Niko Häkkinen

KOHDISTETTU HUIJAUSSÄHKÖPOSTI ORGANISAATIOIDEN TIETOTURVAUHKANA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Häkkinen, Niko
Kohdistettu Huijaussähköposti Organisaatioiden Tietoturvauhkana
Jyväskylä: Jyväskylän yliopisto, 2017, 51 s.
Tietojärjestelmätiede, Pro gradu-tutkielma
Ohjaaja(t): Siponen, Mikko

Tässä pro-gradu tutkielmassa käsitellään kohdistettua huijaussähköpostia organisaation tietoturvauhkana käyttäjien toiminnan näkökulmasta. Tutkielmassa kartoitettiin, mitkä tekijät ovat yhteydessä kohdistetulla huijaussähköpostilla huijatuksi tulemiseen. Tarkastelun kohteina olivat paitsi viestin ominaisuudet myös erilaiset yksilön ominaisuudet, kuten käyttäjän tietoisuus tietoturvariskeistä. Tutkielman aihe on tärkeä, koska organisaatiot ovat yhä riippuvaisempia tietojärjestelmien toiminnasta ja niissä olevista tiedoista. Kohdistetuista huijaussähköposteista voi aiheutua merkittäviä vahinkoja organisaatioille, ja mahdollisuus vahingoille on kasvanut viime vuosien aikana, kun teknologia ja hyökkäystekniikat ovat kehittyneet. Tutkimuksen otos koostui kolmestakymmenestä pankki- ja vakuutusalan organisaatioissa työskentelevästä henkilöstä.

Organisaation tietoturvan näkökulmasta kohdistettu huijaussähköposti (engl. spear phishing) on yksi haastavimmista tietoturvauhista. Teknisellä analyysillä pystytään suodattamaan yksinkertaiset huijaussähköpostit, mutta kohdistettuihin huijaussähköposteihin tekniset ratkaisut toimivat heikosti. Sillä viestin sisältö on personoitu nimenomaiselle sähköpostin vastaanottajalle, eivätkä viestit erotu selkeästi normaalista sähköpostiviestinnästä.

Tässä tutkielmassa muodostettiin lineaarisella regressioanalyysillä malli, joka selitti kohdistetulla huijaussähköpostilla huijatuksi tulemisen todennäköisyyttä. Tämä tutkimus osoitti, että sekä viestiin liittyvillä ominaisuuksilla, että yksilön ominaisuuksilla on yhteyttä huijatuksi tulemiseen kohdistetulla huijaussähköpostilla. Tutkimuksen mukaan, mitä mieluisammaksi tietotekniikan käyttö koettiin, sitä epätodennäköisemmin tuli huijatuksi kohdistetulla huijaussähköpostilla. Lisäksi korkea tietoisuus tietoturvan riskeistä yritykselle näyttäisi ehkäisevän huijatuksi tulemista. Toisaalta viestin ominaisuuksien hyväksi arvioitu luotettavuus ennakoi huijatuksi tulemista kohdistetulla huijaussähköpostilla. Tietoturvan teknisten suojamekanismien ohella käyttäjien koulutus ja asennekasvatus ovat keskeisiä keinoja organisaation tietoturvan kehittämisessä.

Asiasanat: kohdistettu huijaussähköposti, spear phishing, organisaation tietoturva.

ABSTRACT

Häkkinen, Niko
Spear phishing as a threat for organizations' IT security
Jyväskylä: University of Jyväskylä, 2017, 51 p.
Information Systems Science, Master's Thesis
Supervisor(s): Siponen, Mikko

The aim of this study was to shed light on spear phishing as a threat for organizations' IT security from a user action point of view. This study examined which factors associate with the probability to fall for spear phishing email. The focus was both on email qualities and on individual factors such as awareness of IT security risks. This topic is important because organizations are increasingly dependent on availability of IT systems and information those contain. Spear phishing may cause remarkable damages to organizations and the probability of damages has increased during last years as technology and attack techniques have developed. The sample consisted of 30 employees working in banking and insurance sector.

Spear phishing is one of the most challenging security threat for organization IT security point of view. Technical filters can defend against simple phishing emails but spear phishing emails are less likely to be detected with technical solutions. Because spear phishing emails are crafted for certain receiver those are hard to point out from normal email flows.

Linear regression analysis showed that email qualities and individual factors predicted statistically significantly the probability to fraud with spear phishing email. The results indicated that that persons who feel pleasant to use information technology were less likely to be fraud with spear phishing email. In addition, knowledge of IT security risks for organization seems prevent probability to be fraud. However, email's features, high reliability seems to be associated with the probability to fall for spear phishing email. There is two key findings based on this study which helps organizations to concentrate resources for developing IT security. In addition to technical IT security, it is important to put effort on user's general IT and attitudinal education.

Keywords: spear phishing, organization IT-security.

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tässä luvussa esitellään tutkimuksen taustaa, tutkimuksen toteutusta ja tutkimusongelmaa. Tutkimuksen taustalla on ollut tietoturvan merkityksen nousu digitalisoituneessa yhteiskunnassa ja tietoturvan kasvavat riskit eri organisaatioille. Taustan lisäksi esitellään tutkimuksen toteutusta ja tutkimusongelmaa.

1.1 Tutkimuksen tausta

Organisaatiot joutuvat kohtaamaan monimuotoisia tietoturvauhkia, joilla voi olla merkittäviä vaikutuksia liiketoimintaan sekä organisaation maineeseen. Tietoturva ei ole vain teknisiä ratkaisuja, vaan yksittäisten käyttäjien rooli tietoturvassa on entisestään korostunut viime vuosina. Yksittäiset käyttäjät organisaatiossa ovat mahdollisia väyliä tietojärjestelmiin (pahantahtoisten) hyökkääjien näkökulmasta. Sähköpostin yleinen käyttö organisaatioissa on mahdollistanut erilaisten huijaussähköpostien (engl. phishing) hyväksikäyttämisen hyökkääjien toimesta.

Organisaation tietoturvan näkökulmasta kohdistettu huijaussähköposti (engl. spear phishing) on yksi haastavimmista tietoturvauhista. Teknisellä analyysillä pystytään suodattamaan yksinkertaiset huijaussähköpostit, mutta kohdistettuihin huijaussähköposteihin tekniset ratkaisut toimivat heikosti, koska viestin sisältö on personoitu nimenomaiselle sähköpostin vastaanottajalle. Tarkoituksena on saada vastaanottaja, eli uhri, seuraamaan mahdollista Internet-linkkiä tai avaamaan liitetiedosto, jonka seurauksena pyritään saamaan tietoja tai pääsy tietojärjestelmään. Kohdistetuissa huijaussähköposteissa käytetään pääsääntöisesti joko entuudestaan tuntemattomia, ns. nollapäivähaavoittuvuuksia (engl. zero-day vulnerability), jolloin käyttäjä voi yhdelläkin väärällä toimella päästää hyökkääjän käsiksi järjestelmäänsä, tai tunnettuja haavoittuvuuksia, jolloin käyttäjää pyritään viestissä saamaan kiertämään tekniset turvamekanismit.

Kohdistettujen huijaussähköpostien tunnistaminen on lähes kokonaan yksittäisen käyttäjän vastuulla, koska useinkaan organisaatioiden automaattiset sähköpostisuodattimet eivät voi erottaa kohdistettua huijaussähköpostia normaaleista sähköposteista.

Kohdistetuista huijaussähköposteista voi aiheutua merkittäviä vahinkoja organisaatioille, ja mahdollisuus vahingoille on kasvanut viime vuosien aikana, kun teknologia ja hyökkäystekniikat ovat kehittyneet. Monissa organisaatioissa käsitellään arkaluonteisia tietoja, joiden avulla rikollisten on mahdollista hyötyä. Teollisuusvakoilun lisäksi organisaatiot kohtaavat nykyään myös vahingoittamistarkoituksessa tehtyjä verkkohyökkäyksiä ja esimerkiksi kiristystilanteita, joissa yritykseltä vaaditaan rahaa verkkohyökkäyksen lopettamiseksi tai tietojen palauttamiseksi. Tässä tutkimuksessa esitetään yksi esimerkki kohdistetun huijaussähköpostin avulla aloitetusta verkkohyökkäyksestä, jonka yhteydessä varastettiin yrityksen liiketoiminnan kannalta keskeisiä tietoja.

Kohdistettuihin huijaussähköposteihin on tieteellisissä tutkimuksissa perehdytty suhteellisen vähän varsinkaan käyttäjälähtöisestä näkökulmasta. Monet tutkimukset, jotka esitellään kirjallisuuskatsauksessa, pohjautuvat hyviin menetelmiin, mutta otannat ovat usein olleet yliopisto-opiskelijoita tai yliopiston henkilökuntaa ja joissain tapauksissa vielä tietotekniikkaa vähintään sivuaineena opiskelevia, jolloin tuloksista on haastava vetää yleisiä johtopäätelmiä.

1.2 Tutkimus

Tutkimus toteutettiin kirjallisuuskatsaukseen perustuvana empiirisenä tutkimuksena, jossa kyselylomakkeella kartoitettiin tutkittavien reagointiaikomuksia ja tulkintoja esitettyihin sähköpostiviesteihin ja lisäksi tiedusteltiin käsityksiä tietoturvan riskeistä organisaatioille. Tutkittavat rekrytoitiin pankki- ja vakuutusalan työntekijöistä, koska tällä alalla työskentelee paljon ns. tietotyöläisiä, eli henkilöitä, joiden pääasiallinen työ koostuu tietokoneella tehdystä työstä, ja jotka käyttävät päivittäin paljon sähköpostia ja ovat näin ollen erityisen alttiita kohdistetuille huijaussähköposteille. Tutkittavat otettiin samalta toimialalta, jotta tutkimuksessa käytetty kohdistettu huijaussähköposti esimerkki olisi mahdollisimman relevantti kaikille tutkittaville. Tämän tutkimuksen tarkoitus on kartoittaa millaiset tekijät selittävät kohdistettuun huijaussähköpostiin reagoimista ja millaisiin elementteihin käyttäjien huomio kiinnittyy kohdistetuissa huijaussähköposteissa.

Lisäksi tässä tutkimuksessa on tarkoitus selvittää käyttäjien mahdollisten taustatekijöiden, esimerkiksi koetun osaamisen ja koetun mieluisuuden, vaikutusta huijatuksi tulemiseen. Kuten tämän tutkielman kirjallisuuskatsauksessa todetaan, työntekijät ovat keskeinen osa organisaatioiden tietoturvaa ja siksi tässä tutkimuksessa on tarkoitus selvittää huijaussähköpostien lisäksi vastaajien, jotka

olivat kaikki työntekijöitä, tietoisuutta sähköpostin aiheuttamista riskeistä työnantajaa kohtaan.

1.3 Tutkimusongelma

Tässä tutkimuksessa pyrittiin vastaamaan tutkimuskysymykseen:

- Mitkä tekijät ovat yhteydessä todennäköisyyteen tulla huijatuksi kohdistetulla huijausviestillä?

Aiempaan tutkimukseen ja teoriaan perustuen organisaation henkilöstö on tietoturvan kannalta yksi keskeisimmistä osa-alueista, ja henkilöstön sähköposti on yksi hyökkäyskanava, joka kohdistuu organisaation. Tutkimuksen on tarkoitus tuottaa lisätietoa kohdistettuun huijaukseen vaikuttavasti käyttäjien taustatekijöistä, jotta organisaatiot voisivat panostaa oikeisiin toimiin sähköpostin tietoturvan parantamiseksi. Tämän tutkimuksen lähtökohtana on käyttäytymistieteellinen lähestyminen, eli tutkimuksessa ei perehdytä teknisiin kohdistettujen huijaussähköpostien yksityiskohtiin vaan käyttäjien kokemuksiin ja aikomuksiin huijaustilanteessa. Aikaisempiin tutkimuksiin pohjautuen tutkittaville esitettiin väittämiä esitettyjen sähköpostiviestien ominaisuuksista ja tietoturvan riskeistä organisaatiolle. Tuloksia analysoitiin tilastomenetelmillä eri tekijöiden välisten yhteyksien kartoittamiseksi.

2 KIRJALLISUUSKATSAUS

Tässä kirjallisuuskatsauksessa tarkastellaan ensin organisaatioiden tietojärjestelmien turvallisuutta erityisesti organisaation henkilöstön, eli käyttäjien, toiminnan näkökulmasta. Seuraavaksi tarkastellaan verkkohuijauksiin ja huijaussähköposteihin liittyvää tutkimusta. Lopuksi esitetään esimerkkitapaus, joka yhdistää tässä kirjallisuuskatsauksessa esitetyt teemat.

2.1 Työntekijät osana organisaatioiden tietoturvaa

Tietoyhteiskunnassa toimivat organisaatiot ovat riippuvaisempia tietojärjestelmistä kuin aikaisemmin, koska yhä useammin tietojärjestelmien toimimattomuudella on kriittisiä vaikutuksia organisaation toimintaan (Knapp, Morris, Marshall & Byrd, 2009; Ifinedo, 2012). Organisaatioiden on suojeltava arvokasta informaatiotaan jatkuvasti muuttuvia kyberuhkia vastaan (Knapp, ym. 2009). Organisaation hallinnollinen ja tekninen tietoturva ulottuvat myös oman organisaation ulkopuolelle yhteistyöorganisaatioihin, kuten esimerkiksi ulkoisotettuihin toimintoihin (Järveläinen, 2012). Esimerkkitapauksessa vuodelta 2011 suomalaisen pankin liiketoiminta häiriintyi inhimillisen virheen takia: alihankkijan konesalissa oli asennettu verkkokytkin väärin (Ranta, 2011; Järveläinen, 2012). Alkujaan pieni inhimillinen virhe voi johtaa yrityksen liiketoiminnan häiriintymiseen, luottamuksellisen tiedon vuotamiseen vääriin käsiin tai organisaation julkisuuskuvan tahriintumiseen.

Teknisten tietoturvaratkaisuiden, kuten palomuurin, virustorjunnan tai varmuuskopioiden, merkitys on ymmärretty monissa organisaatioissa, mutta tekniset ratkaisut eivät tarjoa kattavaa suojaa, vaan organisaatioissa pitää keskittyä myös ei-tekniseen tietoturvaan (Ifinedo, 2012). Useissa tutkimuksissa on esitetty, että monesti organisaatioiden tietoturvan heikoin lenkki on työntekijä (Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013; Ifinedo, 2012). On esitetty arvioita, että organisaatioiden tietojärjestelmien tietovuodoista ja -murroista jopa puolet johtuu työntekijän virheestä (Stanton, Stam, Mastrangelo & Jolton, 2005; Vance, Siponen & Panhila, 2012). Näin ollen organisaation tietoturvan kannalta yksittäiset työntekijät ovat merkittävässä roolissa kokonaistietoturvallisuuden kannalta (Siponen, 2000). Käyttäjän virheellinen toiminta voi avata hyökkääjälle pääsyn organisaation tietojärjestelmiin ohi teknisten suojamekanismien (Dodge, Carver & Ferguson, 2007). Monissa organisaatioissa pyritäänkin kehittämään käyttäjien tietoturvaosaamista erilaisilla koulutusohjelmilla (Kruger & Kearney, 2006).

Ei-teknisen tietoturvan kannalta keskeinen työkalu organisaation tietoturvalle ovat tietoturvakäytännöt ja tietoturvapolitiikat. Tietoturvapolitiikan keskeisin tarkoitus on turvata elektronisen tiedon yhtenäisyys, saatavuus ja luottamuksellisuus tietojärjestelmissä. Yrityksen tietoturvapolitiikan on tarkoitus ohjata työntekijöiden toimintaa tietoturvaan liittyvissä asioissa ja turvata tältä osin yrityksen liiketoimintaa. Se on viesti yrityksen johdolta työntekijöille, että tietoturva-asioihin pitää kiinnittää huomiota. Yksi haaste tietoturvapolitiikan toteutumissa on keskeisen sisällön viestintä rakentavasti työntekijöille, joiden tulisi omaksua tietoturvapolitiikka osaksi omaa toimintamalliaan. Toinen tietoturvaan liittyvä haaste on se, että työntekijät tuntevat tietoturvakäytännöt ja -politiikat, mutta eivät piittaa niistä. (Knapp, ym. 2009)

2.2 Verkkohuijaus ja huijaussähköpostit

Verkkohuijaus, tai tietojenkalastelu (engl. phishing/phishing attack), voidaan määritellä teknisiä apuvälineitä käyttäen tapahtuvaksi henkilökohtaisten tietojen kavallukseksi, eli tilanteeksi, jossa pahantahtoisesti pyritään hankkimaan tietoja harhaanjohtamalla uhria (Olivo, Santin & Olivera, 2013; Vishwanath, Herath, Chen, Wang & Rao, 2011). Tässä tutkimuksessa käytetään termiä verkkohuijaus, koska tietojenkalastelu terminä on epätarkempi, eikä kuvasta tarkasteltavaa ilmiötä kovin hyvin.

Käyttäjän manipulointi (engl. social engineering) on toimintaa, jossa uhri harhauttamalla saadaan luovuttamaan tietoa tai toimimaan tavalla, joka heikentää hyökkäyksen kohteen tietoturvan tasoa (Sanastokeskus TSK, 2004, s. 17). Verkkohuijaus on siis käsitteenä suppeampi kuin käyttäjän manipulointi, mutta termien erottaminen voi olla useissa tilanteissa vaikeaa. Verkkohuijaus, yhdistettynä käyttäjän manipulointiin, voi myös avata hyökkääjälle pääsy uhrin tietojärjestelmään luottamuksellisen tiedon saamiseksi (Olivo, ym., 2013).

Verkkohuijauksessa, kuten reaalimaailman huijauksissa, yleensä käytetään hyväksi käyttäjän manipulointiin liittyviä elementtejä, kuten esimerkiksi tunteisiin vetoamista, tunnettujen organisaatioiden ja yritysten nimiä sekä ajankohtaisia tapahtumia. Huijausviesti voi yrittää vedota uhriin synnyttämällä tunteita kuten, pelkoa, uhkaa, jännitystä tai kiirettä. Tunnettujen organisaatioiden ja yritysten nimien käytöllä pyritään luomaan uskottavuutta huijausviesteihin. Ajankohtaisten tapahtumien, esimerkiksi urheilutapahtumien, tarkoitus on herättää uhrin kiinnostus ja laskea epäilyksen tasoa. (Vishwanath, ym., 2011)

Robila ja Ragucci (2006) ovat esittäneet, että verkkohuijaus on kehittynyt yhdistelmä roskapostista sekä käyttäjän manipuloinnista. Roskaposti (engl. spam) voidaan määritellä kaupalliseksi sähköpostimainonnaksi, joka pyytämättä lähetetään käyttäjälle (Robila ym., 2006). Roskapostin osuus kaikesta sähköpostiliikenteestä on ollut viime vuosina laskussa, mutta edelleen kaikista sähköposteista yli 60% on roskapostia (Symantec, 2013; McAfee, 2011). Roskapostin ja hui-

jaussähköpostien määrän lasku johtunee siitä, että verkkorikolliset ovat keskittäneet toimintaansa sosiaalisen median palveluihin, joista esimerkkinä mainittakoon Twitter ja Facebook (Symantec, 2013). Huijaussähköpostien levitystekniikka on hyvin samankaltainen kuin roskasähköpostien (Olivo, ym., 2013).
Huijaussähköposti, tai tietojenkalastelusähköposti (engl. phishing email), tarkoittaa sähköpostiviestiä, jossa pahantahtoinen hyökkääjä yrittää urkkia tietoja naamioimalla hyökkäysviestin asialliseksi sähköpostiksi. Huijaussähköposteille ja tietojenkalastelusähköposteille on tyypillistä, että viestejä lähetetään suuria määriä sattumanvaraisille vastaanottajille. Kohdistettu verkkohuijaus perustuu usein tarkasti personoituun huijaussähköpostiviestiin, jota kutsutaan englanniksi nimellä spear phishing. Termin etuliite ”spear” tarkoittaa keihästä ja viittaa nimenomaan kyseistä uhria varten suunniteltuun verkkohuijaukseen. Kohdistettu huijaussähköpostiviesti on sisällöltään usein tarkasti harkittu, ulkoasultaan vaatimattomampi, usein tekstipohjainen, ja lähettäjä esiintyy relevanttina kontaktina. Juuri personoinnista johtuen käyttäjän on vaikea tunnistaa sähköpostiviestiä huijaukseksi ensisilmäyksellä. (Wang, Herath, Chen, Vishwanath & Rao, 2012)

Kohdistetun verkkohuijauksen kohteena voi olla niin yksilö kuin organisaatio, mutta suurimmat julkisuutta saaneet tapaukset liittyvät yleensä yrityksiin ja organisaatioihin. On kuitenkin tärkeää huomioida, että vaikka organisaatio on hyökkääjän kohde, kohdistettu verkkohuijaus on kuitenkin lähes poikkeuksetta kohdistettu johonkin yksittäiseen organisaatiossa työskentelevään henkilöön. Verkkohuijaukset aiheuttavat sekä merkittävää taloudellista vahinkoa että tahraavat organisaation julkisuuskuvaa.

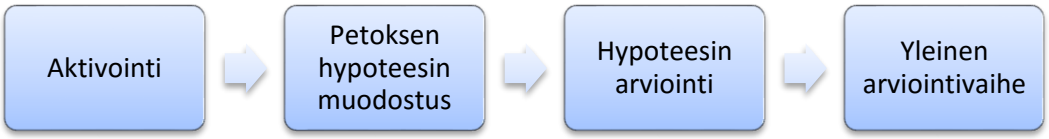
On huomion arvoista, että kohdistettujen verkkohuijausten ja kohdistettujen huijaussähköpostien määrä on viime vuosina ollut kasvussa, vaikka aikaisemminkin mainittu roskapostin ja huijaussähköpostien määrä on ollut laskussa (Symantec, 2013). Tämän voidaan arvioida johtuvan siitä, että perinteisten roskapostien ja huijaussähköpostien onnistumisprosentti on merkittävästi pienempi kuin kohdistettujen verkkohuijausten onnistumisprosentti (Vishwanath, ym., 2011). Lisäksi kohdistettujen verkkohuijausten kohteet valikoidaan usein tarkemmin ja onnistuessaan huijauksen tulokset voivat olla merkittävämpiä esimerkiksi taloudellisesti.

2.3 Käyttäjät verkkohuijauksen kohteina: teoria ja aiempi tutkimus

Verkkohuijauksiin ja huijaussähköposteihin voidaan soveltaa Petosteoriaa (engl. Theory of Deception) (Wang, ym., 2012). Teorian mukaan yksilö tunnistaa petosyrityksen havaitsemalla ja tulkitsemalla epäjohdonmukaisia yksityiskohtia petostilanteessa (Wang, ym., 2012). Havainnot ja tulkinnat perustuvat aikaisem-

piin kokemuksiin ja opittuihin päättelyketjuihin (Wang, ym., 2012). Vishwanathin, ym. (2011) mukaan petoksen tai huijauksen tunnistusprosessi voidaan jäsennellä neljään vaiheeseen: aktivointi (engl. activation), petoksen hypoteesin muodostus (engl. deception hypothesis generation), hypoteesin arviointi (engl. hypothesis evaluation) ja yleinen arviointivaihe (engl. a global assessment stage) (Vishwanath, ym., 2011). Aktivointi tapahtuu, kun petoksen kohde kiinnittää huomion petolliseen informaatioon - tämän jälkeen muodostuu petoksen hypoteesi, kun kohde tulkitsee petollista informaatiota aikaisempaan tietämykseensä pohjautuen (Vishwanath, ym., 2011). Seuraavaksi kohde arvioi tulkintansa petollisesta informaatiosta, eli arvioi hypoteesin, ja lopuksi muodostaa yleisen arvion kokonaisuudesta (Vishwanath, ym., 2011).

Petosteoria sopii huijaussähköpostien tarkasteluun hyvin, koska teoria keskittyy informaation prosessointiin petostilanteessa (Vishwanath, ym., 2011). Teorian perusteella voidaan siis todeta, että mitä johdonmukaisempi petostilanne on, sitä suurempi todennäköisyys huijauksella on onnistua (Vishwanath, ym., 2011).



KUVIO 1: Petoksen arviointiprosessi (Vishwanath, ym., 2011 mukaillen)

Aikaisempi tieteellinen tutkimus verkkohuijausten ja huijaussähköpostien osalta jakautuu kahteen kategoriaan: teknologiseen ja käyttäytymistieteelliseen (Vishwanath, ym., 2011). Tässä tutkimuksessa perehdytään käyttäytymistieteelliseen tutkimukseen, koska tutkimuksen tarkoitus on tutkia käyttäjien reaktioita huijaussähköpostiin, huijatuksi tulemisen todennäköisyyttä ja sitä ennakoivia tekijöitä. Teknologisiin ratkaisuihin ei tässä tutkimuksessa perehdytä.

Käyttäytymistieteellisessä tutkimuksessa on perehdytty mm. sähköpostiviestinnän elementteihin, kuten luottamukseen, uskottavuuteen ja aitouteen. On havaittu, että käyttäjät arvioivat huijaussähköpostia samoilla perusteilla kuin huijausverkkosivua. Jakobsson, ym (2007) toteuttivat tutkimuksen, jossa perehdyttiin sähköpostiviestien elementteihin ja ominaisuuksiin verkkohuijauksen näkökulmasta. Erityisesti kohdistettuja huijaussähköposteja on tarkasteltu kahdessa tutkimuksessa, joissa tutkittaville lähetettiin huijaussähköposti ja viestin sisältäneen Internet-linkin perusteella tunnistettiin, ketkä käyttäjät tulivat huijatuksi. Jagatic, ym. (2007) toteuttivat tutkimuksen, jossa korkeakouluopiskelijoille lähetettiin huijaussähköposti, johon väärennettiin lähettäjä siten, että viesti näytti tulevan vastaanottajan oikealta tuttavalta (Jagatic, Johnson, Jakobsson & Menczer, 2007). Toinen vastaava kohdistettu huijaussähköpostitutkimus tehtiin sotatieteen korkeakoulussa, jossa koreakouluopiskelijoille lähetettiin huijaussähköposti tenttikauden aikaan, jossa kerrottiin tenttitulosten löytyvän avaamalla viestissä oleva Internet-linkki. (Jakobsson, Tsow, Shah, Blevis & Lim, 2007)

Jakobssonin, ym. (2007) tutkimuksessa 17 tutkittavaa arvioi tukijoiden muodostamia sähköpostiviestejä, joista osa sisälsi huijausviesteille tyypillisiä elementtejä. Tutkittavat arvioivat viestien luotettavuutta ja aitoutta koetilanteessa. Tutkijat havaitsivat käyttäjien kiinnittävän erityistä huomiota viestin ulkoasuun ja URL-osoitteisiin; lisäksi keinotekoinen tai vähäinen personointi ja monikanavaisuus vaikuttivat positiivisesti luottamuksen kasvamiseen. Vähäinen personointi tarkoittaa esimerkiksi IP-osoitteen perusteella selvitettyä postinumeroa tai muuta helposti pääteltävää tietoa. Monikanavaisuus viittaa viestinnässä, esimerkiksi sähköpostissa, esitettävään mahdollisuuteen tutustua verkkosivuihin tai jopa mahdollisuuteen soittaa palvelunumeroon. Toisin sanoen, huijauksen uhria pyritään vakuuttamaan viestin aitoudesta tarjoamalla useampia viestintämahdollisuuksia. Keskeinen löydös oli myös se, että käyttäjät pitivät sähköpostiviestejä erittäin epäilyttävinä, verkkosivujen välityksellä viestintää hieman epäilyttävänä ja puhelimitse tapahtuvaa viestintää vähiten epäilyttävänä. Eli käyttäjät olivat hyvin valveutuneita huijaussähköpostien kanssa toimimiseen. Toisaalta, kun verkkohuijaukseen lisätään puhelimitse tapahtuva viestintä, niin käyttäjät suhtautuvat vähemmän epäilevästi huijaukseen. Tutkimuksen johtopäätöksiä ei kuitenkaan voida yleistää, koska tutkimukseen osallistuneet tutkittavat olivat korkeakoulun tietojenkäsittelyyn erikoistuneita opiskelijoita ja työntekijöitä. (Jakobsson, ym., 2007)

Jakobsson, ym. (2007) tutkimuksen perusteella voidaan todeta, että tietotekniikkaan perehtyneet käyttäjät ovat valveutuneita huijaussähköpostien varalta, mutta toisaalta tutkimuksen tulokset viittaavat mahdollisuuteen, että kohdistettu huijaussähköpostiviesti voisi saada käyttäjät harhaan. Kohdistettu huijaussähköpostiviesti on usein personoitu, sisällöltään relevantti kohteelle sekä mahdollisesti tarjoaa monikanavaista viestintää huijauksen kohteelle.

Vishwanath, ym. (2011), esittävät prosessointimallissaan, että yksilön huijaussähköpostin arviointiin vaikuttaa yksilön motivaation taso, uskomukset, aiempi tietämys huijauksista sekä aikaisemmat kokemukset. Tutkimuksessa testattiin prosessointimallin toimintaa todellisen huijaussähköpostin kohteeksi joutuneilla yliopiston opiskelijoilla sekä henkilökunnalla Yhdysvalloissa. Yksilön tiedon prosessoinnissa ensimmäinen vaihe on huomion herääminen ja erityisesti tähän liittyvä huomion määrä, jonka yksilö keskittää tarkasteltavan informaation prosessointiin. Huijaussähköpostissa keskeisimmät elementit, joihin prosessointimallin mukaan yksilön huomio kiinnittyy, ovat lähettäjä, otsikko, oikeinkirjoitus ja kielioppi sekä vihjaukset kiireellisyydestä.

Internetin myötä ihmisistä on tarjolla paljon tietoa erityisesti erilaisissa sosiaalisen median palveluissa, kuten Facebook ja LinkedIn, josta verkkorikollisten on tehokasta ja helppoa kerätä tietoja verkkohuijaukseen. Sosiaalisen median tietojen keräämiseen ja tulkitsemiseen on tarjolla monia eri työkaluja, jotka osaavat yhdistellä tietoa eri lähteistä. Yhdistämällä tietoa eri sosiaalisen median palveluista on mahdollista saada lisäinformaatiota yksittäisestä henkilöstä, kuten esimerkiksi läheisistä ystävistä. Yksittäisestä sosiaalisen median palvelusta saata-

vien tiedon murusten arvo voi olla huijauksen suunnittelijalle pieni, mutta monien eri palveluiden tietojen yhdistäminen voi luoda huijauksen kohteesta yllättävän tarkan kuvan. (Jagatic, Johnson, Jakobsson & Menczer, 2007)

Jagaticin ym. (2007) tutkimuksessa lähetettiin personoituja huijaussähköpostiviestejä yliopiston opiskelijoille. Tutkimuksen tarkoituksena oli kartoittaa, kuinka helppoa sosiaalisesta mediasta saatujen tietojen avulla on toteuttaa verkkohuijaus. Huijausviestit personoitiin siten, että sähköpostiviesti vaikutti tulevan tutulta lähettäjältä, jolla on yliopiston sähköpostiosoite. Kontrolliryhmä sai viestit fiktiivisiltä henkilöiltä. Yliopiston yleisen yhteystietoluettelon tietoja yhdistettiin sosiaalisen median tietoihin, jonka perusteella tutkittavista koottiin verkosto, josta kävi ilmi tuttavuussuhteet. Huijaussähköpostiviesti sisälsi linkin yliopiston kirjautumissivulle, johon kirjautuminen antoi käyttäjälle virheilmoituksen. Käyttäjän tunnuksia ei tutkimuksessa luonnollisesti varastettu, vaan kirjautuminen merkitsi käyttäjän nimitiedot palvelimelle, josta tiedettiin ketkä tutkittavat olivat tulleet huijatuiksi. Erilliset kirjautumiskerrat myös tallennettiin, mikä osoitti, että osa käyttäjistä todella yritti myöhemmin useita kertoja uudelleen. (Jagatic, ym., 2007)

Huijausviestien onnistumisprosentti oli 72%, joka Jagaticin ym. (2007) mukaan oli odotettua suurempi. Toisaalta onnistumisprosentti seuraa aikaisemman huijaussähköpostitutkimuksen tuloksia, joka toteutettiin Yhdysvalloissa sotakorkeakoulussa, jossa onnistumisprosentti oli 80% (Ferguson, 2005). Tutkimuksessa sotakoreakoulun opiskelijoille lähetettiin huijaussähköposti, jossa kuvitteellinen sotilasarvoltaan korkeampi upseeri, eversti, lähetti opiskelijoille viestin, jossa ohjeistettiin tarkastamaan tenttitulokset avaamalla viestissä ollut Internet-linkki (Ferguson, 2005).

Molempien tutkimusten onnistumisprosentit ovat korkeat verrattuna yritysmaailman omiin arvioihin. Yritysmaailman arvion mukaan kohdistettujen verkkohuijausten onnistumisprosentti oli 19% ja kohdistettujen huijaussähköpostien onnistumisprosentti oli noin 5% vuonna 2006 (Parmar, 2012). Onnistumisprosenttien vertailu ei kuitenkaan ole yksiselitteistä. Tutkimuksissa (Jagaticin ym. 2007; Ferguson, 2005) saatujen korkeiden onnistumisprosenttien suuruutta selittää tarkan personoinnin lisäksi dokumentointi. Yritysmaailmassa verkkohuijausten tilastot eivät ole yhtä luotettavia, eivätkä kaikki huijaukset edes aina paljastu. Toisaalta kohdistettujen verkkohuijausten määrä on viime vuosina kasvanut (Symantec, 2013).

Jagaticin ym. (2007) tutkimuksessa todettiin, että suurin yleisö kohdistetulle huijausviestille saatiin ensimmäisten 12 tunnin aikana, jolloin kirjattiin 70% kaikista vastauksista. Vastaavaa onnistumisaikataulua ei Ferguson (2005) esittänyt tutkimuksessaan. Kohdistetun huijaussähköpostin onnistumisen kannalta ensimmäinen lukemiskerta on kriittinen, koska tällöin käyttäjä arvioi viestin luotettavuuden ja uskottavuuden. Kohdistetun verkkohuijausten tutkiminen on eettisesti haastavaa. Jagaticin ym. (2007) ilmoittivat tutkittaville koeasetelmasta tutkimuksen jälkeen verkkosivustolla, jossa osallistujilla oli mahdollisuus keskus-

tella ja antaa palautetta. Tutkijat saivat paljon negatiivista palautetta ja tutkittavilla oli suuri huoli jälkeenpäin, että heidän tietonsa ovat vaarantuneet, vaikka tutkimus tehtiin erillisen eettisen valvonnan alaisuudessa (Jagatic, ym., 2007).

Halevi, Lewis & Memon. (2013) tutkivat kaksiosaisessa tutkimuksessa eikohdistettuja huijaussähköposteja ja niihin liittyviä käyttäjien taustoja. Tutkittavat pyydettiin osallistumaan internetin käyttöön liittyvään tutkimukseen, jossa ensimmäisessä vaiheessa pyydettiin antamaan taustatiedot ja ilmoitettiin, että tutkittaviin otetaan yhteyttä myöhemmin sähköpostilla. Sähköpostilla toimitettiin tutkittaville kuitenkin tutkimukseen liittymätön huijaussähköposti, jossa luvattiin ilmaisia lahjoja nopeimmille, jotka seuraavat linkkiä sen takaa löytyviä ohjeita. Tutkittavista 17% seurasi linkkiä ja antoi yliopiston henkilökohtaiset käyttäjätunnuksen ja salasanan, joten heidät tulkittiin tulleen huijatuksi. Halevi, ym. (2013)

Kun halutaan kehittää suojaa verkkohuijauksien varalle, on tärkeää ymmärtää verkkohuijaukselle altistetun yksilön ajatusprosessia. Downs ym. (2006) tekemässä haastattelututkimuksessa 40 tutkittavalle kerrottiin heidän osallistuva tutkimukseen koskien heidän tietokoneen käyttöään sekä päätöksentekoprosessiaan koskien sähköpostin ja verkkosivustojen käyttöä. Todellisena tarkoituksena oli kartoittaa nimenomaan huijaussähköposteihin liittyvää ajatusprosessia. Tutkimuksen ensimmäinen osa toteutettiin roolipelinä, jossa tutkittaville annettiin uusi identiteetti, mukaan lukien uusi sosiaaliturvatunnus, luottokortti, käyttäjätilien kirjautumistiedot esitettiin seitsemän sähköpostiviestiä, joiden sisällöstä keskusteltiin, osa viesteistä oli normaaleja viestejä ja osa oli huijausviestejä. Tutkimuksen johtopäätöksenä todettiin, että mitä tietoisempia tutkittavat olivat internet-ympäristöstä sitä paremmin he tunnistivat verkkohuijaukset.
(Downs, Holbrook, & Cranor, 2006)

2.4 Viestien sisältö ja tulkinta

Tässä kappaleessa perehdytään aikaisemman tutkimuksen perusteella verkkohuijauksen sisältöön, elementteihin ja käyttäjien tulkintaan, erityisesti kohdistettujen verkkohuijausten näkökulmasta. Tutkimuksessa tarkastellaan erityisesti huijaussähköpostielementtejä: lähettäjä, sisältö ja linkit tai liitetiedostot. Verkkohuijaus koostuu usein kohdistetun huijaussähköpostin lisäksi liitetiedostosta tai URL-linkistä verkkosivustolle, jonka avulla käyttäjän laitteelle ladataan haitallista sisältöä. Tutkittaessa käyttäjien tulkintaa kohdistetusta huijaussähköpostista täytyy tarkastella verkkohuijausta kokonaisuutena, eikä keskittyä vain yksittäiseen huijauksen elementtiin.

Kohdistetun verkkohuijauksen ja huijaussähköpostin yksi keskeinen elementti on viestin lähettäjä. Vakuuttava lähettäjä ja viestin allekirjoitus, jossa mahdolliset lähettäjän yhteystiedot, ovat keskeinen osa onnistunutta verkkohuijausta

(Downs, ym., 2006; Ferguson, 2005). Kohdistetun verkkohuijauksen onnistumisen kannalta on tärkeää, että viestin lähettäjä on relevantti. Esimerkiksi vastaanottaja lukee varmemmin sähköpostin ja avaa liitetiedoston tai linkin, jos lähettäjä esittää edustavansa organisaatiota johon vastaanottaja voisi muutenkin olla yhteydessä (Downs, ym., 2006). Jos huijaussähköpostin lähettäjä tekeytyy sellaiseksi organisaation edustajaksi tai henkilöksi, joka voisi oikeasti viestiä vastaanottajan kanssa, verkkohuijaus todennäköisemmin onnistuu (Jagatic, ym., 2007). Toisaalta tutkimuksissa on todettu, että jos lähettäjä on korkeammassa arvoasemassa viestin vastaanottajan näkökulmasta, verkkohuijaus onnistuu todennäköisemmin (Ferguson, 2005). Esimerkiksi sotilasmaailmassa korean upseerin sähköpostiviestit luetaan todennäköisesti varmemmin (Ferguson, 2005). Vastaava asetelma voidaan olettaa syntyvän esimerkiksi finanssialan yrityksessä, jossa toimintaa valvova viranomainen viestii yrityksen työntekijöille.

Viestin sisältö on myös keskeinen kohdistetun verkkohuijauksen onnistumista ennakoiva tekijä. Viestin sisällön on oltava vastaanottajalle relevanttia ja yksinkertaisesti esitettyä (Ferguson, 2005; Jagatic, ym., 2007). Viestin sisällön tulee olla johdonmukainen ja uskottava, jotta lukija ei epäile viestiä huijaukseksi (Downs, ym., 2006). Monet käyttäjät osaavat epäillä verkkohuijausta, jos viestin sisältö on liian hyvää ollakseen totta (Grazioli, 2004). Viestin sisällön lisäksi esitys muoto on tärkeässä roolissa, sillä huijaussähköpostin huono kirjoitusasu tai kielioppivirheet herättävät lukijat epäilemään mahdollista huijausta (Downs, ym., 2006; Vishwanath, ym.,2011; Wang, ym., 2012). Usein verkkohuijauksissa pyritään luomaan kiireellisyyden tunne lukijalle, jotta lukija ei ehtisi epäillä tai tarkastella viestiä tarkemmin (Downs, ym., 2006).

Viestin lähetysajankohta tulee olla sellainen jolloin vastaavan kaltainen viesti voisi oikeasti saapua, esimerkiksi opiskelijoille arvosanoihin liittyvät viestit ovat relevantteja ajankohtana, kun arvosanoja annetaan (Ferguson, 2005). Vastaavasti yritysmaailmassa rekrytointiin liittyvät sähköpostiviestit ovat relevantteja, jos yritys on rekrytoimassa. Tästä tosielämän kohdistetusta verkkohuijauksesta esimerkki esitellään myöhemmässä kappaleessa 2.7, jossa yhtiön verkkorikollinen esitti olevansa yrityksen käyttämän rekrytointisivuston edustaja.

Huijausviestin mahdollinen liitetiedosto tai linkki ovat kriittisimpiä elementtejä lukijan arvioidessa viestin aitoutta. Esimerkiksi monet käyttäjät osaavat suhtautua kriittisesti linkin URL-osoitteessa tai liitetiedostossa mahdollisesti mainittavaan .exe-tiedosto päätteeseen, joka yleisesti tunnetaan ajettavaksi ohjelmakoodiksi (Downs, ym., 2006). Samoin viestissä mahdollisesti olevan URL-osoite joutuu usein lukijan tarkemman analyysin kohteeksi. Siinä mahdollisesti esiintyvät kirjoitusvirheet tai muut epäloogisuudet saattavat herättää käyttäjässä epäilyn viestin aitoudesta. Kohdistetuissa verkkohuijauksissa suositaan usein liitetiedostomuotoja, jotka ovat normaaleja jokapäiväisessä viestinässä, kuten esimerkiksi teksti- tai taulukkolaskentatiedostot.

On havaittu, että monet käyttäjät luottavat esimerkiksi URL:n https-alkuun, joka viittaa siihen, että sivuston liikenne on salattu. esti luo kiireen tuntua, URL-osoite sisältää IP-soitteen, selkeän epäilyttävän URL:n tai relevantin oloisen

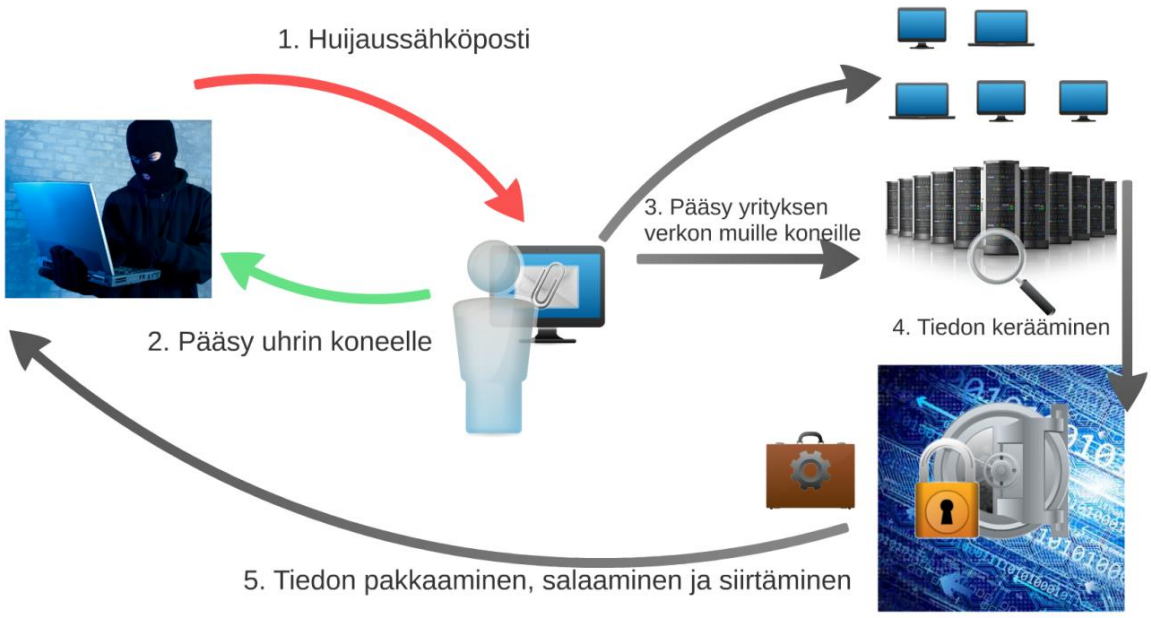
URL:n. Kirjoitusvirheet. Linkeistä avautuvalla sivulla viallisia kuvia. (Downs, ym., 2006)

2.5 Esimerkkitapaus RSA

Seuraavaksi esitetään esimerkkitapaus, jossa hyökkääjä hyväksikäytti kohdistettua huijaussähköpostia tietomurron ensimmäisessä vaiheessa. Esimerkkitapauksen tarkoitus on tuoda esiin yritykseen kohdistuvan tietomurron vaiheita ja esittää, kuinka kohdistettu huijaussähköposti aiheuttaa vaaran yrityksen toiminnalle.

Yksi tunnettu kohdistetun huijaussähköpostin avulla toteutuneista hyökkäyksistä tapahtui tietoturvayhtiö RSA:ta vastaan vuonna 2011. Yhtiön (EMC Corporation - RSA, 2011) omassa verkkojulkaisussa on kerrottu tapahtumien kulku kattavasti, mutta lisäksi tietoturvatutkijat, kuten Parmar (2012) ja Hyppönen (2011), ovat perehtyneet tapaukseen. RSA ei ole julkaissut virallisesti huijausviestin sisältöä, vain tiedot otsikosta ja liitetiedostosta, mutta tietoturvatutkijat ovat löytäneet viestin, joka lähes varmasti on tässä hyökkäyksessä käytetty sähköpostiviesti tietomurtonäytteiden joukosta. (Hyppönen, 2011; Parmar, 2012)

Tietomurron vaiheet on esitetty Kuviossa 2. Tietomurto voidaan jakaa viiteen vaiheeseen: (1.) huijaussähköposti, (2.) pääsy uhrin koneelle, (3.) pääsy yrityksen verkon muille koneille, (4.) tiedon kerääminen sekä (5.) tiedon pakkaaminen, salaaminen ja siirtäminen. Tämän tutkimuksen näkökulmasta kiinnostavat vaiheet 1. ja 2. ovat merkitty kuvaan eri värein korostamaan kohdistettuun huijaussähköpostiin liittyviä vaiheita.



KUVIO 2: RSA tietomurron vaiheet

Seuraavaksi esitetään koko tapahtumien kulku yleisellä tasolla ja kohdistetun huijaussähköpostin sisältö hieman tarkemmalla tasolla. Hyökkäyksen ensimmäisessä vaiheessa pienelle joukolle yrityksen työntekijöitä lähetettiin huijausviesti otsikolla: "2011 Recruitment plan". Viestissä oli otsikon mukaan nimetty Excel-liitetiedosto. Viestin saajat eivät RSA:n mukaan olleet liiketoiminnan kannalta avainhenkilöitä, vaan tavallisia työntekijöitä. Viestin lähettäjä-tieto oli väärennetty ja viesti näytti tulevan asiallisen rekrytointiverkkopalvelun ylläpitäjältä. Viestin sisältö oli lyhyt ja selkeä: "*I forward this file to you for review. Please open and view it.*", joka vapaasti suomennettuna tarkoittaa: "*Välitän tämän tiedoston sinulle tarkasteltavaksi. Ole hyvä avaa ja katso*". Viestissä ei ollut allekirjoitusta tai tervehdystä lähettäjältä. (EMC Corporation - RSA, 2011; Hyppönen, 2011; Parmar 2012)

Kohdistettu huijaussähköpostiviesti meni automaattisesti vastaanottajien "roskaposti"-kansioon, mutta ainakin yksi viestin vastaanottajista löysi ja avasi viestin sekä avasi liitetiedoston. Liitetiedosto sisälsi nollapäivähaavoittuvuuden, jonka avulla hyökkääjä sai pääsyn uhrin tietokoneelle.

Nollapäivähaavoittuvuus (engl. zero-day vulnerability) on entuudestaan tuntematon turvallisuusaukko järjestelmässä tai sovelluksessa, eli tietoturva-aukko, jota ei ole aikaisemmin tiedetty olevan olemassa (Bolzoni, 2009, s. 14). Hyökkääjät pyrkivät löytämään järjestelmistä ja ohjelmista nollapäivähaavoittuvuuksia, joiden avulla on mahdollista toteuttaa hyökkäys haluttuun kohteeseen. Hyökkääjät pyrkivät käyttämään turvallisuusaukkoa hyväksi ennen kuin siihen on saatavilla korjaavaa päivitystä (Kliarsky, 2011).

RSA:n tapauksessa hyökkääjät onnistuivat kohdistetun huijaussähköpostin liitetiedostossa olleen nollapäivähaavoittuvuuden avulla saamaan pääsyn yrityksen sisäverkossa olevalle yhden työntekijän tietokoneelle. Usein liiketoiminnan kannalta kriittinen tieto on yrityksissä suojattu, joten hyökkääjä joutui tekemään tutkimustyötä hyökkäyskohteessa. Hyökkääjä tutki verkkoa, verkossa olevia laitteita, liikkuvaa tietoa ja käyttäjätietoja sekä liikkui verkossa eri laitteiden välillä. Kun avainhenkilöt ja haluttu tieto oli tunnistettu hyökkääjä aloitti tiedon siirron pois yrityksestä. Ennen siirtoa hyökkääjä pakkasi ja salasi tiedot, jotta niitä olisi vaikeampi tunnistaa siirron aikana. (EMC Corporation - RSA, 2011; Hyppönen, 2011)

RSA ei ole julkistanut tarkkoja tietoja hyökkäyksen seurauksista liiketoiminnalle, mutta taloudellisten tappioiden lisäksi tietoturvayhtiön maine kärsi hyökkäyksessä suuren vahingon, jota voi olla vaikea rahassa mitata. Hyökkääjät onnistuivat saamaan käsiinsä RSA tunnistustuotteen, SecureID:n, kriittiset tiedot siitä kuinka tunnistuksessa käytetyt numerosarjat muodostetaan. Tämä mahdollisti hyökkääjille pääsyn tunnistetuotetta käyttävien järjestelmien läpi. RSA joutui vaihtamaan markkinoilla olevat SecureID "avaimet", joita arvioitiin tuolloin olevan noin 40 miljoonaa kappaletta. Uutistoimisto Bloombergin (King, 2011) mukaan taloudelliset vahingot vaihto-operaatiosta ovat pelkästään RSA:n pankkialan asiakkaiden osalta arvioitu noin 100 miljoonan dollarin suuruisiksi. (EMC Corporation - RSA, 2011; Hyppönen, 2011; King, 2011)

Kohdistetun huijaussähköpostin avannut työntekijä oli avainasemassa, estääkseen massiivisen tietomurron. RSA:n tekninen sähköpostin arviointi oli tulkinnut sähköpostin roskapostiksi, mutta tästä huolimatta yksi työntekijä avasi sähköpostiviestin ja liitetiedoston. Liitetiedossa ollut nollapäivähaavoittuvuus liittyi Adoben Flash -mediaan ja tiedoston avautuessa taulukkolaskentasivulla näkyi hetken vain neliöity x-kirjain, joka tässä tapauksessa viittaa tiedostoon asetettuun ulkoiseen Flash-mediaan. Tiedoston avaamisesta muutaman sekunnin kuluttua taulukkolaskentatyökalu Excel-sammuu ilman virheilmoitusta. Tällöin työntekijä olisi voinut epäillä kyseessä olevan huijaussähköposti tai vähintäänkin yrittää ottaa yhteyttä lähettäjään viestin sisällön virheestä. (Hyppönen, 2011)

3 TUTKIMUKSEN TOTEUTTAMINEN

Tässä kappaleessa esitellään tutkimuksen toteutusta. Aluksi käydään läpi tutkimusmetodologia

3.1 Tutkimusmetodologia

Tutkimusmetodologiaksi valittiin kvantitatiivinen korrelatiivinen tutkimusote (Metsämuuronen 2011). Kvantitatiiviset tutkimukset voidaan jakaa kokeellisiin ja korrelatiivisiin tutkimuksiin (Field & Hole, 2002; Nummenmaa, 2009, sivut 32-34). Kokeellisen tutkimuksen keskeinen ero korrelatiiviseen tutkimukseen on se, että kokeellisessa tutkimuksessa tutkija pyrkii kontrolloimaan tutkittavaan ilmiöön vaikuttavia tekijöitä ja olosuhteita (Field & Hole, 2002; Nummenmaa, 2009, sivut 32-33). Yleensä korrelatiivisen tutkimuksen, eli havainnointitutkimuksen, tavoitteena on löytää näyttöä ilmiöiden välisistä yhteyksistä (Nummenmaa, 2009, sivu 34). Korrelatiivinen tutkimus koostuu kolmesta elementistä, jotka on esitetty Kuviossa 3, eli tutkittavat, mittaus ja päätelmät.

KUVIO 3: Korrelatiivinen tutkimusasetelma (Nummenmaa, 2006, sivu 28)

Toisaalta Nummenmaa (2009, sivut 22-24) jakaa tieteellisen tutkimuksen empiiriseen ja teoreettiseen tutkimukseen. Empiirisen tutkimuksen perustuessa päätelmiin, jotka perustuvat havainnointiin, teoreettinen tutkimus sen sijaan ei edellytä mittaamista tai havaintoja vaan se perustuu vain teoreettiseen analyysiin ja kirjallisiin lähteisiin. Tavallisesti kvantitatiivisessa tutkimuksessa hyödynnetään tilastollista päättelyä, joka perustuu tilastotieteellisiin menetelmiin. Kaiken kaikkiaan tämä tutkimus perustui siis kvantitatiiviseen, empiiriseen tutkimusotteeseen, jossa hyödynnettiin tilastollista päättelyä tutkimuskysymykseen vastaamiseksi.

Tutkittavien rekrytointi tapahtui valikoidulla ryväsotannalla, eli klusteriotannalla. Klusteriotanta soveltuu tilanteisiin, jossa tutkijalla ei ole saatavilla kaikista havaintoyksiköistä kattavaa listausta (Yhteiskuntatieteellinen tietoarkisto, 2003). Otanta valittiin pankki- ja vakuutusalan organisaatioista, joihin tutkija pystyi muodostamaan kontaktin. Organisaatioiden sisällä tutkittavia rekrytoitiin yhdyshenkilön välityksellä.

Pankki- ja vakuutusala on esimerkki alasta, jossa toimitaan paljon sähköpostien välityksellä, käsitellään arkojakin tietoja ja suuria rahasummia. Näistä syistä pankki- ja vakuutusala on tässä tutkimuksessa tarkasteltavana, kun aikaisemmat tutkimukset ovat keskittyneet yliopistohenkilöstöön ja opiskelijoihin.

Kirjallisuuskatsaukseen perustuen voidaan todeta, että tieteellinen tutkimus verkkohuijausten ja huijaussähköpostien osalta jakautuu kahteen kategoriaan: teknologiseen ja käyttäytymistieteelliseen (Vishwanath, ym., 2011; Wang, ym., 2012). Teknologinen näkökulma keskittyy huijauksen tekniseen toteutukseen sekä mahdollisiin teknologisiin ratkaisuihin, joilla huijauksen vaikutuksia voidaan rajoittaa (Wang, ym., 2012). Käyttäytymistieteelliset tutkimukset ovat pitkälti olleet kvalitatiivisia, eli laadullisia, ja tuloksiltaan kuvailevia (Wang, ym., 2012). Käyttäytymistieteellisessä tutkimuksessa on vähäisellä huomiolle jäänyt tarkempi analyysi siitä, mihin uhrien reagointi perustuu huijausviestin saatuaan. Tämän tutkimuksen tarkoitus on kartoittaa millaiset tekijät selittävät huijaussähköpostiin reagoimista ja millaisiin viestin ominaisuuksiin käyttäjien huomio kiinnittyy huijaussähköposteissa.

Kuten kirjallisuuskatsauksessa todettiin, työntekijät ovat keskeinen osa organisaatioiden tietoturvaa ja siksi tässä tutkimuksessa on tarkoitus selvittää huijaussähköpostien lisäksi vastaajien, jotka olivat kaikki työntekijöitä, tietoisuutta sähköpostin aiheuttamista riskeistä työnantajaa ja asiakkaita kohtaan.

3.2 Tutkimuksen kulku ja kyselyn sisältö

Tutkimus toteutettiin kirjallisuuskatsaukseen perustuvana empiirisenä tutkimuksena. Tutkittavat rekrytoitiin pankki- ja vakuutusalan työntekijöistä. Kyselytutkimuksen sisältö ja muoto validoitiin kahden vapaaehtoisen vastaajan kanssa siten, että vastaaja vastasi kyselylomakkeen kysymyksiin, jonka jälkeen kaikki kysymykset käytiin tutkittavan kanssa yhdessä läpi. Kyselytutkimuksen koevastaajien tuloksia ei ole otettu mukaan tutkimuksen tuloksiin, koska koetilanne ja kyselylomakkeen sisältö eivät vastanneet lopullista tutkimusasetelmaa. Kyselyyn tehtiin kaksi muutosta koevastaustausten jälkeen. Ensinnäkin kysymys työnantajasta muutettiin vapaaehtoiseksi kysymykseksi, sillä kysymyksen pakollisuus herätti vastaajissa negatiivisia ajatuksia, koska kyselyn aihealue kosketti tutkittavien työelämää. Tutkimukseen lisättiin myös pakollinen vapaamuotoinen kysymys työnantajan toimialasta, jotta tuloksista pystytään erottamaan pankki- ja vakuutusalan vastaajat toisistaan. Kyselylomake saatettiin tutkittavien saataville internet-palvelussa, joka mahdollisti vastaamisen erilaitteilla. Kyselylomake ei ollut yleisesti löydettävissä, vaan vastaamaan pääsi vain suoralla internet-osoitteella, joka toimitettiin tutkittaville sähköpostilinkkinä. Lomake oli myös vain rajoitetun ajan saatavilla, jolla pystyttiin kontrolloimaan, että vastaukset tulivat vain kyselyyn kutsutuilta tahoilta.

Tutkittavat rekrytoitiin pankki- ja vakuutusalan työntekijöiden joukosta siten, että tutkimuskutsu lähetettiin yksittäiselle yhteyshenkilölle, jota pyydettiin välittämään kutsu tutkimukseen noin kymmenelle kollegalleen yrityksen sisällä. Kutsu tutkimukseen välitettiin sähköpostilla, jossa tutkittaville kerrottiin tutkimuksen kartoittavan työsähköpostin käsittelyyn liittyviä tapoja ja tottumuksia. Kutsussa ei kerrottu tutkimuksen kohdistuvan nimenomaisesti työsähköpostin käsittelyyn tietoturvan näkökulmasta. Tutkimuskutsussa annettiin käyttäjille verkko-osoite, jossa kyselylomakkeeseen pystyi vastaamaan.

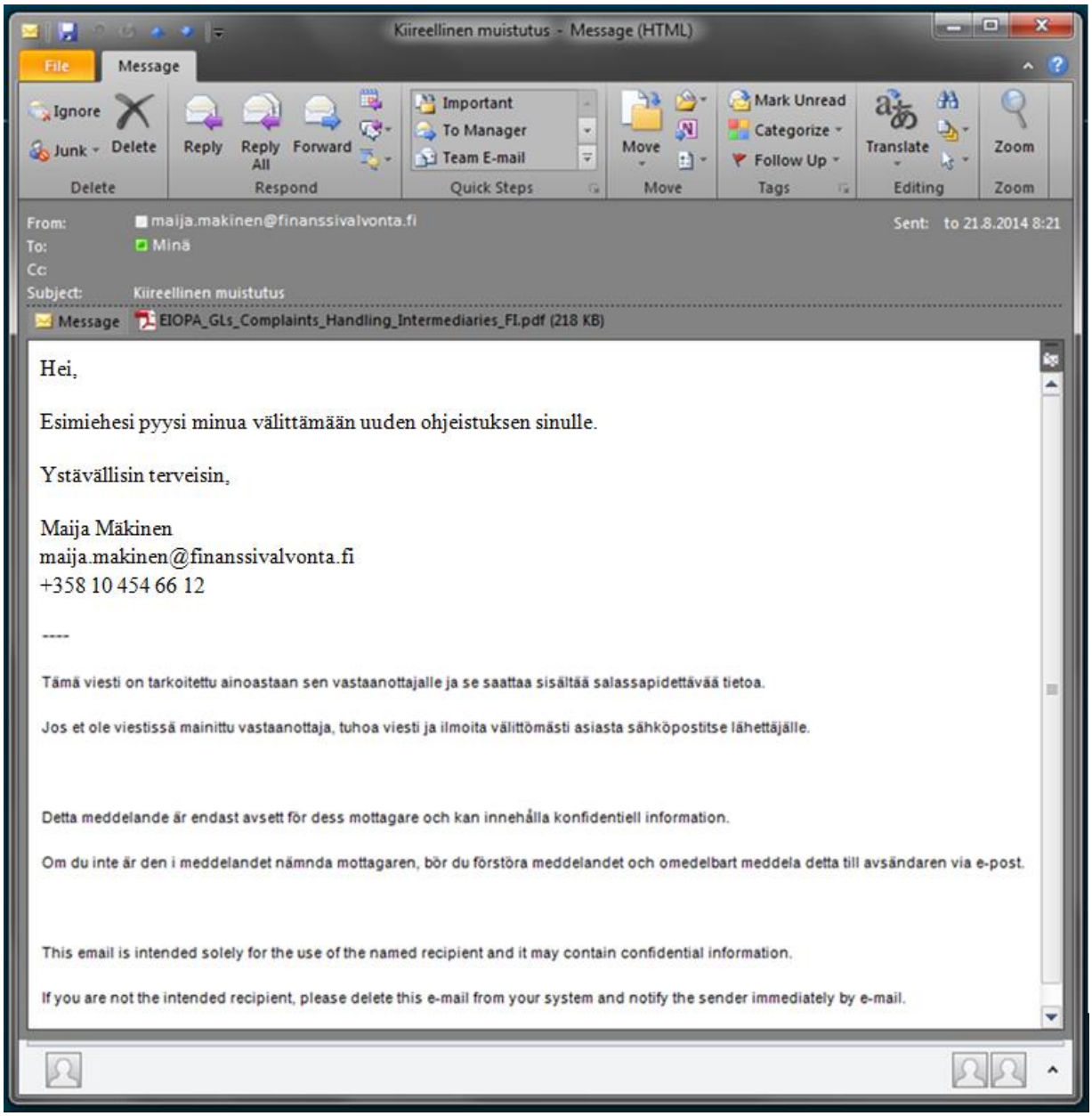
Tutkimusta varten otettiin yhteyttä neljään Suomessa toimivaan organisaatioon, joista kaksi toimii pankkialalla ja kaksi vakuutusalalla. Toisen pankin verkkosivujen suodatin esti tutkittavien pääsyn kyselytutkimukseen, minkä vuoksi kyseisestä organisaatiosta ei saatu lainkaan vastauksia tutkimukseen. Jokaisesta organisaatiosta vastaajia oli 10 henkeä, eli vastauksia saatiin yhteensä 30 kappaletta.

Tutkimuksen huijaussähköposti kohdistettiin pankki- ja vakuutusalan työntekijöille relevantiksi valitsemalla viestin lähettäjän organisaatioksi toimialaa valvova viranomainen. Viestissä kehotettiin tutkittavaa avaamaan viestin liitteenä oleva liitetiedosto, joka nimeltään ja tiedostomuodoltaan vastaa todellisia viranomaisen verkkosivuillaan julkaisemia dokumentteja. Viestin sisällössä annettiin viestin lähettämiselle syyksi, että vastaanottajan esimies oli pyytänyt toimittamaan viestin.

3.2.1 Kyselylomakkeella esitetyt sähköpostit

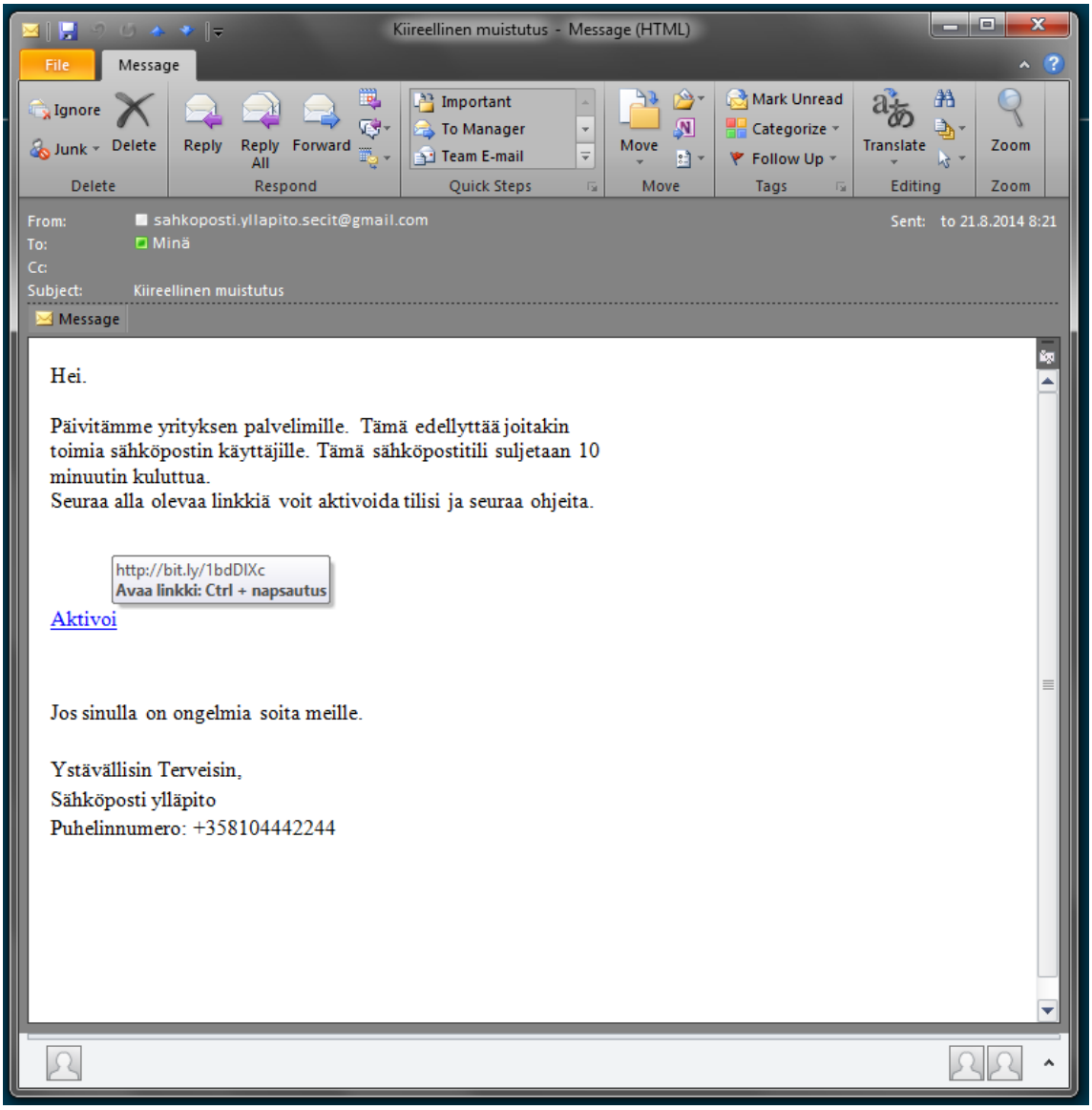
Esimerkki sähköpostit mukailevat ominaisuuksiltaan kirjallisuus katsauksessa esitettyjä kohdistetun huijaussähköpostin ja perinteisen huijaussähköpostin ominaisuuksia. Erityisesti konkreettisia elementtejä viestien rakenteesta ja esitysasusta sovellettiin Halevi ym. (2013) tutkimuksessa esitettyjen esimerkkien pohjalta.

Lähettäjäksi esitetään toimialan valvovaviranomainen ja liitetiedostona on oikean nimeämistavan mukainen dokumentti valvojaviranomaiselta. Viestin otsikko ja teksti pitää sisällään kiireellisyys elementin, joka on keskeinen monissa huijaussähköposteissa ja viitataan esimiehen ohjeistaneen dokumentin toimittamisen, joka mahdollisesti vähentää epäilystä uhrissa. Viestin allekirjoitus tarjoaa käyttäjälle mahdollisuuden ottaa yhteyttä viestin lähettäjään, joka aikaisemman tutkimuksen mukaisesti luo luotettavuuden tunnetta ja viestin lopussa on monissa yrityksissä käytössä oleva sähköpostiviestiin automaattisesti lisättävä loppuhuomio, että viesti on tarkoitettu vain vastaanottajalle. Kohdistettu huijaussähköpostiviesti on esitetty alla.



KUVIO 4 : Sähköposti 1 - Kohdistettu huijaussähköposti

Vertailukohtana tutkimuksessa käytettiin ei personoitua, perinteisempää huijaussähköpostia, joka on esitetty alla. Viesti pitää sisällään monia tunnusmerkkejä, joista käyttäjän pitäisi viesti tunnistaa huijaussähköpostiksi. Viestin lähettäjä on yleinen ilmaissähköpostipalvelun osoite ja viestissä on useita kirjoitusvirheitä. Lisäksi viestin linkki osoitti naamioituun verkko-osoitteeseen, josta ei käy ilmi todellista osoitetta.



KUVIO 5: Sähköposti 2 - Perinteinen huijaussähköposti

3.2.2 Kyselylomake

Tutkittaville välitettiin työsähköposteihin kutsut tutkimukseen osallistumiseen, josta oli linkki kyselylomakkeelle, joka oli tarjolla verkkopalvelussa. Kyselyn kutsussa ja etusivulla kerrottiin, että tutkimuksessa keskitytään työsähköpostin käsittelyyn liittyviin asioihin, eikä tutkittaville kerrottu kyseessä olevan tietoturvaan liittyvä kyselylomake ja tutkimus. Kutsussa ja kyselyn etusivulla korostettiin myös kyselyn luottamuksellisuutta ja sitä, että tällä ei ole tekemistä tutkittavien työnantajaorganisaatioiden kanssa.

Kyselylomakkeella tutkittavia pyydettiin vastaamaan ensin taustatietokysymyksiin.

- tietotekniikan käytön mieluisuus
- osaaminen

Tämän jälkeen esitettiin ensimmäinen sähköpostiviesti ja tutkittavaa pyydettiin tutustumaan viestiin. Sähköpostiviestin esittämisen yhteydessä tiedusteltiin tutkittavalta kuinka todennäköisesti hän avaisi töissä tämän sähköpostiviestin liitetiedoston. Viestin liitetiedoston avaamisen todennäköisyyttä kysyttiin asteikolla: 1 - ei ollenkaan todennäköistä, 2 - hieman todennäköistä, 3 - melko todennäköistä sekä 4 - hyvin todennäköistä. Liitteen avaamisen todennäköisyyttä käsitellään tässä tutkimuksessa huijatuksi tulemisen todennäköisyytenä kohdistetulla huijaussähköpostilla. Tämän jälkeen tutkittava siirtyi seuraavalle sivulle kyselyssä, jossa sähköpostiviesti ei ollut enää nähtävillä. Seuraavaksi käyttäjää pyydettiin arvioimaan edellisessä vaiheessa esitettyä sähköpostia (sähköposti 1) ilman, että viesti oli enää esillä. Tutkittavaa pyydettiin arvioimaan sähköpostiviestin lähettäjän luotettavuutta, viestin ulkoasun uskottavuutta, viestin sisällön uskottavuutta sekä viestin liitetiedoston luotettavuutta pyytämällä vastaukset väittämiin:

- Viestin lähettäjä vaikuttaa luotettavalta.
- Viestin ulkoasu (oikeinkirjoitus, kirjoitustyyli ja esitystapa) on uskottava.
- Viestin sisältö on uskottava.
- Viestin liitetiedosto vaikuttaa luotettavalta.

Edellä esitettyjä viestin ominaisuuksia arvioitiin asteikolla: 1 - täysin eri mieltä, 2 - osittain eri mieltä, 3 - osittain samaa mieltä, 4 - täysin samaa mieltä. Vapaaehtoisesti tutkittavaa pyydettiin myös kommentoimaan vapaaseen tekstikenttään havaintoja sekä huomioita.

Seuraavassa vaiheessa kyselylomakkeella esitettiin tutkittavalle toinen sähköpostiviesti (Sähköposti 2), samalla ohjeistuksella kuin aikaisemmin. Sähköpostiviestin yhteydessä tutkittavalta kysyttiin kuinka todennäköisesti hän avaisi viestissä olleen linkin. Viestin linkin avaamisen todennäköisyyttä kysyttiin asteikolla: 1 - ei ollenkaan todennäköistä, 2 - hieman todennäköistä, 3 - melko todennäköistä sekä 4 - hyvin todennäköistä. Tämän jälkeen tutkittava siirtyi seuraavalle sivulle kyselyssä, jossa sähköpostiviesti ei ollut enää nähtävillä. Seuraavaksi viestin ominaisuuksia pyydettiin arvioimaan vastaavalla tavalla kuin edellä esitettyä ensimmäistäkin sähköpostiviestiä. Eli tutkittavien tuli vastata väittämiin lähettäjän luotettavuudesta, viestin ulkoasusta, sisällöstä ja viestissä olevan linkin luotettavuudesta. Tutkittaville tarjottiin myös mahdollisuus kirjoittaa vapaaehtoiseen tekstikenttään kommentteja sekä huomioita sähköpostiviestistä.

Kahden sähköpostiviestin jälkeen tutkittaville esitettiin kolme sähköpostin riskeihin liittyvää väittämää, jotka kartoittivat tutkittavien käsitystä työnantajan riskeistä liittyen sähköpostin käyttämiseen. Väittämiä arvioitiin samalla asteikolla, jota käytettiin sähköpostiviestien väittämien arviointiin: 1 - täysin eri

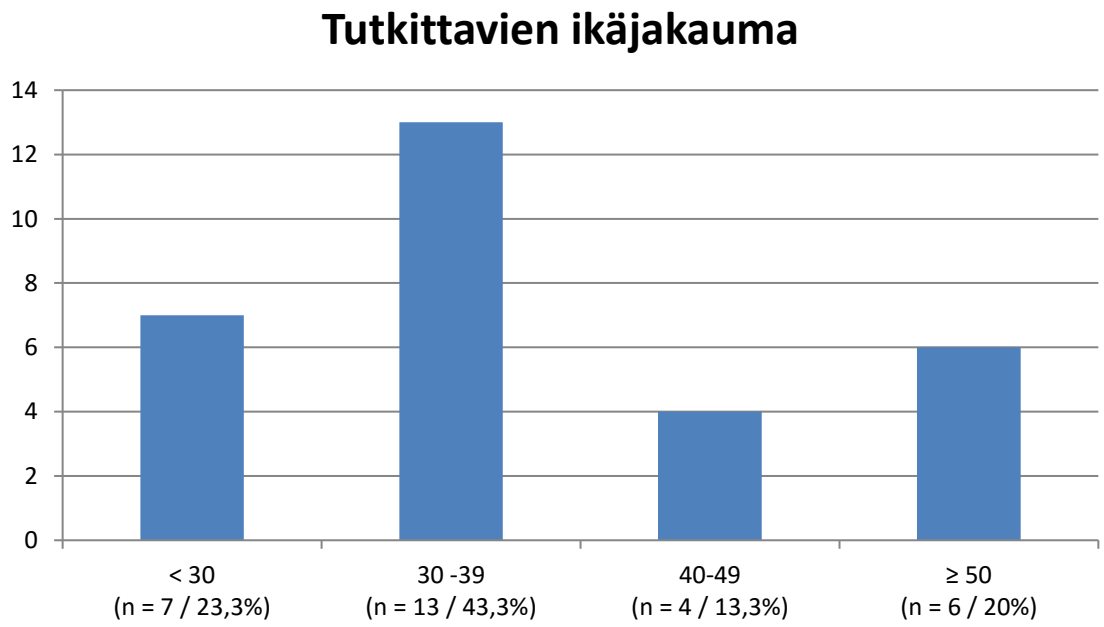
mieltä, 2 - osittain eri mieltä, 3 - osittain samaa mieltä, 4 - täysin samaa mieltä. Sähköpostin riskiin liittyvät väittämät olivat:

- Sähköpostit voivat olla merkittävä riski työpaikkasi tietoturvalle
- Tietoturvan vaarantumisesta voi aiheutua vakavia vahinkoja asiakkaillenne
- Tietoturvan vaarantumisesta voi aiheutua vakavia vahinkoja työnantajallesi

Lopuksi tutkittavilta pyydettiin yhteystiedot arvontaan osallistumista varten ja tarjottiin mahdollisuus antaa palautetta kyselystä.

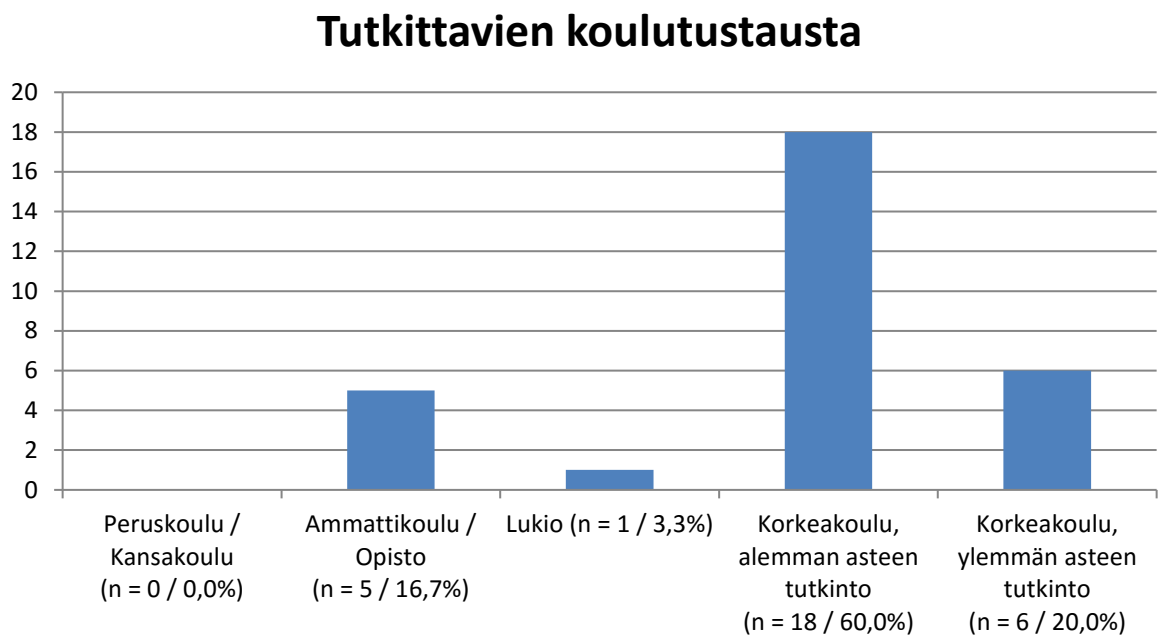
3.3 Tutkittavat

Tutkimuksen kyselyyn vastasi 30 henkilöä (N=30, 23 naista ja 7 miestä) ja tutkittavien keski-ikä oli 37,87 vuotta. Tutkittavien ikäjakauma on esitetty KUVIO 6: Tutkittavien ikäjakauma. Vastaajista 7 henkilöä oli alle 30-vuotiaita, 13 oli iältään 30-39-vuotiaita, 4 oli 40-49-vuotiaita ja 6 henkilöä yli 50-vuotiaita. Tutkimukseen vastasi kolme eri yrityksen työntekijöitä, joista kaksi yritystä edustivat vakuutusalan yrityksiä ja yksi oli pankki- ja rahoitusalan yritys. Eli kaikki tutkittavat työskentelivät pankki- tai vakuutusalalla. Tutkittavat vastasivat vapaamuotoisesti työtehtävä tai työnimike kysymykseen. Tutkittavista 14 oli päälliköitä tai johtajia, 7 oli erilaisia asiantuntijoita, 7 palveluneuvojia tai toimihenkilöitä, 1 sihteeri ja 1 suunnittelija.



KUVIO 6: Tutkittavien ikäjakauma

Tutkimukseen vastanneiden koulutustausta on esitetty Kuviossa 7. Tutkimukseen vastanneista suurin osa, 18 henkilöä (60%), oli suorittanut alemman korkeakoulututkinnon. Ammattikoulun tai -opiston oli suorittanut 5 henkilöä, lukion yksi henkilö ja ylemmän korkeakoulututkinnon oli suorittanut 6 henkilöä.



KUVIO 7: Tutkittavien koulutustausta

Tutkittavilta kysyttiin iän ja koulutustaustan lisäksi muita taustatietoja ennen varsinaisia tutkimuskysymyksiä. Taustatietojen avulla voidaan luokitella käyttäjien ominaisuuksia. Taustatietojen vastaukset on listattu alla **Error! Reference source not found.**. Taulukossa on esitetty vapaa-ajalla käytettävät laitteet sekä vapaa-ajalla käytettävät verkkopalvelut, joihin tutkittavat vastasivat kyllä-ei-periaatteella. Vapaa-ajan internetin käyttöä, tietotekniikan käytön mieluisuutta ja tietotekniikan koettua osaamista kysyttiin järjestysasteikollisella muuttujalla.

Tutkittavista suurella osalla oli käytössä vapaa-ajalla älypuhelin (n = 28 / 93%) ja tietokone (n = 26 / 87%), kahdella kolmesta (n = 20 / 67%) oli käytössään tabletti-laite sekä seitsemällä (n = 7 / 23%) älytelevisio. Lähes kaikki tutkittavat ilmoittivat joskus käyttäneensä vapaa-ajalla verkkopankkia, verkkokauppaa tai sosiaalisen median palveluita. Suomalaisista työikäisistä (16-74 vuotias) 66% käyttää internettiä päivittäin ja 61%:lla on käytössään älypuhelin (Suomen virallinen tilasto, 2013). Tutkimukseen osallistuneet siis käyttivät enemmän intenetiä ja omistivat älypuhelimia useammin kuin keskiverto suomalaiset.

Suuri osa tutkittavista koki tietotekniikan käytön erittäin miellyttäväksi (n = 14 / 47%) tai melko miellyttäväksi (n = 13 / 43%) ja vain kolme (n = 3 / 7%) vastasi tietekniikan käytön olevan "ei miellyttävää eikä epämiellyttävää". Kukaan tutkittavista ei kokenut tietotekniikan käyttöä epämiellyttäväksi. Hieman yli puolet (n = 16 / 53%) tutkittavista arvioi tietoteknisen osaamisensa olevan

keskitasoa, yhdeksän (n = 9 / 30%) arvioi osaamisensa kesitasoista paremmaksi ja viisi (n = 5 / 17%) tietoteknisen osaamisensa olevan erittäin hyvä. Tutkittavista kukaan ei arvioinut omaa tietoteknistä osaamistaan keskitasoista huonommaksi tai erittäin huonoksi. Tutkimukseen vastanneiden kokema tietotekniikan käytön mieluisuus ja osaaminen osoittavat siis myönteistä asennetta tietotekniikan käyttöön, kun otetaan huomioon sekin, että kaikki tutkittavat käyttivät työssään päivittäin tietotekniikkaa.

TAULUKKO 1: Tutkittavien taustatiedot

Teema	**Vastauskategoriat**	***n***	%
Vapaa-ajalla käytettävät laitteet	Älypuhelin	28	93
	tabletti-laite	20	67
	tietokone	26	87
	älytelevisio	7	23
Vapaa-ajan käyttö	Verkkopankki	29	97
	Verkkokauppa	29	97
	Sosiaalinen media	27	90
Internetin käyttö	1 - Useasti päivässä	25	83
	2 - Kerran päivässä	3	10
	3 - Harvemmin kuin päivittäin	2	7
	4 - Harvemmin kuin viikoittain	0	0
	5 - Ei käytä vapaa-ajalla internettiä	0	0
Tietotekniikan käytön koettu mieluisuus	1 - Erittäin miellyttävää	14	47
	2 - Melko miellyttävää	13	43
	3 - Ei miellyttävää eikä epämiellyttävää	3	10
		0	0
	4 - Melko epämiellyttävää	0	0
	5 - Erittäin epämiellyttävää		
Koettu osaaminen	1 - Erittäin hyvä	5	17
	2 - Keskitasoista parempi	9	30
	3 - Keskitasoinen	16	53
	4 - Keskitasoista huonompi	0	0
	5 - Erittäin huono	0	0

3.4 Aineiston analysointi

Tilastollisena analyysimenetelmänä tutkimuskysymyksen tarkastelussa, eli tarkasteltaessa mitkä tekijät ovat yhteydessä todennäköisyyteen tulla huijatuksi kohdistetulla huijausviestillä, käytettiin lineaarista regressioanalyysia. Tutki-

muskysymykseen vastaamisessa lineaarisella regressioanalyysillä saadaan selville selittävien muuttujien lineaarinen yhteys selitettävään muuttujaan. Korrelaatiokertoimien avulla voidaan tarkastella selittävien muuttujien korrelointia selitettään muuttujaan. (Nummenmaa, 2006, sivut 297-317)

Tässä tutkimuksessa regressioanalyysiin valittiin korrelaatioiden perusteella ne muuttujat, jotka korreloivat tilastollisesti merkittävästi kohdistetun huijaussähköpostin liitteen avaamisen kanssa, eli huijatuksi tulemisen kanssa. Analyysi toteutettiin SPSS-tilasto-ohjelmistolla (versio 24), johon tutkimusmateriaali koottiin kyselylomakejärjestelmästä.

4 TULOKSET

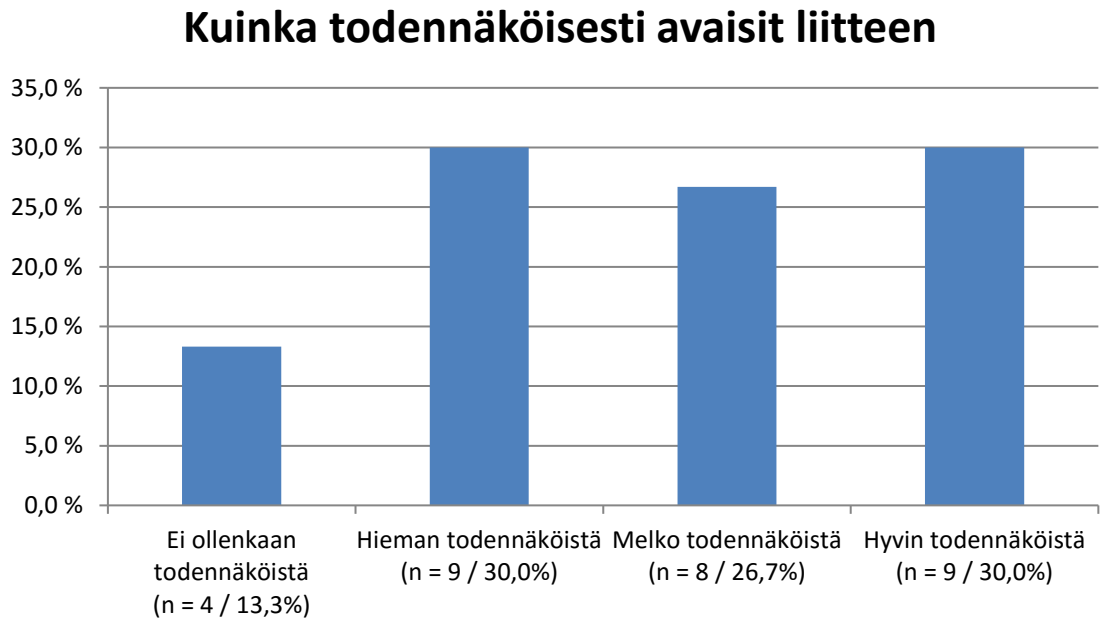
Tässä kappaleessa esitellään tutkimuksen tulokset ja tutkimuskysymykseen vastaaminen.

4.1 Kuvailevat tulokset

Tässä kappaleessa esitetään kuvailevat tulokset tutkimuksesta. Kappale on jaettu siten, että aluksi käydään läpi kohdistetun huijaussähköpostin, eli Sähköpostin 1, vastaukset ja seuraavaksi vastaavat vastaukset perinteisestä huijaussähköpostista, eli Sähköposti 2. Seuraavaksi on lyhyt yhteenveto vapaamuotoisista vastauksista ja lopuksi on esitelty tietoturvariskitietoisuuden kuvailevat tulokset.

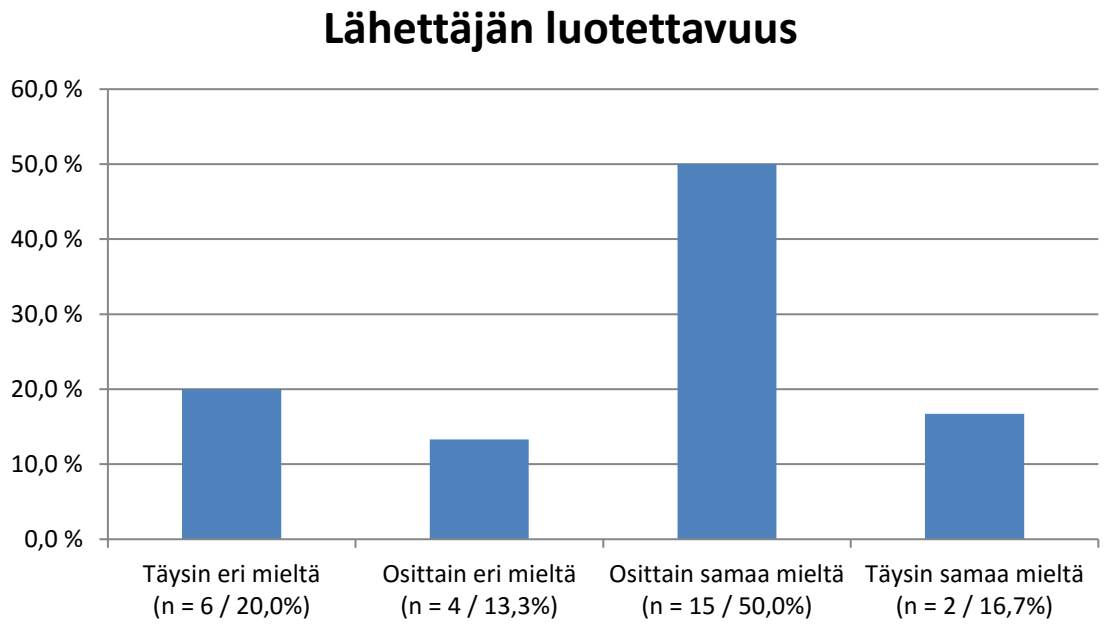
4.1.1 Sähköposti 1 - kohdistettu huijaussähköposti

Tutkittavalle näytettiin kuva sähköpostiviestistä (sähköposti 1) ja kysyttiin: "Kuinka todennäköistä on, että avaisit edellä esitetyn sähköpostiviestin liitetiedoston?", tulokset on esitetty alla Kuviossa 8. Liitteen avaaminen viittaa tässä tapauksessa huijatuksi tulemiseen, sillä kohdistetun huijaussähköpostin liitteen avaaminen voisi mahdollistaa hyökkääjälle pääsyn liitteen avaajan tietokoneeseen. Vastaukset jakaantuivat kohtuullisen tasaisesti, mutta kuitenkin yli puolet vastanneista (n = 17 / 56,6%) avaisi melko tai hyvin todennäköisesti viestin liitetiedoston.



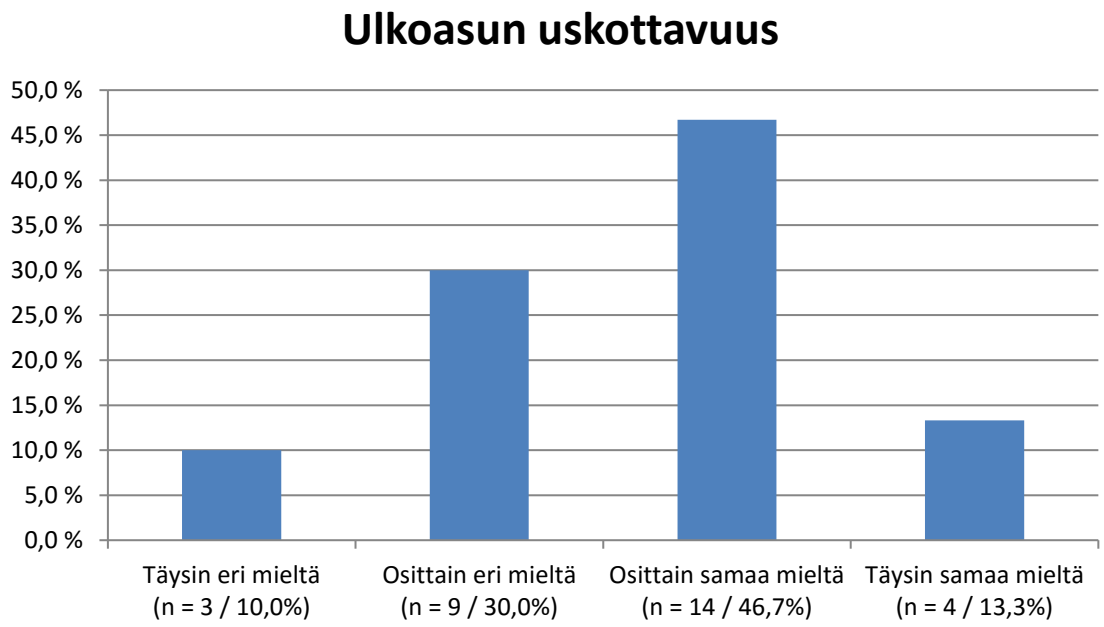
KUVIO 8: Sähköposti 1 - Liitteen avaamisen todennäköisyys

Tutkittavia pyydettiin sähköpostin esittämisen ja liitteen avaamiskysymyksen jälkeen arvioimaan tarkemmin esitettyä sähköpostiviestiä esittämällä väittämiä lähettäjän luotettavuus, ulkoasun ja sisällön uskottavuus sekä liitteen luotettavuus. Lähettäjän luotettavuuden vastaukset on esitetty Kuviossa 9, josta voidaan havaita, että yli puolet vastaajista (n = 17 / 56,6%) pitää lähettäjää luotettavana, eli vastasi väittämään osittain tai täysin samaa mieltä. Kuten korrelaatiotaulukosta (Taulukko 3) voidaan havaita, lähettäjän arvioiminen luotettavaksi ja edellä esitetty liitteen avaamisen todennäköisyys korreloivat tilastollisesti merkitsevästi (.56**).



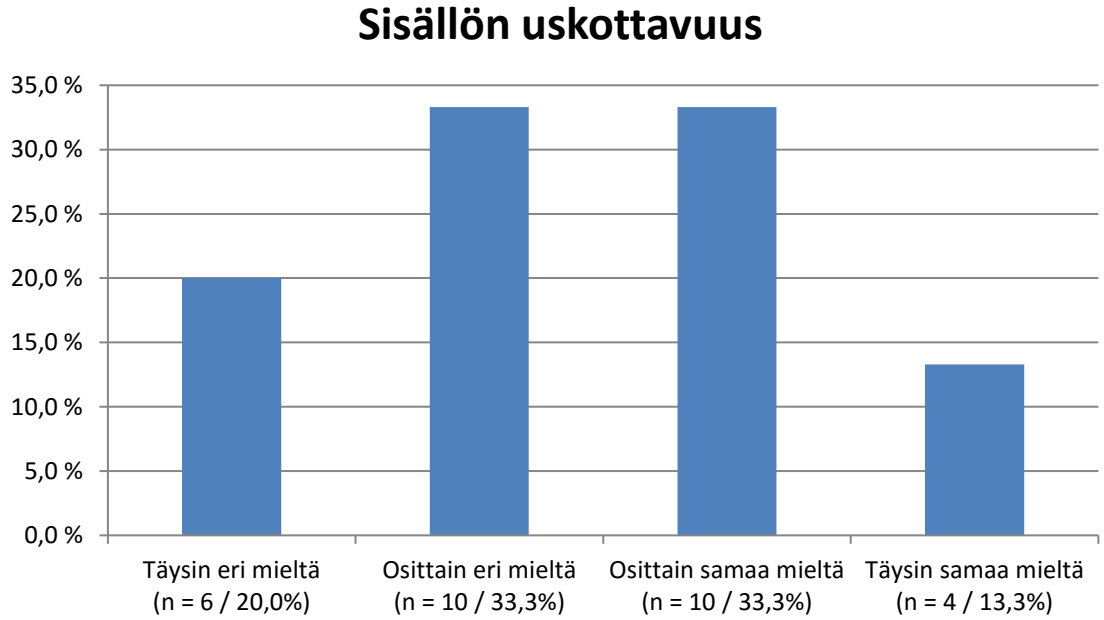
KUVIO 9: Sähköposti 1 - Lähettäjän luotettavuus

Sähköpostiviestin ulkoasun uskottavuuden vastaukset on esitetty alla Kuviossa 10, josta voidaan havaita, että ulkoasua, piti osittain tai täysin luotettavana, yli puolet vastaajista (n = 18 / 60,0%). Toisin kuin muut viestin omaisuuksia mittaavat väitteet, ulkoasun uskottavuus ei korreloinut tilastollisesti merkitsevästi (.31) liitteen avaamisen todennäköisyyden kanssa.



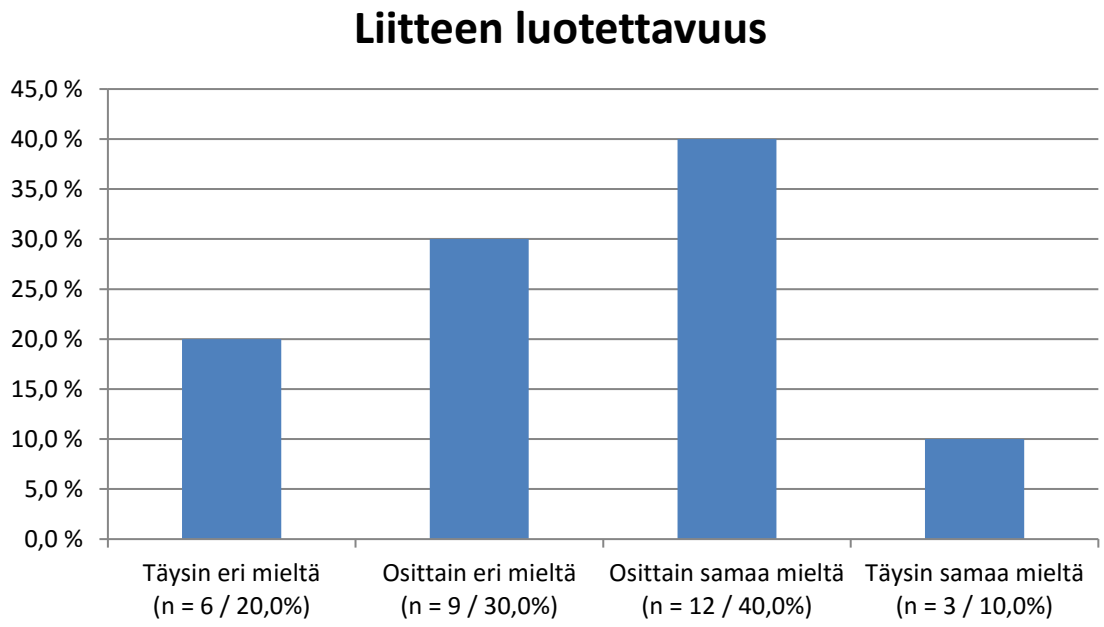
KUVIO 10: Sähköposti 1 - Ulkoasun uskottavuus

Vastaukset sisällön uskottavuudesta jakautui muita viestin ominaisuuksia tasaisemmin, kuitenkin niin, että hieman yli puolet (n = 16 / 53,3%) vastanneista oli täysin tai osittain erimieltä väittämästä "viestin sisältö on uskottava". Sisällön uskottavaksi arvioiminen ja huijatuksi tulemisen todennäköisyys, eli liitteen avaamisen todennäköisyys, korreloivat tilastollisesti merkitsevästi (.51**).



KUVIO 11: Sähköposti 1 - Sisällön uskottavuus

Liitteen luotettavuuden vastaukset on esitetty alla Kuviossa 12, josta voidaan havaita, että puolet vastaajista (n = 15 / 50,0%) pitää liitettä luotettavana, eli vastasi väittämään osittain tai täysin samaa mieltä. Kuten korrelaatiotaulukosta (Taulukko 3) voidaan havaita, liitteen arvioiminen luotettavaksi ja liitteen avaamisen todennäköisyys korreloivat tilastollisesti merkitsevästi (.57**).

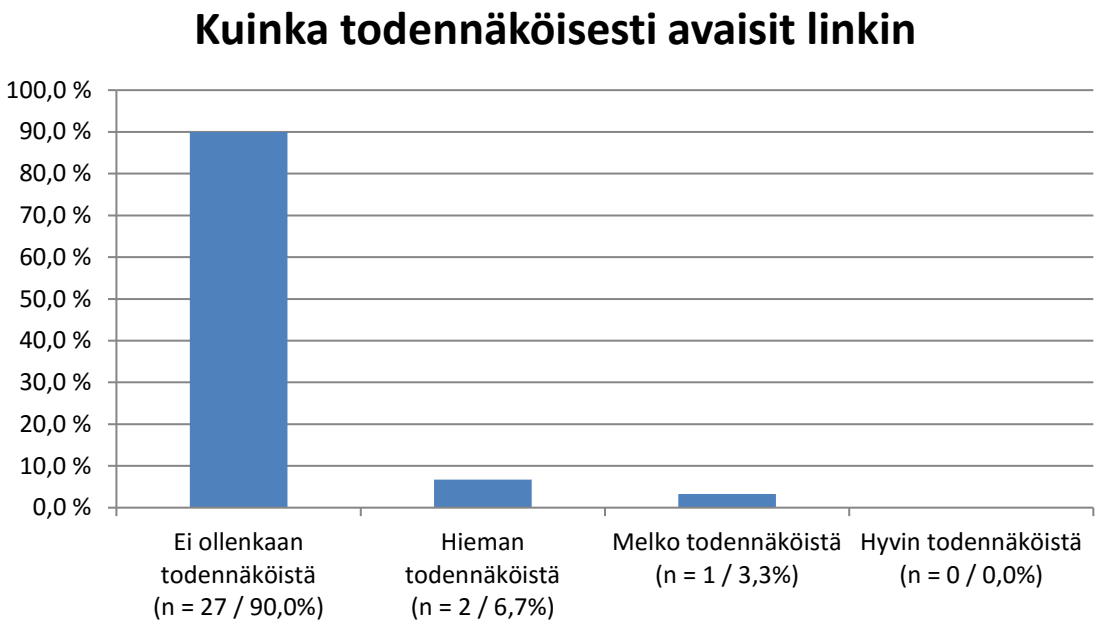


KUVIO 12: Sähköposti 1 - Liitteen luotettavuus

4.1.2 Sähköposti 2 - perinteinen huijaussähköposti

Sähköposti 2 edusti perinteisempää, ei personoitua, huijaussähköpostia. Huijauksen onnistumisen ja tämän tutkimuksen näkökulmasta keskeistä on millä todennäköisyydellä tutkittava avaisi sähköpostissa olevan linkin. Käyttäjän avatessa linkin voidaan olettaa, että pahantahtoinen hyökkääjä voi päästä ohjaamaan käyttäjän verkkosivulle, josta selaimen välityksellä voi latautua koneelle haitallista ohjelmakoodia.

Tutkittavalle näytettiin kuva sähköpostiviestistä (Sähköposti 2) ja kysyttiin: "Kuinka todennäköistä on, että avaisit edellä esitetyn sähköpostiviestin linkin?", vastaukset on esitetty alla Kuviossa 13. Linkin avaaminen viittaa tässä tapauksessa huijatuksi tulemiseen, sillä huijaussähköpostin linkin avaaminen voisi mahdollistaa hyökkääjälle pääsyn linkin avaajan tietokoneeseen verkkoselaimen haavoittuvuuden välityksellä. Vastaukset vinoutuvat voimakkaasti ja lähes kaikki vastaajat (n = 27 / 90%) eivät avaisi todennäköisesti sähköpostilinkkiä.



KUVIO 13: Sähköposti 2 - Linkin avaamisen todennäköisyys

Sähköpostin esittämisen ja linkin avaamiskysymyksen jälkeen tutkittavia pyydettiin arvioimaan tarkemmin esitettyä sähköpostiviestiä (Sähköposti 2) esittämällä väittämiä lähettäjän luotettavuus, ulkoasun ja sisällön uskottavuus sekä liitteen luotettavuus. Jatkokysymykset olivat täsmälleen samat kuin ensimmäisen sähköpostiviestin tapauksessa. Kaikki vastaukset on esitetty alla Taulukossa. Tarkemmat arviot Sähköpostin 2 ominaisuuksista ovat linkin avaamisen todennäköisyyden mukaisesti voimakkaasti vinoutuneet.

TAULUKKO 2: Sähköposti 2 - Viestin ominaisuuksien vastausten yhteenveto

Ominaisuus	**Vastauskategoriat**	***n***	**%**
Lähettäjän luotettavuus	1 - Täysin eri mieltä	25	83,3
	2 - Osittain eri mieltä	4	13,3
	3 - Osittain samaa mieltä	1	3,3
	4 - Täysin samaa mieltä	0	0
Ulkoasun uskottavuus	1 - Täysin eri mieltä	22	73,3
	2 - Osittain eri mieltä	6	20,0
	3 - Osittain samaa mieltä	2	6,7
	4 - Täysin samaa mieltä	0	0
Sisällön uskottavuus	1 - Täysin eri mieltä	26	86,7
	2 - Osittain eri mieltä	4	13,3
	3 - Osittain samaa mieltä	0	0
	4 - Täysin samaa mieltä	0	0

Linkin luotet-	1 - Täysin eri mieltä	27	90,0
tavuus	2 - Osittain eri mieltä	3	10,0
	3 - Osittain samaa mieltä	0	0
	4 - Täysin samaa mieltä	0	0

4.1.3 Avoimet vastaukset

Tutkittavilta kysyttiin avoimella kysymyksellä esitettyihin sähköpostiviesteihin liittyviä vapaamuotoisia havaintoja ja huomioita. Sähköpostin 1 vapaamuotoisia kommentteja jätti 16 tutkittavaa ja Sähköpostiin 2 jätti kommentin 15 tutkittavaa. Kaikki Sähköpostiin 2 kommentoineet kommentoivat myös Sähköpostia 1. Yleisesti kaikista kommenteista ja huomioista huomaa, että tutkittavat vertasivat esitettyjä sähköpostiviestejä omaan työympäristöönsä.

Sähköposti 1 oli tutkittavien kommenttien perusteella osalle hyvin työympäristön sähköpostiviestintää muistuttava, mutta 4 tutkittavaa kommentoivat, että sähköposti ei muistuta oman työympäristön sähköposteja. Tutkittavista, jotka vastasivat, että avaisivat Sähköpostin 1 liitteen melkein tai hyvin todennäköisesti, mainitsivat, että sähköpostin lähettäjä on vakuuttava, mutta muutamat tutkittavat kommentoivat, että varmasti keskustelisivat asiasta esimiehensä kanssa. Muutama henkilö epäili myös viestiä huijaukseksi, vaikka olivat aikaisemmin vastanneet, että melko tai hyvin todennäköisesti avaisi liite tiedoston.

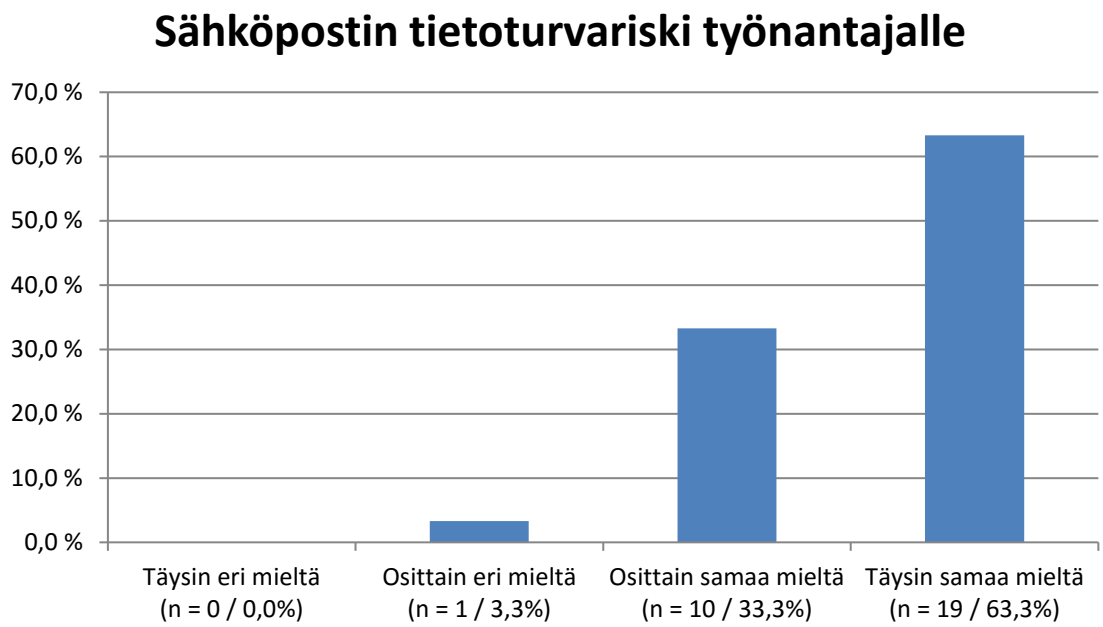
Tutkittavista kolme, jotka vastasivat avaavansa liitetiedoston hieman todennäköisesti kommentoivat, että kysyisivät viestistä esimieheltään tai kollegoilta ennen viestin liitteen avaamista, mutta samalla pitivät lähettäjää ja ulkoasua uskottavana. Yksi tutkittavista kommentoi, että avaisi liitteen kuitenkin, koska työkoneella sähköpostin liitteisiin voi luottaa aina. Yksi tutkittavista, joka vastasi, että ei lainkaan todennäköisesti avaisi liitettä, kommentoi, että varmasti työkiireessä saattaisi avata liitetiedoston, vaikka tutkimuksessa vastasi, että ei avaisi esimerkki sähköpostin liitettä.

Sähköpostista 2 kommentoitiin yleisesti, että näin huonosti kirjoitettuja ja epäselviä viestejä ei työsähköpostiin tule. Yksi tutkittavista mainitsi, että tiukka aikaraja herättää erityisesti epäilyjä. Sähköpostiin 2 kommentoineista 5 kiinnitti huomiota sähköpostin lähettäjän osoitteeseen, joka oli ilmaisen sähköpostipalvelun gmail-osoite. Sähköpostin 2 kommenteissa kukaan tutkittavista ei maininnut linkin todellisen URL-osoitteen piilottamista epäilyttävän.

4.1.4 Riskitietoisuus

Kahden sähköpostin esittämisen jälkeen tutkittavilta kysyttiin sähköpostin merkitystä organisaation tietoturvalle kolmella eri väittämällä ja tällä kartoitettiin tutkittavien riskitietoisuutta. Sähköpostin riskiä työpaikan tietoturvalle kysyttiin

väittämällä: "Sähköpostit voivat olla merkittävä riski työpaikkasi tietoturvalle?", jonka vastaukset on esitetty alla Kuviossa 14. Tutkittavista lähes kaikki (n = 29 / 96,6%) olivat täysin tai osittain samaa mieltä väittämän kanssa.

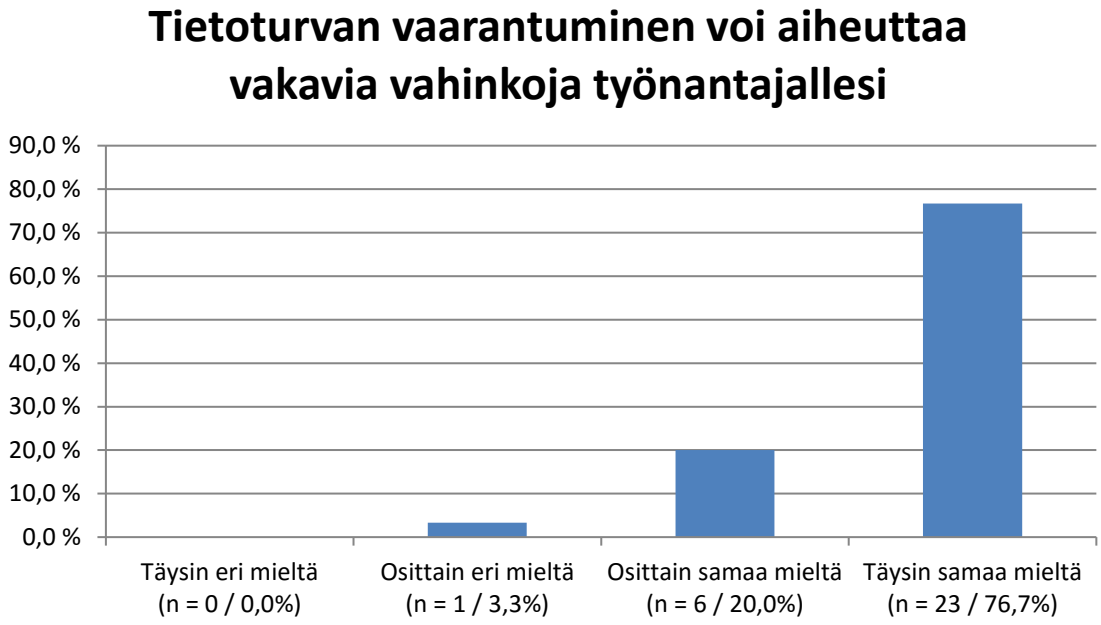


KUVIO 14: Sähköpostin tietoturvariski työnantajalle

Tietoturvan vaarantumisen merkitystä organisaation asiakkaille kysyttiin väittämällä: "Tietoturvan vaarantumisesta voi aiheutua vakavia vahinkoja asiakkaillenne?"", ja vastaukset on esitetty Kuviossa 15 alla. Kahta tutkittavaa lukuun ottamatta kaikki (n = 28 / 93,3%) olivat täysin tai osittain samaa mieltä väittämän kanssa.

KUVIO 15: Tietoturvan vaarantumisen vahinkomahdollisuus asiakkaille

Tietoturvan vaarantumisen merkitystä omalle organisaatiolle kysyttiin väittämällä: "Tietoturvan vaarantumisesta voi aiheutua vakavia vahinkoja työnantajallesi?"", vastaukset löytyvät alta Kuviossa 16. Edellisten riskitietoisuusväittämien mukaisesti lähes kaikki tutkittavat (n = 29 / 96,6%) olivat täysin tai osittain samaa mieltä väittämän kanssa.



KUVIO 16: Tietoturvan vaarantumisen vahinkomahdollisuus työnantajalle

4.2 Tutkimuskysymykseen vastaaminen

Yhteenvetona korrelaatioista, jotka ovat listattuna alla Taulukossa 3, voidaan todeta, että kohdistetun huijaussähköpostin (sähköposti 1) liitteen avaamisen todennäköisyys, eli huijatuksi tulemisen todennäköisyys, korreloi tilastollisesti merkittävästi lähes kaikkien kyseisen sähköpostin ominaisuuksien kanssa: lähettäjän luotettavuus (.56**), sisällön uskottavuus (.51**) ja liitteen luotettavuus (.57**). Ainoa ominaisuus, jonka kanssa tilastollisesti merkittävää korrelaatiota ei esiintynyt oli ulkoasun uskottavuus (.31). Sähköpostin ominaisuuksien lisäksi huijatuksi tulemisen todennäköisyys korreloi tilastollisesti merkitsevästi tietotekniikan käytön koetun mieluisuuden kanssa (.46*). Lisäksi kohdistetulla huijaussähköpostilla huijatuksi tuleminen korreloi tilastollisesti merkitsevästi sähköpostiin liittyvän riskitietoisuuden kanssa (-.40*) ja sen kanssa, miten tietoinen on yrityksen tietoturvan vaarantumisesta aiheutuvista vahingoista (-.46*). Mitä tietoisempi on sähköpostin tietoturvariskistä organisaatiolle, sitä todennäköisemmin ei avaa kohdistetun huijaussähköpostin liitettä, eli ei tule huijatuksi. Vastaavasti mitä tietoisempi sähköpostin tietoturvan vaarantumisesta aiheuttamista vahingoista organisaatiolla, sitä todennäköisemmin ei avaa kohdistetun huijaussähköpostin liitettä, eli ei tule huijatuksi.

TAULUKKO 3: Muuttujien keskiarvot (*kh*), keskihajonnat (*kh*) ja korrelaatiot.

Muuttuja	*ka(kh)*	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.
1. Ikä	37,87(10,16)	–																		
2. Sukupuoli	-	.19	–																	
3. Koulutus	-	–.15	.37*	–																
4. Internetin käyttö	1,23 (0,57)	.12	–.25	–.16	–															
5. Koettu mieluisuus	1,63 (0,67)	.04	–.16	.03	.03	–														
6. Koettu osaaminen	2,37 (0,77)	.16	–.47**	–.18	.27	.26	–													
Sähköposti 1																				
7. Liitteen avaamisen todennäköisyys	2,73 (1,05)	–.09	–.07	.17	–.23	.46*	.04	–												
8. Lähettäjän luotettavuus	2,63 (1,00)	–.04	.09	–.11	–.01	.33	–.08	.56**	–											
9. Ulkoasun uskottavuus	2,63 (0,85)	.20	.17	.12	.04	–.20	.02	.31	.55**	–										
10. Sisällön uskottavuus	2,40 (0,97)	.25	.24	.11	–.28	.12	–.25	.51**	.68**	.57**	–									
11. Liitteen luotettavuus	2,40 (0,93)	.25	.20	.39*	–.16	.23	–.25	.57**	.56**	.42*	.71**	–								
Sähköposti 2																				
12. Linkin avaamisen todennäköisyys	1,13 (0,43)	.10	.10	.36	–.15	–.14	.11	.20	.06	.42*	.21	.24	–							
13. Lähettäjän luotettavuus	1,20 (0,48)	.13	.40*	.15	–.20	–.13	.02	.14	.11	.43*	.20	.14	.77**	–						
14. Ulkoasun uskottavuus	1,33 (0,61)	.19	.42*	.25	–.27	–.22	–.06	.02	.18	.55**	.48**	.34	.57**	.55**	–					
15. Sisällön uskottavuus	1,13 (0,35)	.19	.02	.31	.07	–.06	.19	.19	.07	. 42*	.25	.29	.85**	.63**	.44*	–				
16. Liitteen luotettavuus	1,10 (0,31)	.11	.08	.35	–.15	–.15	.12	.19	.04	.41*	.20	.24	.99**	.76**	.56**	.85**	–			
Riskitietoisuus																				
17. Arvioitu riski	3,60 (0,56)	.11	–.21	–.31	.01	–.12	–.19	–.40*	–.33	–.21	–.08	–.15	–.20	–.21	–.01	–.30	–.19	–		
18. Arvioidut asiakkaan vahingot	3,60 (0,62	–.15	–.50**	–.05	.15	–.13	–.03	–.30	–.15	–.24	–.05	–.13	–.21	–.51**	–.22	–.30	–.20	.43**	–	
19. Arvioidut yrityksen vahingot	3,73 (0,52)	.15	–.28	–.23	–.13	–.07	–.01	–.46*	–.44*	–.42*	–.18	–.21	–.33	–.43*	–.19	–.45*	–.32	.68**	.61**	–

Huom. Internetin käyttö 1 = useasti päivässä, 4 = ei lainkaan; koettu mieluisuus 1 = erittäin miellyttävä, 4 = erittäin epämiellyttävä; koettu osaaminen 1 = erittäin hyvä, 4 = erittäin huono; muuttujat 7 ja 12 1 =ei lainkaan todennäköistä, 4 = hyvin todennäköistä; muuttujat 8-11 ja 13-16 1 = täysin eri mieltä, 4 = täysin samaa mieltä; muuttujat 17-19 1 = Täysin eri mieltä, 4 = täysin samaa mieltä . * $p < .05$, ** $p < .01$.

Regressioanalyysin sisällytettiin ainoastaan tutkimuskysymyksen kannalta tarpeelliset muuttujat, jotka tilastollisesti merkitsevästi korreloivat selitettävän muuttujan kanssa. Tässä tutkimuksessa näin ollen käytettiin analysointiin useamman selittävän muuttujan regressiomallia, jonka avulla voidaan tarkastella selittävien muuttujien lineaarista suhdetta selitettävään muuttujaan. (Nummenmaa, 2006)

Tutkimusaineisto koottiin tilastoanalyysiohjelmisto SPSS:ään, jonka avulla suoritettiin regressio analyysi. Tässä tutkimuksessa regressioanalyysia ryhdyttiin tekemään ainoastaan niiden muuttujien avulla, jotka olivat tutkimuskysymyksen kannalta relevantteja ja jotka korrelaatiotarkasteluissa korreloivat huijatuksi tulemisen, eli Sähköpostin 1 liitteen avaamisen todennäköisyyden kanssa. Liitteen avaamisen todennäköisyyden korrelaatiot löytyvät edellä esitetystä Taulukosta 3 (ks. muuttuja "7. Liitteen avaamisen todennäköisyys"). Regressioanalyysiin valittiin selittäviksi muuttujiksi kaikki muuttujan 7 kanssa korreloineet muuttujat. Näin ollen analyysiin sisällytettiin seuraavat selitettävä muuttuja sekä kuusi selittävää muuttujaa:

- Selitettävä muuttuja:
    - Sähköpostin 1 liitteen avaamisen todennäköisyys (eli huijatuksi tulemisen todennäköisyys)
- Selittävät muuttujat:
    - Tietotekniikan käytön koettu mieluisuus
    - Sähköpostin lähettäjän luotettavuus
    - Sähköpostin sisällön uskottavuus
    - Sähköpostin liitteen luotettavuus
    - Arvioitu sähköpostin tietoturvariski
    - Arvioidut yrityksen vahingot tietoturvan vaarantuessa

Malli sopi aineistoon hyvin ($F = 5.61$, $p < .01$), ja sillä voitiin selittää 49 % huijatuksi tulemisen vaihtelusta tutkittavien joukossa korjatun selitysasteen (adjusted R^2) perusteella. Selittävistä muuttujista kuitenkin ainoastaan tietotekniikan käytön koettu mieluisuus osoitti tilastollista trendiä ($p < .10$), kun taas muiden selittäjien regressiokertoimet eivät yltäneet tilastolliseen merkitsevyyteen. Trendi osoitti, että mitä mieluisammaksi tietotekniikan käyttö koettiin, sitä epätodennäköisemmin tuli huijatuksi kohdistetulla huijaussähköpostilla ($\beta = .28$, $p < .10$).

Tarkasteltaessa ja vertailtaessa regressiokertoimia sekä niiden *t*-testisuureita ja *p*-arvoja (Taulukko 4) myös liitteen luotettavuus ja tietoisuus tietoturvan vaarantumisen vahingoista yritykselle vaikuttivat ennustavan huijatuksi tulemista, vaikka kertoimet eivät saavuttaneet yleisesti hyväksyttyä .05-merkitsevyystasoa. Liitteen hyväksi arvioitu luotettavuus näytti ehkäisevän huijatuksi tulemista kohdistetulla huijaussähköpostilla ($\beta = .32$, $p = .135$), samoin kuin korkea tietoisuus tietoturvan vaarantumisen vahingoista yritykselle ($\beta = -.25$, $p = .159$). Merkitsevyydeltään heikommiksi jäivät viestin ominaisuuksista sähköpostin lähettäjän luotettavuus ($\beta = .13$, $p = .562$) ja sisällön uskottavuus ($\beta = .12$, p

= .608). Vastaavasti tietoisuus sähköpostin riskistä (β = -.07, p = .672) jäi merkitsevyydeltään heikommaksi tässä mallissa, kuin tietoisuus tietoturvan vaarantumisen aiheuttamista vahingoista.

TAULUKKO 4: Kuuden selittävän muuttujan lineaarisen regressioanalyysin tulokset kohdistetulla huijaussähköpostilla (sähköposti 1) huijatuksi tulemisen todennäköisyydelle.

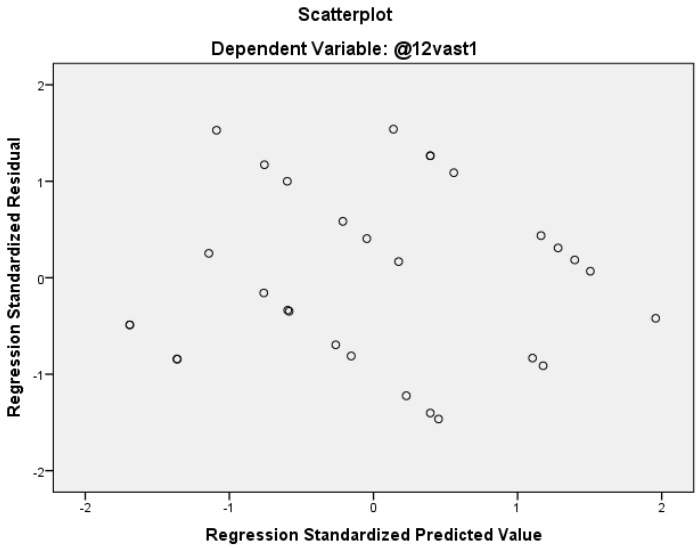
Muuttuja	β	t	p**-arvo**
Tietotekniikan käytön koettu mieluisuus	.28	1.89	.071†
Sähköpostin lähettäjän luotettavuus	.13	0.59	.562
Sähköpostin sisällön uskottavuus	.12	0.52	.608
Sähköpostin liitteen luotettavuus	.32	1.55	.135
Arvioitu sähköpostin riski tietoturvalle	-.07	-0.43	.672
Arvioidut yrityksen vahingot tietoturvan vaarantuessa	-.25	-1.46	.159
Adjusted R^2	.49		
F	5.61		.001**

Huom. β = standardoitu regressiokerroin, t = t-testisuureen arvo, p-arvo = tilastollinen merkitsevyys († p < .10, * p < .05, ** p < .01), Adjusted R^2 = korjattu selitysaste, F = Fisherin F-suhde. Koettu mieluisuus 1 = erittäin miellyttävää, 5 = erittäin epämiellyttävää; liitteen luotettavuus 1 = täysin erimieltä, 4 = täysin samaa mieltä; arvioidut yrityksen vahingot 1 = täysin erimieltä, 4 = täysin samaa mieltä

Regressiomalli edellyttää tiettyjen oletusten toteutumista. Ensinnäkin, selittävät muuttujat eivät saa täysin korreloida toistensa kanssa. Selittävien muuttujien keskinäisiä korrelaatioita ja niiden aiheuttamaa haittaa mallille voidaan arvioida toleransseja tarkastelemalla. Mitä pienempi toleranssi on, sitä kolineaarisempi kyseinen muuttuja on, eli sitä enemmän se korreloi mallin muiden selittävien muuttujien kanssa. Toleranssi voi saada enimmillään arvon 1. Tässä tutki-

muksessa selittävien muuttujien toleranssit vaihtelivat välillä .31-.79. Yleisesti toleransseille ei ole olemassa raja-arvoja, mutta näitä toleransseja voidaan pitää matalahkoina, joskaan ei huolestuttavina. (Nummenmaa, 2006, s. 311)

Lisäksi regressioanalyysi edellyttää, että mallin jäännöstermit ovat toisistaan riippumattomia, satunnaisesti jakautuneita ja, että niiden varianssit ovat yhtä suuria (Nummenmaa, 2006, s. 311-313). Oheisessa sirontakuviossa on havainnollistettu jäännöstermien jakautuminen. X-akselilla on standardoidut, mallin ennustamat selitettävän muuttujan arvot ja y-akselilla niitä vastaavat, standardoidut jäännöstermit. Silloin, kun jäännöstermit täyttävät regressioanalyysin oletukset, ne sijoittuvat 0-akselien molemmille puolille eivätkä muodosta sirontakuvioon säännönmukaista muotoa. Kuten kuvasta nähdään, näyttäisivät jäännökset olevan tässä mallissa satunnaisesti jakautuneita tukien regressiomallin oletuksia jäännöstermeistä.



KUVIO 17: Kuuden selittävän muuttujan lineaarisen regressioanalyysin jäännöstermien sirontakuvio

SPSS-ohjelmiston tulostaman Durbin-Watson-testin avulla voidaan vielä tilastollisesti testata jäännöstermien riippumattomuutta. Jos jäännöstermit ovat toisistaan riippumattomia, testisuure saa suunnilleen arvon 2. Tässä tutkimuksessa Durbin-Watson-testisuure oli 2.18, mitä voidaan pitää hyvänä arvona. (Wooldridge, 2009, s. 415-416)

Kaiken kaikkiaan korrelaatioiden perusteella muodostettu kuuden selittävän muuttujan lineaarinen regressiomalli osoitti trendin, jonka mukaan hyväksi koettu tietotekniikan käytön mieluisuus näyttäisi ehkäisevän huijatuksi tulemista kohdistetulla huijaussähköpostilla. Mallissa ei mikään selittävistä muuttujista ennustanut tilastollisesti merkitsevästi selitettävän muuttujan vaihtelua, vaikka malli yleisesti sopi hyvin aineistoon.

Tutkittavat tulivat todennäköisemmin huijatuiksi sähköpostilla 1 kuin sähköpostilla 2, ja tämä ero oli tilastollisesti merkitsevä, t (29) = -8.45, p < .001). Tämä

tulos oli odotusten mukainen ja linjassa aikaisempien tutkimusten kanssa, eli ihmiset ovat yleisesti hyvin tietoisia perinteisistä huijaus- tai roskasähköposteista.

Tutkimuksessa tehtiin myös tilastoanalyysejä, joista ei saatu tilastollisesti merkitseviä löydöksiä, jotka ovat kuitenkin huomionarvoisia aikaisemman ja mahdollisesti tulevan tutkimuksen kannalta:

- Esimiehet ja työntekijät eivät eronneet toisistaan sähköpostin 1 vastaamistodennäköisyydessä riippumattomien otosten t-testin mukaan, $t\ (28) = -.95$, $p = .35$.
- Koulutustausta ei ollut tilastollisesti merkitsevästi yhteydessä sähköpostin 1 vastaamistodennäköisyyteen, $F\ (3, 26) = .45$, $p = .72$.
- Ikä ei korreloinut sähköpostin 1 liitteen avaamisen todennäköisyyden kanssa (ks. korrelaatiotaulukko)
- Yritysten tai toimiala analysointia ei onnistuttu tekemään, koska useat eivät raportoineet omaa organisaatiotaan ja tutkittavien omat toimialakuvaukset eivät olleet luokiteltavissa analysointia varten.
- Tutkittavien käytettyjen laitteiden tai palveluiden taustalta ei löydetty tilastollisesti merkitseviä yhteyksiä.

5 POHDINTA JA JOHTOPÄÄTÖKSET

Kohdistetut huijaussähköpostit ovat digitaalisen aikakauden haaste organisaatioille, ja koska sähköpostien huijauksen kohteena on organisaation henkilöstö, on teknisten suojaratkaisuiden lisäksi pyrittävä ennaltaehkäisemään yksittäisistä ihmisistä aiheutuvaa riskiä. Tämä tutkimus osoitti, että sekä viestiin liittyvillä ominaisuuksilla että yksilön ominaisuuksilla on yhteyttä huijatuksi tulemiseen kohdistetulla huijaussähköpostilla.

5.1 Tulokset suhteutettuna aiempaan tutkimustietoon

Tämä tutkimus osoitti, että sekä viestiin liittyvillä ominaisuuksilla että yksilön ominaisuuksilla on yhteyttä huijatuksi tulemiseen kohdistetulla huijaussähköpostilla. Mitä mieluisammaksi tutkittavat kokivat tietotekniikan käytön, sitä suuremmalla varauksella he suhtautuivat kohdistettuun huijaussähköpostiin. Viestin ominaisuuksien luottavuuden arviointi oli keskeisessä asemassa sen kanssa, että käyttäjä olisi avannut liitteen ja näin ollen tullut kohdistetun huijaussähköpostin uhriksi, vaikka tilastollisesti merkittävää yhteyttä ei löydetty lineaarisessa regressiomallissa. Korkea riskitietoisuus ja tietoisuus tietoturvan vaarantumisesta aiheutuvista vahingoista pienensi myös riskiä tulla huijatuksi korrelaatioiden perusteella.

Tässä tutkimuksessa tutkittavilta kysyttiin todennäköisyystulkintaa esitetyn kohdistetun huijaussähköpostin avaamisesta. Yli puolet tutkittavista (n = 17 / 56,6%) avaisi melko tai hyvin todennäköisesti viestin liitetiedoston ja vain muutamat (n = 4 / 13,3%) tutkittavat ilmoittivat, että eivät avaisi lainkaan todennäköisesti liitettä. Aikaisemmissa tutkimuksissa, joissa tutkittaville lähetettiin kohdistetut huijaussähköpostit, kohdistetun huijauksen onnistumisprosentit olivat 72% (Jagaticin ym. 2007) ja 80% (Ferguson, 2005). Tämän tutkimuksen tutkittavat eivät siis olleet yhtä valveutuneita kohdistettujen huijaussähköpostien osalta kuin tietotekniikan opiskelijat Jakobsson, ym. (2007) tutkimuksessa. Tämä on linjassa oletuksen kanssa, että tietotekniikan opiskelijat ovat keskivertoa paremmin tietoisia kohdistetuista huijaussähköposteista ja niihin liittyvistä riskeistä. Tämä tukee myös tämän tutkielman regressioanalyysin tulosta, että tietoisuus tietoturvan riskeistä organisaatiolle on yhteydessä huijatuksi tulemisen todennäköisyyteen. Eli valistus, koulutus ja tiedottaminen ovat tärkeitä keinoja organisaation suojautuessa kohdistetulta huijaussähköpostilta. Lisäksi voidaan arvioida, että tietotekniikan opiskelijat kokevat tietotekniikan käytön keskivertoa mieluisammaksi, mikä tukee osaltaan muodostettua regressiomallia.

Tämän tutkimuksen tulokset ovat linjassa myös Vishwanath, ym. (2011) tutkimuksen kanssa siltä osin, että käyttäjien tietoisuus organisaatiolleen aiheu-

tuvista vahingoista tietoturvan vaarantuessa ennakoi parempaa valveutuneisuutta kohdistettuun huijaussähköpostiin. Lisäksi tämän tutkimuksen, kuten myös kuten Vishwanath, ym. (2011) tutkimuksen, mukaan sähköpostin viestielementtien tulkinnalla on merkitystä huijatuksi tulemiselle. Vastaavasti käyttäjien vapaissa kommenteissa molemmista tutkimuksen sähköposteista esiintyi viittauksia viestin ominaisuuksiin, kuten myös Vishwanath, ym. (2011) tutkimuksessaan havaitsivat.

Tässä tutkimuksessa ei huijaussähköposteja lähetetty tai esitetty lähetetyn tutkittaville todellisuudessa tunnetuilta tahoilta, kuten aikaisemmissa tutkimuksissa (Jagatic ym. 2007; Ferguson, 2005). Tunnettavuuselementti oli viestissä kuitenkin mukana, kun esitettiin, että viesti on lähetetty tutkittavan esimiehen pyynnöstä. Vaikka lähettäjän luotettavuus korreloi tilastollisesti merkitsevästi huijatuksi tulemisen kanssa, sillä ei ollut merkittävää selitysastetta regressioanalyysissä.

Tutkimusasetelmaan liittyen voidaan huomata, että kohdistetun huijaussähköpostin (sähköposti 1) liitteen avaamisen todennäköisyyden vastaukset poikkeavat sähköpostin ominaisuuksia mittaavista väittämistä. Tämä voidaan havaita vertaamalla kuvio 8:aa kuvioihin 9-12. Tässä voi vaikuttaa tutkittavien ensireaktio sähköpostiviestiä katsottaessa, joka ei ole niin epäilevä, kun taas seuraavaksi lomakkeella esitetyt väittämät luotettavuudesta ja uskottavuudesta, kun viestin kuva ei ollut enää tutkittavien nähtävissä. Eli kun tutkittavia pyydettiin arvioimaan sähköpostin eri luotettavuuteen liittyviä ominaisuuksia, arviot olivat yleisesti enemmän epäileviä kuin ensireaktiota kysyttäessä. Tämä on erityisen mielenkiintoinen huomio, kun arvioidaan todellisessa työelämässä tapahtuvaa kohdistettua sähköpostihuijausta, jolloin käyttäjä ei välttämättä ole erityisen valppaana. Tämä on merkittävä tekijä tulevien tutkimusten kannalta, koska tietoturvaan liittyvässä tutkimuksessa tutkittavalle helposti jossain vaiheessa tutkimusta selviää, että huomio kiinnittyy tietoturvaan, jolloin tutkittavat saattavat automaattisesti muuttaa omaa tulkintaansa tutkimustilanteessa.

5.2 Tutkimuksen vahvuudet ja rajoitukset

Tutkimuksen vahvuuksiin voidaan lukea otoksen poikkeaminen aikaisemmista tutkimuksista, joissa otokset ovat pääsääntöisesti olleet opiskelijoita tai yliopiston henkilöstöä ja usein tietotekniikkaan erikoistuneista yliopistoista (Jagaticin ym. 2007; Ferguson, 2005; Vishwanath, ym. 2011). Tässä tutkimuksessa tutkittavat olivat pankki- ja vakuutusalan työntekijöitä, mikä antaa paremman yleiskuvan kohdistettujen huijaussähköpostien toimivuudesta suomalaisissa suurissa pankki- ja vakuutusalan organisaatioissa. Lisäksi tässä tutkimuksessa hyödynnettiin perinteistä huijaussähköpostia vertailukohteena kohdistetulle huijaussähköpostille, mikä mahdollisti viestien ominaisuuksien tulkinnan vertailun.

Tutkimuksen keskeisin rajoitus liittyy otokseen, joka jäi tavoiteltua pienemmäksi. Tutkimuksen suunnitteluvaiheessa oltiin yhteydessä useampaa yritystä ja

tiedusteltiin mahdollisuutta järjestää tutkimus osittain työnantajan kanssa yhteistyössä, mutta yhteenkään tiedusteluun ei saatu myöntyvää vastausta. Lisäksi tutkimuksen kohdistuessa useampaan yritykseen saatiin toisaalta laajempaa tietoa, mutta samalla jouduttiin luopumaan siitä, että kohdistettu huijaussähköposti olisi ollut täydellisesti räätälöity kaikille tutkittaville.

Tutkimuksen toinen rajoitus liittyy itsearviointien käyttöön, sillä arviointeihin vaikuttavat aina tutkimukseen osallistuvien halukkuus ja kyvykkyys esittää tarkkoja havaintoja toiminnastaan. Voidaan arvioida, etteivät subjektiiviset arviot välttämättä täysin vastaa objektiivista arviointia tai todellista koeasetelmaa, joka työsähköpostien yhteydessä edellyttäisi käyttäjien oikeaan sähköpostiin lähetettäviä kohdistettuja huijaussähköposteja.

5.3 Jatkotutkimus

Tässä tutkimuksessa esiin nousseita, huijatuksi tulemiseen yhteydessä olevia tekijöitä olisi jatkossa hyödyllistä kartoittaa myös isommilla otoksilla, jolloin tilastolliset johtopäätökset olisivat vielä nykyistä luotettavampia ja mahdollisuuksien mukaan voitaisiin vertailla esimerkiksi eri alojen työntekijöitä toisiinsa. Tulevissakin tutkimuksissa olisi tärkeää kiinnittää huomiota paitsi viestin ominaisuuksiin myös käyttäjän yksilöllisiin tekijöihin. Jatkotutkimuksissa erityisesti tietotekniikan käytön mieluisuuden kokemusta olisi hyvä tutkia lisää, koska sille ei aikaisemmasta kirjallisuudesta ole löytynyt sijaa. Tähän on varmasti voinut vaikuttaa se, että monet aikaisemmat tutkitukset on tehty opiskelijoilla tai tietotekniikkaa opiskelevilla, joilla on lähtökohtaisesti todennäköisesti hyvät tietotekniset valmiudet.

5.4 Käytännön sovellukset

Tämän tutkimuksen pohjalta voidaan löytää kaksi keskeistä käytännön sovellusta, joiden avulla organisaatiot voivat keskittää voimavarojaan henkilöstön tietoturvan kehittämiseen. Tietoturvan teknisten suojamekanismien ohella käyttäjien koulutus ja asennekasvatus ovat keskeisiä keinoja organisaation tietoturvan kehittämisessä.

Tietotekniikan käytön koettu mieluisuus, joka edustaa tunnepohjaista suhtautumista tietotekniikan käyttöön, ja yrityksen tietoturvaan liittyvä riskitietoisuus, joka kuvaa tiedollista käsitystä vahinkojen vaikutuksista, olivat yhteydessä huijatuksi tulemiseen. Näin ollen sekä yksilön asenteisiin että tiedollisiin valmiuksiin vaikuttamalla voidaan todennäköisesti parantaa organisaatioiden tietoturvaa. Tähän tehtävään voivat osallistua paitsi työnantajaorganisaatiot myös esimerkiksi tietoturvayritykset ja oppilaitokset aina peruskoulusta korkeakouluihin.

Koska tietotekniikan käyttöä aletaan omaksua nykyään jo hyvin nuoressa iässä, on olennaista, että kannustava ja ohjaava tietoturvakasvatus aloitetaan mahdollisimman varhain, kuten jo peruskouluaikana. Mitä varhaisemmin asenteisiin ja riskitietoisuuteen panostetaan, sitä todennäköisemmin oppimistulokset näkyvät myös aikuisiällä ja siirryttäessä työelämään. Jatkuvasti muuttuvassa yhteiskunnassa ja työelämässä tietoturvakasvatusta on hyödyllistä yhä jatkaa - tietoturvauhat muuttuvat vuosi vuodelta yhä moniulotteisempaan ja haastavampaan suuntaan, mikä vaatii suojakeinojen ja riskitietoisuuden toistuvaa päivittämistä.

Tietotekniikan käytön mieluisuutta edistää se, että tietotekniikka tarjoaa käyttäjälleen myönteisiä kokemuksia ja onnistumisia. Yleisesti voidaan ajatella, että myönteisiä kokemuksia ja onnistumisia edesauttaa se, että yksilöllä on muun muassa riittävästi osaamista tarvitsemansa tietotekniikan käyttöön sekä se, että hän näkee tietotekniikasta olevan hyötyä itselleen. Käytännössä oppilaitosten ja työnantajien olisi kannattavaa huolehtia riittävän hyvin ihmisten tietoteknisten valmiuksien ylläpitämisestä ja heidän perehdytyksestä uusien tietoteknisten työvälineiden käyttöön. Tietotekniikan käytössä on pitkälti kyse opittavissa olevista taidoista, joita opastuksella ja harjoittelulla on mahdollista parantaa. Tässä voidaan nähdä vaihtoehtona esimerkiksi erilaiset teknologiapäivät, joissa organisaation ihmiset pääsevät tutustumaan uusiin teknologoihin opastetusti, jolloin on hyvä mahdollisuus saavuttaa positiivisia käyttäjäkokemuksia.

Käytännön sovelluksena kohdistettujen huijausviestien liitteistä ja linkeistä korostuu eniten käyttäjien kouluttaminen, eli liitetiedostojen ja internet-linkkien toiminnasta ja riskeistä kertominen. Kun käyttäjät osaavat suhtautua terveellisellä epäilyllä sähköposteihin, organisaatio saattaa onnistua pienentämään riskiä joutua kohdistetun hyökkäyksen kohteeksi. Yrityksissä voidaan myös harkita koulutuksen täydentämistä oikean oloisten harjoitus-huijaussähköpostien lähettämisellä työntekijöille, mikä varmasti lisää tietoisuutta organisaatiossa. Toinen koulutuksen kannalta tärkeä asia on huolehtia siitä, että henkilöstö osaa toimia oikein, jos epäilee avanneensa kyseenalaisen liitetiedoston tai internet-linkin. Kun käyttäjät ovat tietoisia toimintaohjeista, mahdolliset vahingot voidaan onnistua rajaamaan mahdollisimman pieniksi. Toisin sanoen, kun käyttäjät tunnistavat huijauksen internet-linkin tai liitetiedoston avaamisen jälkeen ja ovat tietoisia kuinka tilanteessa kuuluu toimia on hyvin suuri mahdollisuus onnistua rajoittamaan vahinkoja mahdollisimman paljon.

Kohdistetut huijaussähköpostit ovat jatkossakin yksi keskeinen haaste organisaatioiden tietoturvalle, mutta riskiä on mahdollista pienentää oikeilla toimilla organisaatioissa. Tässä tutkimuksessa keskityttiin pankki- ja vakuutusalan henkilöstöön, mutta monessa suhteessa löydöksiä voidaan yleistää organisaatioihin, joissa henkilöstön koulutustausta ja ikärakenne ovat saman kaltaisia.

6 LÄHTEET

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, Sivut: 90-101.

Bolzoni, D. (2009). *Revisiting Anomaly-based Network Intrusion Detection Systems*. Väitöskirja. Alankomaat: Twente:n yliopisto.

Dodge, R., Carver, C. & Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security, 26(1)*, 73-80.

Downs, J., Holbrook, M. & Cranor, L. (2006). Decision strategies and susceptibility to phishing, *In Proceedings of the second symposium on Usable privacy and security (SOUPS '06)*. ACM, New York, Yhdysvallat. Sivut: 79-90.

Elo, A., Leppänen, A., & Jahkola, A. (2003). Validity of a single-item measure of stress symptoms. *Scandinavian Journal of Work, Environment & Health, 29(6)*, 444-451.

Ferguson, A. (2005). Fostering e-mail security awareness: The West Point carronade. *EDUCASE Quarterly, 28(1*), 54-57.

Field, A., & Hole, G. J. (2002). *How to design and report experiments*. Sage.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation, 13(2),* sivut: 149-172.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *In Proceedings of the 22nd international conference on World Wide Web companion* (Sivut 737-744). International World Wide Web Conferences Steering Committee.

Hays, R. D., Reise, S., & Calderón, J. L. (2012). How much is lost in using single items? *Journal of General Internal Medicine, 27(11)*, 1402-1403.

Hyppönen Mikko. (2011, 28. elokuuta) How We Found the File That Was Used to Hack RSA - F-secure Weblog : News from the Lab. Haettu 12.2.2014 osoitteesta: http://www.f-secure.com/weblog/archives/00002226.html

Jagatic, T., Johnson, N., Jakobsson, M. & Menczer, F. (2007). Social phishing. *Commun. ACM 50(10)*. Sivut: 94-100.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007). What instills trust? a qualitative study of phishing. *In Financial Cryptography and Data Security, (4886), Springer*. Sivut: 356-361.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20(5)*, 332 - 349.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31(1)*, 83-95.

Kliarsky, A. (2011). Responding to Zero Day Threats. Julkaisia SANS Instituutti. Haettu 10.04.2014 osoitteesta: http://www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709

Knapp, K., Morris R., Marshall, T. & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28(7)*, 493-508.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M., & Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. *In Proceedings of the 5th Symposium on Usable Privacy and Security (p. 3). ACM.*

McAfee, Inc. (2011). McAfee Threats Report: Second Quarter 2011, Haettu 16.1.2014 osoitteesta: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

Nummenmaa, L. (2006). *Käyttäytymistieteiden tilastolliset menetelmät*. Helsinki: Tammi.

Nummenmaa, L. (2009). *Käyttäytymistieteiden tilastolliset menetelmät*. Helsinki: Tammi

Olivo, C., Santin, A. & Olivera, L. (2013). Obtaining the threat model for e-mail phishing. *Applied Soft Computing, 13(12),* 4841-4848

Parmar, B. (2012). Protecting against spear-phishing. Computer Fraud & Security, 2012(1), 8-11.

Ranta, N. (2011). Tässä syy OP:n poikkeuksellisiin ongelmiin. *Kauppalehti*, 25 Tammikuuta.

Robila, S. & Ragucci, J. (2006). Don't be a phish: steps in user education. *In Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education (ITICSE '06)*. ACM, New York, Yhdysvallat. Sivut: 237-241.

EMC Corporation - RSA. (2011, 1. huhtikuuta) Anatomy of an Attack - Speaking of Security - The RSA Blog and Podcast. Haettu 20.3.2014 osoitteesta: https://blogs.rsa.com/anatomy-of-an-attack/

Sanastokeskus TSK (2004). Tiivis tietoturvasanasto. Haettu 25.10.2013 osoitteesta: http://www.tsk.fi/tiedostot/pdf/TiivisTietoturvasanasto.pdf

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

Siponen, M. (2000) "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security, 8(1),* 31 - 41

Suomen virallinen tilasto (SVT) (2013).: Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. Helsinki: Tilastokeskus. Haettu 22.2.2015 osoitteesta: http://www.stat.fi/til/sutivi/2013/sutivi_2013_2013-11-07_tie_001_fi.html

Symantec Corporation. (2013). Internet Security Threat Report 2013, Volume 18. Haettu 16.1.2014 osoitteesta: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

King, R. (2011, 8. kesäkuuta). EMC's RSA Security Breach May Cost Bank Customers $100 Million - Bloomberg. Haettu 14.2.2014 osoitteesta: http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html

Kruger, H. & Kearney, W. (2006). A prototype for assessing information security awareness, *Computers & Security, 25(4)*,289-296.

Vance, A., Siponen, M. & Panhila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management 49 (3-4)*, 190-198

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H.R. (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.

Yhteiskuntatieteellinen tietoarkisto. (2003). Otos ja otantamenetelmät. Haettu 16.1.2014 osoitteesta: http://www.fsd.uta.fi/menetelmaopetus/otos/otantamenetelmat.html

Wang, J., Herath, T., Chen, R., Vishwanath, A. & Rao, H.R. (2012). Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication, 55(4)*, 345-362.

Wooldridge, J. (2009). *Introductory Econometrics*. Mason, USA: South-Western Cengage Learning.