteluviestejä. Aika-asteikko jäi tutkimuksessa epäselväksi, mutta tulosten mukaan neljän testikerran jälkeen koehenkilöt avasivat haitallisen linkin harvemmin kuin ennen koulutusta. Tutkimuksessa painotettiin sitä, että menetelmiä tulee kehittää sekä koulutuksen että tutkimuksen osalta, sillä tietojenkalasteluun käytetyt menetelmät lisääntyvät jatkuvasti ja niistä tulee yhä monimutkaisempia. (Il-Kwon, Young-Gil & Jae-Kwang 2016.)

Työpaikalla tapahtuvaa oppimista voidaan mitata. Ruohotien (1998: 15-16) mukaan oppimista on tapahtunut, jos saavutettu tulos vastaa toimintasuunnitelmaa, joka on asetettu. Tällöin lopputulos on onnistunut ja työntekijöiden toiminta on ollut oikeanlaista. Oppimisen seurauksena voidaan myös löytää epäonnistumisen aiheuttama virhe ja se voidaan korjata.

Tietojenkalastelun uhkia vastaan toimiessa paras suoja saavutetaan teknologisia ratkaisuja ja koulutusta yhdistämällä.

4 TUTKIMUKSEN HYPOTEESIT JA KOEASETELMA

Tutkielman tarkoituksena on tutkia, miten tietojenkalastelusimulaationa järjestetty koulutus vaikuttaa työntekijöiden kykyyn tunnistaa sähköpostin kautta tulevia haitallisia tietojenkalasteluviestejä.

Tutkimuksen hypoteesit ovat:

1. Ne työntekijät, jotka ovat osallistuneet tietojenkalastelusimulaationa järjestettyyn tietoturvakoulutukseen onnistuvat haitallisten tietojenkalasteluviestien tunnistamisessa useammin kuin ne, jotka eivät ole koulutukseen osallistuneet.

2. Mitä pidempään työntekijä on mukana tietojenkalastelusimulaationa järjestetyssä koulutuksessa, sitä epätodennäköisempää on, että hän avaa tietojenkalasteluviestissä olevan linkin.

Kuvassa 4. on esitetty ensimmäiseen hypoteesiin liittyvä koeasetelma. Sen mukaan tutkimus toteutetaan perinteistenä koeasetelmana, jossa on alkutesti ja lopputesti. Koeryhmään suoritetaan interventio.

Kuva 4. Ensimmäiseen hypoteesiin liittyvä koeasetelma.

Interventiolla tarkoitetaan tässä tutkielmassa tietojenkalastelusimulaationa järjestettyä koulutusta. Koeryhmä eli testiryhmä (eng. test group) on ryhmä, joka osallistuu koulutukseen. Vertailuryhmä eli kontrolliryhmä (eng. control group) ei osallistu koulutukseen.

5 AINEISTO, TOTEUTUS JA MENETELMÄT

Tutkielmassa hyödynnetään Yritys X:n kehittämää tietoturvakoulutusjärjestelmää. Yritys X on kehittänyt tietoturvakoulutukseen soveltuvan järjestelmän, joka simuloi sähköpostitse leviäviä tietojenkalasteluhyökkäyksiä. Koulutussovelluksen toimintaa kuvataan seuraavassa luvussa tarkemmin. Tutkielmassa tullaan käyttämään aineistona tämän koulutussovelluksen keräämää dataa, joka on peräisin asiakasyritys Y:n lokitiedoista. Näistä tiedoista löydetään hakumenetelmiä käyttämällä haluttu tieto. Aineistoa analysoimalla selvitetään koulutuksen vaikuttavuutta. Tutkielmassa tarkastellaan sitä, millainen on yrityksen työntekijöiden kyky tunnistaa tietojenkalasteluviestejä. Aineistoa kerätään useita kertoja peräkkäin neljän kuukauden aikana. Tutkielman tiedoista ei voi päätellä minkä yrityksen aineistosta on kysymys. Aineisto kerättiin 20.11.2019-20.2.2020 välillä.

Tämä tutkielma on otantatutkimus. Tutkielman otoksesta saatuja tuloksia voidaan yleistää perusjoukkoon eli populaatioon. Tässä tutkielmassa ei käytetä sellaisia tilastollisia muuttujia kuten sukupuoli tai ikä. Sen sijaan aineisto koostuu asiakasyrityksen Y henkilökunnasta. Asiakasyritys Y on muiden vastaavanlaisten yritysten joukosta satunnaisesti valikoitunut tutkittavaksi. Kyseessä on siis edustava otos. Otos on kooltaan niin suuri, että siitä saatavat tulokset ovat todennäköisesti varsin hyvin yleistettävissä muiden yritysten tuloksiin.

Tutkielmassa tutkitaan sitä, miten Asiakasyritys Y:n henkilökunta selviytyy tietojenkalasteluviesteistä. Asiakasyritys Y:n koko henkilökunnalle tehdään alkutesti. Siinä asiakasyrityksen Y työntekijät saavat yritys X:n lähettämän tekaistun kalasteluviestin. Simuloiduissa uhissa, kuten oikeissakin kalasteluyrityksissä, sähköpostit saattavat sisältää joko haitallisia liitetiedostoja tai vastaavasti linkkejä kalastelusivuille. Toisin kun aidossa hyökkäyksessä simuloiduissa uhissa linkit eivät vie kalastelusivulle. Sen sijaan, mikäli viestin vastaanottaja klikkaa linkkiä, hänet ohjataan sivulle, jossa kerrotaan, että kyse oli simulaatiosta. Simuloiduissa viesteissä olevia linkkejä seurataan käyttäjäkohtaisesti. Asiakasyritys Y tarjoaa alkutestiin osallistuneille työntekijöilleen mahdollisuutta osallistua tietojenkalastelusimulaationa järjestetyn koulutuksen. Koulutukseen osallistuminen on vapaaehtoista. Tässä vaiheessa tutkielman otos jaetaan kahteen osaan. Näistä toinen puoli osallistuu Yritys X:n tarjoamaan koulutukseen, toinen ei osallistu. Koulutukseen osallistuva joukko Asiakasyritys Y:n koulutusjärjestelmän käyttäjiä saa neljän kuukauden aikana 1-18 simuloitua tietojenkalasteluviestiä.

Simuloituja viestejä lähetetään noin viikon välein. Lopuksi molemmille ryhmille tehdään lopputesti, jonka avulla koulutuksen vaikuttavuutta voidaan arvioida. Arviointi tehdään vertaamalla koulutukseen osallistuneiden ja osallistumattomien reaktioita saamaansa tietojenkalasteluviestiin.

Kun tarkastellaan sitä, miten tietojenkalasteluviestin saaneet henkilön reagoivat viestiin, voidaan reaktiot jakaa kolmeen erilaiseen ryhmään. Ensimmäinen ryhmä reagoi viestiin toivotulla tavalla eli henkilö havaitsee tietojenkalasteluviestin. Koulutuksessa mukana olevan Asiakasyritys Y:n henkilökunta voi sähköpostijärjestelmään liitetyn painikkeen avulla raportoida tästä. Toinen ryhmä ei reagoi viestiin millään tavalla. Kolmannen ryhmän muodostavat ne työntekijät, jotka avaavat linkin ja siten epäonnistuvat tehtävässä.

Tutkielman ensimmäistä hypoteesia tutkittaessa tehdään siis kaksi mittausta. Ensimmäisessä mittauksessa (alkutesti) on mukana koko asiakasyrityksen henkilökunta ja mittaus on toteutettu ennen tietojenkalastelusimulaationa toteutetun koulutuksen alkamista. Toisessa mittauksessa (lopputesti) ovat mukana sekä ne asiakasyrityksen Y työntekijät, jotka ovat osallistuneet koulutukseen, että ne työntekijät, jotka eivät ole osallistuneet koulutukseen.

Hypoteesia testattaessa, asetetaan kaksi hypoteesia. Nollahypoteesin mukaan muuttujien välillä ei ole riippuvuutta tai keskiarvojen välillä ei ole eroa. Tässä tutkielmassa nollahypoteesin mukaan ne työntekijät, jotka ovat osallistuneet tietojenkalastelusimulaationa järjestettyyn tietoturvakoulutukseen **eivät** onnistu haitallisten tietojenkalasteluviestien tunnistamisessa useammin kuin ne, jotka eivät ole koulutukseen osallistuneet.

Vastahypoteesin mukaan muuttujien välillä on eroa. Kun tutkitaan kahden muuttujan välistä yhteyttä, voidaan käyttää erilaisia menetelmiä, kuten esimerkiksi korrelaatiokertoimia, ristiintaulukointia ja khiin neliö -testiä. Kun samoja koehenkilöitä mitataan jonkin intervention jälkeen uudestaan, puhutaan riippuvista otoksista. Kahden riippuvan otoksen t-testillä voidaan testata kahden riippuvan otoksen välisen eron merkitsevyyttä. Tässä tutkielmassa muuttujien välistä riippuvuutta tutkitaan aineiston muodon vuoksi Wilcoxonin testin avulla. Tällä testillä selvitetään, voidaanko riippuvuus, joka otoksesta on saatu, yleistää koskemaan koko perusjoukkoa. Wilcoxonin testi on ei-parametrinen. Parametriset testit hylkäävät helpommin nollahypoteesin ja sen vuoksi

niiden käyttö on suositeltavaa. Tässä tapauksessa päädyttiin kuitenkin käyttämään Wilcoxonin testiä, koska siinä ei tarvitse olettaa, että perusjoukko noudattaa normaalijakaumaa. Keskeinen asia sopivan testin valitsemisessa on se, millaisesta mitta-asteikosta aineistossa on kysymys. Tässä tapauksessa on kysymyksessä asteikko, joka kuvaa sitä, miten henkilöt ovat onnistuneet tehtävässään. Ryhmät ovat siis laadultaan erilaisia, eikä asteikko ole jatkuva.

Toisen hypoteesin mukaan koulutuksen kestolla on vaikutusta siihen, miten hyvin työntekijä havaitsee tietojenkalasteluviestejä. Hypoteesin mukaan, mitä pidempään työntekijä on mukana tietojenkalastelusimulaationa järjestetyssä koulutuksessa, sitä epätodennäköisempää on, että hän avaa tietojenkalasteluviestissä olevan linkin. Tämän hypoteesin testaamiseksi otetaan tarkempaan tarkasteluun se ryhmä, joka osallistuu koulutukseen. Koulutukseen osallistuvien osalta tutkitaan sitä, miten kalasteluviesteihin reagointi muuttuu koulutuksen jatkuessa. Aineistosta nähdään jokaisen koulutukseen osallistuvan henkilön reaktio kaikkiin saamiinsa tehtäviin. Tehtävien määrä vaihtelee eri henkilöillä, ollen 1-18 tehtävän välillä. Koulutuksessa mukana oleville lähetetään simuloituja tietojenkalasteluviestejä epäsäännöllisin väliajoin neljän kuukauden aikana. Simuloitu tietojenkalasteluviesti on jokaisessa tehtävässä vähän erilainen.

Tutkielman tuloksia käsitellään sekä kvantitatiivisesti että kvalitatiivisesti. Kvantitatiivisen aineiston muoto on sellainen, ettei siitä päästy tekemään tarkempaa tilastotieteellistä analyysiä. Näin ollen päädyttiin tarkastelemaan tuloksia myös kvalitatiivisesti.

6 KOULUTUSSOVELLUS

6.1 Järjestelmän implementointi

Tutkielmassa käytetään Yritys X:n kehittämää koulutussovellusta. Kyseinen sovellus on kehitetty nimenomaan tietojenkalastelun ehkäisyyn ja koulutukseen. Sovelluksen avulla asiakasyritysten työntekijöille lähetetään tekaistuja kalasteluviestejä sähköpostitse. Viestejä voidaan lähettää joko koko henkilöstölle tai valitulle ryhmälle asiakasyrityksen valinnan mukaan.

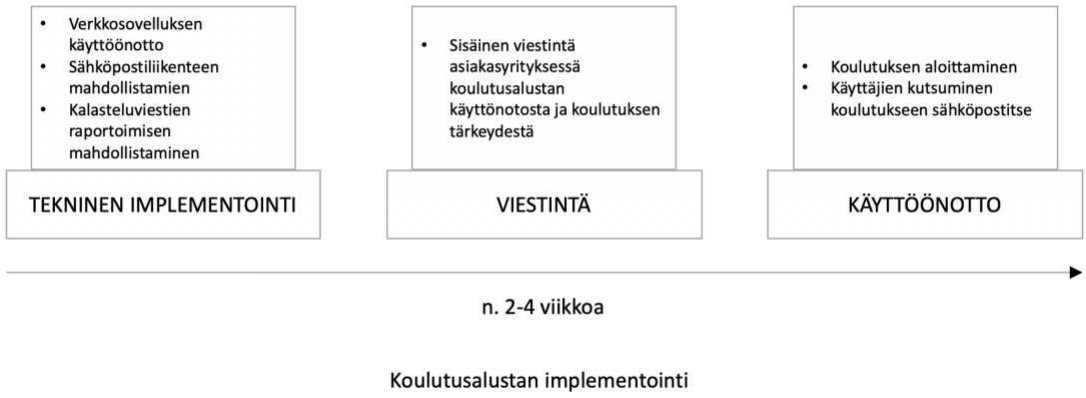
Asiakasyrityksen lähtötilanteessa tehdään tekninen implementointi, joka mahdollistaa koulutussovelluksen käyttöönottoon. Implementointiin kuuluu kolme osa-aluetta; verkkosovelluksen käyttöönotto, sähköpostiliikenteen mahdollistamien sekä kalasteluviestien raportoimisen mahdollistaminen.

Koulutussovellusta käyttöönotettaessa ensimmäinen tehtävä on ottaa käyttöön Yritys X:n kehittämä verkkosovellus ja luoda asiakasyritykselle oma osio sovellukseen. Näin mahdollistetaan järjestelmän asiakaskohtainen ylläpito ja hallinta. Verkkosovellukseen lisätään esimerkiksi tiedot yrityksen työntekijöistä, jotka käsitetään järjestelmän käyttäjinä. Sovellus pitää sisällään myös Yritys X:n kehittämät mallit tekaisutetuista kalasteluviesteistä, joita käytetään koulutuksessa.

Implementoinnin toisessa vaiheessa varmistutaan siitä, että koulutussovellus pystyy lähettämään tekaistut kalasteluviestit asiakasyrityksen työntekijöille. Tämä vaihe on erityisen tärkeä koulutuksen onnistumisen kannalta. Lähtökohta on se, että sähköpostijärjestelmät pyrkivät suodattamaan kalasteluviestejä automaattisesti. Tästä syystä on hyvin mahdollista, että koulutusmielessä lähetetyt sähköpostiviestit tulevat suodatetuksi. Suodatusmenetelmä on tietoturvan kannalta hyvä asia, mutta koulutussovelluksen kannalta se ei ole toivottavaa. Viestien suodatuksen ohittamiseen on muutamia eri vaihtoehtoja. Asiakasyritys voi esimerkiksi sallia kaikki viestit Yritys X:n käyttämästä lähettävästä IP-osoitteesta. On myös mahdollista luoda suora suodattamaton yhteys lähettävän ja vastaanottavan sähköpostipalvelimen välille, mikä mahdollistaa sen, että sähköpostiviestit eivät kulje suodatusjärjestelmien kautta.

Implementoinnin kolmannessa vaiheessa asiakasyrityksen koulutukseen osallistuvien työntekijöiden sähköpostilaatikkoon asennetaan apuohjelma, joka mahdollistaa epäilyttävien viestien raportoinnin. Käytännössä apuohjelma on valintapainike. Painikkeen avulla työntekijä pystyy raportoimaan epäilyttävän viestin. Apuohjelma on yhteydessä koulutussovellukseen.

Kun implementointi on suoritettu onnistuneesti loppuun, voidaan koulutus aloittaa. Asiakasyritystä suositellaan ennen koulutusalustan käyttöönottoa kommunikoimaan koulutuksen aloittamisesti sisäisesti yrityksen työntekijöille. Tämä on usein implementoinnin onnistumisen ja koulutussovelluksen jalkauttamisen kannalta olennainen vaihe. Hyvällä viestinnällä varmistutaan siitä, että yrityksen työntekijät ymmärtävät koulutussovelluksen toimintaperiaatteen ja ennen kaikkea sen pyrkimyksen. Tietojenkalasteluviestit ovat omiaan herättämään voimakkaita tunteita yrityksen työntekijöissä. Tästä johtuen hyvä viestintä ja selkeät ohjeet auttavat rakentamaan luottamusta työntekijöissä. Riippuen asiakasyrityksestä kestää järjestelmän implementointi noin kahdesta neljään viikkoa. Implementoinnin eri vaiheet on esitetty kuvassa 5.



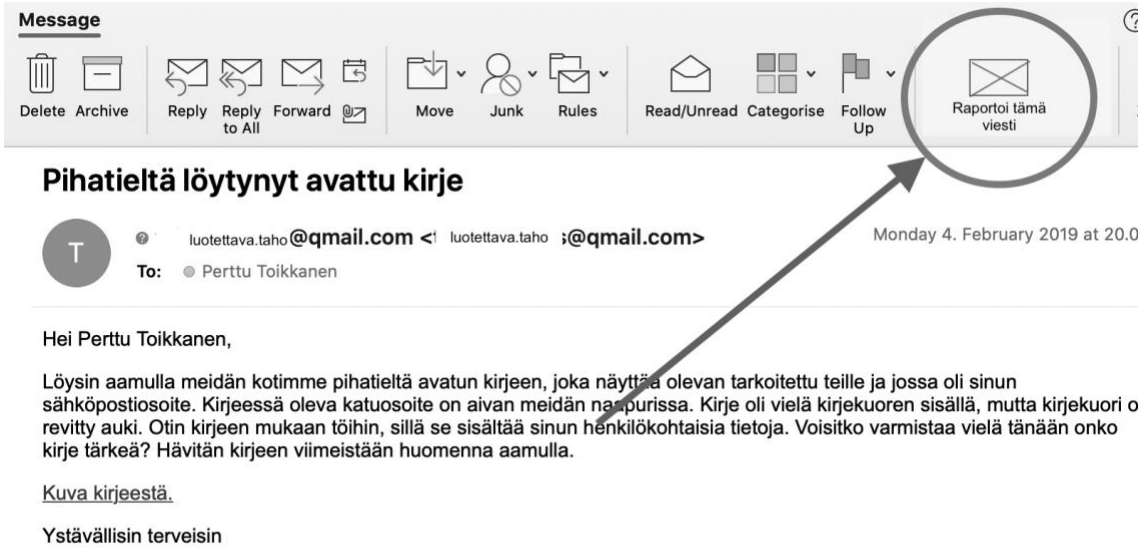
Kuva 5. Koulutusalustan implementoinnin vaiheet.

Koulutussovellusta voidaan soveltaa useaan eri koulutusmalliin, joista yleisin on vapaaehtoinen jatkuva koulutus. Tämä tarkoittaa käytännössä sitä, että asiakasyrityksen työntekijät saavat itse valita osallistuvatko koulutukseen. Mikäli he osallistuvat koulutukseen lähetetään heille keskimäärin yksi tekaistu kalasteluviesti viikossa. Sähköpostiviestien lähetys ja niiden sisällön muodostaminen on automatisoitu

verkkosovelluksessa. Verkkosovellus kerää käyttäjäkohtaista tapahtuma-analytiikkaa, jonka avulla asiakasyritys voi arvioida yrityksen tietoturvan tasoa.

6.2 Tietojenkalastelusimulaation toimintaperiaate ja koulutuksen toteutus

Asiakasyrityksen loppukäyttäjälle tietojenkalastelusimulaatio näyttäytyy kahdella tavalla, sähköpostin apuohjelman ja simuloitujen kalasteluviestien muodossa. Sähköpostiin asennettu apuohjelma mahdollistaa epäilyttävien sähköpostiviestien raportoimisen. Tämä näyttäytyy loppukäyttäjälle kuvan 6 mukaisena painikkeena sähköpostiohjelman valintanauhassa, jossa on teksti ”Raportoi tämä viesti”.



Kuva 6. Raportointipainike valintanauhassa.

Koulutuksessa pyritään toistamaan mahdollisimman aidolta vaikuttava sähköpostitse tapahtuva tietojenkalastelutapaus. Koulutussovellukseen on kehitetty toiminnallisuus, joka hyödyntää html-ohjelmointikielen avulla tehtyjä viestipohjia. Viestipohjat toimivat skaalautuvana tapana mahdollistaa yksilöity koulutus kaikille osallistujille.

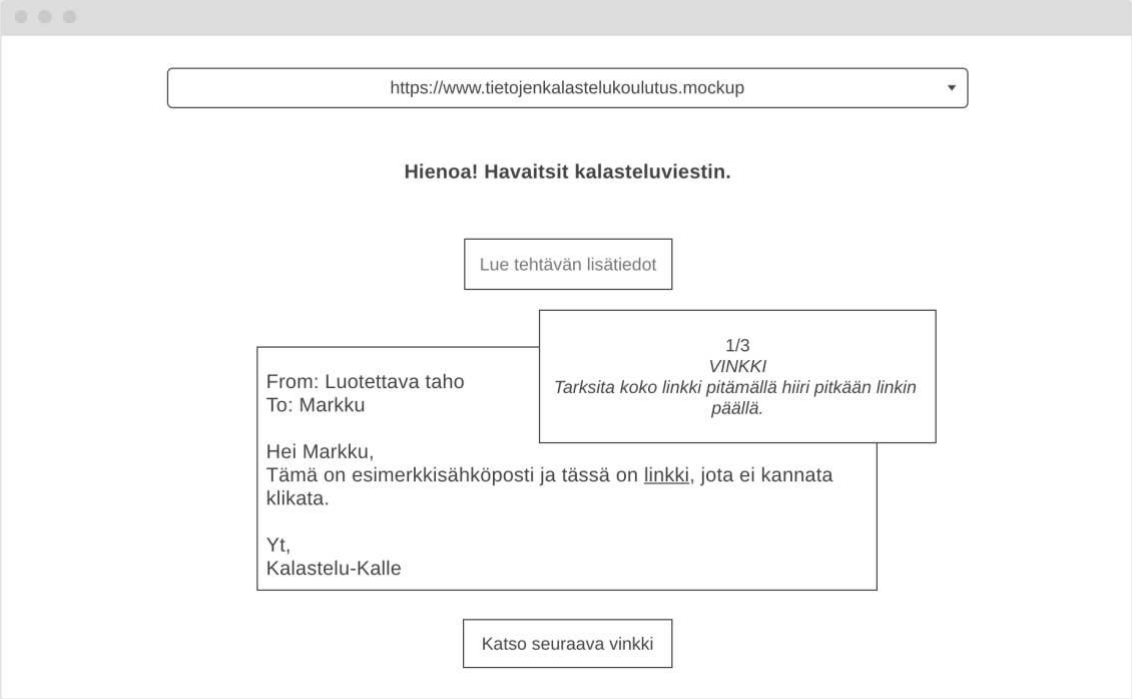
Html-koodi mahdollistaa esimerkiksi seuraavien tietojen automaattisen hakemisen lopulliseen sähköpostiviestiin:

- Asiakasyrityksen nimi/logo
- Asiakasyrityksen käyttämän teleoperaattorin nimi/logo
- Asiakasyrityksen johtohenkilön nimi/sähköpostiosoite
- Kollegan nimi/sähköpostiosoite
- Aikaleima/-vyöhyke
- Koulutettavan tietokoneen käyttöliittymä (vaati sen, että koulutettava on käynyt koulutussovelluksen käyttämällä verkkosivulla)

Näitä tietoja käyttämällä pystytään koulutusta monipuolistamaan ja sillä saadaan aidon tietojenkalastelun vaikutus hyödyntämällä sosiaalisen manipuloinnin keinoja. Tietojenkalastelumenetelmissä saattaa olla pieni eroja, mutta tässä koulutuksessa seurataan ainoastaan sitä, onko sähköpostissa tai sen liitteessä oleva linkki avattu.

Koulutuksen logiikan mukaan koulutettavalla on kolme tapaa reagoida viestiin. Paras vaihtoehto, on että koulutettava raportoi simuloidun uhan sähköpostissa olevan painikkeen avulla. Toiseksi paras vaihtoehto on se, että koulutettava ei reagoi viestiin (avaa linkkiä). Huonoin vaihtoehto on se, että koulutettava avaa viestissä olevan linkin. Mikäli koulutettava reagoi viestiin joko raportoimalla sen tai klikkaamalla linkkiä päätyy hän koulutussovelluksen sivulle. Sivulla kerrotaan, että kyseessä on simuloitu uhka ja

samalla koulutettavalle annetaan mahdollisuus nopeaan oppimishetkeen tehtävään liittyen.



Kuva 6. Mallinnettu kuva tulossivusta.

Koulutussovelluksessa esitetty oppimiskokemus sisältää lisätietoa kyseisestä tehtävästä. Koulutettavalle saatetaan esimerkiksi kertoa, mitä sosiaalisen manipuloinnin keinoa on käytetty ja miten vastaavan tilanteen voi tunnistaa jatkossa. Samoin koulutettavalle voidaan esittää lisätietoa haitallisesta linkistä ja siitä, miten linkin voi tarkistaa turvallista ilman sen avaamista. Nämä oppimishetket näyttäytyvät käyttäjälle pop-up viesteinä ikkunassa, jossa on auki kopio juuri raportoidusta tai epäonnistuneesta tehtävästä. Näiden tehokkaiden oppimishetkien tarkoitus on parantaa koulutettavan valmiutta ja valveutuneisuutta, jotta hän osaa tunnistaa vastaavat hyökkäykset myös jatkossa. Koulutusalusta antaa myös käyttäjälle/koulutettavalle mahdollisuuden seurata koulutuksen etenemistä.

Koulutusalustaan on rakennettu automaatio, joka lähettää simuloituja kalasteluviestejä koulutettaville. Vaikka viestien lähetys on automatisoitu, pyrkii järjestelmä hajauttamaan viestien lähetysajankohdan, niin että käyttäjä ei tunnista viestiä simuloiduksi uhaksi. Kalasteluviestien lähetysväli koulutukseen osallistuville on noin 1 viesti/viikko.

Normaalissa tilanteessa koulutus on jatkuva, eli se on aktiivinen, kunnes toisin määrätään tai mikäli Yritys X:n ja asiakasyrityksen sopimus katkeaa.

Kuten moni verkkosovellus, myös Yritys X:n kehittämä sovellus kerää lokitietoa käyttäjien tapahtumista. Tämän lokitiedon avulla on kerätty tähän tutkielmaan liittyvä aineisto. Tässä tutkimuksessa tullaan käyttämään seuraavia lokitietoja; simuloidun tietojenkalasteluviestin onnistunut lähetys, linkin avaaminen ja viestin onnistunut raportointi sähköpostissa olevan apuohjelman kautta.

7 TULOKSET

7.1 Yleistä tuloksista

Tutkielman hypoteesit ovat selkeitä ja tulosten mittaaminen on siitä syystä yksiselitteistä. Asiakasyrityksen tuloksia tutkittaessa mittarin validiteetti on siis hyvä ja mittaus mittaa todellakin sitä asiaa, jota sillä halutaan mitata. Hyvän reliabiliteetin edellytys on se, että mittauksia voidaan toistaa useita kertoja samanlaisena. Tässä tutkielmassa asiakasyritys Y:n saamat simuloidut viestit ovat eri kertoina erilaisia. Näin ollen ei mitata tarkalleen ottaen täysin samaa asiaa. Aineisto on kuitenkin niin suuri, että tällä tuskin on suurta vaikutusta lopputuloksiin.

Tutkielman otos on riittävän suuri, jotta tuloksia voidaan pitää luotettavina. Yhteensä tutkielman otoksessa oli 36444 henkilöä. Vain alku- ja lopputestiin osallistuneita henkilöitä oli 33488. Koulutukseen osallistuneita oli 2956. Koulutukseen osallistuneiden henkilöiden tuloksia kerättiin useasta eri tehtävästä. He saivat simuloituja tietojenkalasteluviestejä neljän kuukauden aikana 1-18 kappaletta.

Jos tarkoituksena on tutkia, miten muuttuja x vaikuttaa muuttujaan Y, on jotenkin pystyttävä kontrolloimaan muiden muuttujaan y vaikuttavien tekijöiden osuus. Hypoteesin mukaan oletettiin, että koulutuksella on vaikutusta siihen, miten hyvin henkilökunta osaa reagoida tietojenkalasteluviesteihin. Tässä tapauksessa voi väliin tulla muitakin muuttujia kuin koulutus. Lopputuloksiin voi vaikuttaa ajankohtainen julkinen keskustelu, laajalle levinnyt lehtiartikkeli, asiasta keskusteleminen työpaikalla tai muu sellainen tekijä. Tässä tutkielmassa oli kuitenkin niin suuri otos, että tämän tapaisten muuttujien vaikutus tuskin voi vaikuttaa lopputuloksiin.

Työntekijöiden reaktiot jaettiin kaikissa tutkielman testeissä kolmeen osaan:

1. Henkilöt, jotka havaitsevat tietojenkalasteluviestin ja raportoivat siitä sähköpostijärjestelmään liitetyn painikkeen avulla. Tutkielmassa tästä ryhmästä käytetään nimitystä **raportoineet.**

2. Henkilöt, jotka eivät reagoi viestiin millään tavalla. Tästä ryhmästä käytetään tutkielmassa nimitystä **ei reaktiota**.

3. Henkilöt, jotka avaavat linkin ja siten epäonnistuvat tehtävässä. Tästä ryhmästä tutkielmassa käytetään nimitystä **epäonnistuneet**.

Tietoturvan kannalta olisi tietenkin toivottavaa, että henkilöt havaitsisivat saamansa tietojenkalasteluviestit. Näin ollen olisi toivottavaa, että ryhmä 1 muodostuisi mahdollisimman suureksi. Toiseksi paras vaihtoehto olisi se, ettei henkilö reagoi viestiin lainkaan. Tässä tapauksessa ei mitään vahinkoa pääse syntymään. Huonoin vaihtoehto on se, että henkilö avaa linkin. Kun kyseessä on simuloitu uhka, linkit eivät vie kalastelusivulle. Sen sijaan, mikäli viestin vastaanottaja klikkaa linkkiä, hänet ohjataan sivulle, jossa kerrotaan, että kyse oli simulaatiosta. Tässäkään ei siis vahinkoa synny, mutta työntekijän on mahdollista pohtia sitä, ovatko hän taitonsa havaita haitallisia tietojenkalasteluviestejä riittävän korkealla tasolla.

Tutkielman tuloksia käsitellään sekä tilastojen valossa kvantitatiivisesti että kvalitatiivisesti tuloksia analysoiden. Näin tutkielman tekijä yrittää ymmärtää tutkittavan ilmiön ominaisuuksia kokonaisvaltaisesti.

7.2 Ensimmäiseen hypoteesiin liittyvät tulokset

Hypoteesi: Ne työntekijät, jotka ovat osallistuneet tietojenkalastelusimulaationa järjestettyyn tietoturvakoulutukseen onnistuvat haitallisten tietojenkalasteluviestien tunnistamisessa useammin kuin ne, jotka eivät ole koulutukseen osallistuneet.

Nollahypoteesin mukaan koulutuksella ei ole vaikutusta.

Tutkimusasetelman mukaisesti suoritettiin ensin alkutesti. Sen tekivät kaikki Asiakasyritys Y:n työntekijät. Näitä henkilöitä oli 33 488. Alkutestissä Yritys X lähetti asiakasyrityksen työntekijöille simuloidun tietojenkalasteluviestin.

Alkutestissä työntekijöiden reaktiot jakautuivat seuraavanlaisesti:

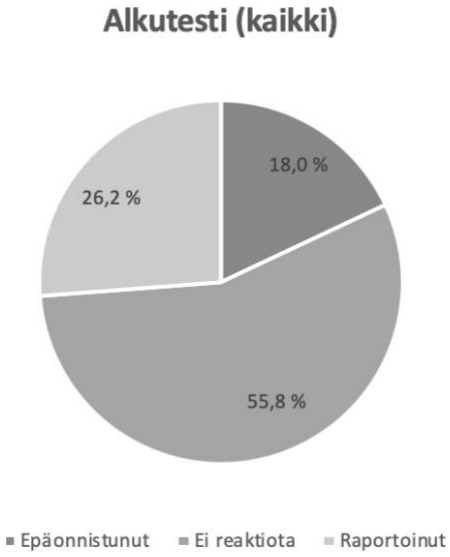
1. Tietojenkalasteluviestistä raportoineita henkilöitä oli 9553 eli 26,2 prosenttia.

2. Niitä henkilöitä, jotka eivät reagoineet saamaansa viestiin millään tavalla oli 20 329 eli 55,8 prosenttia.

3. Epäonnistuneita eli niitä, jotka avasivat linkin, oli 6 562 eli 18 prosenttia.

Alkutesti (kaikki)		
	n	%
Epäonnistunut	6562	18,0 %
Ei reaktiota	20329	55,8 %
Raportoinut	9553	26,2 %
Yhteensä	36444	100,0 %

Taulukko 1. Alkutestin tulokset.



Kuvio 1. Alkutestin tulokset.

Alkutestin jälkeen Asiakasyritys Y:n työntekijöille annettiin mahdollisuus osallistua tietojenkalastelusimulaationa järjestettyyn koulutuksen. Koulutukseen osallistuminen oli vapaaehtoista. Alkutestiin osallistuneista yli 36000:sta henkilöstä koulutukseen halusi osallistua 2956 henkilöä. Tässä vaiheessa tutkielman otos jaettiin kahteen osaan. Näistä toinen puoli osallistui Yritys X:n tarjoamaan koulutukseen, toinen ei osallistunut. Koulutukseen osallistuva joukko Asiakasyritys Y:n koulutusjärjestelmän käyttäjiä sai sähköpostiinsa vaihtelevan määrän simuloitua tietojenkalasteluviestiä. Simuloituja viestejä lähetettiin neljän kuukauden aikana 1-18 kappaletta. Ne lähetettiin noin viikon välein.

Lopuksi molemmille ryhmille tehtiin lopputesti. Tähän testiin osallistuivat siis sekä koulutuksessa mukana olleet, että ne henkilöt, jotka eivät olleet koulutuksessa mukana (yhteensä 36444 henkilöä).

Lopputestissä kaikkien työntekijöiden reaktiot jakautuvat näin:

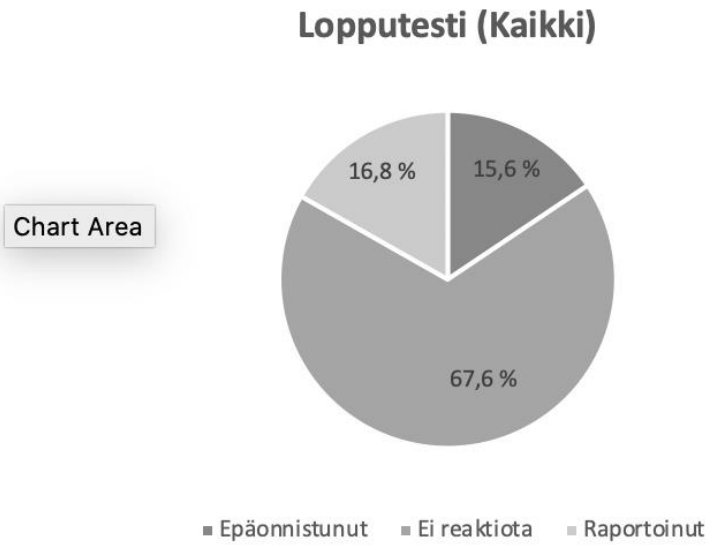
1. Tietojenkalasteluviestistä raportoineita henkilöitä oli 6 122 eli 16,8 prosenttia.

2. Niitä henkilöitä, jotka eivät reagoineet saamaansa viestiin millään tavalla oli 24636 eli 67,6 prosenttia.

3. Epäonnistuneita eli niitä, jotka avasivat linkin oli 5686 eli 15,6 prosenttia.

Lopputesti (Kaikki)		
	n	%
Epäonnistunut	5686	15,6 %
Ei reaktiota	24636	67,6 %
Raportoinut	6122	16,8 %
Yhteensä	36444	100,0 %

Taulukko 2. Lopputestin tulokset.



Kuvio 2. Lopputestin tulokset

Koko ryhmän alku- ja lopputestejä verrattaessa huomataan, että niitä henkilöitä, jotka olivat epäonnistuneet tehtävässä avaamalla linkin, oli lopputestissä hieman vähemmän kuin alkutestissä. Sekä reagoimatta jättäminen, että kalasteluviestistä ilmoittaminen lisääntyivät vastaavasti hieman. Se, että niiden henkilöiden määrä pieneni, jotka epäonnistuivat lopputestissä, oli Asiakasyritys Y:n kannalta hyvä tulos. Ero ei kuitenkaan ollut suuri. Tuloksissa huomiota herättää se, että arveluttavasta kalasteluviestistä

ilmoittaneiden määrä pieneni lopputestauksessa. Tämän tuloksen syyhyn ei tutkielmasta löydy selitystä.

Tutkielman aiheesta johtuen mielenkiintoisimmat tulokset löytyvät siitä henkilöiden ryhmästä, joka osallistui koulutukseen. Tähän ryhmään kuului 2956 henkilöä.

Koulutuksessa olleiden työntekijöiden lopputestin reaktiot jakautuvat näin:

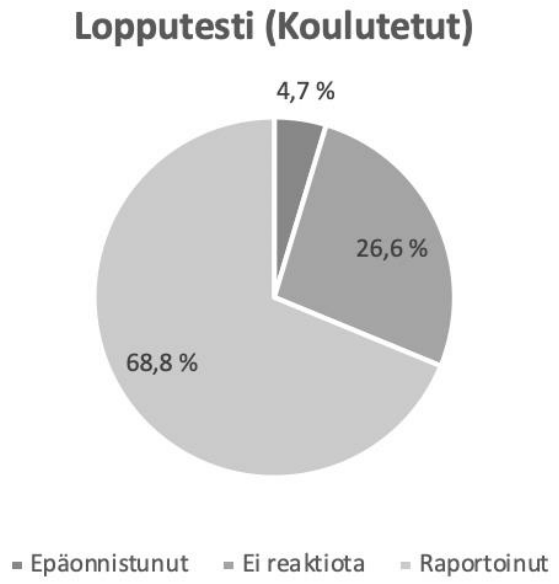
1. Tietojenkalasteluviestistä raportoineita henkilöitä oli 2033 eli 68,8 prosenttia.

2. Niitä henkilöitä, jotka eivät reagoineet saamaansa viestiin millään tavalla oli 785 eli 26,6 prosenttia.

3. Epäonnistuneita eli niitä, jotka avasivat linkin oli 138 eli 4,7 prosenttia.

Lopputesti (Koulutetut)		
	n	%
Epäonnistunut	138	4,7 %
Ei reaktiota	785	26,6 %
Raportoinut	2033	68,8 %
Yhteensä	2956	100,0 %

Taulukko 3. Lopputestin tulokset koulutettujen käyttäjien osalta.



Kuvio 3. Lopputestin tulokset koulutettujen käyttäjien osalta.

Näiden lukujen valossa näyttää siltä, että koulutuksella on suuri vaikutus siihen, miten henkilö oppii tunnistamaan haitallisia tietojenkalasteluviestejä. Suurin muutos alkutestiin nähden on tapahtunut siinä, miten aktiivisesti työntekijät ovat ilmoittaneet havaitsemistaan tietojenkalasteluviesteistä. Alkutestin tehneistä henkilöistä 26,2 % raportoi sähköpostijärjestelmään liitetyllä painikkeella havainneensa tietojenkalasteluviestin. Lopputestin tulos niiden osalta, jotka olivat osallistuneet koulutukseen, oli peräti 68,8 prosenttia. Käyttäjät, jotka olivat saaneet alkutestin jälkeen ainakin yhden simuloidun kalasteluviestin epäonnistumisprosentti putosi 4,7 prosenttiin, vastaavan osuuden ollessa alkutestissä 18%.

Koulutukseen osallistuneiden tulosten kehittymistä koulutuksen edetessä tarkastellaan seuraavassa luvussa.

Lopputestiin osallistui 33 488 sellaista henkilöä, jotka eivät osallistuneet koulutukseen.

Lopputestin tulokset niiden osalta, jotka eivät osallistuneet koulutukseen:

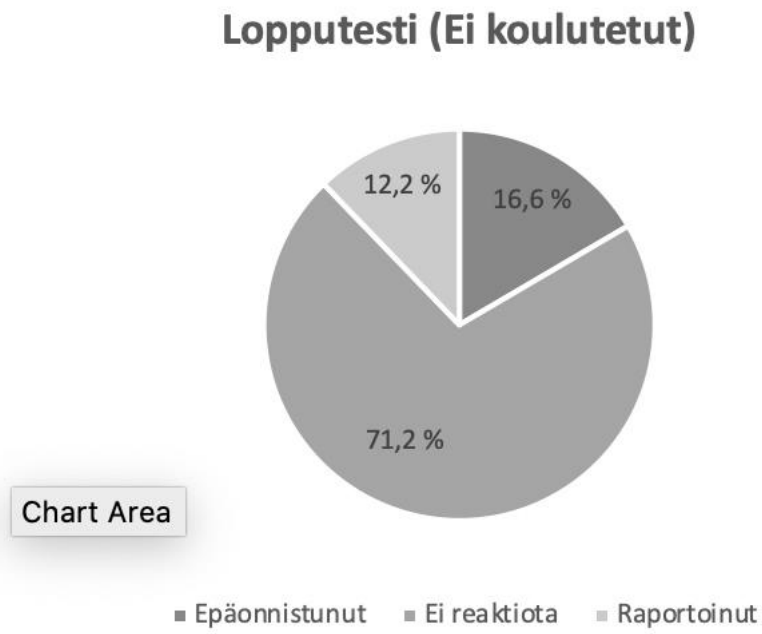
1. Tietojenkalasteluviestistä raportoineita henkilöitä oli 4089 eli 12,2 prosenttia.

2. Niitä henkilöitä, jotka eivät reagoineet saamaansa viestiin millään tavalla oli 23851 eli 71,2 prosenttia.

3. Epäonnistuneita eli niitä, jotka avasivat linkin oli 5 548 eli 16,6 prosenttia.

Lopputesti (Ei koulutetut)		
	n	%
Epäonnistunut	5548	16,6 %
Ei reaktiota	23851	71,2 %
Raportoinut	4089	12,2 %
Yhteensä	33488	100,0 %

Taulukko 4. Lopputestin tulokset ei koulutettujen käyttäjien osalta.



Kuvio 4. Lopputestin tulokset ei koulutettujen käyttäjien osalta.

Kun kouluttamattomien tuloksia verrataan koulutettujen saamiin tuloksiin, huomataan merkittävä ero. Koulutetuista henkilöistä 68,8 % ilmoitti havainneensa kalasteluviestin. Kouluttamattomien ryhmässä vastaava luku oli 12,2 %. Kouluttamattomien ryhmässä oli huomattavan paljon (71,2 %) niitä, jotka eivät reagoineet simuloituihin viesteihin millään lailla.

Kaikkien edellä esitettyjen tulosten valossa voidaan arvioida koulutuksen vaikuttavuutta. Arviointi tehdään vertaamalla koulutukseen osallistuneiden ja osallistumattomien reaktioita tietojenkalasteluviestiin, jonka he saivat sähköpostiinsa. Edellä vaikuttavuutta arvioitiin prosenttilukujen avulla.

Tässä tutkielmassa haluttiin myös tilastotieteellisin keinoin testata kahden muuttujan välisen riippuvuuden merkitsevyyttä. Kerätty aineisto aiheutti testaamiselle reunaehtoja. Ne liittyivät tutkittuun aineistoon, joka kuvasi sitä, miten henkilöt onnistuivat tehtävässään. Mitta-asteikko ei ollut jatkuva. Ryhmät olivat laadultaan erilaisia, eikä perusjoukon normaalijakaumaa ollut mahdollista tavoitella. Tutkielmassa päädyttiin käyttämään Wilcoxonin testiä. Testin tulosten perusteella voidaan todeta, että riippuvuus, joka otoksesta on saatu, voidaan yleistää koskemaan koko perusjoukkoa.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between Alkutesti and Lopputesti equals 0.	Related-Samples Wilcoxon Signed Rank Test	,000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is ,050.

Related-Samples Wilcoxon Signed Rank Test

Alkutesti, Lopputesti

Related-Samples Wilcoxon Signed Rank Test Summary

Total N	2956
Test Statistic	73008,000
Standard Error	2242,138
Standardized Test Statistic	11,801
Asymptotic Sig.(2-sided test)	,000

Kuva 5. Wilcoxonin testin tulokset.

Yllä olevassa kuvassa tärkeä arvo on Sig. Sen arvo tässä aineistossa on 0,000. Sig kertoo merkitsevyystasosta (Significance). Merkitsevyys- eli riskitason avulla selvitetään kuinka suuri on riski siihen, että saatu riippuvuus johtuu sattumasta. Raportoinneissa merkitsevyystasosta käytetään lyhennettä p (probability). Testatun riippuvuuden sanotaan olevan tilastollisesti erittäin merkitsevä, jos p on pienempi tai yhtä suuri kuin 0,001 (Tarja Heikkilä: 2014).

Tutkielman aineiston ja käytetyn Wilcoxonin testin avulla voidaan siis todeta tutkielmassa esiintyvän riippuvuuden olevan tilastollisesti merkitsevä. Kaksisuuntaisen

Wilcoxon merkittyjen sijalukujen testin p-arvo on tässä aineistossa pienempi kuin 0,05. Näin ollen nollahypoteesi voidaan hylätä.

Tutkielman hypoteesi on: *Ne työntekijät, jotka ovat osallistuneet tietojenkalastelusimulaationa järjestettyyn tietoturvakoulutukseen onnistuvat haitallisten tietojenkalasteluviestien tunnistamisessa useammin kuin ne, jotka eivät ole koulutukseen osallistuneet.*

Tämä hypoteesi voidaan tämän tutkielman tulosten mukaan todeta oikeaksi.

7.3 Toiseen hypoteesiin liittyvät tulokset

Tutkielman toisen hypoteesin mukaan, mitä pidempään työntekijä on mukana tietojenkalastelusimulaationa järjestetyssä koulutuksessa, sitä epätodennäköisempää on, että hän avaa tietojenkalasteluviestissä olevan linkin.

Kerätyn aineiston avulla tarkastellaan sitä, vaikuttaako koulutuksen (simulaation) pituus yritysten työntekijöiden kykyyn havaita haitallisia sähköposteja ja kuinka voimakas vaikutus on.

Aineistoa on kerätty samasta havaintoyksiköstä (asiakasyritys Y) useita kertoja neljän kuukauden aikana.

Alkutestin jälkeen Asiakasyrityksen Y työntekijöillä oli mahdollisuus osallistua tietojenkalastelusimulaationa järjestettyyn koulutukseen. Koulutuksen aikana Yritys X lähetti asiakasyritys Y:n työntekijöille tekaistuja kalasteluviestejä sähköpostitse. Heille lähetettiin keskimäärin yksi tekaistu kalasteluviesti viikossa. Viestien sisältö vaihteli koulutuksen aikana ollen joka kerralla erilainen. Koulutukseen osallistuneiden työntekijöiden saamien tekaistujen viestien määrä vaihteli 1-18 välillä.

Yrityksen X verkkosovellus kerää käyttäjäkohtaista tapahtuma-analytiikkaa, jonka avulla asiakasyritys voi arvioida yrityksen tietoturvan tasoa. Tämän datan tuottamaa aineistoa tarkastellaan tässä tutkielmassa seuraavaksi.

Jatkuva koulutus (n)

	Tehtävä 1	Tehtävä 2	Tehtävä 3	Tehtävä 4	Tehtävä 5	Tehtävä 6	Tehtävä 7	Tehtävä 8	Tehtävä 9	Tehtävä 10	Tehtävä 11	Tehtävä 12	Tehtävä 13	Tehtävä 14	Tehtävä 15	Tehtävä 16	Tehtävä 17	Tehtävä 18
Epäonnistunut	454	205	243	102	228	235	275	259	241	172	115	59	30	16	3	2	0	0
Ei reaktiota	858	910	575	821	1160	1091	1037	951	847	753	509	298	120	62	15	1	2	0
Raportoinut	1643	1836	2060	1837	1267	1251	1197	1257	1315	1336	1332	1123	822	450	197	49	18	1
Yhteensä	2955	2951	2878	2760	2655	2577	2509	2467	2403	2261	1956	1480	972	528	215	52	20	1

Taulukko 5. Jatkuvaan koulutuksen osallistuneiden henkilöiden reaktiot kalasteluviesteihin numeroina.

Ensimmäisen tehtävän, joka työntekijöille lähetettiin, sai 2955 henkilöä. Koulutuksessa mukana olleet saivat vaihtelevan määrän viestejä. Niiden henkilöiden lukumäärä, jotka saivat tekaistuja viestejä pienenee loppua kohden. Tehtävän 12 sai 1480 henkilöä. Niitä henkilöitä, jotka saivat 17 viestiä on otoksessa 20 ja vain yksi henkilö sai 18 viestiä. Näin ollen aineiston loppupään tulokset eivät tuota asian kannalta merkityksellistä tulosta.

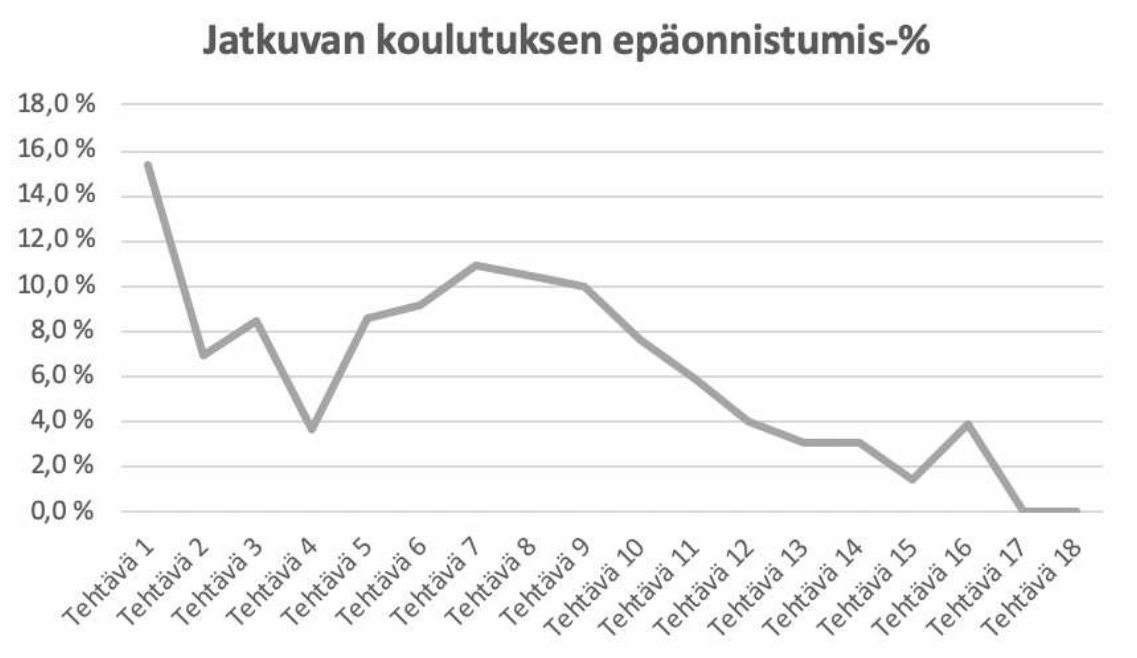
Aineistosta nähdään jokaisen tehtävän kohdalta se, miten henkilöt ovat reagoineet simuloituun kalasteluviestiin.

Jatkuva koulutus (%)

	Tehtävä 1	Tehtävä 2	Tehtävä 3	Tehtävä 4	Tehtävä 5	Tehtävä 6	Tehtävä 7	Tehtävä 8	Tehtävä 9	Tehtävä 10	Tehtävä 11	Tehtävä 12	Tehtävä 13	Tehtävä 14	Tehtävä 15	Tehtävä 16	Tehtävä 17	Tehtävä 18
Epäonnistunut	15,4 %	6,9 %	8,4 %	3,7 %	8,6 %	9,1 %	11,0 %	10,5 %	10,0 %	7,6 %	5,9 %	4,0 %	3,1 %	3,0 %	1,4 %	3,8 %	0,0 %	0,0 %
Ei reaktiota	29,0 %	30,8 %	20,0 %	29,7 %	43,7 %	42,3 %	41,3 %	38,5 %	35,2 %	33,3 %	26,0 %	20,1 %	12,3 %	11,7 %	7,0 %	1,9 %	10,0 %	0,0 %
Raportoinut	55,6 %	62,2 %	71,6 %	66,6 %	47,7 %	48,5 %	47,7 %	51,0 %	54,7 %	59,1 %	68,1 %	75,9 %	84,6 %	85,2 %	91,6 %	94,2 %	90,0 %	100,0 %
Yhteensä	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %

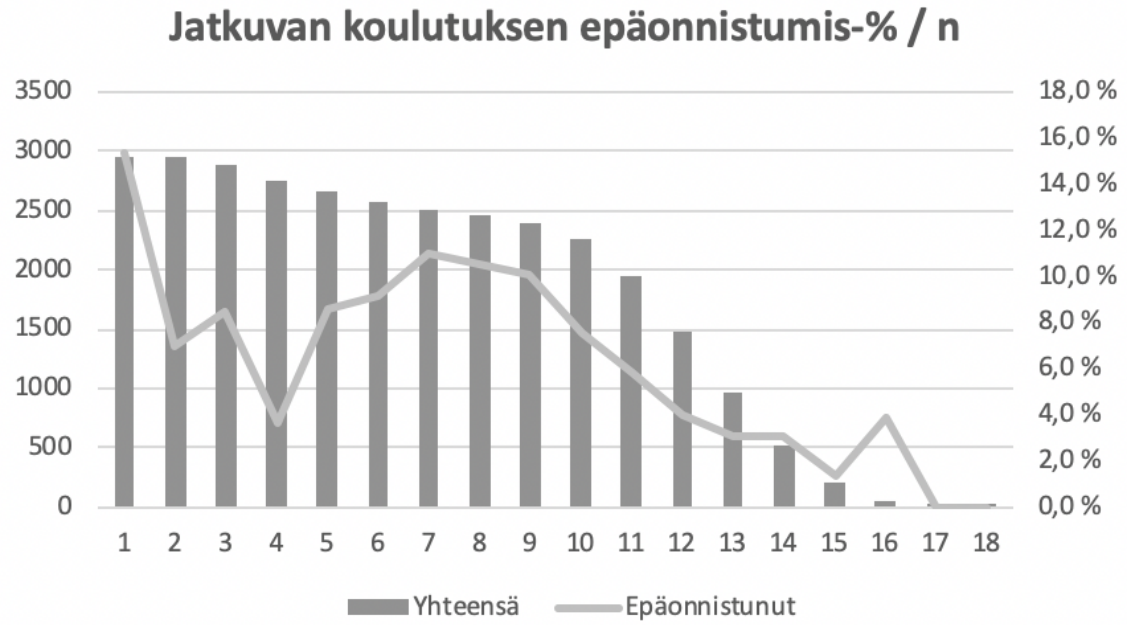
Taulukko 6. Jatkuvaan koulutukseen osallistuneiden henkilöiden reaktiot prosentteina.

Prosenteiksi muutettuina aikaisemmassa kuvassa olevat numerot ovat helpommin ymmärrettävässä muodossa, koska viestin saaneiden henkilöiden määrä vaihtelee eri tehtävissä. Suurinta mielenkiintoa aiheuttaa epäonnistumisprosentti.



Kuvio 5. Jatkuvan koulutuksen kuuluneiden tehtävien epäonnistumisprosentit viivadiagrammin muodossa.

Tästä diagrammista nähdään havainnollisesti epäonnistumisprosentin laskeva kehityssuunta. Se ei kuitenkaan ole suoraviivaisesti laskeva. Tätä huomiota selittää se, että tehtävät vaihtelivat eri kertoina. Todennäköisesti niinä kertoina, jolloin epäonnistumisprosentti on ollut aikaisempia suurempi (esim. tehtävät 7, 8 ja 9), tehtävät ovat voineet olla vaikeampia. Niitä on ehkä ollut hankalampi havaita kalasteluviesteiksi. Kuten edellä jo mainittiin loppupään tuloksiin ei kannata pienen otoksen vuoksi kiinnittää suurta huomiota.

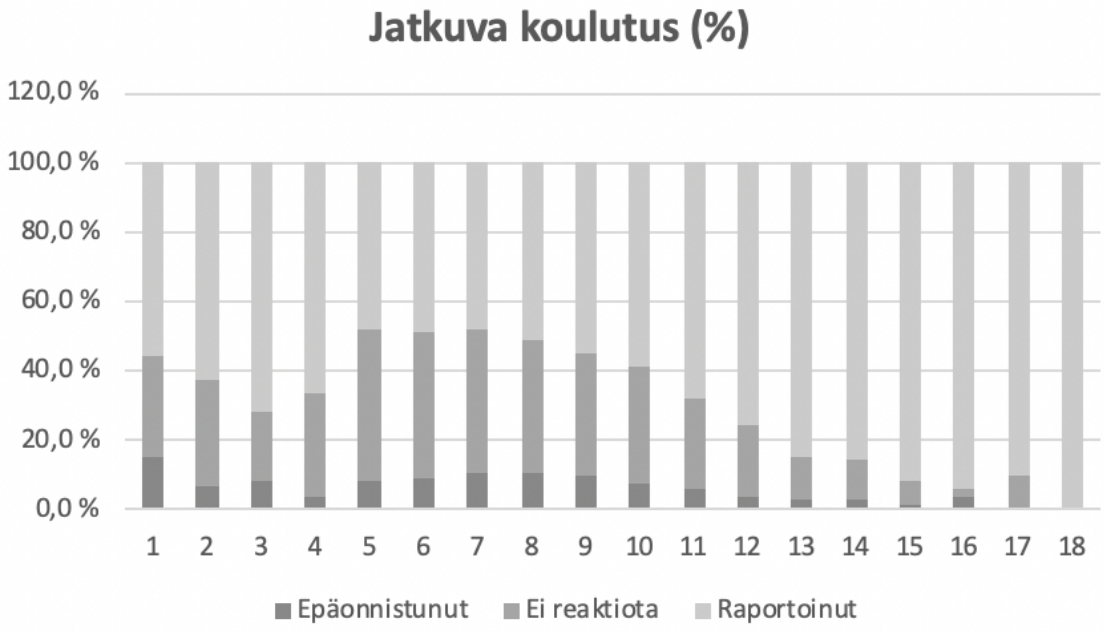


Kuvio 6. Jatkuvan koulutuksen epäonnistumisprosentti suhteessa tehtävän tehneiden lukumäärään.

Neljännen tehtävän kohdalla nähdään, että tehtävän tehneitä on suuri ryhmä ja epäonnistumisprosentti on hyvin alhainen (3,7 %). Tämä tehtävä on todennäköisesti ollut hyvin helppo.

Tehtävissä 12-15 otos on vielä melko suuri. Epäonnistumisprosentti on laskenut alle viiteen. Ensimmäisessä testissä se oli 15,4 %.

Tehtävän 15 teki 215 henkilöä. Siinä epäonnistumisprosentti oli vain 1,4 %.



Kuvio 7. Henkilöiden reagointi tehtävittäin.

Tässä kuvassa näkyy henkilöiden reagointi jokaisen simuloidun viestin osalta erikseen. Siinä näkyvät epäonnistumisen lisäksi myös se, miten usein henkilö ei reagoi tehtävään lainkaan ja miten usein hän ilmoittaa huomanneensa tietojenkalasteluviestin. Se, jos henkilö ei reagoi kalasteluviestiin mitenkään, on tietoturvan kannalta hyvä reaktio. Uhasta ilmoittaminen eli raportoiminen on vielä parempi. Raportoineiden osuus kasvoi koulutuksen edetessä.

Koulutusjakson keskivaiheilla olevissa tehtävissä (tehtävät 5-10) niiden osuus, jotka eivät reagoineet mitenkään oli melko suuri (33-43 %).

Koulutuksen loppupuolella niiden henkilöiden määrä, jotka ilmoittivat havainneensa simuloidun kalasteluviestin, kasvoi suureksi. Tehtävässä 15, jossa otos oli 215 henkilöä, 91,6 % henkilöistä ilmoitti kalasteluviestistä. Ensimmäisen tehtävän kohdalla vastaava arvo oli 55,6 %.

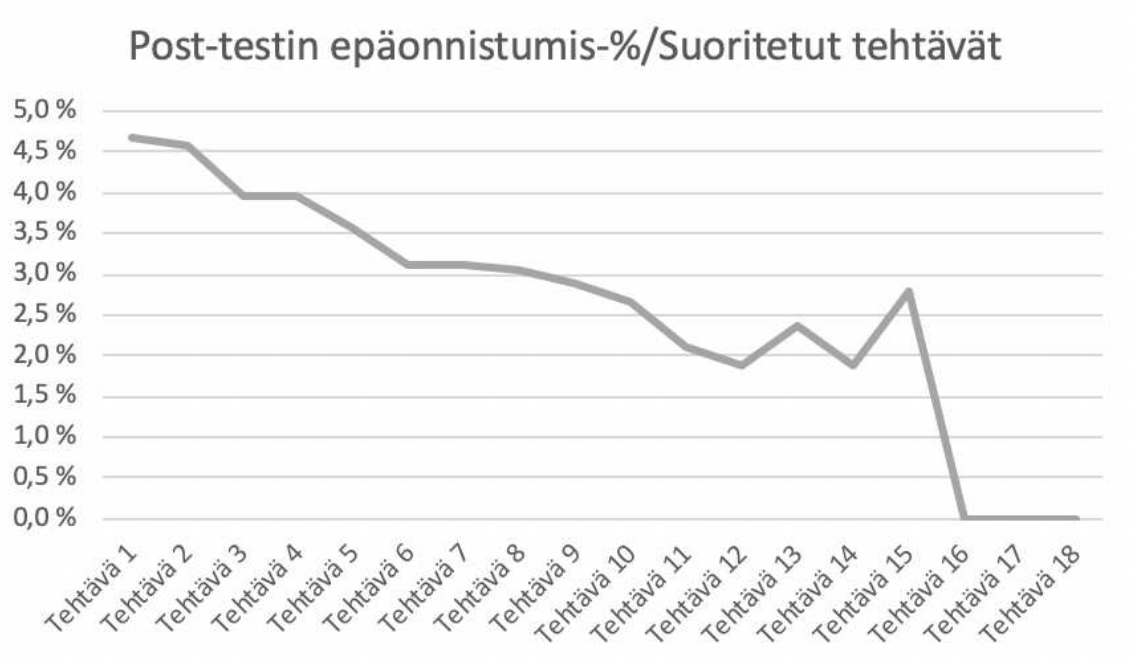
Post-testin tulos/koulutustehtävä (n)

	Tehtävä 1	Tehtävä 2	Tehtävä 3	Tehtävä 4	Tehtävä 5	Tehtävä 6	Tehtävä 7	Tehtävä 8	Tehtävä 9	Tehtävä 10	Tehtävä 11	Tehtävä 12	Tehtävä 13	Tehtävä 14	Tehtävä 15	Tehtävä 16	Tehtävä 17	Tehtävä 18
Epäonnistunut	138	135	114	109	95	80	78	75	69	60	41	28	23	10	6	0	0	0
Ei reaktiota	785	785	785	773	716	689	682	675	636	538	387	228	113	45	16	4	1	0
Raportoinut	2032	2031	1979	1878	1844	1808	1749	1717	1698	1663	1528	1224	836	473	193	48	19	1
Yhteensä	2955	2951	2878	2760	2655	2577	2509	2467	2403	2261	1956	1480	972	528	215	52	20	1

Post-testin tulos/koulutustehtävä (%)

	Tehtävä 1	Tehtävä 2	Tehtävä 3	Tehtävä 4	Tehtävä 5	Tehtävä 6	Tehtävä 7	Tehtävä 8	Tehtävä 9	Tehtävä 10	Tehtävä 11	Tehtävä 12	Tehtävä 13	Tehtävä 14	Tehtävä 15	Tehtävä 16	Tehtävä 17	Tehtävä 18
Epäonnistunut	4,7 %	4,6 %	4,0 %	3,9 %	3,6 %	3,1 %	3,1 %	3,0 %	2,9 %	2,7 %	2,1 %	1,9 %	2,4 %	1,9 %	2,8 %	0,0 %	0,0 %	0,0 %
Ei reaktiota	26,6 %	26,6 %	27,3 %	28,0 %	27,0 %	26,7 %	27,2 %	27,4 %	26,5 %	23,8 %	19,8 %	15,4 %	11,6 %	8,5 %	7,4 %	7,7 %	5,0 %	0,0 %
Raportoinut	68,8 %	68,8 %	68,8 %	68,0 %	69,5 %	70,2 %	69,7 %	69,6 %	70,7 %	73,6 %	78,1 %	82,7 %	86,0 %	89,6 %	89,8 %	92,3 %	95,0 %	100,0 %
Yhteensä	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %

Taulukko 7. Lopputestin epäonnistumisprosentti suhteessa suoritettuihin tehtäviin.



Kuvio 8. Lopputestin epäonnistumisprosentti suhteessa suoritettuihin tehtäviin.

Huomion arvoista on se, että lopputestissä kaikki tekivät saman tehtävän. Niiden henkilöiden, jotka olivat saaneet vain yhden tehtävän, epäonnistumisprosentti lopputehtävässä oli 4,7. Alkutestissä kaikkien työntekijöiden epäonnistumisprosentti oli 18 %. Tämä tulos antaa sellaisen vaikutelman, että jo yhden tehtävän tekeminen laskisi epäonnistumisprosenttia huomattavasti. Tällaisen johtopäätöksen tekeminen on kuitenkin liian suoraviivaista. Voi toki olla, että jotkut henkilöt ovat havahtuneet kalasteluviestien varomiseen jo heti yhden tehtävän (alkutesti) tehtyään. Toisaalta tulokseen voi vaikuttaa se, että lopputesti on saattanut olla alkutestiä helpompi. Tässä tutkielmassa ei lainkaan selvitetty tehtävien sisältöön liittyviä asioita. Tärkeämpää kuin kahden yksittäisen tehtävän vertaaminen, on suuren linjan tarkastelu. Yllä oleva kuva havainnollistaa sen, että linja on laskeva eli koulutus pienentää epäonnistumisen riskiä.

Toinen hypoteesi oli: *Mitä pidempään työntekijä on mukana tietojenkalastelusimulaationa järjestetyssä koulutuksessa, sitä epätodennäköisempää on, että hän avaa tietojenkalasteluviestissä olevan linkin.* Tämä hypoteesi voidaan tutkielman

tulosten mukaan todeta oikeaksi. Johtopäätös tuloksista on siis se, että mitä pidempään henkilö on osallistunut koulutukseen, sitä pienemmäksi epäonnistumisprosentti laskee.

8 DISKUSSIO JA YHTEENVETO

Tietoturva on tutkimuskohteena todella laaja. Tässä tutkielmassa onnistuttiin rajaamaan tutkittava alue hyvin. Tutkielmassa tutkittiin tietoturvakoulutuksen vaikuttavuutta. Tietoturvakoulutusta on monenlaista, mutta tässä tutkielmassa tutkittiin vain sähköpostitse tuleviin kalasteluviesteihin reagointia ja koulutuksen vaikutusta siihen.

Tutkielman tuloksia tarkasteltiin sekä kvantitatiivisin että kvalitatiivisin keinoin. Kvantitatiivinen tutkimus perustuu numeroihin ja tilastoihin. Tilastollisten menetelmien käyttö jäi aineiston muodosta johtuen tässä tutkielmassa suppeaksi. Kvalitatiivisen eli laadullisen tutkimisen avulla pyritään ymmärtämään tutkittavaa ilmiötä kokonaisvaltaisesti. Tässä tutkielmassa nämä menetelmät täydentävät toisiaan. Tutkittavaan asiaan voidaan näin paneutua monipuolisesti ottaen huomioon ilmiön eri ominaisuudet.

Tutkielman tavoitteena oli tutkia tietojenkalastelusimulaationa järjestetyn koulutuksen vaikutusta työntekijöiden kykyyn tunnistaa sähköpostin kautta tulevia haitallisia tietojenkalasteluviestejä. Tähän kysymykseen saatiin tieteellisesti luotettava vastaus, joka oli ennakolta odotettu. Jatkuvalla tietojenkalastelusimulaatiolla todettiin olevan suuri vaikutus yrityksen työntekijöiden kykyyn tunnistaa haitallisia sähköposteja. Jo tutkielman lyhyen, neljän kuukauden mittaisen, ajanjakson aikana riski haitallisen kalasteluviestin avaamiseen pieneni huomattavasti. Tässä tutkielmassa saatiin siis vahva näyttö siitä, että näiden muuttujien välillä on riippuvuutta.

Henkilöiden sähköpostiin tulevat haitalliset linkit voivat olla vaikeasti havaittavissa monestakin eri syystä. Näin voi olla esimerkiksi silloin, jos viesti tulee “tutulta” taholta. Tutkielmassa näyttöä saatiin siitä, että koulutuksen jatkuessa kyky tunnistaa kalasteluviestejä paranee. Tässä tutkielmassa otos oli sellainen, että viimeisten kolmen tehtävän kohdalla tulokset eivät tuota relevanttia tietoa. Tehtävässä 15 epäonnistumisprosentti oli vain 1,4 %. Luku on niin alhainen, että oletettavasti jo 15 tehtävää riittäisi varsin hyvin varmistamaan henkilökunnan kyvyn tunnistaa kalasteluviestejä.

Monissa yrityksissä työntekijät saavat valtavan määrän sähköposteja. Se, miten niihin reagoidaan, vaihtelee. Työntekijän olisi löydettävä tärkeimmät ja toimintaa vaativat viestit muiden joukosta ja toisaalta esimerkiksi kalasteluviestejä pitäisi osata välttää.

Tässä erottelussa vaikuttavat monet arkiset tekijät, kuten väsymys. Päivän lopuksi ei ehkä erota sähköpostien virrasta vaarallisia viestejä yhtä hyvin kuin pirteänä.

Koulutuksen tuottajan kannalta linkin avaaminen ei ole pelkästään huono asia. Jos kyseessä on simuloitu viesti, sen avaamisesta ei synny haittaa. Sen sijaan, mikäli viestin vastaanottaja klikkaa linkkiä, hänet ohjataan sivulle, jossa kerrotaan, että kyse oli simulaatiosta. Näin henkilöllä on tilaisuus oppia paremmin tunnistamaan kalasteluviestejä.

Tässä tutkielmassa koulutusjakso oli neljän kuukauden mittainen. Simuloituja viestejä lähetettiin noin viikon välein. Jatkotutkimus voisi selvittää eripituisten koulutusjaksojen toimivuutta. Onko viikon välein tuleva viesti optimaalinen? Entä jos viestejä lähetettäisiinkin vain kerran kuussa esimerkiksi vuoden ajan? Miten se muuttaisi tuloksia? Olisi myös kiinnostava tutkia sitä, miten pitkään saavutettu hyöty säilyy ja kuinka usein koulutusjakso olisi syytä tarjota työntekijöille. Todennäköistä on, että asian jatkuva esillä pitäminen on välttämätöntä hyvän tietoturvan saavuttamiseksi.

Tutkielman asetelmassa alku- ja lopputestin välillä tehtiin interventio, jonka vaikuttavuutta tutkittiin. Kun on kysymys tällaisesta asetelmasta, on syytä pohtia mahdollisia väliin tulevia muuttujia. Onko jokin muu asia kuin koulutus voinut vaikuttaa lopputulokseen? Tällainen väliin tuleva muuttaja voisi olla esimerkiksi tutkitun ajanjakson aikana käyty julkinen keskustelu. Tutkielman otos oli kuitenkin niin laaja, että tämäntapaiset väliin tulevat muuttujat tuskin vaikuttavat lopputulokseen.

Otoksen suuruus, yli 36000 henkilöä, paljastaa sen, että tutkittava yritys on iso. Kun Asiakasyritys Y oli tehnyt päätöksen hankkia tietoturvakoulutusta Yritys X:ltä, lähetettiin kaikille työntekijöille alkutesti. Sen jälkeen työntekijöillä oli mahdollisuus osallistua koulutukseen tai jättää osallistumatta. Tässä tutkielmassa huomiota herättää se, että 36444 henkilöstä vain 2956 halusi osallistua koulutukseen. Jatkossa olisi mielenkiintoista tietää, miksi koulutukseen mukaan lähti niin pieni ryhmä ja millaiset henkilöt valikoituvat koulutukseen. Oliko heillä hyvät valmiudet jo alussa vai kokivatko he taitonsa puutteellisiksi ja osallistuivat sen vuoksi koulutukseen. Tätä voisi jatkotutkimuksissa selvittää.

Koulutuksen aikana Asiakasyrityksen Y työntekijät saivat sähköpostiinsa vaihtelevan määrän simuloituja tietojenkalasteluviestejä. Simuloinnissa voidaan käyttää hyvin

erilaisia tehtäviä. Niiden sisältö ja vaikeustaso vaihtelivat myös tutkitun koulutuksen aikana. Tässä tutkielmassa ei selvitetty viestien sisältöä millään tavalla. Jatkotutkimuksen kannalta voisi olla mielenkiintoista selvittää millaisia reaktioita erityyppiset viestit saavat vastaanottajissa aikaan. Erityisesti se, millaiset viestit ovat kaikkein vaikeimmin havaittavia, olisi tärkeätä tietää. Mahdollisimman monipuolisten tehtävätyyppien käyttäminen tuottaa todennäköisesti koulutukselle parhaan mahdollisen vaikuttavuuden.

Tutkittaessa tietoturvakoulutusta asiakaskunta voitaisiin jakaa pienempiin osiin. Tässä tutkielmassa ei otettu huomioon työntekijöiden aikaisempaa osaamistasoa, työtehtävää tai esimerkiksi kansallisuutta. Myös yrityksen toimiala ja koko voisi olla validi tutkimuskohde tämän aiheen kannalta. Tämä onkin ehdotus jatkotutkimusta ajatellen.

Pienet ja keskisuuret yritykset ovat tietoturvan osalta heikommassa tilanteessa, ja usein vailla tarvittavaa osaamista. Tietojenkalastelusimulaatio on näille yrityksille relevantti koulutuksen kohde, mutta usein havaitut haavoittuvuudet ovat laajemman tietoturvan kannalta niin vakavia, että resurssien käyttämien niihin on perusteltavaa ja jopa suositeltavaa. Suuret yritykset ovat pääosin pystyneet rakentamaan tietoturvaratkaisut tavalla, joka mahdollistaa investointien lisäämisen koulutukseen. Usein suuret yritykset ovat myös havainneet riskit tietojenkalastelun osalta, ja ovat halukkaita panostamaan sen puolen kehittämiseen. Erittäin suuret yritykset ovat usein jo ottaneet seuraavan askeleen tietojenkalastelun estämiseksi, ja näyttävät sitä kautta esimerkkiä. Toisaalta on todettava, että mitä suurempi yritys, sen suurempi on myös todennäköisyys joutua tietojenkalasteluhyökkäyksen uhriksi. Myös kohdistetut tietojenkalasteluyritykset ovat yleisempiä näissä organisaatioissa.

Tulevaisuudessakin yrityksillä on monenlaisia tietoturvaan liittyviä haasteita. Tietojenkalastelu on yksi niistä. Kalastelua käytetään, kun halutaan päästä käsiksi johonkin arkaluontoiseen. Tietojenkalastelun haittojen minimoimiseksi voidaan muun muassa henkilökunnalle tarjota koulutusta. Tietoturva-aukkojen löytäminen on työläämpi tapa. Hyvin toimiva tietoturvakulttuuri tekee työntekijälle helpoksi uhasta ilmoittamisen. Uhasta voi ilmoittaa napilla. Sen jälkeen varoitetaan ja reagoidaan.

Yritysten on pakko seurata tarkasti tietoturvaan liittyviä riskejä ja uhkia. Tietoturvasta huolehtiminen vaatii asian jatkuvaa esillä pitämistä. Tekniset ratkaisut, joita tietoturvasta huolehtimisessa käytetään, kehittyvät. Se ei kuitenkaan riitä. Henkilökunnan on oltava tietoisia riskeistä ja uhista. Heidän täytyy toimia vastuullisesti. Tämä vaatii uusien

työntekijöiden huolellista perehdyttämistä ja vanhojen työntekijöiden osaamisen päivittämistä. Tulevaisuudessa tarvitaan monenlaista tietoturvakoulutusta. Tietoturvakoulutuksen osalta voidaan sanoa, että luokkahuoneopetus ei toimi parhaalla mahdollisella tavalla. Onneksi on muitakin mahdollisuuksia.

Tässä tutkielmassa ei pohdittu yritysten tietoturvakouluksiin liittyviä haasteita. Niiden osalta on todettava, että jatkotutkimukset voisivat olla tarpeen. Eräs tällainen haaste tuli vastaan tätä tutkielmaa tehdessä. Koulutukseen mukaan lähteminen oli vapaaehtoista. Tämän tutkielman aineistosta voitiin nähdä, että vain hyvin pieni joukko yrityksen koko henkilökunnasta tarttui tähän mahdollisuuteen. Eräänä mahdollisena selityksenä voisi pitää tiedonkulun ongelmia. On mahdollista, että viesti tästä koulutuksesta ei tavoittanut kaikkia työntekijöitä riittävän tehokkaasti.

Koulutuksen järjestäminen työntekijöille lähtee yrityksen tarpeista. Yrityksellä on tavoite, mihin koulutuksen avulla halutaan päästä. Se jälkeen yrityksessä pohditaan, millä resursseilla koulutus järjestetään ja mitä toimenpiteitä tehdään. Joskus näiden pohdintojen seurauksena syntyy jonkinlainen muutos yrityksen tietoturvakulttuurissa.

Yritys X:n kannattaa pohtia, tuottaako heidän palvelunsa sen tuotoksen, jota varten se on olemassa. Millaisia vaikutuksia toiminnalla on asiakasyrityksen kannalta ja syntyykö välittömistä tuloksista pitkäkestoista vaikutusta? Vaikuttavuuden arvioinnissa verrataan lopputilannetta alkutilanteeseen. On syytä miettiä, keiden osalta interventio oli vaikuttava, millä lailla ja miksi. Vaikuttavuus saavutetaan tässä tutkielmassa koulutuksen avulla ja koulutus synnyttää muutoksen tietoturvallisuuden osaamisessa. Vaikuttavuutta on tässä tapauksessa mahdollista mitata yksinkertaisin keinoin.

Tässä tutkielmassa saaduilla tuloksilla on merkitystä käytännössä. Jokainen yritys kohtaa riskejä tietojenkalastelun myötä. Näitä riskejä voidaan tämän tutkielman johtopäätösten mukaan helposti hallita ja pienentää jatkuvan simuloidun tietojenkalastelukoulutuksen avulla. Yrityksen tietoturvan kannalta vaikuttaa sitä, että koulutukseen investoiminen kannattaa. Koulutuksella saatava hyöty on huomattava. Kyky tunnistaa sähköpostin kautta tulevia haitallisia tietojenkalasteluviestejä paranee paljon jo lyhyelläkin ajanjaksolla.

LÄHDELUETTELO

Alaskar, Mohamed, Shahper Vodanovich & Kathy Ning Shen (2015). Evolvement of information security research on employees' behavior: A systematic review and future direction. *Proceedings of the Annual Hawaii International Conference on System Sciences* 2015, 4241-4250. Saatavissa: doi:10.1109/HICSS.2015.508.

Almomani, Ammar, B. B. Gupta, Samer Atawneh, A. Meulenberg & Eman Almomani (2013). A Survey of Phishing Email Filtering Techniques. *IEEE Communications Surveys & Tutorials* 15:4, 2070-2090. Saatavissa: doi: 10.1109/SURV.2013.030713.00020.

Bannert, Maria (2002). Managing Cognitive Load—recent Trends in Cognitive Load Theory. *Learning and Instruction* 12:1, 139-146. Saatavissa: doi: 10.1016/S0959-4752(01)00021-4.

Chaudhary, Sunil (2016). *The Use of Usable Security and Security Education to Fight Phishing Attacks.* Tampereen yliopisto. Tietojenkäsittelyoppi. Akateeminen väitöskirja. Tampere. Saatavissa: http://urn.fi/URN:ISBN:978-952-03-0292-4.

Chaudhry, Junaid Ahsenali, Shafique Ahmad Chaudhry & Robert G. Rittenhouse. Phishing Attacks and Defenses. *International Journal of Security and Its Applications* 10:1, 247-256. Saatavissa: doi: 10.14257/ijsia.2016.10.1.23.

Colwill, Carl (2009). Human factors in information security: The insider threat – Who can you trust these days?. *Information Security Technical Report* 14:4, 186-196. Saatavissa: doi: 10.1016/j.istr.2010.04.004.

Computer Security Institute (2009). CSI Computer Crime and Security Survey - Executive Summary [Viitattu 21.4.2020]. Saatavissa: http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf.

Computer Weekly (2019). *Almost half UK firms hit by phishing attacks.* Computer Weekly: Warcik Ashford [Viitattu 20.4.2020]. Saatavissa:

https://www.computerweekly.com/news/252459363/Almost-half-UK-firms-hit-by-phishing-attacks.

Cox, Andrew, Sarah Connolly & James Currall (2001). Raising Information Security Awareness in the Academic Setting. *VINE* 31:2, 11-16. Saatavissa: doi:10.1108/03055720010803961.

Danielsson, Petri (2019). Rikollisuustilanne 2018: Rikollisuuskehitys tilastojen ja tutkimusten valossa. *Katsauksia, no. 36/2019*. Helsingin yliopisto, kriminologian ja oikeuspolitiikan instituutti. Helsinki. ISSN 2342-7779. Saatavissa: http://urn.fi/URN:ISBN:978-951-51-0667-4.

Downs, Julie, Mandy Holbrook & Lorrie Cranor (2007). *Behavioral response to phishing risk*. Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, 37-44. Saatavissa: doi: 10.1145/1299015.1299019.

Gragg, David (2003). *A Multi-Level Defense Against Social Engineering*. SANS Institute: Information Security Reading Room [Viitattu 22.4.202]. Saatavissa: https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920.

Hadnagy, Christopher & Michele Fincher (2015). *Phishing Dark Waters. The Offence and Defensive Sides of Malicious E-mails.* Indianapolis: John Wiley & Sons, Inc.. ISBN 978-1-118-95847-6.

Hakala, Mika, Mika Vainio & Olli Vuorinen (2006). *Tietoturvallisuuden käsikirja.* Jyväskylä: Dodenco. ISBN 951-846-273-9.

Harrison, Brynne, Elena Svetieva & Arun Vishwanath (2016). Individual Processing of Phishing Emails: How Attention and Elaboration Protect against Phishing. *Online Information Review* 40:2, 265-281. Saatavissa: doi:10.1108/OIR-04-2015-0106.

Heartfield, Ryan & George Loukas (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computer Surveys* 48:3, 1-39. Saatavissa: doi: 10.1145/2835375.

Heikkilä, Tarja (2014). *Tilastollinen tutkimus*. Helsinki: Edita Publishing Oy, 2014. ISBN 9789513769420. Saatavissa: http://www.tilastollinentutkimus.fi/index.html.

Helsingin seudun kauppakamari, Helsingin kamari, Juha-Matti Heljaste, Jari Korkiamäki, Heljo Laukkala, Juha Mustonen, Jere Peltonen, Panu Vesterinen & Esa Nurminen (2008). *Yrityksen Turvallisuusopas*. Helsinki: Helsingin seudun kauppakamari. ISBN 978-952-99823-6-3.

Herath, Tejaswini & H.R. Rao (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47:2, 154-165. ISSN 0167-9236. Saatavissa: doi:10.1016/j.dss.2009.02.005.

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

Hong, Jason (2012). The State of Phishing Attacks. *Communications of the ACM* 55:1, 74-81. Saatavissa: doi:10.1145/2063176.2063197.

Hu, Qing, Tamara Dinev, Paul Hart & Donna Cooke (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences* 43:4, 615-660. Saatavissa: doi:10.1111/j.1540-5915.2012.00361.x.

Il-kwon, Lim, Young-Gil Park & Jae-Kwang Lee (2016). Design of Security Training System for Individual Users. *Wireless Personal Communications* 90:3, 1105-1120. ISSN 1572-834X. Saatavissa: doi: 10.1007/s11277-016-3380-z.

Information Age (2019). *Phishing attacks hook almost half of UK firms*. Information Age: Andrew Ross [Viitattu 20.4.2020]. Saatavissa: https://www.information-age.com/phishing-attacks-hook-almost-half-of-uk-firms-123480666/.

Jagatic, Tom, Nathaniel Johnson, Markus Jakobsson, Filippo Menczer (2007). Social phishing. *Communications of the ACM* 50:10, 94-100. Saatavissa: doi:10.1145/1290958.1290968.

Jansson, K. & R. Von Solms (2013). Phishing for Phishing Awareness. *Behaviour & Information Technology* 32:6, 584-593. Saatavissa: doi: 10.1080/0144929X.2011.632650.

Järvinen, Petteri (2018). *Kyberuhkia ja somesotaa. Digiaikana sinäkin olet etulinjassa.* Jyväskylä: Dodenco. ISBN 978-952-291-528-3.

Karjalainen, Mari (2011). *Improving employees' information systems (IS) security behavior : toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior*. Oulun yliopisto. Luonnontieteellinen tiedekunta. Akateeminen väitöskirja. Oulu. Saatavissa: http://urn.fi/urn:isbn:9789514295676.

Karjalainen, Mari & Mikko Siponen (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems* 12:8, 518-555. Saatavissa: doi: 10.17705/1jais.00274.

Kauppakamari (2017). *Yritysten rikosturvallisuus 2017: Riskit ja niiden hallinta.* Helsinki: Keskuskauppakamari [Viitattu 22.4.2020]. ISBN 978-952-5620-85-6. Saatavissa: https://kauppakamari.fi/wp-content/uploads/2017/10/yritysten-rikosturvallisuus-2017web.pdf.

Kauppakamari (2018a). *Yrityksiin kohdistuva rikollisuus jatkaa kasvuaan*. Helsinki: Keskuskauppakamari [Viitattu 23.4.2020]. Saatavissa. https://kauppakamari.fi/2018/04/23/yrityksiin-kohdistuva-rikollisuus-jatkaa-kasvuaan/.

Kauppakamari (2018b). *Sähköpostitunnukset vaarassa – varo uutta turvapostiviestiksi naamioitunutta huijausviestiä.* Helsinki: Keskuskauppakamari [Viitattu 22.4.2020]. Saatavissa. https://helsinki.chamber.fi/sahkopostitunnukset-vaarassa-varo-uutta-turvapostiviestiksi-naamioitunutta-huijausviestia/.

Kay, Russell (2004). *Sidebar: The Origins of Phishing*. Computerworld [Viitattu 24.4.2020]. Saatavissa: https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html.

Kinnunen, Nina (2015). *Tietoturvaohjeistuksen noudattamisen motivaatio ja sen muuttuminen.* Vaasan yliopisto. Teknillinen tiedekunta. Akateeminen väitöskirja. ISBN 978-952-476-637-1. Saatavissa: https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-637-1.pdf.

Ku, Cheng-Yuan, Yi-Wen Chang, & David C. Yen (2009. National Information Security Policy and Its Implementation: A Case Study in Taiwan. *Telecommunications Policy* 33:7, 371-384. Saatavissa: doi:10.1016/j.telpol.2009.03.002.

Kumaraguru, Ponnurangam, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Blair & Theodore Pham (2009). *School of Phish: A Real-world Evaluation of Anti-phishing Training*. SOUPS '09 Proceedings of the 5th Symposium on Usable Privacy and Security 3, 1-12. Saatavissa: doi: 10.1145/1572532.1572536.

Kyberturvallisuuskeskus (2017). *Näin meitä huijataan! Verkossa yleisesti tavattuja huijausmenetelmiä.* Helsinki: Viestintävirasto [Viitattu 22.4.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Nain_meita_huijataan.pdf.

Kyberturvallisuuskeskus (2018b). Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota!. Helsinki: Liikenne ja viestintäministeriö [Viitattu 22.4.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota.

Kyberturvallisuuskeskus (2020a). *Kyberturvallisuus ja yrityksen hallituksen vastuu* [Verkkodokumentti]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyKyber_digiAUK_220120.pdf.

Kyberturvallisuuskeskus (2020b). *Toimi näin, jos havaitset tietoturvapoikkeaman.* Helsinki: Liikenne ja viestintäministeriö [Viitattu 22.4.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman.

Laaksonen, Mika, Terho Nevasalo & Karri Tomula (2006). *Yrityksen Tietoturvakäsikirja: Ohjeistus, Toteutus Ja Lainsäädäntö.* Helsinki: Edita. ISBN 951-37-4701-8.

Leppänen, Juha (2006). *Yritysturvallisuus Käytännössä: Turvallisuusjohtamisen Portfolio*. Helsinki: Talentum. ISBN 952-14-0887-1.

Li, Ying (2015). *Users' information systems (IS) security behavior in different contexts.* Oulun yliopisto. Tieto- ja sähkötekniikan tiedekunta. Akateeminen väitöskirja. Oulu. Saatavissa: http://urn.fi/urn:isbn:9789526209395.

Liang, Huigang & Yajiong Xue (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective*. *Journal of the Association for Information Systems* 11:7, 394-413. ISSN 1536-9323. Saatavissa: doi: 10.17705/1jais.00232.

Limnéll, Jarno, Majewski Klaus & Salminen Mirva (2014). *Kyberturvallisuus.* Jyväskylä: Dodenco. ISBN 978-952-291-047-9.

Moody, Gregory (2011*). A multi-theoretical perspective on IS security behaviors.* Oulun yliopisto. Luonnontieteellinen tiedekunta. Akateeminen väitöskirja. Oulu. Saatavissa: http://urn.fi/urn:isbn:9789514295614.

Myyry, Liisa, Mikko Siponen, Seppo Pahnila, Tero Vartiainen & Anthony Vance (2009). What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. *European Journal of Information Systems: Special Issue: Behavioral and Policy Issues in Information Systems Security* 18:2, 126-139. Saatavissa: doi:10.1057/ejis.2009.10.

Niermeyer, Rainer & Manuel Seyffert (2004). *Motivaatio*. Helsinki: Rastor Oy. ISBN 9789525024524.

Nurmi, Jari-Erik & Katariina Salmela-Aro (2005). Modernin motivaatiopsykologian perusta ja käsitteet. Teoksessa: *Mikä meitä liikuttaa*. Modernin motivaatiopsykologian perusteet, 10-27. Toim. Jari-Erik Nurmi. Keuruu: PS-Kustannus. ISBN 9789524510554.

Nuutila, Ari-Matti & Martti Majanen (2009). RL 36 Luku. Petos ja muu epärehellisyys. Teoksessa: *Rikosoikeus*, 973-1005. Toim. Tapio Lappi-Seppälä, Kaarlo Hakamies, Pekka Koskinen, Martti Majanen, Sakari Melander, Kimmo Nuotio, Ari-Matti Nuutila, Timo Ojala, ja Ilkka Rautio. Helsinki: WSOYpro. ISBN 978-951-0-33997-8.

Nykänen, Kari (2011). *Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen.* Oulun yliopisto. Luonnontieteellinen tiedekunta. Akateeminen väitöskirja. Oulu. Saatavissa: http://urn.fi/urn:isbn:9789514295713.

Ollmann, Gunter (2007). *The Phishing Guide Understanding & Preventing Phishing Attacks.* USA: IBM Global Technology Services [Viitattu 24.4.2020]. Saatavissa: https://www.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems.

Parmar, Bimal (2012). Protecting against Spear-phishing. *Computer Fraud & Security* 2012:1, 8-11. Saatavissa: doi 10.1016/S1361-3723(12)70007-6.

Pattinson, Malcolm, Cate Jerram, Kathryn Parsons, Agata McCormac & Marcus Butavicius. (2012). Why Do Some People Manage Phishing E-mails Better Than Others?. *Information Management & Computer Security* 20:1, 18-28. Saatavissa: doi:10.1108/09685221211219173.

Pollock, E., P. Chandler & J. Sweller (2002). Assimilating Complex Information. *Learning and Instruction* 12:1, 61-86. Saatavissa: doi: 0.1016/S0959-4752(01)00016-0.

Prem, Santi Priyanka & B. Indira Reddy (2019). Phishing and Anti-Phishing Techniques. *International Research Journal of Engineering and Technology* 6:7, 1446-1452. ISSN 2395-0056. Saatavissa: https://www.irjet.net/archives/V6/i7/IRJET-V6I7184.pdf.

Puhakainen, Petri (2006). *A design theory for information security awareness.* Oulun yliopisto. Luonnontieteellinen tiedekunta. Akateeminen väitöskirja. Oulu. Saatavissa: http://urn.fi/urn:isbn:9514281144.

Puolimatka, Tapio (2002). *Opetuksen teoria: Konstruktivismista realismiin*. Helsinki: Tammi. ISBN 951-26-4816-4.

Räikkönen, Iiro-Antti (2017). *Motivations behind employee information security behavior*. Jyväskylän yliopisto. Tietojenkäsittelytieteen laitos. Pro-gradu -tutkielma. Saatavissa: http://urn.fi/URN:NBN:fi:jyu-201708313625.

Rikoslaki 19.12.1889/36.

Rikoslaki 19.12.1889/38.

Rikoslaki 19.12.1889/39.

Robila, Stefan A. & James W. Ragucci (2006). Don't be a phish: Steps in user education. *ACM SIGCSE Bulletin* 38:32, 237-241. Saatavissa: doi: 10.1145/1140123.1140187.

Roy Sarkar, Kuheli (2010). Assessing insider threats to information security using technical, behavioural and organizational measures. *Information Security Technical Report* 15:3, 112–133. Saatavissa: doi:10.1016/j.istr.2010.11.002.

Ruohotie, Pekka (1998). *Motivaatio, Tahto Ja Oppiminen*. Helsinki: Edita. ISBN 951-37-2628-2.

Ryan, Richard & Edvard Deci (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology* 25:1, 54-67. Saatavissa: doi:10.1006/ceps.1999.1020.

Sanastokeskus (2015). *Tietoturva*. Saatavissa: http://www.tsk.fi/tsk/termitalkoot/fi/node/266.

Schimanke, Florian, Robert Mertens & Oliver Vornberger (2013). What to learn next? Content selection support in mobile game-based training. *Conference: E-LEARN World Conference on E-Learning* [Verkkodokumentti]. Saatavissa: https://www.researchgate.net/publication/261952026.

Sheng, Steve, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Cranor, Jason Hong & Elizabeth Nunge (2007). *Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish*. SOUPS ’07 Proceedings of the 3rd Symposium on Usable Privacy and Security, 88-99. Saatavissa: doi: 10.1145/1280680.1280692.

Siponen, Mikko (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* 8:1, 31-41. Saatavissa: doi:10.1108/09685220010371394.

Spears, Janine & Henri Barki (2010). User Participation in Information Systems Security Risk Management. *Management Information Systems* 34:3, 503-522. ISSN 0276-7783. Saatavissa: doi: 10.2307/25750689.

Speed, Tim, Darla Nykamp, Mari Heiser, Joseph Anderson & Jaya Nampalli (2014). Mobile Security: How to secure, privatize and recover your devices. *Network Security* 2014:4, 4. Saatavissa: doi:10.1016/S1353-4858(14)70017-0.

Stanton, Jeffrey, Katharyn Stam, Paul Mastrangelo & Jeffrey Jolton (2005). Analysis of end user security behaviors. *Computers & Security* 24:2, 124-133. Saatavissa: doi:10.1016/j.cose.2004.07.001.

Sumner, Alex & Xiaohong Yuan (2019). Mitigating Phishing Attacks: An Overview. *ACM SE '19: Proceedings of the 2019 ACM Southeast Conference* [Viitattu 22.4.2020], 72-77. Saatavissa: doi: 10.1145/3299815.3314437.

Thomson, Kerry-Lynn & Rossouw Von Solms (2005). Information Security Obedience: A Definition. *Computers & Security* 24:1, 69-75. Saatavissa: doi: 10.1016/j.cose.2004.10.005.

Tietotekniikan liitto & Ilmari Pietarinen (2008). *Atk-sanakirja: Tietotekniikan monikielinen hakuteos. 1, Termit, määritelmät ja vastineet eri kielillä*. 14. uud. p. Helsinki: Talentum. ISBN 978-952-14-1093-2.

Twitchell, Douglas (2006). Social Engineering in Information Assurance Curricula. *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security*

curriculum development [Viitattu 22.4.2020]. 191-193. ISBN 1595934375. Saatavissa: doi: 10.1145/1231047.1231062.

Tynjälä, Päivi (1999). Oppiminen tiedon rakentamisena: Konstruktivistisen oppimiskäsityksen perusteita. Helsinki: Kirjayhtymä. ISBN 951-26-4419-3.

Van Niekerk, J.F. & R. Von Solms (2010). Information security culture: A management perspective. *Computers & Security* 29:4, 476-486. Saatavissa: doi:10.1016/j.cose.2009.10.005.

Vartiainen, Matti & Kirsi Nurmela (2005). Tavoitteet ja tulkinnat – motivaatio ja palkitseminen työelämässä. Teoksessa: *Mikä meitä liikuttaa*. Modernin motivaatiopsykologian perusteet, 188-212. Toim. Jari-Erik Nurmi. Kuruu: PS-Kustannus. ISBN 9789524510554.

Vishwanath, Arun, Tejaswini Herath, Rui Chen, Jingguo Wang & H. Raghav Rao (2011). Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability Within an Integrated, Information Processing Model. *Decision Support Systems* 51:3, 576-586. Saatavissa: doi:10.1016/j.dss.2011.03.002.

Yleinen suomalainen asiasanasto (2019). Tietoturva. [viitattu 24.4.2020]. Saatavissa: http://www.yso.fi/onto/ysa/Y106522.

LIITE 1.

Wilcoxin testin tulokset

Nonparametric Tests

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between Alkutesti and Lopputesti equals 0.	Related-Samples Wilcoxon Signed Rank Test	,000	Reject the null hypothesis.

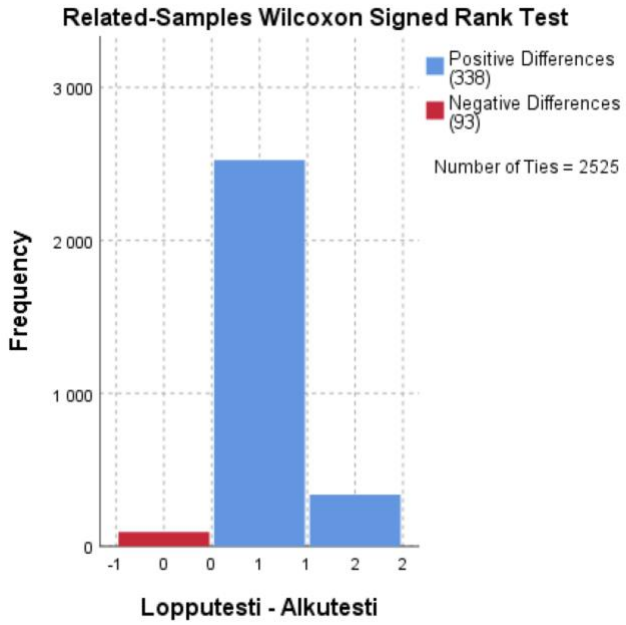
Asymptotic significances are displayed. The significance level is ,050.

Related-Samples Wilcoxon Signed Rank Test

Alkutesti, Lopputesti

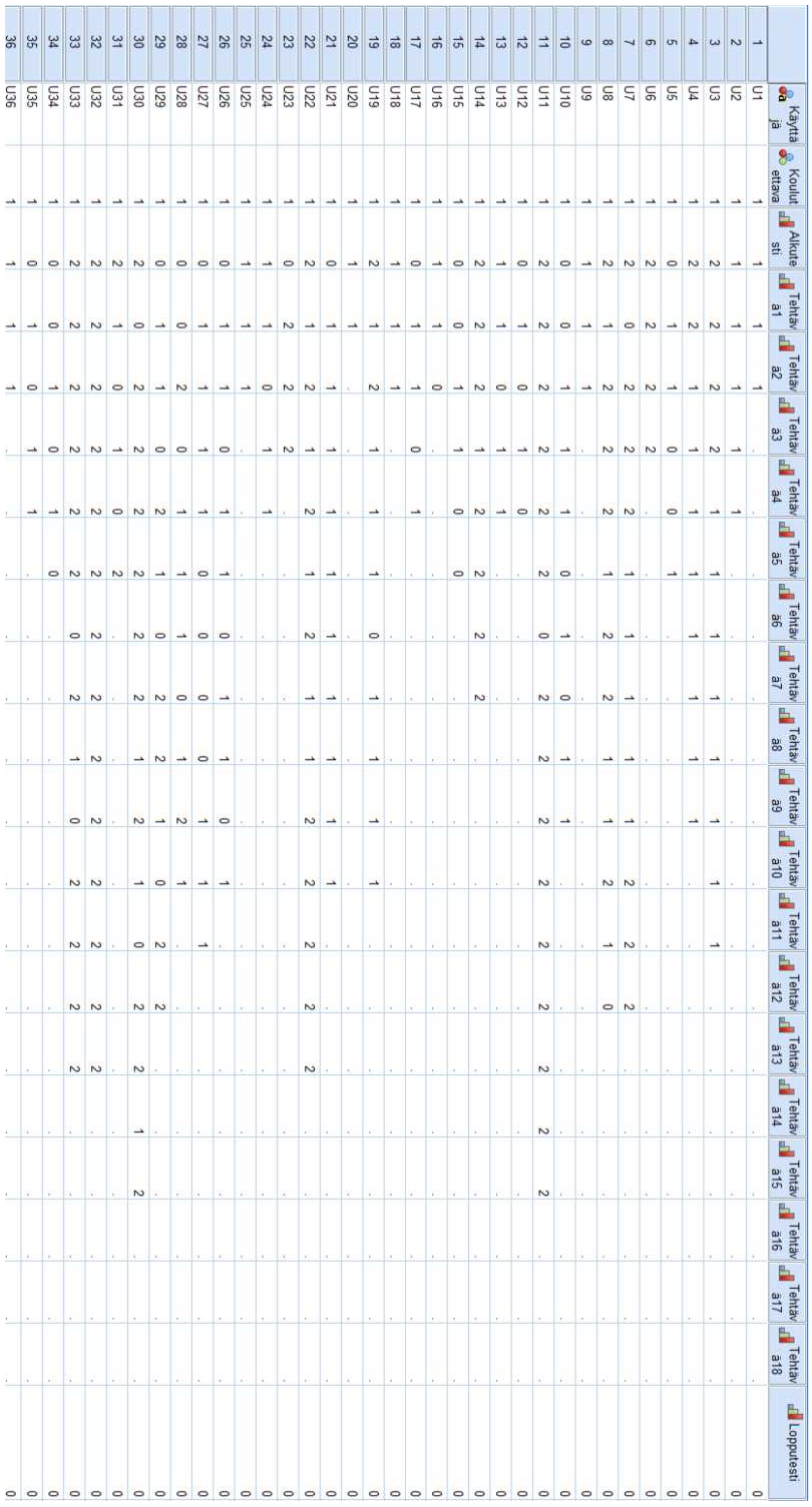
Related-Samples Wilcoxon Signed Rank Test Summary

Total N	2956
Test Statistic	73008,000
Standard Error	2242,138
Standardized Test Statistic	11,801
Asymptotic Sig.(2-sided test)	,000



LIITE 2.

Ote aineistosta



	Käyttäjä	Koulutettava	Alkutesti	Tehtävä1	Tehtävä2	Tehtävä3	Tehtävä4	Tehtävä5	Tehtävä6	Tehtävä7	Tehtävä8	Tehtävä9	Tehtävä10	Tehtävä11	Tehtävä12	Tehtävä13	Tehtävä14	Tehtävä15	Tehtävä16	Tehtävä17	Tehtävä18	Lopputesti
1	U1	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
2	U2	1	1	1	1	1	1	.	.	.	.	.	1	.	.	.	.	.	.	.	.	0
3	U3	1	2	2	2	2	1	1	1	1	1	1	.	1	.	.	.	.	.	.	.	0
4	U4	1	2	2	1	1	1	1	1	1	1	1	.	.	.	.	.	.	.	.	.	0
5	U5	1	0	1	1	0	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	0
6	U6	1	2	2	2	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
7	U7	1	2	0	2	2	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
8	U8	1	2	1	2	2	2	1	2	2	1	1	2	1	0	.	.	.	.	.	.	0
9	U9	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
10	U10	1	0	1	1	1	1	0	1	0	1	1	.	.	.	.	.	.	.	.	.	0
11	U11	1	2	2	2	2	2	2	0	2	2	2	2	2	.	.	.	2	.	.	.	0
12	U12	1	0	1	0	1	0	.	.	.	.	.	.	.	.	.	.	.	2	.	.	0
13	U13	1	1	1	0	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
14	U14	1	2	2	2	1	2	2	2	2	.	.	.	.	.	.	.	.	.	.	.	0
15	U15	1	0	0	1	1	0	0	.	.	.	.	.	.	.	.	.	.	.	.	.	0
16	U16	1	1	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
17	U17	1	0	1	1	0	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
18	U18	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
19	U19	1	2	1	2	1	1	1	0	1	1	1	1	.	.	.	.	.	.	.	.	0
20	U20	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
21	U21	1	0	1	1	1	1	1	1	1	1	1	1	.	.	.	.	.	.	.	.	0
22	U22	1	2	1	2	1	2	1	2	1	1	2	2	2	.	.	.	.	.	.	.	0
23	U23	1	0	2	2	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
24	U24	1	1	1	0	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
25	U25	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
26	U26	1	0	1	1	0	.	.	0	1	1	0	1	.	.	.	.	.	.	.	.	0
27	U27	1	0	1	1	1	1	0	0	0	1	1	1	1	.	.	.	.	.	.	.	0
28	U28	1	0	0	2	0	1	1	1	0	1	2	1	.	.	.	.	.	.	.	.	0
29	U29	1	0	1	1	0	2	1	0	2	2	1	0	2	2	.	.	.	.	.	.	0
30	U30	1	2	0	2	2	2	2	2	2	1	2	1	0	2	.	.	1	.	.	.	0
31	U31	1	2	1	0	1	0	2	.	.	.	.	.	.	.	.	.	.	.	.	.	0
32	U32	1	2	2	2	2	2	2	2	2	2	2	2	2	2	.	.	.	.	.	.	0
33	U33	1	2	2	2	2	2	2	2	2	1	0	2	2	2	.	.	.	.	.	.	0
34	U34	1	0	0	1	0	1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	0
35	U35	1	0	1	0	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0
36	U36	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	0