Minna Uusitalo

KALASTELUVIESTINTÄ ILMIÖNÄ JA KIIREELLISYYDEN KOKEMUKSEN VAIKUTUS HUIJAUKSEN ONNISTUMISEEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Uusitalo, Minna
Kalasteluviestintä ilmiönä ja kiireellisyyden kokemuksen vaikutus huijauksen onnistumiseen
Jyväskylä: Jyväskylän yliopisto, 2018, 84 sivua
Kyberturvallisuus, pro gradu -tutkielma
Ohjaajat: Granroth, Lasse; Siponen, Mikko

Tässä tutkielmassa halutaan lisätä ymmärrystä kalasteluviestinnästä ilmiönä, sekä tarkastella kalasteluviesteissä käytettyjen, kiireellisyyden kokemusta lisäävien elementtien vaikutusta vastaanottajan toimintaan. Kiireellisyyden kokemusta lisäävät elementit kalasteluviestinnässä vaikuttavat olevan hyökkääjien yleinen tehokeino, jolla pyritään vaikuttamaan huijauksen onnistumiseen. Samalla se on hyvin vähän tutkittu aihe kalasteluviestinnän näkökulmasta.

Tutkielman aineistona käytetään kolmea eri kalastelukampanjaa, jotka olivat osa kohdeorganisaatiolle tuotettua kyberhyökkäyssimulaatiota vuonna 2017. Aineisto perustuu käytännön toimintaan työelämässä silloin, kun organisaatio on kyberhyökkäyksen kohteena. Aineisto poikkeaa aiemmasta alan tutkimuksesta siten, että tulokset perustuvat oikeassa työelämässä toteutettuihin kampanjoihin ja vastaanottajat ovat olleet henkilöitä, jotka eivät tienneet, että kyseessä on tilattu kyberhyökkäyssimulaatio. Aineistossa kuvattu vastaanottajien toiminta on siis verrattavissa siihen, miten henkilöt todellisuudessa oikeasti toimivat kalastelutilanteissa.

Kirjallisuuskatsauksella pyritään selittämään kalasteluviestintää ilmiönä ja tarkastelemaan syitä, miksi kalasteluviestit toimivat, perustuen aiempaan tieteelliseen tutkimukseen ja ammattikirjallisuuteen. Tutkielma pyrkii löytämään kirjallisuuskatsauksesta selityksen sille, miksi aineistossa tapahtui muutoksia eri kalastelukertojen välillä. Tavoitteena on ymmärtää paremmin, miksi kalasteluviestit toimivat ja miten kiireellisyyden kokemusta luovat elementit vaikuttavat vastaanottajan toimintaan.

Tutkielman tulosten mukaan kiireellisyyden kokemusta lisäävät elementit näyttävät vaikuttavan positiivisesti siihen, että henkilö tulee huijatuksi. Koettu uhka ja kiireellisyys vaikuttavat toimivan yhdessä hyvinä motivaattoreina kalasteluviestin avaamiselle ja viestin ohjeiden mukaan toimimiselle. Myös kiireellisyys ja niukkuus sekä potentiaalinen hyöty vaikuttavat olevan hyvä suostuttelutekniikoiden yhdistelmä.

Tutkielma toimii tiedeyhteisöissä ponnistuslautana uusille tutkimuksille. Tämä tutkielma osoittaa, että kalastelu kaipaa lisätutkimusta monista eri näkökulmista ja lähtökohdista. Tutkielmaa voidaan hyödyntää myös työyhteisöissä, joissa kalasteluviestinnältä halutaan oppia suojautumaan paremmin.

Asiasanat: kalastelu, kyberhyökkäys, kyberhyökkäyssimulaatio, puhelinkalastelu, sähköpostikalastelu, tietoturvallisuus, tietovuoto

ABSTRACT

Uusitalo, Minna
Phishing phenomenon and urgency cues impact on successful deceptions
Jyväskylä: University of Jyväskylä, 2018, 84 pp.
Cyber Security, Master's Thesis
Supervisors: Granroth, Lasse; Siponen, Mikko

The purpose of this thesis is to increase understanding of the phishing phenomenon and to study the impacts of urgency cues used in phishing emails on the activity of the recipient. Attackers seem to use urgency cues as a common technique to influence the recipients and to increase the likelihood of a successful phishing attack. Nonetheless, there are only a few studies which evaluate the impacts of urgency cues in a phishing context.

The research material consists of three different phishing camapings which was part of a wide cyber attack simulation produced in 2017 for a target organization. The material differs from previous research in that the results are based on real life actions in an organization when it is under attack. The phishing email recipients did not know that the organization had bought a cyber attack simulation nor that the organization was under an attack. The recipients' activities described in the material are thus comparable to how the individuals act in real life phishing situations.

The literature review aims to explain phishing as a phenomenon and to examine the reasons why phishing emails work, based on previous scientific research and professional literature. The thesis attends to find an explanation from the literature review for the changes in recipients' behaviour that occurred in the material between different phishing campaigns. The objective is to better understand why phishing messages work and how the elements that create the urgency experience affect the recipient's actions.

According to the results, the elements that increase the experience of urgency seem to have a positive effect on the recipient being scammed. Perceived threat and urgency cues seem to work together as a good motivator for the recipient to open the phishing email and follow the attacker's requests. Emergency and scarcity as well as potential benefits also seem to be a good combination of persuasion techniques.

This thesis can be used to develop further knowledge on understanding phishing phenomenon and why some phishing emails are more successful than others. The results indicate that there is a need for further phishing research on different perspectives. Thesis could also be useful for organizations that want to learn to protect themselves against phishing.

Keywords: cyber attack simulation, data leakage, email phishing, information security, phishing, vishing

TAULUKOT

KESKEISET KÄSITTEET

Ihmissuhteisiin liittyvä viestintä (eng. interpersonal communication) on Buller & Burgoonin (1996) mukaan dynaamista viestienvaihtoa kahden tai useamman henkilön välillä. Viestintä on interaktiivista silloin, kun viestinnässä voidaan vaikuttaa toiseen tai jakaa palautetta. Buller & Burgoonin (1996) mukaan viestintä kasvotusten on interaktiivisempaa, kuin muissa formaateissa (esimerkiksi sähköinen viestintä tai puhelinkeskustelu).

Kiireellisyys (eng. urgency) tarkoittaa Princen (1982) mukaan painetta (eng. pressure). Ajalliset paineet ovat ulkoisesti koettua kiireellisyyttä suorittaa tehtävä (Staudenmayer ym., 2002). Ajalliset paineet luovat stressiä ja tarvetta suorittaa tehtävä rajatussa ajassa (Ben Zur & Brenznitz, 1980; Wang ym., 2012).

Kalastelu (eng. phsihing) on urkintaa, jossa pyritään saamaan tietoja hyökkäyksen kohteelta usein huijaamalla (Vishwanath, Herath, Chen, Wang & Rao, 2011) ja viesti naamioimalla (mm. Wang, Herath, Chen, Viswanath & Rao, 2012). Hyökkääjän kiinnostuksen kohteena ovat usein luottamukselliset tiedot kuten luottokortti- tai pankkitiedot, käyttäjänimet tai salasanat (Mitnick, 2017). Huijaus voi tapahtua esimerkiksi esiintymällä tahona, johon huijauksen uhri luottaa. Yleensä kalasteluviestinnässä uhrin on klikattava esimerkiksi saastunutta linkkiä tai ladattava haitallinen liite, jolloin esimerkiksi haittaohjelma latautuu koneelle tai linkki vie saastuneelle sivustolle (Mitnick, 2017).

Kohdennettu kalastelu (eng. spear phishing) on kohdennettua verkkourkintaa (Sanastokeskus, 2016), jossa hyökkääjän kohteena olevaan henkilöön tai organisaation henkilöstöön pyritään vaikuttamaan käyttäjän manipuloinnin keinoilla (Butavicius ym., 2015). Kohdennettu kalastelu nimensä mukaisesti kohdentuu esimerkiksi tiettyyn henkilöön ja viesti on personoitu häntä varten (mm. Hadnagy & Fincher, 2015; Hong, 2012). Hyökkääjä voi tietää vastaanottajan nimi- ja yhteystietojen lisäksi myös kohdehenkilön harrastuksista, töistä, perheestä ja muista kiinnostuksenkohteista (mm. Butavicius ym., 2015; Hadnagy & Fincher, 2015). Hyökkääjä voi saada tarkan kuvan kohdeorganisaatiosta tai -henkilöstä esimerkiksi sosiaalisten medioiden palveluiden eri tietoja yhdistelemällä (Jagatic, Johnson, Jakobsson & Menczer, 2007). Näitä tietoja hyökkääjä käyttää hyväkseen saadakseen vastaanottajan toimimaan haluamallaan tavalla. Kohdennetut ja hyvin tehdyt kalasteluviestit voi olla erittäin vaikea tunnistaa (mm. (Butavicius ym., 2015; Hadnagy & Fincher, 2015, Wright & Marett, 2010).

Kyberhyökkäys on haitallinen ja lopulta tietovuotoon tai -murtoon johtava prosessi, joka koostuu käytännössä viidestä eri vaiheesta: tiedustelu, skannaus, hyökkäys (eng. exploiting), pääsyn varmistaminen ja jälkien peittely (Niemelä, 2016). Jos ajatellaan kalasteluviesti kyberhyökkäyksenä, niin yksinkertaistettuna tiedusteluvaiheessa etsitään tietoa kohteesta (esim. sähköpostipalvelin ja

kohteen kontaktit), sitten ”skannataan” tai etsitään eri rajapintoja ja haavoittuvuuksia (esim. sähköpostipalvelimen tai kohdeorganisaation muiden käytössä olevien järjestelmien haavoittuvuuksia), joita hyökkääjä voi hyödyntää, jonka jälkeen hyökkääjä valitsee, mihin ja miten hyökkää. Siitä seuraa varsinainen hyökkäysvaihe (se, mitä tapahtuu ja mihin hyökkääjä saa pääsyn, kun kalasteluviestin vastaanottaja tulee huijatuksi ja avaa haitallisen linkin tai liitteen). Jos on esimerkiksi saatu kalasteltua käyttäjätunnus ja salasana järjestelmään, hyökkääjä varmistaa, että hän pääsee kyseiseen järjestelmään niin pitkään kuin tarve vaatii, ja peittää jälkensä, jotta hänen toimintaansa ei huomattaisi.

Petos (eng. deception) tarkoittaa tapahtumaa, jossa petoksen tekijä kontrolloi tahallaan ja tietoisesti viestiä, jonka tarkoituksena on poiketa totuudesta ja johtaa harhaan viestin vastaanottajaa (Knapp & Comadena, 1979). Vastaanottaja voi epäillä tai kyseenalaistaa lähettäjän luotettavuuden huolimatta siitä, oliko kyseessä oikea petos vai pelkkä kokemus siitä (Buller & Burgoon, 1996). Verkossa petos on yleinen kyberrikollisuuden muoto, jossa suostuttelua ja harhaan johtamista käytetään huijaamaan verkon käyttäjiä (Ebot, 2017).

Päätöksenteko on prosessi, jossa aktivoituu erilaisia kognitiivisia ominaisuuksia (mm. Goel, 2017; Viswanath, 2015). Prosessin valinta vaikuttaa henkilön toimintaan eli siihen, millaisen päätöksen henkilö tekee.

Social engineeringillä eli käyttäjän manipuloinnilla tarkoitetaan Hadnagyn ja Fincherin (2015) mukaan toiseen ihmiseen vaikuttamista kyseenalaisin keinoin. Usein manipuloinnin seurauksena henkilö tekee jotain, joka ei ole hänen edun mukaistaan (Hadnagy & Fincher, 2015). Manipuloiva taho voi käyttää esimerkiksi valtaa, rangaistuksia tai uhkailua vaikuttaakseen toiseen (Hadnagy & Fincher, 2015). Käyttäjän manipulointi johtaa usein tietototurvan heikentymiseen (Sanastokeskus TSK, 2004).

Spoofing tarkoittaa yksinkertaistetusti sähköpostiviestinnässä sitä, että lähettäjä väärennetään (Jagatic ym., 2005). Hyökkääjä tekeytyy esimerkiksi kalasteluviestin vastaanottajan tuntemaksi tahoksi, jolloin viesti näyttää tulevan esimerkiksi osoitteesta info(at)organisaatio.fi, vaikka todellisuudessa kyseiseltä tililtä ei ole sähköpostiviestiä lähetetty. Spoofaus on helppoa, eikä vaadi lähettäjän sähköpostitilin hakkerointia (Jagatic ym., 2005).

Späm tarkoittaa roskapostia, kuten kaupallisia mainoksia, joita lähetetään vastaanottajalle hänen pyytämättään. Joskus spämmillä viitataan myös massana lähetettäviin, pahantahtoisiin, geneerisiin kalastelukirjeisiin, lempinimeltään ”nigerialaiskirjeisiin” (Hong, 2012). Näissä pyydetään yleensä rahaa ja toivotaan, että joku lukuisista vastaanottajista vastaa (mm. Hong, 2012; Niemelä, 2016). Spämmifiltteri on tekninen tietoturvakontrolli, jonka tarkoituksena on suodattaa roskaposti siten, ettei se näy vastaanottajan saapuneet -sähköpostikansiossa vain siirtyy automaattisesti roskapostikansioon.

Suostuttelu on toimintaa, jossa suostuttelija käyttää psykologisia keinoja saadakseen suostuteltavan tahon toimimaan haluamallaan tavalla (Cialdini, 2001).

Tietoturvariski on tietoturvauhan seurauksena mahdollisesti tapahtuvan vahingon ja sen toteutumisen todennäköisyys (Sanastokeskus TSK, 2004).

SISÄLLYS

1 JOHDANTO

Tämä Pro Gradu -tutkielma keskittyy selittämään kalasteluviestintää ilmiönä ja pureutuu siihen, millaiset kalasteluviestit johtavat hyökkääjän kannalta haluttuihin tuloksiin. Tutkielmassa tarkastellaan myös sitä, miten kiireellisen kokemusta lisäävät elementit kalasteluviestinnässä vaikuttavat viestiin reagointiin.

Kalastelun tavoitteena on varastaa käyttäjältä tietoa, kuten luottokorttitietoja, tai päästä johonkin järjestelmään (mm. Butavicius ym., 2015). Kalastelun kohteena on järjestelmien sijaan ihmiset, jotka niitä käyttävät (Hong, 2012). Suurin osa talousrikoksista ja identiteettivarkauksista johtuu kalastelusta (Ebot, 2017). Kalastelu on uhka tietoturvallisuuden (Workman, 2008) lisäksi yksityisyydelle (Ebot, 2017).

Kalasteluhyökkäys voi johtaa maineen, arkaluontoisen tiedon tai IPR-omaisuuden menetykseen, tai kriittisen tiedon muuttumiseen tai menetykseen (Butavicius ym., 2015). Esimerkiksi identiteettivarkaudet, asiakastiedot, yrityssalaisuudet ja kansalliset salaisuudet ovat hyökkääjän kannalta kiinnostavia (Hong, 2012). Hongin (2012) mukaan esimerkiksi pelkkä käyttäjän sähköpostin salasanan vuotamien hyökkääjälle voi olla tuhoisaa: suuri osa käyttäjistä kierrättää salasanojaan käyttäen samaa salasanaa joka paikassa, jolloin sähköpostin salasana todennäköisesti käy myös muihin palveluihin. Suuri osa palveluntarjoajista myös palauttaa unohtuneen salasanan sähköpostiin (Hong, 2012). Tällöin hyökkääjä pääsee käytännössä lähes kaikkiin palveluihin, joihin kyseistä sähköpostitiliä on käytetty palveluun rekisteröityessä (esimerkiksi erilaiset lippupalvelut, sosiaalisen median palvelut, verkkokaupat). Sähköpostiin pääsy avaa siis usein pääsyn moneen muuhun paikkaan.

On epätodennäköistä, että organisaatio voisi kokonaan estää ulkopuolelta tulevaa, pahantahtoista kalasteluviestintää. Markkinoilla on tarjolla erilaisia kalasteluviestinnältä suojautumiseen tarkoitettuja työkaluja (mm. Downs ym., 2006; Jagatic ym., 2005). Kuitenkin kalasteluviesteiltä on vaikea suojautua täysin teknisin keinoin (mm. Hong, 2012; Jakobsson, Tsow, Shah, Blevis & Lim, 2007; Hadnagy & Fincher 2015; Viswanath, Herath, Chen, Wang & Rao, 2011). Hyökkääjä voi kiertää palomuurisäännöt ja/tai lähettää kalasteluviestejä kohdennetusti (mm. (Butavicius ym., 2015; Goel, Williams & Dincelli, 2017; Hong,

2012; Williams & Dincelli, 2017) vain muutamille henkilöille tai henkilöryhmille, jolloin viesti voi organisaation tietoturvakontrolleista riippuen päätyä vastaanottajan saapuneet-kansioon normaalisti, eikä jää spämmifiltteriin (Jagatic ym., 2005; Viswanath, 2011).

Wright & Marett (2010) arvioivat, että vain 35 % kalasteluyrityksistä estetään teknisten kontrollien, kuten spämmifiltterien avulla. Palomuureilla, sertifikaateilla, kaksivaiheisella tunnistautumisella tai salausohjelmilla ei ole suojaavaa vaikutusta, jos henkilö tulee huijatuksi kalasteluviestin avulla (Hong, 2012). On myös näyttöä siitä, että vaikka spämmifiltterit ohjaisivat kalasteluviestin suoraan roskapostikansioon, voivat käyttäjät käydä siitä huolimatta avaamassa viestin ja kiertää teknisiä tietoturvakontrolleja (mm. Downs ym., 2006; Hadnagy & Fincher, 2015).

Kalastelu ei myöskään enää rajoitu pelkkiin sähköposteihin. Myös puhelin, tekstiviestit, viestipalvelut (eng. instant messaging), verkostoitumissivustot sosiaalisessa mediassa ja jopa monipelaajapelit verkossa ovat kalastelijan leikkikenttää (Hong, 2012). Usein henkilöstölle on epäselvää, mitä tietoa erilaisissa viestintävälineissä kuten puhelimessa tai sähköpostissa voi antaa, ja miten kysyjän henkilöllisyydestä voidaan varmistua. Kalastelu on tehokasta, sillä kaikki eivät osaa olla varovaisia, tai eivät ymmärrä kalasteluviestiin vastaamisen tai tietojen luovuttamiseen liittyviä riskejä (Hadnagy & Fincher 2015).

Hyökkäys voidaan räätälöidä siten, että viestit ja viestien välityskanavat suunnitellaan petoksen mukaan, jotta kohteen olisi mahdollisimman helppo hyväksyä petos (Wright & MArett, 2010). Hyökkääjän konstit ovat monet: käyttäjiä voidaan lähestyä kalasteluviesteillä ja kysellä salasanoja, hyökkääjä voi pyrkiä tunkeutumaan organisaatioon fyysisesti esimerkiksi henkilöstön tupakkapaikan kautta varastaakseen dataa, tunkeutuakseen koneelle tai verkkoon, tai jättääkseen toimitiloihin esimerkiksi saastuneen muistitikun. Muistitikku voi sisältää esimerkiksi takaoven (eng. backdoor) koneelle, josta USB avataan. Viime kädessä henkilöstön vastuulle jää, miten he toimivat vastaanottaessaan kalasteluyrityksiä (mm. Hadnagy & Fincher, 2015).

Suurin osa viimeaikaisista hyökkäyksistä on sisältänyt käyttäjien manipulointia (eng. social engineering) jonka tavoitteena on saada käyttäjä toimimaan hyökkääjän haluamalla tavalla (mm. Ebot, 2017; Hadnagy & Fincher, 2015; Workman, 2008). Social engineeringillä viitataan menetelmiin, joiden avulla voidaan manipuloida ihmisiä psykologisia keinoja käyttäen joko paljastamaan tietoja tai tekemään hyökkääjän pyytämiä asioita. Menetelmiin kuuluvat tietoturvallisuuden yhteydessä muun muassa suostuttelu, valehtelu, esiintyminen toisena henkilönä, peitetarinat ja tietojen kalastelu eri keinoin kuten sähköpostin, valeverkkosivujen tai puhelimen välityksellä. Onnistuneen manipuloinnin lopputuloksena on, että hyökkääjä a) saa tietoa (esim. käyttäjätunnuksen ja salasanan), b) saavuttaa tavoitteensa (esim. haitallisen liitteen avaamisen johdosta koneelle asentuu haittaohjelma) tai c) käyttäjä houkutellaan tekemään jotain hyökkääjälle hyödyllistä, esim. välittämään huijausviestin eteenpäin.

Hadnagy & Fincher (2015) esittävät, että 60 % hyökkäyksistä on sisältänyt ”inhimillisen tekijän” (eng. human factor), joka on ollut oleellinen osa

hyökkäyksen onnistumista. Inhimillinen tekijä tarkoittaa tässä kontekstissa sitä, että hyökkäys on onnistunut käyttäjän toiminnasta johtuneen seikan vuoksi, eli kalastelun uhri on esimerkiksi klikannut viestin sisältämää, haitallista linkkiä tai ladannut viestissä olleen, haitallisen liitteen. Vastaanottajaa houkutellaan avaamaan viesti herättämällä tunteita kuten pelkoa, ahneutta tai auttamisen halua (mm. Goel ym., 2017). Käytännössä vastaanottaja on avannut hyökkääjälle väylän organisaatioon toimiessaan kalasteluviestissä pyydetyllä tavalla. Usein kalasteluhyökkäykset hyödyntävät sekä sosiaalisia, että teknisiä haavoittuvuuksia (Jagatic ym., 2005).

Käyttäjien manipulointi on nykypäivän nopeiten kasvava kyberturvallisuusuhka (Niemelä, 2016). Tästä syystä on kiinnostavaa tutkia, millaisiin kalasteluviesteihin henkilöstö todennäköisesti lankeaa. Kalasteluviestien toimivuuteen vaikuttaa mm. viestien sisältö ja ulkonäkö ja kirjoitusvirheet (esim. Hadnagy & Fincher, 2015; Wang ym., 2012). Kalasteluviestit voivat olla myös niin taidokkaasti tehty, että niiden tunnistaminen huijaukseksi on erittäin vaikeaa.

Suojautumista ajatellen haasteena on, että kuka tahansa voi luoda vakuuttavan näköisen kalasteluviestin (Mitnick, 2017). Ebot jakaa väitöskirjassaan (2017) kalasteluviestit kahteen eri kategoriaan: uhkan sisältävät viestit (esim. ”käyttäjätunnuksesi ovat vuotaneet”) ja jonkinlaisen hyödyn tai palkinnon sisältävät viestit (esim. ”onneksi olkoon, olet voittanut arvonnan”). Myös Goel ym. (2017, s. 29) käyttää tätä jakoa, mutta viittaa lisäksi Lawrenceen ja Nohriaan (2012), joiden mukaan hankkimisen (eng. drive to aquire) ja turvaamisen (eng. drive to defend) lisäksi ihmisten motivaattoreita ovat myös sosiaaliset halut kuulua yhteen tai verkostoitua (eng. drive to bond) ja halu oppia (eng. drive to learn). Suuri osa aiemmasta kalasteluun liittyvästä tutkimuksesta liittyy kahteen ensimmäiseen motivaattoriin (potentiaaliset hyödyt ja uhat). Näitä käsitellään laajasti myöhemmin tässä tutkimuksessa.

Esimerkiksi sosiaaliseen mediaan liittyvät kontaktipyynnöt avataan usein varauksetta, ja mikäli viesti näyttää ja tuntuu aidolta sekä lähettäjä on tuttu, kuten LinkedIn tai Facebook, kontaktipyyntö usein hyväksytään sähköpostin sisältämän (haitallisen) linkin kautta (Mitnick, 2017). Tällainen kontaktipyyntö sisältää motivaattorin luoda sosiaalisia kontakteja (eng. drive to bond). Kasvotusten osaamme usein tunnistaa petokset jo alkukantaisen, evolutiivisen selviytymisvaiston myötä, mutta nämä vaistot eivät suurimmalla osalla toimi verkossa (Mitnick, 2017).

Käyttäjien manipuloinnin estämiseksi tulisi hallussa olla teknologiat, prosessit, tietoisuus ja koulutukset (Mitnick & Simon, 2002). Hadnagyn (2010) mukaan kalasteluyritysten tunnistaminen, turvallisuuskulttuuri organisaatiossa sekä ymmärrys organisaation omistamien tietojen arvokkuudesta ja järjestelmäpäivitykset ovat tie estää käyttäjien manipulointia.

Kun tiedämme, millaiset kalasteluviestit todennäköisesti johtavat vastaanottajan harhaan johtamiseen ja kohdeorganisaation kannalta haitallisiin seurauksiin, voimme keskittyä näihin seikkoihin ja tämän tiedon pohjalta kehittää organisaation tietoturvakulttuuria ja henkilöstön tietoturvakoulutuksia, koska tekniset tietoturvakontrollit eivät yksinkertaisesti riitä.

1.1 Tutkimustarve

Aiempi tieteellinen tutkimus kalasteluviesteistä jakautuu käyttäytymistieteelliseen ja teknologiseen kategoriaan (Vishwanath, ym., 2011; Wang, 2012). Tässä Pro Gradu - tutkielmassa teknologinen lähestymistapa on rajattu tutkimuksen ulkopuolelle. Kalasteluaiheinen tutkimus voidaan jakaa myös kahteen kategoriaan siten, että osa tutkimuksista tutkii kalasteluun liittyviä epäilyksiä, yksilöllisiä tekijöitä ja psykologisia tekijöitä, kun taas toinen osa tutkimuksesta keskittyy siihen, mitä kalasteluviestit sisältävät ja miten kalasteluviestien petoksilta voitaisiin välttyä (Goel ym., 2017). Tämä tutkimus keskittyy molempiin kategorioihin: luvussa 2.2. syvennytään tarkemmin kalasteluviestien toimivuuteen käyttäytymistieteellisestä näkökulmasta ja luvussa 2.3 käsitellään kalasteluviestien sisältöä ja ulkonäköä. Pohdinnassa (luku 5) punnitaan tuloksia sekä käyttäytymistieteen että viestien sisällön näkökulmasta.

Kalastelu ja käyttäjien manipulointi (eng. social engineering) ovat aiheina paljon esillä mediassa, mutta vaikuttaa siltä, etteivät ne ole suosittuja aiheita tieteellisessä tutkimuksessa (mm. Ebot, 2017; Workman, 2008), tiedeyhteisöjen konferensseissa tai julkaisuissa, vaikkakin verkkohuijaukset ja kalastelu ovat jatkuvasti esillä uutisissa (Ebot, 2017). Kuitenkin mikäli kalastelulta suojautumiseksi halutaan kehittää työkaluja, tulee ensin ymmärtää, miten ja miksi kalasteluviestit toimivat ja ihmiset tulevat huijatuksi (Downs ym., 2006; Viswanath ym., 2011).

Oikean elämän verkkohuijauksen uhrit ovat ilmeisesti jääneet kokonaan tieteellisen tutkimuksen ulkopuolelle. Ebot (2017) toteaa, että verkkohuijausten uhrien sekä verkkohuijareiden ja -rikollisten tutkiminen ja ymmärtäminen voisivat johtaa uuden teorian muodostumiseen tietoturvallisuuden tiedeyhteisöissä.

Kalastelua ei tässä Pro Gradu -tutkielman yhteydessä tehdyn kirjallisuuskatsauksen mukaan ole juurikaan tieteellisesti tutkittu niin, että tutkimuksen aineistona käytettäisi organisaatiossa tapahtuneesta, oikeaa hyökkäystä simuloivasta hyökkäyksestä saatua dataa siten, että tutkimuksen kohteena olisi organisaation henkilöstö. Tieteellisten tutkimusten aineistona on käytetty esimerkiksi Yhdysvalloissa korkeakouluopiskelijoilta saatua dataa, eikä työpaikalla henkilöstöltä saatua dataa (esim. Butavicius, Parsons, Pattinson & McCormac, 2015; Goel, Williams & Dincelli, 2017; Jagatic, Johnson, Jakobsson & Menczer, 2005; Vishwanath, 2015; Wang, Herath, Chen, Viswanath & Rao, 2012; Wright & Marrett, 2010).

Opiskelijoihin koeryhmänä liittyvät rajoitukset jättävät joitakin avoimia kysymyksiä. Korkeakouluopiskelijoilla voi olla toisenlaisia intressejä kuin esimerkiksi työyhteisön jäsenillä. Opiskelijoilla ei ole esimerkiksi velvoitetta pitää huolta yliopiston tiedoista, kun taas työntekijät työskentelevät sopimussuhteessa ja heitä velvoittaa yleensä aina salassapitovelvollisuus. Siten korkeakouluopiskelijat eivät välttämättä koe yliopistojen tietovuotoja asiana, joka koskettaa heitä, ja mikäli kalasteluviestissä esimerkiksi kysytään tunnuksia yliopiston

järjestelmään, opiskelijat saattavat suhtautua kalasteluun välinpitämättömämmin kuin yliopiston työntekijät. Goelin ym. (2017) tutkimus (lisää luvussa 2.3.1) on harvinainen siinä mielessä, että koetilanteessa simuloitiin oikeaa hyökkäystä, eivätkä kalasteluviestin saaneet tienneet, että kyseessä on kalasteluyritys. Siten tutkimustuloksia ainakin klikkausalttiuden osalta voidaan pitää luotettavampina kuin haastatteluun tai pelkkään kyselyyn perustuvia tutkimuksia, joissa vastaanottajan vastaukset eivät välttämättä ole aina todenmukaisia.

Aina eivät tutkimusten kohderyhmänä ole olleet opiskelijat. Jos kohderyhmänä on ollut jotain muuta kuin opiskelijat, kalasteluaiheisen tutkimuksen data on usein kerätty kyselyiden tai laboratoriokokeiden avulla. Kirjallisuuskatsauksen perusteella simulaatioiden (koehyökkäysten) avulla henkilöstöä on testattu harvoin. Moni aiemmasta tieteellisestä, kansainvälisestä tutkimuksesta perustuu dataan, jossa henkilöiltä on esimerkiksi kysytty, miten toimisit vastaanottaessasi tietynalaisen kalasteluviestin, mutta ei ole mitattu sitä, miten henkilöstö tosiasiassa reagoi saadessaan viestin, jota hän ei etukäteen tiedä kalasteluyritykseksi. Tällaisia ”miten reagoisit jos”-tyylisiä kysely- ja haastattelututkimuksia löytyy (mm. Downs, Holbrook & Cranor, 2006; Ebot ym., 2017; Jakobsson, Tsow, Shah, Blevis & Lim, 2007). Näitä tutkimuksia avataan lisää tämän tutkielman kirjallisuuskatsauksessa (luku 2).

Kyselyissä ja haastatteluissa haasteena on, että vastaajat voivat ylitai aliarvioida kalasteluhyökkäykset eivätkä vastaajat välttämättä tahdo myöntää, vaikka olisivatkin joutuneet hyökkäyksen uhriksi ja tulleet huijatuiksi (Goel ym. 2017; Jagatic ym., 2005). Laboratorio-olosuhteissa taas haasteena on, että testiryhmät tietävät olevansa mukana tutkimuksessa, joka voi vaikuttaa tuloksiin (Goel ym. 2017). Kaikista lähemmäs aitoja tuloksia päästään siis todellisuutta simuloivalla koehyökkäyksellä, johon toisaalta liittyy myös eettisiä haasteita (ks. luku 1.4). Koehyökkäyksille voi olla myös vaikea saada lupaa näiden haasteiden vuoksi (Wang ym., 2012).

Toisaalta koehyökkäyksissä mittarina ei käytetä lainkaan tavallisia sähköpostiviestejä, vaan kerätään vain käyttäytymiseen liittyvää dataa vain kalasteluviestikontekstissa (Butavicius ym., 2015). Silloin ei voida mitata sitä, milloin vastaanottaja arvioi viestin tavalliseksi ja milloin kalasteluksi (Butavicius ym., 2015). Kalasteluviesti on voinut jäädä avaamatta myös muista syistä kuin siksi, että se olisi tunnistettu huiijausyritykseksi. Tällaisia syitä voivat olla esimerkiksi se, että käyttäjä ei ole kiinnittänyt huomioita koko viestiin, tai se on unohtunut lukea. Wangin ym. (2012) mukaan tutkimustarve on suuri etenkin teoreettiselle tutkimukselle kalasteluviestien prosessoinnista, ja empiiriset tutkimukset voisivat auttaa ymmärtämään tätä pettämisen muotoa. Myös etenkin kiireellisyyden kokeminen kaipaa Wangin ym. (2012) mukaan lisätutkimusta.

Yksi keino manipuloida vastaanottajaa on siis käyttää kiireellisyyden kokemusta lisääviä elementtejä, jotta vastaanottaja tekisi hätäisiä päätöksiä. Kiireellisyys kalasteluviestinnässä vaikuttaa olevan yleinen tehokeino, jolla pyritään vaikuttamaan huijauksen onnistumiseen, mutta samalla se on hyvin vähän tutkittu aihe kalasteluviestinnän näkökulmasta, koska yhtäkään vastaavaa tutkimusta ei kirjallisuuskatsausta tehtäessä löytynyt.

Kiireellisyyden kokemukseen liittyviä tutkimuksia haettiin tietoturvallissusaiheisista tiedelehdistä (MIS Quarterly, Journal of Management Information Systems, Information Systems Research, Journal for the Association of Information Systems, Journal of Information Technology, Information Systems Journal, Journal of Strategic Information Systems ja European Journal of Information Systems), Google Scholarista ja Jyväskylän yliopiston JYKDOK-palvelun kansainvälisistä e-aineistoista hakusanoilla ”urgency” ja ”urgent”, sekä ”urgency + phishing”. Aiheesta löytyi vain muutama tämän Pro Gradu - tutkielman kannalta relevantti julkaisu, jossa näkökulmaksi on otettu kiireellisyys. Suurin osa julkaisuista kiireellisyyden kokemukseen (eng. urgency) liittyen on kirjoitettu neuropsykologian lähtökohdista. Kiireellisyyttä kirjallisuuskatsauksen pohjalta tarkastellaan luvussa 2.4.

Naidoo (2015), Wang ym. (2012) ja Viswanath ym. (2011) toteavat, että kiireellisyydestä (eng. urgency cues) kalasteluviestikontekstissa ei löydy tarpeeksi tutkimuksia. Jatkotutkimusta kaipaavat erityisesti kiireellisyyden kokemuksen vaikutukset ja petosta implikoivat tekijät viestissä, sekä kalasteluhyökkäysten todelliset uhrit (Viswanath ym., 2011; Wang ym., 2012). Tutkimuksia voitaisi hyödyntää esimerkiksi koulutuksia suunnitellessa ja kalasteluhyökkäyksiltä suojautumisessa (mm. Naidoo, 2015).

Todellisia uhreja on erittäin vaikea Wangin ym. (2012) mukaan tutkia, koska uhritietokantoja ei ole tutkijoiden saatavilla, eivätkä uhrit eivät välttämättä edes tiedä olleensa kalasteluhyökkäyksen kohteita, tai he eivät ole raportoineet kalastelusta. Näin ollen esimerkiksi Wang ym. (2012) eivät olleet löytäneet yhtäkään tutkimusta, jossa olisi voitu käyttää koeryhmänä kalastelun todellisia uhreja. Todellisten uhrien käyttäminen kohderyhmänä auttaisi validoimaan aiempia tutkimuksia (Wang ym., 2012).

Todettakoon, että kaikki tässä tutkielmassa lähteinä käytetyt tutkimukset olivat määrällisiä siltä osin, että esimerkiksi kyselyiden vastaukset analysoitiin jonkin ohjelman, kuten SPSS:n avulla. Tämä tutkielma on laadullinen.

1.2 Tutkimuksen tausta ja aineisto

Organisaation nykytila ja reagointikyky ”oikeaan” kalasteluyritykseen voidaan selvittää nk. hyökkäyssimulaattorilla, eli oikeaa maailmaa simuloivalla hyökkäyksellä toteutettuna siten, ettei henkilöstöä tiedoteta aiheesta etukäteen (Hadnagy & Fincher, 2015). Hyökkäyssimulaattoria voidaan käyttää koulutuksen välineenä (Hadnagy & Fincher, 2015). Kokonaisvaltaiseen hyökkäyssimulaattoriin kuuluu usein kalastelukampanjoiden lisäksi julkisten lähteiden tiedustelu, sekä erilaiset tekniset hyökkäykset kohdeorganisaation järjestelmiin.

Suunnittelemme ja toteutamme töissä erilaisia hyökkäyssimulaattoreita ja kalastelukampanjoita asiakasorganisaatioille, jotka haluavat testata omia valmiuksiaan toimia tällaisten hyökkäysten aikana ja niiden jälkeen. Kalastelukampanjoissa lähetämme erilaisia kalasteluviestejä, soitamme kalastelupuheluita ja välillä hyökkäyksiin kuuluu myös fyysinen tunkeutuminen.

Hyökkäyksissä testataan mm. henkilöstön käyttäytymistä ja organisaation sisäisen raportointiprosessin toimivuutta, ja tarkoituksena on löytää organisaation haavoittuvuudet, jotta tietoturva-aukot voidaan tukkia.

Tämän tutkimuksen aineistona on käytetty palaa asiakkaan loppuraportista, jossa kuvataan laajan hyökkäyssimulaation toteutusta asiakasorganisaatiossa. Tutkimusaiheen rajauksen vuoksi ei ole relevanttia tarkastella koko loppuraporttia, vaan aineistossa huomioidaan vain kalastelukampanjat. Kyseiseen kohteeseen teimme organisaation tilauksesta kolme eri kalastelukampanjaa vuoden 2017 aikana. Kalasteluhyökkäykseen kuului julkisten lähteiden tiedustelu, erilaisten (3) kalasteluviestien lähettäminen ja erilaisten kalastelupuheluiden soittaminen. Viesteistä osa sisälsi kiireellisyyden kokemusta lisääviä elementtejä, ja osa ei. Kaikki tiedot kohdeorganisaatiosta on muokattu siten, ettei kohdeorganisaatiota voida tunnistaa.

Kampanjoissa on mitattu sitä, miten henkilöstö reagoi kalasteluviesteihin (avattiinko viestit ja niiden sisältämät linkit/liitteet) tietämättä etukäteen, että tällainen kampanja on käynnissä. Vastaavia aineistoja on tieteellisessä tutkimuksessa käytetty hyvin vähän, eikä tämän tutkimuksen kirjallisuuskatsaukseen löydetty yhtäkään vastaavaa tutkimusta.

Kohdeorganisaatiosta lähtöisin oleva halu testata omaa toimintakykyään viestii usein edistyksellisestä tietoturvallisuuskulttuurista, ja säännöllinen testaaminen vaikuttaa positiivisesti organisaation turvallisuuskulttuuriin (Hadnagy & Fincher, 2015). Töissä tehtyjen kampanjoiden myötä todettakoon, että edellä mainittu väite tuntuu pitävän paikkansa. Muita motiiveja kohdeorganisaatiolle toteuttaa kalastelukampanja on mm. jokin ulkoinen vaatimus tai auditointi, jo sattunut tietovuoto tai -murto, tai penetraatiotestauksen yhteydessä haluttu laajempi testaus (Hadnagy & Fincher, 2015).

Toteuttamiimme hyökkäyssimulaattoreihin kuuluu kalastelukampanjoiden välissä tai niiden jälkeen tietoturvakoulutus, jossa kerrotaan kalastelusta, kohdeorganisaatiolle toteutetuista kampanjoista ja niiden tuloksista, sekä keinoista tunnistaa kalasteluyritykset. Koulutuksissa käydään läpi, millaisia seurauksia tosielämän oikealla, pahantahtoisella hyökkäyksellä olisi voinut olla kyseiselle kohdeorganisaatiolle ja sen henkilöstölle. Tosiasiallisesti näissä hyökkäyssimulaattoreissa ei tallenneta sellaisia tietoja, joista voisi koitua kohdeorganisaatiolle haittaa. Tässä kohdeorganisaatiossa henkilöstöä koulutettiin toisen ja kolmannen kampanjan välissä.

1.3 Tutkimustavoitteet ja -menetelmät

Tässä Pro Gradu - tutkielmassa pyritään vastaamaan seuraavaan tutkimuskysymykseen:

- Millaiset seikat vaikuttavat kalasteluviestien toimivuuteen?

Apukysymykset ovat:

- Missä määrin kiireellisyyden kokeminen kalasteluviesteissä vaikuttaa viestin vastaanottajien toimintaan?

- Miksi kalasteluyritykset toimivat?

Tutkielmassa tutkitaan kalasteluviestinnän onnistumista ilmiönä ja tarkastellaan erityisesti sitä, että jos viesti sisältää kiireellisyyden elementtejä tai voi luoda kiireellisyyden kokemuksen, johtaako se todennäköisemmin käyttäjän toimintaan verrattuna sellaisiin kalasteluviesteihin, joista kiireellisyyden elementit puuttuvat. Tutkimuskysymykseen pyritään vastaamaan ja kalasteluviestintää ilmiönä selittämään aineiston sekä kirjallisuuskatsauksen (luku 2) avulla. Kirjallisuuskatsaus koostuu kalasteluviesteihin ja käyttäytymistieteeseen liittyvästä tutkimuksesta, sekä ammattikirjallisuudesta.

Tutkielmaan ei ole kirjallisuuskatsauksessa valittu yhtä yksittäistä teoriaa, vaan erilaisia käyttäytymistieteen teorioita ja periaatteita tarkastellaan niiltä osin, miten ne selittävät sitä, miksi ja miten kalasteluviestintä onnistuu. Kirjallisuuskatsauksen monimuotoisuus ja värikkyys johtuu siitä, että tutkimuskysymys huomioon ottaen minkään yksittäisen teorian tarkastelu ei riitä selittämään tutkittavaa ilmiötä. Käytössä oleva aineisto on myös niin suppea ja eri tarkoitukseen kerätty, että kalasteluviestintää ilmiönä kuvataan ennemmin kirjallisuuskatsauksen pohjalta, ja tutkimuskysymykseen pyritään vastaamaan siitä näkökulmasta, että käytetty aineisto tukee kirjallisuuskatsauksessa esiin nousseita havaintoja.

Odotetut tulokset ovat, että kiireellisyyden kokemusta lisäävät elementit ja viestin merkityksellisyys (toteutuuko esimerkiksi jokin uhkakuva, mikäli vastaanottaja ei toimi viestissä pyydetyllä tavalla) lisäävät todennäköisyyttä siihen, että viestien vastaanottajat tulevat huijatuksi ja reagoivat viestiin hyökkääjän toivomalla tavalla. Tavoitteena on, että tuloksia voidaan hyödyntää tiedeyhteisössä, mutta myös työelämässä esimerkiksi tietoturvakoulutuksien suunnittelussa.

Näkökulma on käyttäjälähtöinen siltä kannalta, että tutkimuksessa tarkastellaan sitä, miten käyttäjä tunnistaa tai jättää tunnistamatta huijausviestit. Vaikka tutkimustulokset ovat tarkoitettu organisaatioiden hyödynnettäväksi tietoturvakoulutuksia ajatellen, tutkimusta ei ole kirjoitettu organisaationäkökulmasta siten, että tutkimuksessa ei käsitellä syvällisesti organisaatioiden teknisiä tai hallinnollisia tietoturvakontrolleja. Tutkimuksessa ei käsitellä sitä, mitä seurauksia kalasteluviesteillä on organisaation, viestien vastaanottajien tai hyökkääjän näkökulmasta.

Aineisto ei sisällä tietoa vastaanottajien ominaisuuksista (kulttuuri, ikä, sukupuoli, uskonto ja muut mahdollisesti käyttäytymiseen tai kokemukseen vaikuttavat seikat) tai kognitiivisista resursseista (tunnetiloista, tai osaamisesta esimerkiksi tietotekniikkaan, tietoturvallisuuteen ja eri sovellusten käyttöön liittyen), vaikka näillä tekijöillä voi olla vaikutusta kalasteluviestinnän onnistumiseen. Kalasteluviestien ja kiireellisyyden kokemusta luovien elementtien tehokkuutta arvioidaan kirjallisuuskatsauksen, sekä tutkimusaineistossa kerätyn statistiikan osalta (kuinka moni henkilö avasi viestin, antoi tietoja tai latasi

haitallisen liitteen). Kalasteluyritysten tutkiminen rajoittuu kalasteluviesteihin ja niitä tukeviin kalastelupuheluihin, eikä tässä tutkimuksessa käsitellä muita kalastelumetodeja (mm. fyysinen tunkeutuminen, pikaviestintä, sosiaalinen media, kirjeet).

1.4 Tutkimusetiikka

Koehyökkäys, jossa simuloidaan tosielämän tilannetta, altistaa vastaanottajat petokselle mahdollisimman todenmukaisissa olosuhteissa. Tällainen hyökkäyssimulaatio voi aiheuttaa negatiivisia reaktioita ja vastaanottajat voivat kokea olonsa petetyiksi (Goel ym., 2017). Siksi on tärkeää, että hyökkäyssimulaatiot suunnitellaan siten, etteivät ne esimerkiksi loukkaa kenenkään yksityisyyttä. Hyökkäyssimulaatioiden tavoitteena on kehittää organisaation tietoturvallisuuskulttuuria, prosesseja ja osaamista kokonaisuutena, eikä esimerkiksi ”etsiä potentiaalisia syyllisiä tuleviin tietovuotoihin”.

Kampanjoiden aikana saatujen tietojen (tietovuotojen) ei ajatella olevan yksittäisten työntekijöiden vastuulla. Organisaation kehityskohteet löytyvät esimerkiksi organisaation koulutuksista (tai niiden puutteesta), epäselvistä tai päivittämättömistä prosesseista ja politiikoista, jotka eivät vastaa käytäntöä, heikoista (tai puuttuvista) tiedon luokitteluohjeista, puutteellisista tai toimimattomista teknologioista, suojaamattomista tiedonvaihtokanavista, epäselvistä vastuista ja heikoista raportointiprosesseista.

Usein organisaatiot, jotka tilaavat hyökkäyssimulaatioita, ilmoittavat henkilöstölleen testauksesta esimerkiksi YT-neuvottelujen kautta. Ilmoituksen sisältö voi esimerkiksi vain ilmoitus tietoturvallisuustestauksesta, tai yksityiskohtaisempi tiedote tulevista kalastelusimulaatioista.

Kalastelukampanjoissa, joiden tuloksia tässä Pro Gradu - tutkielmassa käytetään, ei vastaanottajille etukäteen kerrottu koehyökkäyksestä siten, että he olisivat tietäneet olevansa testauksen kohteena. Toisen ja kolmannen kampanjan välissä olevassa koulutuksessa kuitenkin kerrottiin perinpohjaisesti, miksi tällaisia koehyökkäyksiä tehdään ja mikä niiden tarkoituksena on. Koulutuksissa käytiin läpi kahden ensimmäisen kalastelukampanjan tuloksia sekä keskusteltiin siitä, miten kalasteluyritykset voidaan tunnistaa, miksi hyökkäykset usein toimivat, ja miten jatkossa tulisi toimia vastaavassa tilanteessa.

Koulutus sai erittäin hyvää palautetta ja kolmannessa kampanjassa henkilöt, jotka vielä klikkasivat kalasteluviestin linkkiä, palautettiin automaattisesti sellaiselle sivulle, jossa kerrottiin, että kyseessä oli simuloitu kalasteluhyökkäys. Sivustolla kerrattiin koehyökkäyksen tarkoitus sekä se, miten viestin olisi voinut tunnistaa huijaukseksi ja mikä on oikea tapa toimia tilanteessa, jos epäilee, että kyseessä on kalasteluyritys.

Vastaanottajille selvennettiin, ettei heidän henkilötietojaan koskaan kirjata minnekään, vaan kohdeorganisaation tilaajat saavat vain statistiikat (eli määrän, kuinka moni klikkasi linkkejä ja/tai luovutti tietoja). Sitä, kuka luovutti,

ei paljasteta, eikä talleteta. Raporttiin kirjataan siis vain, kuinka moni esimerkiksi salasanansa antoi, tai kuinka moni klikkasi haitallista linkkiä.

Kuitenkaan kalasteluviestin saaneille ei tarjottu mahdollisuutta jättää kirjallista palautetta. Jagatig ym. (2005) tarjosivat tällaisen palautteenantomahdollisuuden koehyökkäyksen jälkeen korkeakouluopiskelijoille (ks. tutkimuksesta lisää luvussa 2.2.3). Palautetta ja kommentteja pystyi antamaan anonyymisti keskustelufoorumilla, jonne kalasteluviestin vastaanottajat (eli tutkimukseen osallistuneet) kutsuttiin. Suuri osa palautteesta oli koetta tukevaa, mutta tutkimus sai myös 30 valitusta (1.7 % osallistujista) ja 7 osallistujaa (0.4 %) halusi, ettei heidän tuloksiaan käsitellä tutkimuksessa. Negatiivinen palaute sisälsi seuraavia elementtejä (Jagatic ym., 2005):

- **Viha.** Joidenkin osallistujien mielestä tutkimus oli epäeettinen, laiton, epäammattimainen, vilpillinen ja/tai hyödytön, ja että tutkijoita tulisi rangaista esimerkiksi irtisanomalla heidät (Jagatic ym., 2005). Vaikkei tutkimuksessa kerätty arkaluontoista dataa, uhrit (osallistujat) kokivat tulleensa huijatuiksi ja kärsivät negatiivisista psykologisista tuntemuksista. (Jagatic ym., 2005)
- **Kieltäminen.** Yksikään palautetta jättänyt ei myöntänyt tulleensa huijatuksi vaan moni ilmoitti, ettei koskaan menisi lankaan tällaisessa kalasteluhyökkäyksessä (Jagatic ym., 2005). Tästä voidaan päätellä, että oma haavoittuvuus voi olla vaikea myöntää ja kalasteluhyökkäykset voivat jäädä raportoimatta, jolloin esimerkiksi kyselytutkimuksien tuloksiin ei juuri voida luottaa. (Jagatic ym., 2005)
- **Sähköpostin väärinymmärtäminen.** Moni oli varma siitä, että tutkijat olivat hakkeroineet vastaanottajien sähköpostitilit, ja että se on ainoa mahdollinen tapa spoofata lähettäjän osoite eli esiintyä vastaanottajan tuntemana tahona (Jagatic ym., 2005). Tästä voidaan päätellä, että vain harva ymmärtää, kuinka helppoa spoofaus on ja moni aliarvioi sähköpostin ja tietoturvan. (Jagatic ym., 2005)
- **Omien, verkosta löytyvien julkisten tietojen vaarojen aliarviointi**. Moni ei ymmärtänyt, kuinka tutkijat olivat hankkineet tietoa vastaanottajien sosiaalisista verkostoista ja olettivat, että tutkijoilla on ollut pääsy vastaanottajien osoitekirjoihin (Jagatic ym., 2005). Osa taas piti julkisten tietojen käyttöä yksityisyyttä loukkaavana, joka viestii siitä, etteivät käyttäjät ymmärrä väärinkäytösten mahdollisuuksia julkaistessaan verkossa tietoja itsestään. (Jagatic ym., 2005)

Edellä mainittujen lisäksi, spoofauksen vuoksi osa luuli, että heidän koneellaan on virus, jonka vuoksi jotkut ovat saattaneet asentaa virustorjuntaohjelman ja vaihtaa salasanansa (Jagatic ym., 2005). Tutkimus on siis voinut aiheuttaa osallistujille stressiä, vaikkakin nämä varotoimet ovat harmittomia (Jagatic ym., 2005). Lisäksi palautesivusto sai niin paljon asiattomia ja loukkaavia viestejä, että sivusto jouduttiin sulkemaan kolmen päivän jälkeen, vaikkakin näistä viesteistä osa tuli kohdeyliopiston ulkopuolelta (Jagatic ym., 2005).

On mahdollista, ellei jopa todennäköistä, että vastaavia negatiivisia tuntemuksia on herännyt myös kohdeorganisaatiossa, jonka aineistoa käytetään tässä Pro Gradu - tutkielmassa. Epäselvää on, kannattaako organisaatioille luoda anonyymiä palautteenantoympäristöä, vai voiko se ruokkia mahdollisesti entisestään negatiivisia käsityksiä ja saada koehyökkäyksen negatiiviseen valoon. Olisi hyvä keksiä keino, jolla näitä kalastelun uhrien potentiaalisesti negatiivisia tuntemuksia voitaisiin hallita myös kampanjoiden aikana niin, ettei henkilöstö kuitenkaan tiedä olevansa testauksen kohteena.

Esimerkiksi opettavaisille ja selittäville infosivuille käyttäjän ohjaaminen kalasteluviestin sisältämän ”haitallisen” linkin kautta johtaa siihen, että testauskampanjoita osataan odottaa. Silloin tulokset eivät ole yhtä luotettavia. Ongelmana myös on, että jos käyttäjä tietää heti, että kyseessä oli testi, ei voida luotettavasti arvioida sitä, toimiiko organisaation sisäinen raportointiprosessi kalasteluyrityksiin liittyen halutulla tavalla. Yleensä organisaatio haluaa tietää, osaako henkilöstö raportoida hyökkäysepäilyksistään, ja kuinka raportit vastaanottava taho (usein IT-tuki) reagoi. Organisaation kannalta pahin tilanne on, jos kukaan kalasteluviestin saaneista ei raportoi epäilyksiään eteenpäin, tai että IT-tuki ei suhtaudu saamiinsa raportteihin vakavasti.

Usein myös yksiköissä työntekijät juttelevat vastaavista aiheista keskenään, jolloin sillä hetkellä, kun yksikössä ensimmäinen työntekijä klikkaa kalasteluviestiä ja ajautuu haitallisen linkin kautta infosivulle, on todennäköistä, että hän kertoo siitä koko yksikölle. Silloin hyökkäyssimulaation tulokset eivät vastaa tilannetta, jossa kohdeorganisaatio olisi pahantahtoisen hyökkäyksen alla, koska pahantahtoinen hyökkääjä ei kerro, että kyseessä on kalasteluyritys.

Jos hyökkäyssimulaation tulokset eivät ole luotettavia, ne eivät ole vertailukelpoisia, eikä organisaatio voi esimerkiksi mitata kehitystään statistiikkojen avulla vuosittaisten kampanjoiden tulosten kautta. Toisaalta, jos hyökkäyssimulaation tarkoitus on vain opettaa henkilöstöä toimimaan oikein ja tunnistamaan kalasteluviestit, eli simulaation on opetusväline eikä testaustyökalu, niin infosivulle palauttaminen on erittäin hyvä tapa hälventää kalasten uhrin mahdolliset epäilykset ja negatiiviset tuntemukset välittömästi.

2 KIRJALLISUUSKATSAUS

Kirjallisuuskatsaus on tehty siitä näkökulmasta, mitä, miten ja miksi kalasteluviestejä suunnitellaan, ja kuinka vastaanottajia voidaan johtaa harhaan siten, että hyökkääjä (viestin lähettäjä) saavuttaa tavoitteensa. Kiireellisyyden kokemuksesta kalasteluviestinnässä ei löytynyt juurikaan sellaisia lähteitä, joita olisi tässä tutkimuksessa voitu käyttää, joten kiireellisyyttä käsitellään pääaisassa käyttäytymistieteellisestä näkökulmasta. Kirjallisuuskatsauksessa käytetään sekä akateemisia, että ammatillisia lähteitä.

Syyt, joiden vuoksi vastaanottaja toimii kalasteluviestissä pyydetyllä tavalla vaihtelevat, mutta varsinainen toiminta (eli itse viestin klikkaus tai liitteen lataus) on syistä huolimatta aina sama (Ebot, 2017). Goel ym. (2017) jakaa kalasteluviestin käsittelyyn liittyvän prosessin seuraavasti: 1) petos, jossa vastaanottaja lukee viestin ja motivoituu toimimaan 2), vastaanottaja klikkaa viestin linkkiä ja ajautuu kalastelusivulle, sekä arvioi sivulla olevaa tietoa 3) vastaanottaja voi ajautua syvemmälle petokseen kalastelusivulla antamalla pyydettyjä tietoja, kuten luottokortin numeroita. Jo linkkiä klikatessa vastaanottaja on saattanut avata hyökkääjälle väylän (esim. vastaanottajan koneelle latautuu haittaohjelma tai takaovi, jonka kautta hyökkääjä voi vakoilla käyttäjää tai pahimmassa tapauksessa ottaa koneen haltuunsa), eli välttämättä kolmosvaiheen tietojen antoa ei edes tarvita (Goel ym., 2017). Tässä kirjallisuuskatsauksessa pyritään selittämään sitä, miksi näitä kalasteluviestejä klikataan.

2.1 Kalastelu osana laajempia kyberhyökkäyksiä

Kalasteluviestit ovat kyberhyökkäyksiä jo itsessään, mutta voivat toimia myös elementteinä laajemmissa kyberhyökkäyksissä, joissa hyökätään organisaation järjestelmiin tai tietovarantoihin. Jotta ymmärrettäisiin kalasteluilmiön moniulotteisuus ja tarkoitus, hyökkäyksen vaiheet on avattu tarkemmin tässä alaluvussa lyhyesti.

Lähteestä ja kontekstista riippuu, montako vaihetta hyökkäyksessä katsotaan olevan ja miten ne kuvataan. Esimerkiksi Hong (2012) jakaa kalasteluhyökkäyksen kolmeen vaiheeseen: ensimmäisessä vaiheessa vastaanottaja saa kalasteluviestin, toisessa vaiheessa vastaanottaja toimii halutulla tavalla (luovuttaa tietoja, asentaa haittaohjelman tai käy jossakin linkissä), ja kolmannessa vaiheessa hyökkääjä myy varastetut tiedot.

Yleensä sellaiset kalasteluyritykset, jotka eivät ole geneerisiä massahuijauksia (nk. nigerialaiskirjeitä), ovat osa jotakin kohdennettua kyberhyökkäystä. Hyökkäyksen kohteena voi olla esimerkiksi jokin tietty organisaatio, järjestelmä tai henkilö. Kalastelu, joka kohdennetaan vain ylimmälle johdolle ja arvovaltaisille henkilöille, kutsutaan nimellä ”whaling” (mm. Butavicius ym., 2015; Hong, 2012). Ylin johto on kiinnostava kohde, koska heillä on usein pääsy

arkaluontoisiin tietoihin sekä laajemmat käyttöoikeudet muuhun henkilöstöön verrattuna (Butavicius ym., 2015). Niemelän (2016) kuvaus kyberhyökkäyksen anatomiasta laajempi, kuin Hongin (2012), ja selittää paremmin sitä, kuinka etenkin kohdennettuja (kalastelu)hyökkäyksiä tehdään.

Kohdennetut kyberhyökkäykset alkavat tiedusteluvaiheella (1. vaihe), jossa hyökkäyskohteet, kuten verkkoinfrastruktuuri, toimipaikat ja henkilöstö kartoitetaan käyttämällä julkisia tietolähteitä eli esimerkiksi yrityksen omia verkkosivuja, julkisia hakemistoja ja sosiaalista mediaa (Niemelä, 2016).

Tiedustelua voidaan syventää käyttämällä social engineering -menetelmiä, keinoja, joilla manipuloidaan käyttäjiä, jotta voidaan saada tietoja, joita ei ole julkisesti saatavilla. Kalastelussakin hyödynnetään näitä menetelmiä. Hyökkääjä voi käyttää esimerkiksi 3+1-manipulointimenetelmää (Niemelä, 2016). Siinä hyökkääjä etsii usein julkisista lähteistä kolme kalastelun uhria koskettavaa asiaa, jota ovat totta (esimerkiksi työntekijän rooli, käytössä oleva järjestelmä ja käyttäjätunnus). Kertomalla kolme totuutta rakennetaan luottamusta hyökkääjän ja kohdehenkilön välillä, jolloin kohde helpommin uskoo neljännen asian, joka onkin valhe. Otetaan esimerkiksi seuraava dialogi, miten hyökkääjä voi esimerkiksi esiintyä oikean IT-tuen henkilön nimissä, ja soittaa hyökkäyksen kohteena olevan organisaation taloushallintojohtajalle:

> Taloushallintojohtaja: ”-Merja Miettinen puhelimessa”
> Hyökkääjä: ”-IT-tuesta Matti Mainio terve. Teidän käyttämänne taloushallintajärjestelmä Tehoeurot on ollut hyökkäyksen kohteena, ja sen seurauksena kaikki käyttäjälistat ovat jumiutuneet. Epäilen, että tunnuksesi ovat vuotaneet ja hyökkääjä on voinut käyttää niitä päästäkseen järjestelmään. Joudun nollaamaan tilisi ja lisäämään sinut uudelleen järjestelmään. Onhan käyttäjätunnuksesi miettinenm?”
> Taloushallintojohtaja: ”-On joo”
> Hyökkääjä: ”-Ja olihan salasanasi qwerty123?”
> Taloushallintojohtaja: ”-Ei, vaan Mustikoira2015”

Tässä esimerkkipuhelussa hyökkääjällä oli tiedossa taloushallintojohtajan tiedot (nimi ja puhelinnumero), käytössä olevan taloushallintojärjestelmän nimi, ja säännöt miten käyttäjätunnukset organisaatiossa muodostuvat. Käyttäjätunnuksen muoto on esimerkiksi voitu kysyä kalastelupuhelussa, joka on aiemmin soitettu jollekin muulle kohdeorganisaation henkilölle. On todennäköistä, että kalastelupuhelun uhri korjaa hyökkääjän antamaa väärää tietoa (tässä tapauksessa salasana) tai vuotaa muita tietoja, kun luottamus on kolmen totuuden avulla saavutettu.

Tiedusteluvaiheen jälkeen skannataan (2. vaihe) usein automaattisten työkalujen avulla kohdeorganisaation heikkouksia (Niemelä, 2016). Jos tiedusteluvaiheessa on esimerkiksi saatu selville, että kohdeorganisaation kriittiset tiedot sijaitsevat tietyssä järjestelmässä, voidaan tämän järjestelmän haavoittuvuuksia nyt etsiä automatiikkaa hyödyntäen. Maanläheisin käytännön tason vertauskuva skannausvaiheesta voisi olla, että murtoaikeissa oleva henkilö kulkee

kadulla kokeillen, onko jonkin kadulla olevan auton ovet jääneet auki. Kun haavoittuvuudet ovat kartoitettu, siirrytään varsinaiseen hyökkäysvaiheeseen (Niemelä, 2016). Varsinaisen hyökkäyksen (3. vaihe) tavoitteena on saada arvokasta tietoa tai päästä johonkin järjestelmään, ja kalasteluviestinnässä hyökkäys tapahtuu usein lähettämällä kalasteluviesti tai soittamalla kalastelupuhelu. Kalasteluviestinnässä tähän liittyy yleensä social engineering, eli käyttäjien manipulointi (Niemelä, 2016).

Hyökkäyksen onnistuttua hyökkääjä haluaa usein varmistaa, että hänellä on pääsy saamaansa tietoon tai järjestelmään (4. vaihe) niin pitkään kuin hän haluaa tai tarve vaatii (Niemelä, 2016). Hyökkääjä voi esimerkiksi luoda murtamaansa järjestelmään uuden käyttäjän ja teeskennellä olevansa yksi validi käyttäjä muiden joukossa (Niemelä, 2016).

Yleisesti ottaen on hyökkääjän edun mukaista pysyä huomaamattomana sen jälkeen, kun pääsy on saavutettu (Niemelä, 2016). Kun kalasteluviestinnän uhri ei huomaa tulleensa petetyksi, ei kohdeorganisaatiossa aktivoida mitään varotoimia ja esimerkiksi tarkisteta järjestelmän lokitietoja ja validoida olemassa olevia käyttäjätunnuksia. Näin hyökkääjälle jää aikaa kerätä tietoja ja halutessaan mahdollisuus suorittaa järeämpi hyökkäys haluttuna ajankohtana. Usein hyökkääjä ei halua jäädä kiinni, jolloin viimeinen (5. vaihe) kyberhyökkäyksen vaihe on jälkien peittely (Niemelä, 2016).

2.2 Ihmisten manipulointi käyttäytymisteorioiden näkökulmasta

Tässä alaluvussa käsitellään sitä, miten toiseen ihmiseen voidaan vaikuttaa käyttäytymistieteen näkökulmasta. Teoriat ovat usein oletuksia ja hyväksyttyjä näkökulmia, miten, milloin ja miksi jotakin ilmiötä, kuten ihmisten manipulointia, voidaan selittää (Bacharach, 1989). Teoriat perustuvat pääasiassa tutkimustietoon, ja ilmiötä selitetään usein yksinkertaisessa ja yleisessä muodossa.

Manipulointia käsitellään tässä alaluvussa siksi, että kalastelun tavoitteena on, että kalastelija eli hyökkääjä saa uhriltaan jotakin hyötyä, kuten tietoa, rahaa, tai pääsyn johonkin järjestelmään. Päästäkseen tavoitteeseensa, hyökkääjän on usein tehtävä petos huijaamalla tai johtamalla harhaan uhriaan (Hadnagy & Fincher, 2015). Petoksia käsitellään alaluvuissa 2.2.1-2.2.2.

Kalastelijat ymmärtävät, mitkä tekijät vaikuttavat ihmisten päätöksentekokykyyn ja toimintaan, ja hyväksikäyttävät tätä tietoa saadakseen ihmiset toiminaan haluamallaan tavalla (Hadnagy & Fincher, 2015). Suostuttelun periaatteita hyödyntämällä voidaan petoksen uhri saada reagoimaan halutulla tavalla. Voidaan ajatella, että suostuttelun periaatteita voi hyödyntää siinä, miten hyökkääjä viestinsä tai pyyntönsä esittää. Suostuttelua käsitellään alaluvussa 2.2.3.

Koska kalasteluviestinnän uhriksi joutuminen vaatii viestin vastaanottajalta toimia (linkin tai liitteen avaamista, tai tiedon luovuttamista), vastaanottajan toiminta liittyy päätöksentekoprosessiin. Sitä käsitellään luvussa 2.2.4.

Lopuksi luvussa 2.2.5 käydään läpi vielä yksilöllisiä ominaisuuksia, jotka voivat vaikuttaa kalastelun onnistumisen todennäköisyyteen.

2.2.1 Petosteoriat viitekehyksenä aiemmissa tutkimuksissa

Keskeisenä ajatuksena kalasteluviestinnän kontekstissa petosteorioissa on, että vastaanottajan aiemmat kokemukset vaikuttavat siihen, huomaako hän kalasteluviestit huijausyrityksiksi vai ei (mm. Viswanath ym., 2011; Wang ym., 2012). Petosteoriat (eng. Theory of Deception ja Interpersonal Deception Theory) selittävät informaation käsittelyä petostilanteessa. Siksi petosteorioita on käytetty aiemmissa kalasteluun liittyvissä tutkimuksissa (mm. Viswanath ym., 2011; Wang ym., 2012; Writgh & Marett, 2010) selittämään petosta, joka tapahtuu, jos hyökkääjä onnistuu kalasteluyrityksessään.

Petosteorian mukaan (Buller & Burgoon, 1996, Johnson, Grazioli, Jamal & Zualkernan, 1992; Mitchell & Thompson 1986; Thagard, 1992) petos on viestintää kahden tai useamman osapuolen välillä ristiriitatilanteessa, jossa toinen osapuoli (pettäjä) manipuloi toista (vastaanottajaa) esimerkiksi lähettämällä viestin, jonka johdosta petoksen uhri saa vääristyneen käsityksen tilanteesta ja sen seurauksena toimii pettäjän tahtomalla tavalla. Petosteorian mukaan yksilöt voivat tunnistaa petoksen vihjeistä, peilaten niitä omiin kokemuksiinsa ja kognitiivisiin toimintoihin (mm. Viswanath ym., 2011; Wang ym., 2012). Petosteorian mukaan petoksen prosessoinnissa on neljä vaihetta (Johnson ym., 1992; Viswanath ym. 2011; Wang ym., 2012):

1) aktivointi, jossa kohteet kiinnittävät huomiota petosta indikoiviin tekijöihin
2) hypoteesin muodostaminen petoksesta aiemmat yksilölliset kokemukset ja tiedot petoksista huomioiden,
3) hypoteesin arviointi
4) lopullinen ja subjektiivinen arvio siitä, onko kyseessä petos.

Petosteoriaa tutkineet Buller & Burgoon (1996) esittävät, että henkilöt, jotka tahtovat tehdä petoksen, keskittyvät tiedon, mielikuvien ja käyttäytymisen hallintaan. Tiedonhallinta liittyy viestin sisällön luotettavuuden kasvattamiseen. Esimerkiksi eheä, todenmukainen, merkityksellinen ja informatiivinen viesti lisää luotettavuutta ja vähentää epäilyjä. Mielikuvia voidaan hallita vaikuttamalla luottamuksen arvoiselta ja mukavalta, ja käyttäytymistä toimimalla siten, että se vähentää epäilyjä eivätkä petosta suorittavan tahon todelliset motiivit tule ilmi. (Buller & Burgoon, 1996)

Varhaisimmat petostilainteisiin liittyvät käytösteoriat ovat vuodelta 1968, Jolloin Maier ja Thurber tutkivat sitä, miten petos havaitaan erilaisissa haastattelutilanteissa. Vuonna 1974 Ekman ja Friesen tutkivat, millaisista ei-verbaaleista seikoista petoksen voi huomata. Myös Zuckerman on 1980-luvulla tutkinut sitä, miten petokset opitaan havaitsemaan (Zuckerman, Koestner & Alton, 1984).

On huomioitava, että varhaisimmissa tutkimuksissa käsitellään paljon verbaalisia seikkoja, kehonkieltä ja ilmeitä (Buller & Burgoon 1996; Kalbfleisch 1992; Ekman & Friesen 1974; Stiff ym., 1989). Kasvokkain viestintä on välitöntä, tietyssä paikassa ja tässä ajanhetkessä tapahtuvaa (Mehrabian, 1981; Wiener & Mehrabian 1968), eikä se siksi ole suoraan verrattavissa esimerksiksi sähköpostiviestintään, jossa vastaanottaja voi avata viestin missä ja milloin tahansa lähettäjästä riippumatta.

Buller & Burgoonin (1996) mukaan kasvokkain voidaan ajallisesti ja paikallisesti kokea ääntä, tilaa, kosketusta, katseita ja kehonkieltä. Mitä enemmän kokemuksellisia kanavia ja mitä fyysisesti lähempänä henkilöt ovat, sitä välittömämpi tilanne on. Välittömyys edesauttaa sitoutuneisuuden kokemusta osapuolten välillä. Ajallinen välittömyys saavutetaan tässä hetkessä, jolloin korostuu nykyinen hetki, eikä esimerkiksi menneisyys tai tulevaisuus (Buller & Burgoon, 1996).

Voidaankin ajatella, että kiireellisyyden kokemusta lisäävät elementit viestinnässä saavat vastaanottajan keskittymään nykyhetkeen, jolloin ajallinen välittömyys saavutetaan. Vahva kokemus sosiaalisesta läsnäolosta (tässä ja nyt) voi vaikuttaa viestien vastaanottokykyyn ja huomiointikykyyn, sekä johtaa mahdollisesti kognitiiviseen ylikuormitukseen häiriöihin ja tiedonkäsittelyyn liittyviin sekaannuksiin (Zajnoc, 1980). Kasvokkain tapahtuviin petoksiin liittyy oletettavasti sellaisia vaatimuksia, joita ei tarvitse täyttää ei-kasvokkain tapahtuvassa petoksessa (Buller & Burgoon, 1996). Esimerkiksi äänenpainoa tai katsetta ei vastaanottaja näe, eikä siten voi havaita petosta lähettäjän kehonkielestä (Wright & Marett, 2010).

Buller & Burgoon, 1996) toteavat, että ei-välittömässä, ei-kasvokkaisessa viestinnässä ilmenee usein etäisyyttä ja dissosiaatiota, kun taas välittömässä viestinnässä ilmenee psykologista ja fyysistä läheisyyttä sekä ajattomuutta. Voidaan olettaa, että sähköpostiviesintä on ei-välitöntä, koska viesti voi odottaa toisen laatikoissa eikä viestintä välttämättä ole reaaliaikaista. Wrightin ja Marettin (2010) mukaan kalasteluviestinnässä kommunikointi on interaktiivisuudeltaan rajoitettua siten, että huijausviestiä voidaan muokata vain ennen sen lähetystä, eikä hyökkääjä voi lukea vastaanottajan kehonkieltä. Vaikka sähköpostiviestissä vastaanottajalla on enemmän itsenäistä aikaa prosessoida viestiä, näyttää siltä, että moni siitä huolimatta tekee nopeita toimenpiteitä esimerkiksi poistamalla viestin, etsimällä lisätietoa siitä tai vastaamalla siihen (Wright & Marett, 2010). Tähän toimintaan liittyvät myös päätöksenteon kognitiiviset prosessit, joita on kuvattu luvussa 2.2.4.

Buller & Burgoon esittävät, että petosteoriaa on harvoin tutkittu aktiivisena kommunikaationa, vaan toimintana, jossa osapuoli lähettää toiselle jotakin, ja tuloksia tarkastellaan esimerkiksi motivaation, tavoitteiden ja tunteiden, eikä interaktion ja dialogin näkökulmasta. Petoksia voidaankin tarkastella myös keskinäisten ihmissuhteiden ja kommunikaation valossa, joissa tilanteen kulkuun vaikuttaa se, että henkilöt voivat vaikuttaa toisiinsa interaktiivisesti ja vapaasti (eng. Interpersonal Deception Theory). Wangin ym. (2012) ja Viswanathin ym. (2011) mukaan sähköpostiviestintä ei ole interaktiivista, koska se on vain

väline tavoittaa potentiaalisia uhreja. Kuitenkin tässä tutkielmassa argumentoidaan väitettä vastaan: sähköposti on väliinputoaja siinä mielessä, että vastaanottaja voi olla passiivinen tai vastata viestiin, jolloin viestinnästä tulee interaktiivista. Viestintä ei välttämättä ole etukäteen suunniteltua ja mietittyä, vaan voi olla myös tahatonta, alitajuista käytöstä. (Buller & Burgoon, 1996)

Buller & Burgoonin (1996) mukaan ihmissuhteet ja viestintä rakentuvat usein luottamukselle ja luottamus lisääntyy, kun oletetaan toisen osapuolen olevan rehellinen ja luotettava. Lisäksi odotetaan toteutuvan myös vastavuoroisuuden periaate, eli että ihmisten välisessä viestinnässä on oletus siitä, että kun antaa hyvää, saa takaisin hyvää (eng. ”good will”), eikä pahaa. Näitä oletuksia voidaan myös väärinkäyttää interaktiivisessa viestinnässä (Buller & Burgoon, 1996) suostuttelun periaatteina (ks. luku 2.2.3).

Wrightin ja Marettin tutkimuksessa ”The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived” (2010) pyritään ymmärtämään käyttäytymistä, joka voi lisätä vastaanottajan herkkyyttä luovuttaa kalastelijan pyytämiä henkilötietoja. Wrightin ja Marettin (2010) kiinnostuksen kohteena on petoksen onnistuminen. Petosteoriaa käytetään selittämään petosten uhrien antamia vastauksia kalasteluviesteihin ja tutkitaan petoksen onnistumista. Tutkimustulosten mukaan neljä eri käyttäytymistekijää vaikuttivat siihen, onnistuiko petos tai ei, eli luovuttivatko osallistujat arkaluontoisia tietoja kalasteluviestin lähettäjälle (Wright & Marett, 2010). Luvussa 2.2.5 käsitellään tarkemmin tätä tutkimusta, yksilöllisiä eroja ja käyttäytymistekijöiden vaikutuksia petoksen onnistumiseen.

Wangin ym., (2012) ja Viswanathin ym. (2011) mukaan vastaanottajalla on mahdollisuus tunnistaa petos aiempien kokemusten ja opittujen päättelyketjujen avulla kiinnittämällä huomiota kalasteluviestin epäjohdonmukaisiin yksityiskohtiin. Siitä huolimatta etenkin kohdennetussa kalastelussa petosta ei aina huomata. Pettämiseen liittyvien lainalaisuuksien ja näkökulmien ymmärtäminen voivat osaltaan selittää sitä, miksi uhrit eivät tunnista kalasteluviestintää huijaukseksi vaan usein lankeavat siihen ja tulevat petetyiksi.

2.2.2 Petoksen tunnistamisen haasteet

Tässä alaluvussa keskustellaan siitä, miten ja miksi petoksia tunnistetaan tai jätetään tunnistamatta. Esimerkiksi kiireellisiä toimia vastaanottajalta vaativa, huolimattomasti kirjoitettu viesti tulisi herättää vastaanottajassa valppautta ja epäilyksiä. Viestissä annetaan usein ymmärtää, että ellei vastaanottaja toimi pyydetyllä tavalla, seuraukset voivat olla kohtalokkaita. Epäilysten sijaan tai niistä huolimatta vastaanottaja usein hätääntyy ja toimii kuten viestissä pyydetään. Jos viesti on tavanomaisesta poikkeava tai se herättää vahvoja tunteita, kuten pelkoa, tulisi vastaanottajan aina rauhoittua ja harkita eri vaihtoehtoja ennen toimenpiteisiin ryhtymistä.

Petosteorian tutkijat ovat todenneet, että ihmiset olettavat lähtökohtaisesti toisten ihmisten olevan luotettavia tai puhuvan totta (Buller & Burgoon, 1996; Kalbfleisch, 1992), mikä tekee petoksen tunnistamisesta haastavaa. Sellaiset

henkilöt, jotka lähtökohtaisesti suhtautuvat toisiin varauksella eikä luottamuksella, kiinnittävät enemmän huomiota luotettavuuteen liittyviin tekijöihin (Buller & Burgoon, 1996).

Downs ym. (2006) haastattelivat kahtakymmentä tietokoneen käyttäjää (yksityishenkilöä) ymmärtääkseen käyttäjien strategioita ja päätöksentekoprosessia epäilyttäviä sähköposteja saadessaan. Haastatteluissa oli kaksi osiota: sähköpostin käyttö ja roolipeli -osio, jossa käyttäjät lukivat ja vastasivat erilaisiin sähköposteihin annetun identiteetin (roolin) pohjalta, sekä turvallisuus ja päätöksenteko -osio, jossa kysyttiin tietokoneen käyttöön sekä luotettavuuden kokemuksiin liittyviä kysymyksiä. Tulokset implikoivat, että käyttäjät voivat hallita tuntemiaan riskejä, mutta eivät tuntemattomia (Downs ym., 2006). Tunnetuilta sähköpostihuijauksilta osattiin suojautua paremmin kuin tuntemattomilta (Downs ym., 2006; Wang, 2012). Myös Goelin ym. (2017) tutkimuksessa arvioitiin, että pankkihuijauksen klikkausalttius jäi pieneksi mahdollisesti siksi, että kyseessä on niin tunnettu huijaus (ks. luku 2.3.1).

Keskiverto uhri tunnistaa petoksen vain noin 53-63 % tapauksista (Kalbfleisch (1992). Toisaalta henkilöt usein yliarvoivat kykynsä tunnistaa petokset, joka voi johtaa siihen, että uhri on varma, että totta puhuva henkilö on epärehellinen, ja samalla pettäjät voivat johtaa harhaan näitä vastaanottajia, jotka luulevat, etteivät he voi tulla huijatuiksi (Kalbfleisch, 1992).

Kalbfleischin (1992) mukaan eri ammattiryhmien (poliisit, psykologit, lainvalvonta, tuomarit) välillä ei kuitenkaan ole merkittäviä eroja siinä, tunnistetaanko petoksia vai ei. Kalbfleischin tutkimuksessa (1992) salaisen palvelun agentit Yhdysvalloissa saivat kuitenkin keskivertoa paremmat tulokset petosten tunnistamisessa. Tutkimustulosten mukaan naiset ovat hieman herkempiä tunnistamaan petoksen, mutta taas naiset pettävinä osapuolina jäävät petoksista kiinni useammin kuin miehet (Kalbfleisch 1992). Voidaan siis ajatella, että petoksen tekijäksi ja uhriksi parhaiten sopii mies, mutta ammattiryhmällä ei ole juurikaan merkitystä.

Buller & Burgoon (1996) toteavat, että petoksen vaikutuksia uhrin päässä on harvoin tutkittu. Kuitenkin, jos vastaanottaja (uhri) alkaa epäillä petosta, vastaanottaja käyttää usein strategisia keinoja, kuten harkittuja jatkokysymyksiä, selvittääkseen luotettavuutta (Buller & Burgoon 1996).

Maier ja Thurber (1968) totesivat tutkimuksessaan, että jos uhri vain kuuli tai luki lähettäjän viestin näkemättä lähettäjää, voitiin petos tunnistaa 77 % tapauksista, kun taas audio- ja videoaineistojen pohjalta petokset tunnistettiin vain 58 % tapauksista. Toisaalta Kalbfleisch (1992) toteaa tutkimuksensa pohjalta, että ne, jotka lukivat viestin näkemättä viestin lähettäjää, havaitsivat petoksen kaikista parhaiten. Tutkimuksia, jotka tukevat väitettä, että petos tunnistetaan paremmin kirjoitetusta viestistä verrattuna siihen, että uhri näkee ja/tai kuulee lähettäjää, on kuitenkin enemmän (Kalbfleisch 1992). Tämä tukee väitettä, että kalastelupuhelut voivat hyökkääjän kannalta olla tehokkaampia kuin kalasteluviestit.

Viestien vastaanottajat arvioivat viestien uskottavuutta seuraavien tekijöiden avulla: luonne (miten rehelliseltä ja luotettavalta lähettäjä vaikuttaa),

kompetenssi (miten osaavalta, vastuulliselta ja kokeneelta lähettäjä vaikuttaa), maltillisuus (miten valmiilta, rauhalliselta ja rennolta lähettäjä vaikuttaa), sosiaalisuus (miten ystävälliseltä lähettäjä vaikuttaa) sekä dynamiikka (miten energiseltä tai puheliaalta lähettäjä vaikuttaa (McCroskey, 1972; McCroskey & Young, 1981). Viestien uskottavuuteen vaikuttaa siis interaktiivisuus ja informaation prosessointiin liittyvät oletukset (Buller & Burgoon, 1996).

Buller & Burgoon (1996) viittaavat useisiin lähteisiin, joiden mukaan myös osapuolten yhteinen, ennalta tuttu käytösmalli (tyypillinen tapa toimia), lisää luottamusta verrattuna vieraiden ihmisten kanssa tapahtuvaan tai ennalta tuntemattomaan viestintään (Buller, Strzyzewski, & Comstock, 1991; Burgoon, Buller, Ebesu, & Rockwell, 1994; McCornack & Parks, 1986; Stiff, Kim, & Ramesh, 1989). Luottamussuhteet voivat vähentää uhrien kykyä huomata mahdollinen petos viestinnässä, kun taas vanhoihin käytösmalleihin perustuvat tutut tavat toimia voivat lisätä huomiokykyä petoksen havaitsemisessa, mikäli vanhasta tavasta poiketaan (Buller & Burgoon, 1996). Voidaan esimerkiksi olettaa, että jos HR-työntekijä saa usein viestejä käytössä olevalta rekrytointitoimistolta, hän avaa ne herkemmin kuin vieraiden rekrytointitoimistojen viestit. Kuitenkin, jos käytössä olevan rekrytointiviestin sisältö on normaalista poikkeava, se todennäköisesti herättää epäilyksiä. Kalbfleisch (1992) myös esittää, että jos osapuolet tuntevat toisensa, petos havaitaan helpommin, lukuun ottamatta läheisiä ja intiimejä suhteita, kuten parisuhteita. Esimerkiksi jos HR-työntekijä saa spoofatun sähköpostin hyvältä kollegaltaan, huijaus ei välttämättä mene läpi, koska HR-työntekijä saattaa huomata, että viesti on kirjoitettu tavanomaisesta poikkeavalla tavalla.

Motivaatio vaikuttaa kykyyn havaita petos (Buller & Burgoon, 1996). Mikäli vastaanottajalla (uhrilla) on saman tyyppiset tavoitteet kuin viestin lähettäjällä, vastaanottaja usein kiinnittää vähemmän huomiota viestin luotettavuuteen liittyviin tekijöihin (Buller & Burgoon, 1996). Ajatellaan esimerkiksi, että edellä mainittu HR-työntekijä toivoo rekrytointitoimiston ilmoittavan, että avoinna olevaan tehtävään on löytynyt erittäin lupaavia kandidaatteja. Tällaisen viestin saatuaan HR-työntekijä ei välttämättä kiinnitä juurikaan huomiota lähettäjän sähköpostisoitteen kirjoitusasuun tai allekirjoituksen yksityiskohtiin. Hadnagyn ja Fincherin (2015) mukaan kyseessä on ennakkoasenne, joka liittyy ihmisten taipumukseen hakea uskomuksilleen vahvistuksia (eng. confirmation bias). Jos henkilö esimerkiksi uskoo Dobermannin olevan aggressiivinen ja vaarallinen rotu, henkilö herkästi mieltää Dobermannin haukunnan aggressiiviseksi, eikä leikkisäksi. Sen sijaan, jos henkilö objektiivisesti arvioisi kaikkea saatavilla olevaa tietoa Dobermannien luonteesta, hän saattaisi tulla toiseen lopputulemaan haukkumisesta (Hadnagy & Fincher, 2015).

Tiivistettynä voidaan sanoa, että petoksen huomaamista edesauttaa, kun a) tiedetään, miten normaalitilanteissa viestitään, millainen on luotettava viestintä ja esimerkiksi tunnetaan viestin lähettäjä, sekä osataan tunnistaa mahdolliset petokset (kokemuksen tai koulutuksen kautta saatu tieto), b) kommunikointitaidot ja taidot kyseenalaistaa toinen osapuoli ja viestin luotettavuus, sekä c) kyky tunnistaa normaalista (normeista) poikkeava käytös (Buller & Burgoon,

1996). Vastaanottaja myös epäilee enemmän lähettäjää, jos lähettäjä on hermostunut, etäinen, kireä tai epävarma (Buller & Burgoon, 1996).

2.2.3 Suostuttelun periaatteiden käyttäminen kalasteluviestinnässä

Kalasteluviestintää voidaan ajatella toimintana, jossa lähettäjä pyrkii suostuttelemaan vastaanottajan toimimaan halunsa mukaan. Sellaisten (psykologisten) vaikuttamisen keinojen tunnistaminen, jotka johtavat hyökkääjän kannalta haluttuun lopputulokseen, auttavat ymmärtämään, ovatko jotkin kalasteluviestit suostuttelevampia kuin toiset. Wang ym. (2012) toteavat, että suostuttelutaktiikat pysyvät samoina, oli kyseessä sitten geneerinen tai kohdennettu kalastelu.

Cialdinin mukaan suostuttelutaktiikoita voi olla satoja tai tuhansia, mutta suostuttelun periaatteita on tunnistettu vain kuusi (Stitcher, 2018). Cialdinin suostuttelun periaatteet (2001) ovat laajimmin hyväksytty luokittelu suostuttelun strategioille (Butavicius ym., 2015). Cialdinin (2001) mukaan suostutteluun liittyviä periaatteita voi opettaa, opetella ja noudattaa. Kyseisiä periaatteita käytetään myös kalasteluviestinnässä, kun hyökkääjä tahtoo uhrinsa toimivan tietyllä tavalla. Cialdinin (2001) suostuttelun periaatteet ovat seuraavat:

- **Pitäminen** (engl. liking). Cialdinin (2001) mukaan ihmiset pitävät henkilöistä, jotka pitävät heistä. Samankaltaisuuden ja kehumisen on todettu lisäävän toisesta henkilöstä pitämistä. Samankaltaisuutta voi olla yhteenkuuluvuuden tunne tai kokemus esimerkiksi jaetuista arvoista, uskomusista tai harrastuksista. Kehut taas lisäävät välittämisen kokemusta sekä pitämistä, ja kehuilla voidaan parantaa tulehtuneita ihmissuhteita. (Cialdini 2001)
- **Vastavuoroisuus** (eng. reciprocity). Cialdinin (2001) mukaan ihmiset toimivat siten, kuin heitä kohti toimitaan. Jos esimerkiksi yritys tarjoaa lahjoja asiakkailleen, asiakkaiden halukkuus ostaa tuotteita kyseiseltä yritykseltä nousee. Johtaja voi hyödyntää vastavuoroisuuden periaatteella käyttäytymällä henkilöstöään kohtaan siten, kuin hän toivoo henkilöstönsä käyttäytyvän itseään kohtaan. (Cialdini 2001)
- **Sosiaalinen todiste** (eng. social proof). Cialdinin (2001) mukaan ihmiset toimivat siten, kuin heidän (sosiaalisesti) odotetaan toimivan. Periaatteeseen liittyy kokemus siitä, että ”näin kuuluu tehdä, koska muutkin tekevät näin” (Cialdini, 2001). Periaate pätee Cialdinin (2001) mukaan paremmin nk. horisontaalisissa ryhmissä, eikä niinkään ylhäältä alas (esimieheltä työntekijälle). Ryhmän tai yhteisön jäsenet siis ottavat mallia toisistaan. Ryhmä voi tarkoittaa esimerkiksi naapuruston asukkaita tai tiimiä yrityksessä. Butaviciuksen ym. (2015) mukaan sosiaalista todistetta voidaan kalasteluviestinnässä hyödyntää esimerkiksi antamalla vastaanottajan ymmärtää, että muut ovat jo hyödyntäneet tarjouksen, joka vastaanottajalle lähetetään.
- **Johdonmukaisuus** (eng. consistency). Cialdinin (2001) mukaan ihmiset noudattavat selkeitä sitoumuksiaan. Ihmisten tulee siis tuntea olevansa

sitoutuneita toimintaan. On todisteita siitä, että kirjoitetut tai ääneen todetut asiat, esimerkiksi tavoitteet, johtavat useammin tavoitteeseen pääsyyn, kuin sanomatta tai kirjoittamatta jätetyt tavoitteet. Tavoitteen julkiseksi tekeminen tai sen muodollisesti esittäminen (esimerkiksi työympäristössä) lisää sitoutuneisuutta. Ulkopuolinen painostus tai pakottaminen toimintaan, jota henkilö ei itse halua, ei kuitenkaan lisää sitoutuneisuutta. (Cialdini, 2001)

- **Auktoriteetti** (eng. authority). Cialdinin (2001) mukaan ihmiset tottelevat auktoriteetteja. Auktoriteetin asemaan pääsy edellyttää, että henkilöt tietävät auktoriteetin taustat ja luottavat hänen osaamiseensa (Cialdini, 2001). Butaviciuksen ym. (2015) mukaan kalasteluviestinnässä esimerkiksi toimitusjohtajalta tuleva pyyntö on tehokkaampi, kuin henkilöstöltä tuleva pyyntö. Auktoriteetti näyttää aiemman kalastelututkimuksen valossa olevan yksi tehokkaimmista suostuttelun periaatteista (esim. Butavicius ym., 2015; Workman, 2008).
- **Niukkuus** (eng. scarcity). Cialdinin (2001) mukaan ihmiset tahtovat asioita, joita heillä on vähän tai jotka eivät ole saatavilla. Rajoitettu tieto, taito tai resurssit koetaan arvoltaan arvokkaampina verrattuna tietoon, taitoon tai resursseihin, jotka ovat kaiken aikaa saatavilla (Cialdini, 2001). Periaatetta voidaan hyväksikäyttää esimerkiksi korostamalla sitä, mitä menetetään, jos ei toimita nyt halutulla tavalla (Cialdini, 2001). On näyttöä siitä, että menettämisen pelko johtaa varmemmin haluttuun toimintaan kuin tietoisuus siitä, mitä voi saada, jos tekee tietyllä tavalla. Cialdini (2001) kertoi tohtoriopiskelijansa tutkimuksesta, jossa oluen myynti kaksinkertaistui, kun ostajille kerrottiin, että sääolosuhteista johtuen oluen saanti voi lähitulevaisuudessa olla rajoitettua. Kun ostajille kerrottiin, että kukaan muu ei vielä tiedä mahdollisesta tulevasta rajoituksesta, myynti nousi 600 % (Cialdini, 2001). Butaviciuksen ym. (2015) ja Naidoon (2015) mukaan niukkuuden periaatetta voidaan kalasteluviestinnässä hyödyntää esimerkiksi väittämällä, että vastaanottajan saama tarjous on vain rajatun ajan saatavilla. Näin ollen voidaan yhdistää kiireellisyys ja niukkuus.

Nämä kaikki suostuttelun periaatteet ilmenevät myös kalastelukirjallisuudessa (esim. Hadnagy & Fincher, 2015). Hadnagy & Fincher (2015) mainitsevat suostuttelun keinoiksi vielä **velvollisuuden** (eng. obligation) ja **myönnytyksen** (eng. concession). Velvollisuuden periaate liittyy tunteisiin, tapoihin ja rooleihin. Velvollisuus eroaa vastavuoroisuuden periaatteesta siten, että jälkimmäinen keskittyy pääasiassa lahjojen antamiseen ja saamiseen (Hadnagy & Fincher, 2015). Myönnytys tarkoittaa periksi antoa, ja usein periksi antavat henkilöt tekevät näin myös jatkossa (Hadnagy & Fincher, 2015). Jos hyökkääjä saa uhriltaan kerran rahaa, se todennäköisesti saa sitä myös jatkossa (Hadnagy & Fincher, 2015).

Hadnagyn ja Fincherin (2015) mukaan myös syyn selittäminen suostuttelun kohteelle auttaa suostuttelijaa saamaan tahtonsa läpi. Hadnagy ja Fincher (2015) viittaavat tohtori Langerin, Blankin ja Chanowitzin tutkimukseen vuodelta 1978, jossa johtopäätöksenä oli, että minkä tahansa (järjettömänkin)

syyn tai perustelun kertominen edesauttaa suostuttelijaa (Hadnagy & Fincher, 2015).

Ebotin (2017) mukaan aiempaan tieteelliseen tutkimukseen perustuen hyökkääjät vaikuttavat kalasteluviestien vastaanottajaan käyttäen hyväksi vaikutelmaa luotettavuudesta, vastavuoroisuudesta, johdonmukaisuudesta tai niukkuudesta (esim. ”ainutkertainen tilaisuus”) tai esiintyen auktoriteettina. Nämä ovat kaikki Cialdinin (2001) suostuttelun periaatteita.

Myös periferisen ajattelutavan (ks. luku 2.2.4) hyväksikäyttöön hyökkääjän näkökulmasta liittyvät Workmanin (2008, 3) mukaan Cialdinin (20001) suostuttelun periaatteet. Ensin uhri halutaan johdatella periferisessä ajatteluprosessiin rationaalisen sijaan, jonka jälkeen suostuttelustrategioita voidaan hyödyntää (Workman, 2008).

Workman (2008) testasi suostuttelun periaatteiden teoriaa empiirisessä kenttätutkimuksessaan periferisten ajatteluprosessien kautta siitä näkökulmasta, miten henkilöitä voidaan suostutella ostamaan markkinointikampanjoiden avulla asioita ja voidaanko näitä tuloksia soveltaa myös käyttäjien manipulointiin. Workman (2008) käyttää tutkimuksensa teoriana prosessoinnin todennäköisyysmallia (eng. elaboration likelihood model, ks. luku 2.2.4) testaten sen soveltuvuutta selittämään käyttäjien manipulointiin liittyviä uhkia.

Workmanin (2008) kenttätutkimuksen kohdeorganisaatio oli yhdysvaltalainen vakuutus- ja finanssialan laitos, ja tutkimusaineisto on kerätty kyselyiden ja objektiivisen havainnoinnin avulla. Kohderyhmä (850 henkilöä) valittiin satunnaisesti, ja kattavia vastauksia saatiin 69 %:lta. Objektiiviset havainnot kerättiin koehyökkäyksistä, joissa testattiin henkilöiden toimintaa ”tositilanteessa”. Workmanin (2008) tutkimustulokset osoittavat muun muassa, että luottamus, pelko ja sitoutuneisuus korreloivat käyttäjien manipuloinnissa ja esimerkiksi henkilöt, jotka tottelevat auktoriteettia, todennäköisemmin altistuvat kalastelulle, mikäli hyökkääjä esiintyy auktoriteettina. Usein hyökkääjät hyödyntävät tätä esiintyen esimerkiksi tunnetun organisaation nimissä niin, että viesti on usein brändätty logoineen päivineen kyseisen organisaation näköiseksi (Wright & Marett, 2010).

Myös henkilöt, jotka ovat luottavaisia, altistuvat kalastelulle todennäköisemmin kuin vähemmän luottavaiset henkilöt (Workman, 2008). Osaan henkilöistä toimi paremmin luottamuksen herättäminen ja ystävällisyys, kun taas osa on suostuvaisempia auktoriteetteihin ja pelkoon (Workman, 2008). Workman (2008) suosittelee esimerkiksi, että johtajat opettaisivat henkilöstöä olemaan sitoutuneita suojelemaan organisaatiota uhilta, ja että kaikessa tiedonvaihdossa tulisi noudattaa tarveperustaista arviota (eng. ”need to know”), jotta arkaluontoinen tieto ei joutuisi henkilöille, jotka eivät sitä tarvitse.

Jagatic ym. (2005) tutki, kuinka helposti ja tehokkaasti hyökkääjä voi käyttää sosiaalisten verkostojen dataa parantaakseen kalasteluviestinsä toimivuutta. He toteuttivat koehyökkäyksen Indianan yliopiston 18-24-vuotiaille opiskelijoille siten, että kohteena oli yhteensä 1731 henkilöä, joista löytyi helposti tietoa avoimista lähteistä verkossa. Toiselle kohderyhmälle lähetettiin opiskelijan tunteman henkilön nimissä spoofattu kalasteluviesti, jossa haluttiin

vastaanottajan klikkaavan haitallista linkkiä, joka ohjasi vastaanottajan yliopiston kloonattuun portaaliin ja pyydettiin yliopiston käyttäjätunnusta sekä salasanaa. Toiselle kohderyhmälle lähetettiin vastaava viesti, mutta fiktiivisen henkilön nimissä yliopiston osoitteesta. Tutun henkilön lähettämänä klikkausalttius ja tunnusten antajien määrä oli 72 %, kun tuntemattoman henkilön lähettämänä viestin avasi ja tunnukset antoivat vain 16 % vastaanottajista. Tutkimustulokset osoittavat, että jos hyökkääjä esiintyy uhrin tuttavana, hyökkäys onnistuu neljä kertaa todennäköisemmin (Jagatic ym., 2005). Pääaineella oli pieniä eroja tuloksiin, lisäksi naiset avasivat ja antoivat tietonsa useammin kuin miehet. Lähettäjän sukupuolella ei sen sijaan ollut vaikutusta (Jagatic ym., 2005). Käyttäjätunnuksia ja salasanoja ei todellisuudessa tutkimuksessa kerätty, ja kyseisen kohdennetun kalasteluviestin toteutus on idealtaan sama kuin tässä tutkimuksessa osana aineistoa ollut toisen kalastelukampanjan viesti (luku 3.2.2).

Myös Butavicius ym. (2015) tutkivat suostuttelun periaatteiden (auktoriteetin, niukkuuden ja sosiaalisen todisteen) vaikutusta vastaanottajien arviointikykyyn kalasteluviestin luotattavuudesta. Tutkimukseen rekrytoitiin 121 bisnes- ja tietojärjestelmätieteen 18-29-vuotiasta opiskelijaa Etelä-Australian yliopistosta, ja heille lähetettiin kontrolloiduissa (laboratorio)olosuhteissa tavallisia viestejä, kalasteluviestejä tai kohdennettuja kalasteluviestejä (yhteensä 12 erilaista).

Auktoriteettia hyödyntävät viestit saivat vastaanottajan vakuuttuneimmaksi siitä, että viestin sisältämä linkki on turvallinen (Butavicius ym., 2015). Tutkimukseen osallistujat myös epäonnistuivat erottamaan tavalliset viestit haitallisista viesteistä silloin, kun viestissä esiinnyttiin auktoriteetin nimissä (Butavicius ym., 2015). Sosiaalista todistetta hyväksikäyttävät viestit vastaanottajat tunnistivat kalasteluksi helpoiten (Butavicius ym., 2015). Myös henkilöt, jotka olivat vähemmän impulsiivisia päätöksenteossa, pitivät todennäköisemmin linkkiä haitallisessa viestissä turvattomana (Butavicius ym., 2015).

Kalasteluviestinnässä kognitiivisilla prosesseilla on vaikutusta siihen, mitkä viestit onnistuvat. Osa näistä prosesseista on kultuurisidonnaisia (Stitcher, 2018). Näin ollen esimerkiksi auktoriteettiin perustuvat viestit voivat olla tehokkaampia Lähi-Idässä kuin pohjoismaissa ja Välimerellä ystävyys voi toimia suostuttelun keinona paremmin (Stitcher, 2018).

Cialdinin mukaan suostuttelun uhriksi joutumiselta voi välttyä, jos osaa kyseenalaistaa oman toimintansa siinä vaiheessa, kun on suostumassa toisen pyyntöön (Stitcher, 2018). Silloin tulisi kysyä itseltään, mitä pyytäjä on tehnyt tai sanonut ja mitkä ovat todisteet näistä asioista, jotta pyyntöön kannattaa suostua. Tavoitteena on olla luottamatta intuitioon ja olla toimimatta "siten mikä tuntuu normaalilta", vaan kyseenalaistaa tekijät, jotka vaikuttavat päätöksentekoon. (Stitcher 2018)

Cialdinia haastateltiin myös Stitcherin The Social Engineer Podcastissa (9.4.2018), jossa aiheena oli Cialdinin uusi kirja "Pre-Suasion". Kirjassa käsitellään niitä seikkoja, jotka vaikuttavat henkilön päätöksentekoon jo ennen kuin varsinainen pyyntö on esitetty. Nämä seikat ovat jo johtaneet tilanteeseen, jossa

henkilö kokee, että tulevaan pyyntöön tulee suostua (esim. vastavuoroisuuden periaate).

Asioiden muotoilu (eng. Framing effect) vaikuttaa siihen, mihin tulokseen päätöksentekijä tulee (Hadnagy & Fincher, 2015). Cialdinin mukaan esimerkiksi eräässä hyväntekeväisyyskampanjassa "Even a penny would help" -lauseen lisääminen kampanjaan nosti kampanjaan osallistumisprosentin 30:stä 50 prosenttiin, ja lahjoituksen keskiarvo pysyi samana (Stitcher, 2018). Cialdini perustelee osallistumisprosentin nousua analysoimalla, että osallistujat ovat ajatelleet: "what kind of person wouldn't give a penny?" (suom. millainen ihminen ei voisi lahjoittaa penniä?). Kampanja osoittaa, että kontekstilla eli sillä, miten asiat on ilmaistu, on merkitystä. Samaan tulokseen tulevat Hadnagy ja Fincher (2015), jotka esittävät, että esimerkiksi 80 % rasvattomaksi mainostettu liha myy paremmin, kuin 20 % rasvaa sisältävä liha, vaikka kyseessä on sama tuote. Asioiden esitystapa (konteksti) vaikuttaa siis vastaanottajan reaktioon.

Myös ulkonäöllä on vaikutusta. Cialdini esittää, että mikäli huonekaluja myyvän verkkokaupan taustakuva on "kotoisa ja pörröinen", ihmiset ostavat enemmän mukavia huonekaluja (Stitcher, 2018). Jos taustalla on kolikon kuvia, mielentila keskittyy kustannuksiin, jolloin ostetaan edullisimpia huonekaluja. Kyse on "Pre-Suoasionissa" Cialdinin mukaan siitä, millaiseen mielentilaan ihmiset ohjataan. Tässä tutkielmassa kalasteluviestien kontekstia (sisältöjä) ja ulkonäköä tarkastellaan enemmän luvussa 2.3.

Viestin lähettäjä pyrkii siis muokkaamaan sitä, missä kontekstissa tai mihin henkilö vertaa saamaansa viestiä, jolloin erilaisia kognitiivisia prosesseja aktivoituu. Kalasteluviestit, jotka viestivät esimerkiksi visuaalisilla tekijöillä kiireestä ja poikkeustilanteesta saattavat tehdä henkilön tietoiseksi päätöksentekotilanteesta, miten tulisi toimia. Toisaalta viestit, jotka näyttävät mahdollisimman tavanomaisilta ja tutuilta pyrkivät välttämään tietoista pohdintaa ja saaman henkilön toimimaan, kuten ennenkin. Päätöksentekoa käsitellään tarkemmin seuraavassa alaluvussa (2.2.4).

2.2.4 Päätöksentekoon liittyviä vaikuttajia

Tässä Pro Gradu - tutkielmassa käytössä ollut aineisto ei sisällä tietoa siitä, onko kalasteluviestin vastaanottaja tehnyt tietoisen päätöksen siitä, toimiiko hän viestissä halutulla tavalla, vai onko vastaanottaja toiminut esimerkiksi vahingossa tai vaistonvaraisesti. Päätöksenteko kuitenkin liittyy oleellisesti siihen, kokeeko vastaanottaja olevansa valinnan edessä (esimerkiksi klikkaako hän viestissä ollutta linkkiä tai lataako hän viestissä olleen liitteen), vai ei.

Päätöksentekoa aiheena käsitellään paljon aiemmassa tutkimuksessa (esim. Goel, 2017; Viswanath, 2015; Viswanath ym., 2011; Wang ym., 2012) ja ammatillisessa kirjallisuudessa (esim. Hadnagy & Fincher, 2015) kalastelukontekstiin liittyen. Päätöksenteossa hyökkääjä houkuttelee uhria tekemään epärationaalisen päätöksen esimerkiksi tunteiden pohjalta sen sijaan, että vastaanottaja käyttäisi päätöksenteossa loogista ajattelua (mm. Goel ym., 2017; Workman, 2008).

Tässä Pro Gradu - tutkielmassa kuvataan kalastelua ilmiönä ja siksi esitellään päätöksentekoa siltä osin, kuinka se selittää kalasteluviestien toimivuutta. Aihetta lähestytään siitä näkökulmasta, että vastaanottaja tekee päätöksen joka tapauksessa viestin saadessaan. Päätöksentekoon liittyy se, koetaanko viestin tiedot riittävinä siten, että vastaanottaja voi toimia intuition, tapojen tai vaistonsa varassa, vai tarvitseeko hänen arvioida viestiä systemaattisesti. Vastaavaa näkökulmaa käyttää myös esimerkiksi Viswanath tutkimuksessaan (2015).

Vishwanathin (2015) mukaan kalastelun uhriksi joutuneet eivät todennäköisemmin prosessoi tietoa systemaattisesti, eli eivät ajattele kognitiivisesti tai tee tietoisia päätöksiä. Tiedostamaton päätöskin on kuitenkin päätös. Jos henkilö systemaattisesti prosessoi vastaanottamaansa sähköpostia epäillen sitä kalasteluksi, hän tarkastelee sitä aiempien kokemuksiensa ja oppiensa pohjalta ja muodostaa tietoisen päätöksen (mm. Ebot, 2017; Viswanath, 2015). Vastaanottajat, jotka prosessoivat informaatiota systemaattisesti, huomaavat herkemmin kalasteluviestin huijausyritykseksi (Viswanath, 2015).

Perifeerisessä prosessoinnissa (eng. peripheral processing) systemaattisen prosessoinnin ja viestin (tietoisen) analysoinnin sijaan vastaanottaja keskittyykin viestin nopeaan prosessointiin ja houkuttelevuuteen (mm. Ebot, 2017; Viswanath, 2015; Viswanath ym., 2011; Wang ym., 2012). Goel ym. (2017, s. 27) määrittelevät tutkimuksessaan perifeeristä ajattelua viittaamalla Pettyn ja Cacioppon vuoden 1986 prosessoinnin todennäköisyysmalliin (eng. Elaboration likelihood model), jonka mukaan suostuttelun kohde valitsee joko suoran tai periferisen tavan prosessoida tietoa. Periferinen ajatteluprosessi on luonnollinen ja nopeampi tapa prosessoida tietoa (Butavicius ym., 2015). Se ei vaadi yhtä paljon kognitiivisia ponnisteluita (Viswanath, 2015).

Suora tapa perustuu rationaaliseen ajatteluun ja tiedonkäsittelyyn, kun taas periferinen malli perustuu vihjeisiin ja nk. ”ajattelun oikoteihin”, jotka voivat ohittaa järkiajattelun (mm. Butavicius ym., 2015; Geol ym., 2017; Viswanath, 2015). Voidaan ajatella, että periferinen prosessointi on verrattavissa siihen, että vastaanottaja näkee ja uskoo viestistä sen, mitä haluaa nähdä (”Olet voittanut arvonnassa!”) sen sijaan, että kiinnittäisi huomiota siihen seikkaan, ettei vastaanottaja ole osallistunut mihinkään arvontaan, tai että viesti tulee epämääräisestä osoitteesta. Suuri osa kalasteluviesteistä prosessoidaan periferisen mallin mukaan (Viswanath ym., 2011).

Kalasteluviestien sisällöt on usein pyritty suunnittelemaan siten, että ne esimerkiksi kiireellisyydellään tai auktoriteetin asemaa käyttämällä pyrkivät herättämään vastaanottajassa periferisen ajatteluprosessin rationaalisen prosessin sijaan (Naidoo, 2015; Goel ym., 2017; Wang ym., 2012) tai sotkemaan rationaalista päätöksentekoprosessia (Wang ym., 2012). Viswanath (2015) viittaa heuristis-systemaattiseen malliin (eng. Heuristic-Systematic Model) ja toteaa, että hyökkääjä voisi käyttää periferista prosessointia hyväksi esimerkiksi spoofaamalla viestin lähettäjäksi jonkun vastaanottajan ystävän, jolloin vastaanottaja saattaisi klikata viestin haitallista linkkiä ajattelematta enempää ”ystäviin voi luottaa”-heuristiikan vuoksi. Heuristiikalla tarkoitetaan tässä yhteydessä, että käyttäjillä on muistissaan ”sääntöjä” perustuen aiempiin kokemuksiin, ja tietyt

vihjeet ohjaavat päätöksentekoprosessia toimimaan näiden sääntöjen mukaan, jolloin tiedon käsittely voi olla valikoitua ja rajallista (Wang ym., 2012). Eli vastaanottajan tuttu osoite voi esimerkiksi ohjata käyttäjän toimimaan sen säännön mukaan, että ystäviin voi luottaa.

Viswanath (2015) tutki kognitiivisten prosessien ja tapojen vaikutusta kalastelun uhriksi tulemiselle. Tutkimuksessa simuloitiin oikeaa kalasteluhyökkäystä ja kalasteluviestejä lähetettiin satunnaiselle 200 korkeakouluopiskelijalle Buffalon yliopistossa. Kohderyhmältä kysyttiin etukäteen lupa tutkimukseen. Lähetetyssä kalasteluviestissä kerrottiin, että sähköpostitili suljetaan ja vastaanottajan tulee klikata viestin hyperlinkkiä. Hyperlinkki johti kyselyyn, jossa pyrittiin selvittämään, miksi vastaanottaja klikkasi linkkiä. Tutkijat mittasivat myös teknisin keinoin, kuinka moni avasi viestin ja kuinka moni avasi viestin linkin. Niille, jotka eivät olleet avanneet viestiä, lähetettiin muistutus ja niille, jotka olivat avanneet viestin mutta jotka eivät olleet täyttäneet kyselyä, tutkijat soittivat vastausten saamiseksi. (Viswanath, 2015)

Viswanathin (2015) tutkimuksessa 200 vastaanottajasta 192 vastasi lopulta kyselyyn, ja vain 8 ei avannut kalasteluviestin linkkiä tai ei vastannut kyselyyn. Jos avasi viestin, muttei klikannut haitallista linkkiä, tutkimuksessa vastaanottajaa ei katsottu kalastelun uhriksi. Siten uhreiksi laskettiin lopulta 159 vastaanottajaa (83 % kaikista viestin saaneista). Viswanathin (2015) tutkimustulosten mukaan yksilöt, jotka olivat tunnollisia ja ne, jotka olivat emotionaalisesti epätasapainoisia, omasivat vahvat (impulsiiviset) sähköpostinkäyttötavat (sähköpostia avattiin usein ja siihen reagoitiin). Nämä luonteenpiirteet eivät kuitenkaan tulosten mukaan vaikuttaneet siihen, aktivoituiko heuristinen vai systemaattinen prosessointi vastanottajan tehdessä päätöstä siitä, avaako linkin vai ei. Kuitenkin systemaattinen prosessointi aktivoitui silloin, kun kalasteluviestin tiedot koettiin riittämättömiksi. Systemaattinen prosessointi vähensi huomattavasti kalastelun uhriksi joutumista. Henkilöt, jotka käyttävät sähköpostia ”tapojensa orjina” ja prosessoivat kalasteluviestin heuristisesti, tulevat todennäköisemmin kalastelun uhreiksi. (Viswanath, 2015)

Tiivistettynä, vastaanottajalla aktivoituu periferinen tai suora prosessimalli riippuen siitä, havainnoiko hän viestin tiedot riittäviksi, viestin vihjeiden (esim. lähettäjän nimi) ja päätöksen merkityksellisyyden pohjalta (Viswanath, 2015). Jos tiedot koetaan riittämättömiksi ja/tai päätös tärkeäksi, kognitiiviset toiminnot ja systemaattinen prosessointi aktivoituu (Viswanath, 2015).

Samassa kontekstissa Viswanath (2015) puhuu median käyttöön liittyvistä tavoista tai mentaalisista skripteistä, jotka johtavat petetyksi tulemiseen. Tavat voivat olla automaattisia. Tapa voi olla esimerkiksi tarkistaa sähköpostit (ja klikata niiden linkit) useita kertoja päivässä (Viswanath, 2015). Ihminen toimii tapansa ohjaamana helposti tiedostamattaan, huomaamattaan ja tahattomasti (Viswanath, 2015; Viswanath ym., 2011). Välillä esimerkiksi sähköpostien tarkastaminen voi olla tietoista ja kontrolloitua, välillä taas tiedostamatonta (esim. autolla ajaessa) (Viswanath, 2015; Viswanath ym., 2011). Viswanath (2015) kysyykin, johtavatko tavat tiedon prosessointiin vai tiedon prosessointi tapoihin.

Aiempi tutkimus ei anna yksiselitteistä vastausta sille, mikä on prosessointimallin ja tapojen vaikutus päätöksentekoon (Viswanath, 2015).

Päätöksenteko ei siis aina ole loogista eikä rationaalista. Sitä ohjaavat mielentila, tunteet, kyky havainnoida sekä kognitiiviset ennakkoasenteet ja -luulot, jotka usein pohjautuvat aiempiin kokemuksiin (Hadnagy & Fincher, 2015). Suuret tunteet voivat sulkea järkiperäisen ja loogisen ajattelun pois jopa kokonaan, joka voi johtaa erittäin huonoihin päätöksiin (Hadnagy & Fincher, 2015). Jos henkilö huomaa reagoivansa vahvasti ja tunteikkaasti sillä hetkellä, kun päätös tulisi tehdä, olisi hyvä ottaa vähintään kolmenkymmenen sekunnin tauko ennen kuin mitään päätöstä tai toimea tekee (Hadnagy & Fincher, 2015).

Alla oleva kuva 1 kuvaa päätöksentekoon liittyvää prosessia. Kuvio on suomennettu versio Hadnagyn ja Fincherin alkuperäisestä kuviosta ”Emotional decision-making cycle” (2015, s. 43).

Kuva 1 Tunteisiin perustuva päätöksentekoprosessi

Kalastelijat pyrkivät usein vaikuttamaan vastaanottajan päätöksentekokykyyn ja logiikkaan viesteillä, jotka herättävät vastaanottajissa vahvoja tunteita (Hadnagy & Fincher, 2015). Vahvat tunteet herättävät vastaanottajassa fyysisiä reaktioita, kuten verenpaineen nousua, ja mikäli ärsyke on riittävän vahva, henkilö voi menettää kykynsä arvioida tilannetta kriittisesti (Hadnagy & Fincher, 2015). Käytännössä voidaan ajatella, että jos hyökkääjä voi vaikuttaa uhrinsa stressitasoon, he voivat vaikuttaa myös uhrin päätöksentekoon (Hadnagy & Fincher, 2015). Vahvojen tunteiden herättäminen voi saada vastaanottajan toimimaan hetkellisesti tavalla, joka ei ole vastaanottajan edun mukaista (Hadnagy & Fincher, 2015).

On tutkittu, että esimerkiksi univaje vähentää negatiivisten seurausten prosessointia ja lisää optimismia (Hadnagy & Fincher, 2015). Väsyneenä henkilö voi siis yliarvioida mahdollisuutensa onnistua. Myös nälkä lisää

riskinottohalukkuutta päätöksenteossa (Hadnagy & Fincher, 2015). Joskus teemme pieniä tai suuria päätöksiä miettimättä lainkaan (Hadnagy & Fincher, 2015).

Hadnagyn ja Fincherin (2015) mukaan ennakkoasenteet ja -luulot voivat auttaa tekemään parempia tai huonompia päätöksiä. Huonoon päätökseen johtanut päätöksentekoprosessi voi johtua siitä, ettei henkilö ole huomioinut kaikkea saatavilla olevaa tietoa. Tämä on tyypillistä päätöksille, jotka muodostetaan ennakkoasenteiden ohjaamina. (Hadnagy & Fincher, 2015)

Hadnagyn ja Fincherin (2015) mukaan eräs ennakkoasenne, mikä vaikuttaa päätöksentekokykyyn, on saatavuuteen liittyvä heuristiikka (eng. availability heuristic). Sillä tarkoitetaan päätöksentekoa nopeuttavaa tietoa, joka on heti muistivarannoista saatavilla. Mieleen jääneet asiat voivat korostaa tai liioitella jonkin asian merkitystä. Esimerkiksi moni saattaa ajatella, että hait tuottavat enemmän kuolemia kuin myyntiautomaatit, vaikka tilastojen mukaan tämä ei ole totta. Päätelmä saattaa johtua siitä, että haiden hyökkäyksistä uutisoidaan enemmän kuin myyntiautomaattien tuottamista kuolemista. (Hadnagy & Fincher, 2015)

Hyökkääjä voi pyrkiä kontrolloimaan ja määrittämään uhrinsa käytöstä myös rangaistuksen kautta (Hadnagy & Fincher, 2015). Rankaiseminen ei ole manipulointia, vaan suoraa vaikuttamista siihen, että teolla on negatiiviset seuraukset. Vakavat rangaistukset aiheuttavat reaktioita, ja hyökkääjät osaavat hyväksikäyttää näitä reaktioita (Hadnagy & Fincher, 2015).

Hadnagy & Fincher (2015) esittävät myös manipulointiin liittyvät piirteet, joiden tavoitteena on vaikuttaa uhrin päätöksentekoprosessiin. Näitä piirteitä ovat a) **altistaminen** erilaisin keinoin, jotta henkilö on herkempi tekemään huonoja päätöksiä, b) **ympäristön kontrollointi** esimerkiksi soluttautumalla uhrin sosiaalisiin piireihin, c) **pakotettu uudelleenarviointi,** jolloin uhri kyseenalaistaa oppimansa asiat ja alkaa toimia hyökkääjän haluamalla tavalla, d) **valta-asetelman poistaminen** siten, että uhri kokee, ettei voi muuta, kuin totella, jo edellä mainittu e) **rangaistus** ja f) rangaistuksilla **uhkailu** (Hadnagy & Fincher 2015). Voidaan esimerkiksi ajatella, että hyökkääjä haluaa alistaa uhrinsa stressille ja tekemään hätäisiä päätöksiä lisäämällä kalasteluviestiin kiireellisyyden kokemukselle altistavia elementtejä.

Hadnagy & Fincher (2015) esittävät viisi askelta, jotka voivat johtaa harkitumpaan päätöksentekoprosessiin antautumatta esimerkiksi tunteiden tai ennakkoasenteiden valtaan. Ne ovat seuraavat:

1) varmistuminen siitä, että tilanteesta on hyvä ymmärrys; onko asiasta riittävästi tietoa ja tulisiko huomioida muidenkin näkökulmia
2) kaiken mahdollisen tiedon keruu aiheesta; vaikuttaako päätöksentekoon joku, herättääkö aihe vahvoja henkilökohtaisia tuntemuksia
3) muiden vaihtoehtojen harkinta; mitkä ovat mahdolliset seuraukset ja muut näkökulmat asiaan
4) varsinainen päätöksenteko

5) päätöksen arviointi.

2.2.5 Vastaanottajien yksilöllisten erojen vaikutukset toimintaan

Tässä Pro Gradu - tutkielman aineistossa ei ole kerätty tietoa yksilöllisistä tekijöistä tai henkilöiden kokemuksista, mutta huomioitavaa on, että myös esimerkiksi kiireellisyyden kokeminen voi vaikuttaa yksilöihin eri tavoin. On mahdollista, ellei jopa todennäköistä, että vastaanottajasta riippuen saman viestin kiireellisyys koetaan eri tavoin. Esimerkiksi henkilö, joka saa kalasteluviestin, että ”tunnuksesi ovat vuotaneet, käy vaihtamassa salasanasi heti”, muttei juuri koskaan käytä kyseistä järjestelmää tai ei pidä siinä olevaa tietoa merkityksellisenä, ei myöskään koe salasanan vaihtoa kiireelliseksi seikaksi. Sen sijaan esimerkiksi tietoturvasta valveutuneempi henkilö saattaa pitää kyseistä viestiä erittäin kiireisenä ja välittömiä toimia vaativana. Eri asia on, epäileekö vastaanottaja mitään tai huomaako vastaanottaja tulleensa huijatuksi.

Petosteoriaa (luku 2.2.1) tutkineet Buller & Burgoon (1996) olettavat, että vuorovaikutusta sekä viestintää prosessoidaan valikoivasti. Informaation valikoivaan prosessointiin vaikuttaa se, millaisia kognitiivisia resursseja henkilöllä on käytössään esimerkiksi tietyllä ajanhetkellä ja/tai missä tunnetilassa henkilö on (Buller & Burgoon, 1996), sekä millaisia kokemuksia petoksista henkilöllä on (mm. Viswanath ym., 2011; Wang ym., 2012). Koska henkilöillä on erilaiset valmiudet ja resurssit, oletetaan että kompetenssiin perustuva henkilöiden välinen viestintä vaatii taitoja, ja hyvät sosiaaliset taidot omaavilla on paremmat lähtökohdat täyttää vuorovaikutussuhteeseen liittyviä vaatimuksia (Buller & Burgoon, 1996).

Buller & Burgoon (1996, 219) viittaavat Riggioon (1986) todetessaan, että spontaanit ja ulospäin suuntautuneet verbaaliset viestintätaidot, sekä tunnetasolla tilannetaju ja kyvyt hallita omia tunteitaan sekä vihjailla ja ilmaista asenteita, edesauttavat petosta suorittavaa osapuolta. Yksilöllisiä viestin lähettäjän ja vastaanottajan viestintätaitoja voidaan arvioida seuraavista näkökulmista: a) ilmaisukyky viestiä luodessa, b) kyky hallita viestinkulkua ja c) emotionaalinen ja viestien käsittelytaidon herkkyys, joka liittyy viestien purkamiseen vastaanottajan päässä (Buller & Burgoon, 1996; Riggio, 1986; Riggio, 1993). Petosta tavoittelevan osapuolen on varmistuttava siitä, että hän näyttää uskottavalta, heikentää vastaanottajien epäilyt, minimoi omat vastuunsa petoksesta ja välttää kiinnijäämisen seuraukset (Buller & Burgoon, 1996).

On joitakin tutkimuksia, jotka auttavat ymmärtämään miksi kalasteluviestit toimivat ja ihmiset tulevat huijatuksi (mm. Ebot, 2017; Goel ym.; Wang ym., 2012; Wang, Li, Rao & Raghav, 2016; Wright & Marett, 2010; Vishwanath, 2015), ja näistä muutamat (Ebot, 2017; Wang ym. 2016; Wright & Marett, 2010; Viswanath, 2015) käsittelevät kalastelua yksilöllisten erojen näkökulmasta.

Viswanath (2015) käsittelee yksilöllisiä eroja eri näkökulmasta, tutkien yksilöllistä tunnollisuuden ja emotionaalisen epätasapainoisuuden vaikutusta siihen, millainen päätöksentekoprosessi vastaanottajassa aktivoituu kalastelutilanteessa ja kuinka nämä luonteenpiirteet vaikuttavat sähköpostin

käyttötapoihin. Tutkimustulosten mukaan luonteenpiirteillä ei ole vaikutusta siihen, kumpi prosessointimalli (ks. 2.2.4) aktivoituu, mutta henkilöt, jotka käyttävät sähköpostia ”tapojensa orjina” tai impulsiivisesti, ja prosessoivat kalasteluviestin heuristisesti eivätkä rationaalisesti, tulevat todennäköisemmin kalastelun uhreiksi.

Wang ym. tutkivat vuonna 2016 yli-itsevarmuuden vaikutusta kalasteluviestien tunnistamiseen. Tutkijoiden mukaan yli-itsevarmuus voi johtaa riskialttiiseen toimintaan päätöksentekotilanteissa. Tässä tapauksessa yli-itsevarmuudella tarkoitetaan, että vastaanottaja on varma siitä, että kyseessä on normaali sähköposti eikä kalasteluyritys, ja luovuttaa siksi viestissä pyydetyt tiedot (Wang ym., 2016). Vähemmän itsevarma henkilö sen sijaan saattaa arvioida viestin luotettavuutta tarkemmin (Wang ym., 2016). Yli-itsearvioinnin vaikutukset voidaan huomioida esimerkiksi koulutuksia suunnitellessa, jotta henkilöiden arviointikykyä voidaan kehittää (Wang ym., 2016).

Wangin ym. (2016) tutkimuksessa testattiin mallia lähettämällä kysely 600 :lle Yhdysvaltojen eri osavaltioissa asuville vastaajille, jotka arvioivat satunnaisia kalasteluviestejä ja aitoja sähköpostiviestejä. Vastaajat saatiin Qualtrics-nimisen yrityksen kautta, joka mahdollisti laajan ja demografisesti monipuolisen koeryhmän koon. Ryhmässä oli koulutettuja ja kouluttamattomia miehiä ja naisia 19-89 -ikävuosien väliltä. Keski-ikä vastaajilla oli 52 vuotta. (Wang ym., 2016)

Kalasteluyrityksen tunnistamisessa tarkasteltiin vastaajien kognitiivisia toimintoja, huomion jakautumista, optimismia ja viestien lähettäjien tuttuutta, joiden uskottiin myös vaikuttavan yli-itsevarmuuteen (Wang ym., 2016). Tutkimustulosten mukaan kognitiivinen vaivannäkö (kalasteluviestien tarkempi prosessointi) vähensi yli-itsevarmuutta, kun taas vastaajan huomion valikoiva jakautuminen, optimismi ja kokemus siitä, että viestin lähettäjä on tuttu taho, lisäsivät yli-itsevarmuutta (Wang ym., 2016).

Ebotin (2017) mukaan aiemmissa kalasteluaiheisissa tutkimuksissa on harvoin huomioitu sitä, että erilaiset yksilölliset tekijät kuten vuosien kokemus, tietokoneen käyttötaidot, osaaminen ja online-käyttäytyminen vaikuttavat siihen, miten vastaanottaja prosessoi kalasteluviestiä ja arvioi sen luotettavuutta. Wright ja Marett ovat yksi harvoista, jotka ovat aihetta tutkineet.

Wrightin ja Marettin (2010) kiinnostuksen kohteena on petoksen onnistuminen, ja tutkimuskysymys on, miten verkkokäyttäjien kokemusperäiset ja taipumukselliset ominaisuudet vaikuttavat heidän herkkyyteensä suhteessa potentiaalisesti haitallisiin sähköposteihin (eng. ”How do the experimental and dispositional characteristics of online users affect their suspectibility to potentially malicious phishing emails?”).

He ovat kehittäneet mallin, jossa keskitytään kahteen kategoriaan yksilöllisistä tekijöistä: 1) kokemusperäinen kategoria, joka sisältää tietokoneen käyttötaidot, verkkokokemukset ja tietämys turvallisuuspolitiikoista, sekä 2) taipumuksiin liittyvä kategoria, joka sisältää taipumuksen luottavaisuuteen, taipumuksen kokea riskejä ja taipumukset epäilyyn ihmiskuntaa kohtaan (Wright & Marett, 2010).

Wrightin ja Marettin (2010) mukaan henkilö, jolla on heikko tietokoneen käyttötaito, on hyökkääjän kannalta otollinen kohde, koska hän on usein epävarma siitä, mitä tai miksi jotakin tietoa kysytään, ja on epätodennäköistä, että henkilö kysyisi muilta neuvoa, miten toimia. Myöskin kokeneemmat henkilöt ovat itsevarmempia kykyihinsä huomata petokset ja tunnistavat kalastelun uhkana todennäköisemmin kuin kokemattomat (Wright & Marett, 2010; Wang ym., 2012). Koulutuksella (ks. luku 2.3.4) voidaan positiivisesti vaikuttaa turvallisuustietoisuuteen, joka vaikuttaa siihen, kuinka hyvin käyttäjä tietää esimerkiksi kalasteluun liittyvät uhat (Wright & Marett, 2010).

Taipumus luottavaisuudelle tarkoittaa, että henkilö on luottavainen muihin tai riippuvainen muista erilaisissa tilanteissa ja konteksteissa (Wright & Marett, 2010). Onnistunut petos vaatii, että vastaanottaja luottaa viestin autenttisuuteen sen verran, että toimii siinä halutulla tavalla, ja otolliset uhrit ovat siten taipumuksiltaan luottavaisia (mm. Workman, 2008; Wright & Marett, 2010). Koettu riski tarkoittaa tässä yhteydessä, että vastaanottajalla on taipumus nähdä riskejä esim. yksityisyyteensä liittyen (Wright & Marett, 2010). Koetun riskin vastakohdaksi voidaan ajatella huolettomuus. Epäily ihmiskuntaa kohtaan tarkoittaa tässä kontekstissa taipumuksia epäillä muita, jolloin kyseiset henkilöt ovat usein puolustuskannalla ja itsesuojelevaisia, jopa paranoideja (Wright & Marett, 2010).

Kuusi Wrightin ja Marettin (2010) hypoteesia, jotka koskevat uutta mallia, olivat seuraavat:

1) Korkeat tietokoneen käyttötaidot vähentävät todennäköisyyttä, että henkilö tulee petetyksi kalastelusähköpostilla
2) Kokeneisuus verkossa vähentää todennäköisyyttä, että henkilö tulee petetyksi kalastelusähköpostilla
3) Turvallisuustietoisuus vähentää todennäköisyyttä, että henkilö tulee petetyksi kalastelusähköpostilla
4) Taipumus luottavaisuuteen lisää todennäköisyyttä, että henkilö tulee petetyksi kalastelusähköpostilla
5) Taipumukset kokea riskejä vähentää todennäköisyyttä, että henkilö tulee petetyksi kalastelusähköpostilla
6) Taipumukset epäilyksille ihmiskuntaa kohtaan vähentävät todennäköisyyttä, että henkilö tulee petetyksi kalastelusähköpostilla

Wrightin ja Marettin (2010) mallia testattiin kenttätutkimuksena, jossa 446 liiketalouden korkeakouluopiskelijaa yhdysvaltalaisessa yliopistossa saivat kalasteluviestejä, joissa pyydettiin luovuttamaan henkilökohtainen kurssiavain pääkäyttäjän (eng. admin) nimissä viestillä, joka sisälsi jonkin verran kirjoitusvirheitä. Ennen kalasteluviestien lähetystä heillä teetettiin etukäteiskysely, jossa mitattiin heidän kokemuksiaan ja taipumuksiaan. Kyselyssä haluttiin myös selvittää, pitivätkö opiskelijat kurssiavainta tärkeänä ja ymmärsivätkö he, että sen eteenpäin luovuttaminen olisi kurssiohjeiden rikkomista. Kurssiavainta luovutettaessa opiskelijoille oli aiemmin tehty selväksi, että sitä ei saa luovuttaa eteenpäin. (Wright & Marett, 2010)

Kalasteluviestin vastaanottajista 32 % vastaanottajista lähetti pyydettäessä tämän salaisen kurssiavaimen, 57 % ei vastannut lainkaan, 9 % raportoi kalasteluyrityksestä ja 1 % vastasi kysymyksellä tai kommentilla, sekä 1 % vastasi väärällä kurssiavaimella (Wright & Marett, 2010). Analyysiä varten 446:sta jouduttiin tiputtamaan pois 147 osallistujaa erilaisista tutkimuksen validiteettiin vaikuttavista syistä, joten tulosten analyysissä oli mukana enää 299 opiskelijaa (Wright & Marett, 2010).

Wrightin ja Marettin (2010) tutkimustulosten mukaan neljä käyttäytymistekijää vaikuttivat siihen, luovuttivatko osallistujat arkaluontoisia tietoja kalasteluviestin lähettäjälle. Hypoteesit 1, 2, 3 ja 6 saivat tukea tutkimustuloksista eli kalastelun uhriksi joutumisen todennäköisyyteen vaikuttavat käyttäjän tietokoneen käyttötaidot, kokemus verkon käytöstä, sekä turvallisuustietoisuus (Wright & Marett, 2010). Myös epäilykset ihmiskuntaan näyttivät vaikuttavan siihen, että mitä epäilevämpi vastaanottaja oli, sitä todennäköisemmin hän ei vastannut viestiin kurssiavaimella. (Wright & Marett, 2010)

Tutkimustulosten pohjalta Wright ja Marett (2010) suosittelevat, että nämä käyttäytymistekijät huomioidaan suuniteltaessa kalastelun estämiseen liittyviä materiaaleja ja työkaluja. Kokemukset ja kokemukset näyttävät vaikuttavan kalasteluyritysten uhriksi joutumisen todennäköisyyteen enemmän kuin yksilölliset taipumukset, mikä tarkoittaa sitä, että koulutusta tulisi keskittää sähköpostin käyttäjien tietotaidon kehittämiseen (Wright & Marett, 2010).

Väitöskirjassaan (2017) Ebot argumentoi, että kalasteluviestin klikkaukseen johtaneet syyt eivät ole aina yksiselitteisesti samat, vaikka aiempi tieteellinen tutkimus perustuu tähän oletukseen. Ebotin mukaan (2017) sen sijaan, että kalasteluviestien toimivuutta voitaisiin selittää vastaanottajien päässä yhteisillä, selkeillä tekijöillä, voivat syyt olla myös yksilöllisiä, kuten verkkokäyttäytymiseen tai kokemukseen perustuvia. Kokemukset vaikuttavat ihmisiin eri tavoin (Ebot, 2017). Ebot mainitsee, että kalasteluviestien elementit, kuten kiireellisyyden elementit (eng. urgency cues) ovat aiemassa tutkimuksessa olleet näitä yhteisiä tekijöitä, joilla on selitetty viestien toimivuutta ajatellen, että syy kalasteluviestin toimivuuteen on vastaanottajasta riippuen aina sama (2017). Syy voi olla, että viesti esimerkiksi vaikuttaa kiireelliseltä, tai että vastaanottajilla ei ole riittävää tietoturvatietoisuutta (Ebot, 2017).

Ebot tutkii grounded theory -tutkimusmenetelmää hyödyntävässä väitöskirjassaan (2017), miten eroavaisuudet yksilöiden verkkokäyttäytymisessä vaikuttavat siihen, miten he toimivat kalasteluviestin kohdatessaan. Tutkimus on induktiivinen ja perustuu tosielämän kalasteluviestien uhrien puolistruktuuroituihin haastatteluihin (yhteensä 17 haastateltavaa, toteutettiin Suomessa ja Cameroonissa). Aihe on lähes sama kuin Wrightin ja Marettin (2010), mutta tutkimusmetodologia on eri.

Ebotin (2017) mukaan kalasteluviestin prosessointiin vaikuttaa se, miten vastaanottaja käyttää sähköpostia ja internetiä (prosessi 1), aiemmat kohtaamiset turvallisuusasioiden kanssa (prosessi 2), tietoturvallisuuteen ja yksityisyyteen liittyvät huolet (prosessi 3), sekä kalasteluviestien kohtaamiset (prosessi 4). Esimerkiksi, vastaanottaja voi tulla huijatuksi, koska hän keskittyy vain

kalasteluviestin sisältöön, eikä tunnista sitä kalasteluksi (prosessi ja ”osaamistaso” 1), tai vastaanottaja voi epäillä viestiä kalasteluksi, mutta siitä huolimatta toimia kuten viestissä halutaan, koska vastaanottaja on hämmentynyt ja epäileväinen muttei tiedä, miten muutenkaan toimia (prosessi ja ”osaamistaso” 2). (Ebot, 2017)

Eri prosesseilla tai tasoilla olevat vastaanottajat reagoivat viesteihin eri syistä, ja tason määrittää onlinekäyttäytyminen sekä turvallisuustietoisuus (Ebot, 2017). Tasojen huomiointi koulutuksissa esimerkiksi jakamalla käyttäjät eri tasoryhmiin ja kouluttamalla eri ryhmät eri tavoin voisi johtaa parempiin lopputuloksiin kalasteluviestien huijaukseksi joutumisen välttymiseen liittyen (Ebot, 2017). Tasot ja osaaminen voivat yksilöllisesti muuttua ajan kanssa (Ebot, 2017), kuitenkin siten, että kalastelun uhrit sijoittuvat osaamistasolle 1 tai 2 (Ebot, 2017). Muilla tasoilla olevat henkilöt eivät enää tule huijatuksi, eli kalasteluyritys ei onnistu.

Kun vastaanottaja toimii (kalastelu)viestissä pyydetyllä tavalla, hän kokee, että mahdollisuus siitä, että viesti on tosi, nk. ”ylikirjoittaa” (Ebot, 2017) muut mahdollisuudet (esim. epäilykset siitä, että viesti onkin huijaus). Eli vastaanottaja katsoo tärkeämmäksi toimia viestissä pyydetyllä tavalla kuin jättää toimimatta. Osaamistasolla 1 olevat henkilöt eivät yleensä tunnista kalastelua lainkaan, kun taas osaamistasolla 2 olevat henkilöt voivat epäillä viestin autenttisuutta, mutta eivät tiedä, miten tulisi toimia (Ebot, 2017). Löydökset tukevat Wrightin & Marettin (2010) aiempaa tutkimusta, jossa argumentoitiin, että kokemattomat ja tietokoneen käyttötaidoiltaan heikot henkilöt ovat alttiimpia kalastelulle.

Ebotin tutkimuksen (2017) tulokset viittaavat siihen, että tietoturvakontrolleja suunniteltaessa yksilölliset eroavaisuudet tulisi ottaa huomioon sen sijaan, että ajatellaan että tekijä X (esimerkiksi viestin sisältämät kiireelliset elementit) johtavat aina asiaan Y (uhri toimii viestissä halutulla tavalla ja tulee huijatuksi), ja että esimerkiksi sama tietoturvakoulutus sopii siksi kaikille sähköpostin käyttäjille. Ebotin (2017) tutkimuksen mukaan myös yksilölliset syyt käyttää sähköpostia tai nettiä vaikuttavat siihen, miten vastaanottaja kokee kalasteluviestien pyynnöt.

2.3 Kalasteluviestinnän piirteitä

Tässä alaluvussa keskustellaan kalasteluviestinnän toteutuksista sekä sovelletaan edellisen alaluvun (2.1) käyttäytymistieteen teorioita ja periaatteita käytännön tasolle kalasteluviestinnässä. Hyökkääjät pyrkivät manipuloimaan uhrejaan kalasteluyrityksissään saadakseen uhrit toimimaan haluamallaan tavalla (Hadnagy & Fincher, 2015). Parhaat hyökkääjät onnistuvat luomaan sellaiset olosuhteet, jossa epäaito tai teennäinen tilanne saadaan tuntumaan luonnolliselta ja tavanomaiselta (Hadnagy & Fincher, 2015). Hyökkääjät tulevat jatkuvasti fiksummaksi ja hyökkäykset kehittyvät sofistikoituneemmiksi (mm. Workman, 2008; Jagatic ym., 2005).

Pretexting keskittyy kalasteluviestin sisältöön eli siihen, mitä pyydetään. Sen jälkeen käsitellään kalasteluviestinnän tyypillisimpiä toteutustapoja ja seikkoja, mistä viestit voidaan tunnistaa kalasteluyrityksiksi. Viimeisessä alaluvussa käsitellään lyhyesti sitä, voidaanko koulutuksella vaikuttaa positiivisesti henkilöstön osaamiseen kalasteluviestintäkontekstissa.

2.3.1 Pretexting

Pretextingillä tarkoitetaan viestin sisällön suunnittelua (mm. Goel, 2017; Workman, 2008). Se on olennainen osa kalasteluviestin onnistumista, sillä vaikka viesti voitaisiin huomata huijaukseksi, hyvin suunnitellut viestit aktivoivat vastaanottajissa motiivin toimia viestissä pyydetyllä tavalla (mm. Goel, 2017; Ebot, 2017). Näyttää siltä, että vastaanottajan arviointiin viestin luotettavuudesta liittyy nimenomaan viestin sisältö, ei niinkään otsikko (Goel, 2017).

Yksinkertaisimmat ja tyypillisimmät, opportunistiset kalasteluviestit vetoavat usein ahneuteen, koulutuksen puutteeseen ja hyväntahtoisuuteen (mm. Hadnagy & Fincher, 2015). Tyypillisimmät kalasteluviestien teemat näkyvät opportunistisissa ”nigerialaiskirjeissä”, joiden tavoitteena on saada rahaa tai varastaa uhrin identiteetti, ja viestin aiheena on usein maksupalvelut, sosiaalinen media tai ajankohtaiset, valtamediassa kiinnostusta herättävät tapahtumat, kuten terrrori-iskut (mm. Hadnagy & Fincher, 2015; Hong, 2012). Yhteistä viesteissä usein on, että hyökkääjä pyytää apua tavalla tai toisella (Hadnagy & Fincher, 2015).

Usein hyökkääjä pyrkii herättämään vastaanottajassa ahneuden, pelon, halun tai uteliaisuuden tunteita (Hadnagy & Fincher, 2015). Kalastelun uhrille tarjotaan mahdollisuutta esimerkiksi rikastua äkillisesti (Hadnagy & Fincher, 2015). Muita tunteita, joihin kalastelija voi vedota, on mm. pelko, auktoriteetin kunnioitus, halu verkostoitua, uteliaisuus ja myötätuntoisuus (Hadnagy & Fincher, 2015). Esimerkiksi kalasteluviesti, joka ilmoittaa, että vastaanottajan verikokeiden tulokset ovat huolestuttavat ja viittaavat syöpään, herättää vastaanottajassa usein pelkoa ja saa vastaanottajan esimerkiksi avaamaan viestin liitteenä olevat “verikokeen tulokset” (Hadnagy & Fincher, 2015).

Geneeriset kalasteluviestit sisältävät usein teemoja, jotka koskettavat mahdollisimman monia. Esimerkiksi veroihin tai pankkitietoihin liittyvät teemat ovat suosittuja, koska suurin osa ihmisistä maksaa veroja ja omistaa pankkitilin (Hadnagy & Fincher, 2015). Viesti voi esimerkiksi väittää, että pankkitilisi on jäädytetty, koska verkkopalveluun on tehty useita eri kirjautumisyrityksiä, tai että lainan- tai verojenmaksu on myöhässä, ja käyttäjän tulee toimia nopeasti tai jokin uhkakuva toteutuu (Hadnay & Fincher, 2015).

Goelin ym. (2017, s. 28) viittaaman prospektiteorian (Kahneman & Tversky, 1979) mukaan mahdolliset menetykset vaikuttavat ihmisten arviointikykyyn ja toimintaan enemmän kuin potentiaaliset hyödyt. Prospektiteoria selittää osaltaan ihmisten riskinottohalukkuutta epävarmoissa olosuhteissa päätöksentekotilanteissa (Goel ym., 2017). Näin ollen kalasteluviestien sisällöissä kannattaisi viljellä uhkakuvia. Goel ym. (2017) tulkitsee prospektiteoriaa

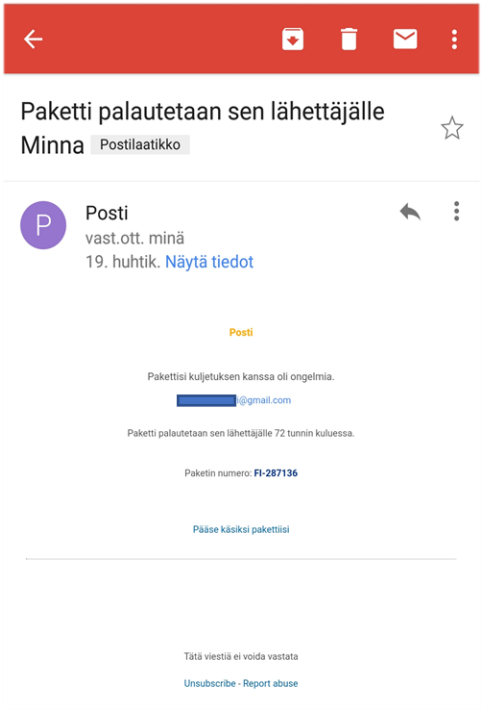
kalastelukontekstissa siten, että a) kalasteluviestit, jotka aiheuttavat välitöntä muutosta (vastaanottaja saa tai menettää jotakin) johtavat todennäköisesti petokseen ja b) välittömän menettämisen riski ajaa vastanottajan todennäköisesti toimimaan (esimerkiksi klikkaamaan linkkiä).

Hyökkääjät osaavat myös hyödyntää esimerkiksi uutisia ja mediailmiöitä (Hadnagy & Fincher, 2015; Viswanath ym., 2011). Hyökkääjät lähettivät Yhdysvalloissa runsaasti kalasteluviestejä välittömästi esimerkiksi Bostonin maratonien pommituksien jälkeen esimerkiksi CNN:n nimissä väittäen haitallisen linkin vievän pommituksiin liittyviin videoihin (Hadnagy & Fincher, 2015). Näissä viesteissä vedottiin sekä auktoriteettiin, että ihmisten luonnolliseen uteliaisuuteen (Hadnagy & Fincher, 2015). Toisaalta viesti voi olla houkutteleva myös muilla tavoin, kuten ”Näe Britney Spears alasti!” (Hong, 2012).

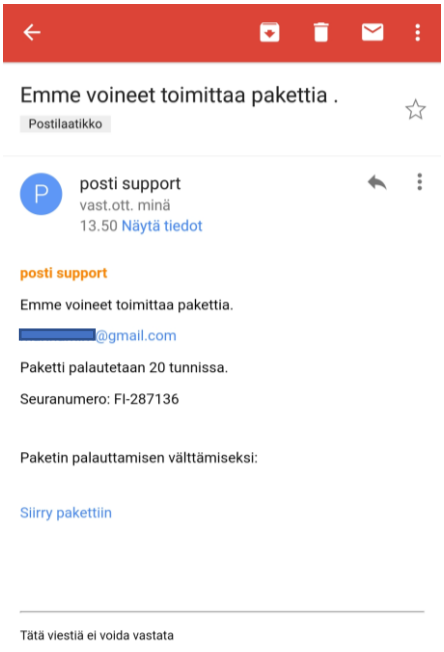
Hadnagy ja Fincher (2015) jakavat kalasteluviestit neljälle eri tasolle. Ensimmäisen tason geneeriset viestit eivät yleensä puhuttele vastaanottajaa nimellä, tulevat tuntemattomalta lähettäjältä ja saattavat olla myös kömpelösti kirjoitettuja. Kun kyseisiä viestejä lähetetään massana tuhansia tai satoja tuhansia, voidaan olettaa, että joku aina lankeaa ansaan. Toisen tason viestit ovat hieman monimutkaisempia, asteen verran paremmin kirjoitettuja ja vetoavat usein ahneuteen, pelkoon tai uteliaisuuteen (Hadnagy & Fincher, 2015).

Alla on esimerkki (kuvat 2 ja 3) toisen tason viestistä, jotka ovat saapuneet tämän Pro Gradu -tutkielman kirjoittajan ”spämmipostilaatikkoon”. Spämmipostilaatikko tarkoittaa sellaista sähköpostitiliä, jonka osoite annetaan esimerkiksi kaupallisiin palveluihin rekisteröityessä silloin, kun käyttäjä voi olettaa, että sähköpostiosoitteet voivat vuotaa tai ne myydään eteenpäin kaupallisiin tarkoituksiin. Näin ollen todennäköisesti spämmipostilaatikko täytyy erilaisista mainoksista ja kalastelukirjeistä.

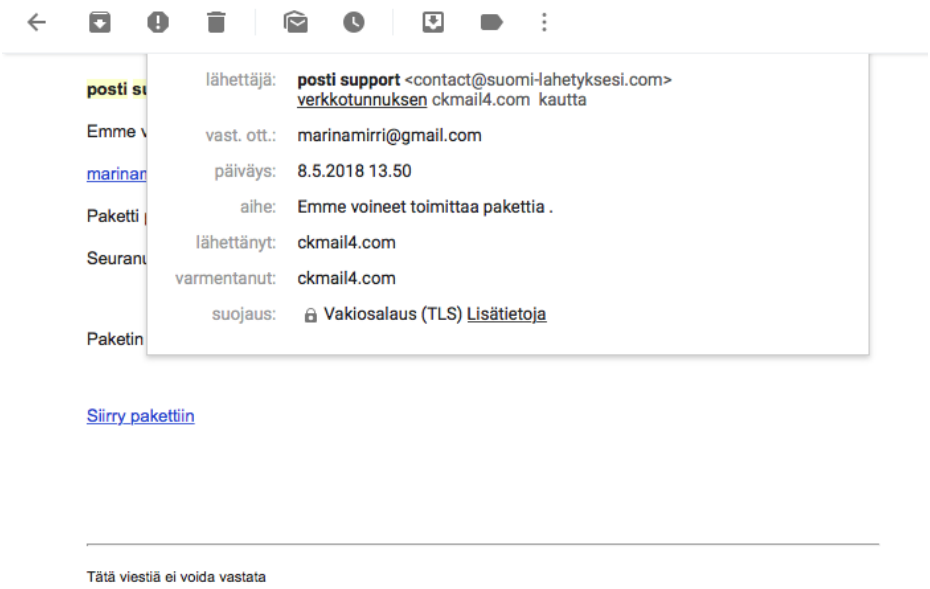
Kuvien 3 ja 4 kalasteluviestien lähettäjät ovat nähneet vaivaa tapaillakseen postin logoa, mutta ei kuitenkaan täysin vakuuta. Logo myös muuttuu hieman kahta sähköpostia verratessa. Seurantanumero vaikuttaa erikoisen lyhyeltä, ”pääse käsiksi pakettiisi” ja ”siirry pakettiin” ei kuulosta luontevalta, ja allekirjoitus puuttuu. Tilalla on kirjoitusvirheitä sisältävä toteamus ”Tätä viestiä ei voida vastata”. Viestin lähettäjä on kuitenkin nähnyt vaivaa lähettääkseen kaksi viestiä ajallisesti järkevässä järjestyksessä siten, että toinen viesti saapui noin 50 tuntia ensimmäisestä viestistä. Viimeinen kuva 5 sen sijaan osoittaa, että lähettäjän tietojen tarkastelu paljastaa huijauksen heti. Posti tuskin käyttää contact(at)suomi-lahetyksesi.com -osoitetta.



Kuva 2 Toisen tason kalasteluviesti 1/2



Kuva 3 Toisen tason kalasteluviesti 2/2



Kuva 4 Kalasteluviestin lähettäjän tiedot

Hadnagyn ja Fincherin (2015) mukaan kolmannen tason viesteissä vastaanottajaa tervehditään nimeltä, viesti on kirjoitettu huolella, vetoaa usein uteliaisuuteen tai pelkoon, viestin ulkoasu on huoliteltu ja joskus myös brändätty niin, että se näyttää ja tuntuu aidolta. Vastaavia hyökkäyskampanjoita on uutisoitu useita, ja esimerkiksi LinkedIn ja erilaiset deittipalvelut ovat joutuneet hyökkäysten uhriksi (BBC News, 2012). Viestit näyttävät tulevan palveluntarjoajalta (esim. LinkedIn) ja niissä usein pyydetään uusimaan salasana tai vahvistamaan sähköpostiosoite (BBC News, 2012). Hyökkäysten seurauksena miljoonat käyttäjätunnukset ja salasanat vuotavat nettiin muiden saataville (Ars Technica, 2012). Riski tunnusten väärinkäyttöön on suuri varsinkin silloin, jos käyttäjä käyttää samaa salasanaa useissa eri paikoissa, jolloin hakkerilla on pääsy useampiin palveluihin samoilla tunnuksilla.

Neljännen tason viestit ovat vaikeimpia havaita kalasteluksi, koska ne ovat teemoiltaan niin personoituja, ettei vastaanottaja osaa epäillä huijausta (Hadnagy & Fincher, 2015). Voidaan lähettää esimerkiksi työntekijän nimissä organisaation sisältä tulevan näköinen viesti kirjanpitoon, jonka liitteenä on (haitallinen) matkakululasku (Hadnagy & Fincher, 2015). Lähettäjän spoofaaminen on tehokas keino, joka vaatii kalastelun kohteeseen perehtymistä esimerkiksi sosiaalisessa mediassa sen verran, että tiedetään kohteen kontaktit. Esimerkiksi Jagaticin ym. (2007) tutkimuksen mukaan henkilöt, jotka vastaanottavat kalasteluviestin ”tuttavaltaan”, tulevat huijatuksi 4.5 kertaa useammin kuin henkilöt, jotka saivat viestejä tuntemattomilta (ks. luku 2.2.3).

Neljännen tason kalasteluviestit ovat kohdennettuja, ja hyökkääjä on tiedustellut julkisia lähteitä saadakseen selville luonnollisimman ja vakuuttavimman tavan lähestyä vastaanottajaa (Hadnagy & Fincher, 2015). Hyvin suunniteltu (ja usein spoofattu) viesti voi esimerkiksi näyttää tulevan tutulta henkilöltä,

joka lisää vastaanottajan luottamusta ja voi aktivoida vastaanottajassa periferisen ajatteluprosessin rationaalisen ajattelun sijaan (Goel, 2017). Periferisestä ajatteluprosessista on kerrottu lisää luvussa 2.2.4.

Hyökkääjä on esimerkiksi voinut selvittää vastaanottajan suosikkiravintolan ja lähestyy vastaanottajaa sen nimissä, ja hyökkäykseen voi liittyä myös kalastelupuheluita, joiden tehtävä on usein manipuloida vastaanottajaa niin, että kalasteluviestin haitallinen linkki tai liite tulee avatuksi (Hadnagy & Fincher, 2015). Esimerkiksi Puolustusvoimien virkamiestä taas voitaisiin lähestyä kutsulla johonkin Puolustusvoimien tunnettuun tilaisuuteen, ja siihen tulee ilmoittautua (haitallisen) linkin kautta (Hong, 2012). Aiemman tutkimuksen mukaan kohdennetut kalasteluviestit saattavat olla tehokkaampia kuin geneeriset (mm. Hong, 2012; Goel ym., 2017).

Goel ym. (2017) tutki, miten sisällöltään erilaiset kalasteluviestit vaikuttavat vastaanottajan toimintaan. Goel ym. (2017) testasivat kokeen avulla väitettä, että kalasteluviestin sisältö ja konteksti vaikuttavat oleellisesti kalasteluviestin toimivuuteen. Ensimmäinen hypoteesi oli, että sellaiset kalasteluviestit, jotka sisällöltään herättävät vastaanottajassa erityistä huolta ja joiden sisältö on suunniteltu (kohdennettu) vastaanottajaa varten, lisäävät vastaanottajan epäilyksiä verrattuna viesteihin, jotka ovat geneerisempiä. Toinen hypoteesi on, että kalasteluviestit, jotka sisältävät vastaanottajalle potentiaalisen uhkan, ovat toimivampia kuin potentiaalisen hyödyn sisältävät viestit. Kolmantena hypoteesina oli, että kalasteluviestit, jotka mahdollistavat vastaanottajalle uusia aineellisia tai aineettomia hankintoja ovat toimivampia kuin viestit, jotka mahdollistavat (vain) sosiaalisia etuja (eng. drive to bond, ks. luku 1).

Testatakseen hypoteeseja Goel ym. (2017) lähettivät 7225 fiktiivistä kalasteluviestiä yhdysvaltalaisille korkeakouluopiskelijoille. Tutkimuksessa kerättiin tietoa siitä, montako vastaanottajaa avasi kalasteluviestin ja moniko heistä klikkasi kalasteluviestissä ollutta linkkiä. Tutkimuksessa kerättiin statistiikkaa myös vastaanottajien sukupuolesta ja akateemisesta pääaineesta. Kalasteluviestit sisälsivät uhan menettää jotakin, tai saada jotakin.

Tutkimuksen tavoitteena oli tutkia kalasteluviestien toimivuutta siitä näkökulmasta, mitä tunteita se vastaanottajassa herättää. Viestejä oli 8 erilaista ja ne suunniteltiin siten, että niiden tarkoitus ruokkia vastaanottajan haluja saada jotakin (4 viestiä), tai pelkoa menettää jotakin (4 viestiä). Myös Ebot (2017) käyttää vastaavaa kategorisointia kalasteluviesteille väitöskirjassaan.

Goelin ym. (2017) tutkimuksessa tunnistetaan, millaiset kalasteluviestityypit todennäköisimmin johtavat vastaanottajan pettämiseen eli huijatuksi tulemiseen. Kalasteluviestin linkkiä klikattuaan vastaanottaja ajautuu informatiiviselle sivulle, jossa kerrotaan, että he ovat joutuneet kalasteluyrityksen uhriksi, sekä kuinka välttyä uhriksi joutumiselta tulevaisuudessa, ja heitä pyydetään täyttämään kyselylomake heidän turvallisuuskäsityksiinsä liittyen. Kyselylomakkeessa arvioitiin vastaanottajien turvallisuuskäyttäytymistä ja kalasteluun liittyvää käyttäytymistä. Aineiston keruutapaan vaikutti se, että aineisto haluttiin kerätä simuloiden todellista tilannetta eli opiskelijat eivät tienneet viestien

olevan kalastelua, ennen kuin he klikkasivat viestien haitallisia linkkejä (Goel ym., 2017).

Goelin ym. (2017) tutkimuksessa 1975 opiskelijaa 7225:stä avasi viestin (27,3 % vastaanottajista), ja 964 opiskelijaa avasi viestin linkin (13.3 % vastaanottajista). 964:sta opiskelijasta 206 (21.4 %) täytti vapaaehtoisen kyselylomakkeen. Jokaisen muuttujan suhteen vastaajia ei ollut tarpeeksi, jotta kaiken kattavaa analyysiä olisi voitu tehdä, mutta tuloksista voidaan päätellä, että sukupuolieroilla, pääaineella tai virustorjunnan tai palomuurin omaamisella ei ollut vaikutusta haitallisten linkkien avaamisen todennäköisyyteen.

Goelin ym. (2017) tutkimustulosten mukaan viestien sisältö (pelko menetyksestä tai jonkin asian saamisesta) lisäsi epäilyksiä petoksesta ja kalastelusta. Viestityyppien toimivuudessa oli siis eroja. Yli puolet vastaanottajista avasi kalasteluviestin liittyen kurssi-ilmoittautumisiin, ja heistä 68.7 % klikkasi viestin haitallista linkkiä. Goel ym. (2017) arvioi, että viestin sisällön koettu tärkeys vaikutti siihen, että viestiin haluttiin vastata heti, ”ylikirjoittaen” tarpeen arvioida viestin luotettavuutta. Kyselylomakkeeseen vastanneet sanoivat, että olivat epäilleet viestin aitoutta, mutta siitä huolimatta klikkasivat linkkiä.

Goelin ym. (2017) tutkimustulokset tukivat ensimmäistä hypoteesia, jonka mukaan tärkeäksi koetut, kohdennetut ja huolta aiheuttavat viestit toimivat paremmin kuin geneeriset viestit. Kyselyn vastaukset tukevat myös Ebotin (201´7) tutkimustuloksia siitä, että osaamistasolla 2 olevat vastaanottajat osaavat epäillä viestejä, mutta toimivat siitä huolimatta niissä pyydetyllä tavalla, koska eivät tiedä mitä muutakaan tekisivät. Toisaalta viestit olivat kohdennettuja, ja myös Butaviciuksen ym. (2015) tutkimuksessa todettiin, että kohdennetut viestit on vaikeampi huomata kuin geneeriset kalasteluviestit.

Voidaan ajatella, että avaamiseen vaikutti kaksi seikkaa: a) koettu uhka siitä, että ei pääse haluamilleen kursseille, ellei toimi heti, ja b) huoliteltu sisältö, jonka tarkoitus on vakuuttaa vastaanottaja viestin autenttisuudesta (Goel ym., 2017). Toisaalta viesti, joka liittyi pankkikorttitietoihin, sai vähiten klikkauksia, mutta tuloksia voidaan selittää mm. sillä, että pankkikorttihuijaukset ovat hyvin tunnettuja (Goel ym., 2017), ja tunnetut uhat tunnistetaan herkemmin (Downs ym., 2006; Goel ym., 2017).

Goel ym. (2017, 34-35) viittaa myös Halevin ym. (2015) tutkimukseen, jossa 62.5% työntekijöistä oli klikannut kalasteluviestin haitallista linkkiä silloin, kun kalasteluviesti näytti tulleen organisaation IT-osastolta, ja vastaanottajaa puhuteltiin nimellä. Goel ym. (2017) argumentoi, että heidän tutkimuksensa mukaan nimellä puhuttelu ei ole tarpeen vaan vähempikin personointi riittää, jotta kalasteluviesti toimii.

Toinen hypoteesi, jonka mukaan menettämisen uhka altistaa kalasteluviesteille enemmän kuin saamisen mahdollisuus, ei saanut selkeää tuke tuloksista. Näyttää siltä, että hypoteesi voi olla tosi vain silloin, kun kalasteluviestin sisältö on suunniteltu ja kohdennettu tarkoin (Goel ym., 2017). 20 % opiskelijoista, jotka saivat kalasteluviestin, jossa luvattiin lahjakortti tai iPad, avasivat haitallisen linkin. Näyttää siltä, että myös kalasteluviestit, joissa luvataan ”ilmaisia hyödykkeitä”, voivat ylikirjoittaa vastaanottajan mahdolliset epäilykset viestin

aitoudesta ja koettu potentiaalinen hyöty ohittaa potentiaaliset viestin avaamisen riskit (Goel ym., 2017).

Vastaanottajat eivät olleet yhtä alttiita kalasteluviesteille, jotka sisälsivät sosiaalisia mahdollisuuksia kuin materialistisia mahdollisuuksia (Goel ym., 2017). Toisaalta, tutkimustuloksiin on voinut vaikuttaa viestien uskottavuus ja se, että opiskelijoilla on monia eri kanavia verkostoitua, ja siksi sähköposteja ei ehkä koettu motivoivina (Goel ym., 2017).

Goelin ym. (2017) tutkimuksen mukaan tilannesidonnaiset ja sisällöltään kohdennetut kalasteluviestit vaikuttavat viestien toimivuuteen. Vastaanottajien päätöksentekoon vaikuttaa koettu riski tai palkinto (Goel ym., 2017). Varsinkin kohdennettu viesti, joka sisältää riskin menettää jotain vastaanottajalle tärkeää, voi ylikirjoittaa tarpeen arvioida seurauksia ja saada vastaanottajan toimimaan nopeasti hyökkääjän eduksi (Goel ym., 2017). Vastaanottaja voi olla tietoinen kalastelumetodeista ja esimerkiksi etsiä tietoa viestin aitoudesta verkosta ennen klikkausta, mutta epäilyksistä huolimatta vastaanottaja saattaa lopulta klikata kalasteluviestin haitallista linkkiä (Ebot, 2017; Goel ym., 2017).

Liiallisuuksiin menevä viestien monimutkainen, strateginen suunnittelu voi heikentää lopputulosta, mikäli esimerkiksi spontaanius viestinnässä vähenee strategisen suunnittelun myötä (Buller & Burgoon, 1996). Onnistuneet petokset onnistuvat silloin, kun pettävä osapuoli onnistuu peittämään epärehelliset tarkoitusperänsä ja epämukavat tunteet petoshetkellä (Buller & Burgoon, 1996).

2.3.2 Kalasteluviestinnän tyypilliset toteutukset

Kalasteluviesteissä voidaan hyödyntää erilaisia keinoja viestin luotettavuuden lisäämiseksi. Vastaanottaja avaa herkemmin esimerkiksi hänen tuntemaltaan taholta tulleen viestin liitteineen verrattuna tuntemattomien viesteihin (mm. Hadnagy & Fincher, 2015; Jagatic ym., 2005). Tästä syystä hyökkääjät ovat kiinnostuneita esimerkiksi kohdeorganisaation yhteistyökumppaneista aina jätteenkeräysfirmoista internetin tarjoajiin saakka (Hadnagy & Fincher, 2015). Hyökkääjä voi lähestyä kohdettaan myös esiintymällä esimerkiksi organisaation työntekijänä (Hadnagy & Fincher, 2015).

Email spoofing tarkoittaa sitä, että viestin lähettäjä on väärennetty (Hadnagy & Fincher, 2015). Viesti siis näyttää tulevan esimerkiksi osoitteesta webmaster@yritys.com mutta todellisuudessa viesti tulee hyökkääjältä, ja viestiin vastattaessa vastauskin päätyy hyökkääjälle. Toisaalta hyökkääjä on saattanut hakkeroida sähköpostipalvelimen tai tietokoneen, jolloin hyökkääjän viesti on lähetetty oikeasta osoitteesta ja oikealta palvelimelta (Hadnagy & Fincher, 2015). Silloin edes sähköpostin osoitetietojen (eng. email headers), eli tarkempien sähköpostin reitin tietojen tarkastelu, ei auta tunnistamaan viestiä kalasteluyritykseksi (Hadnagy & Fincher, 2015). Headereiden tutkiminen auttaa kuitenkin tunnistamaan edellä mainitut "spoofatut" osoitteet (Hadnagy & Fincher, 2015).

Kalasteluviesti voi sisältää myös **haitallisen linkin** esimerkiksi **kloonatulle verkkosivulle** (mm. Hong, 2012). Helpoin tapa huomata kloonattu

sivu on tarkastella URL-osoitetta viemällä hiiri linkin päälle (Hadnagy & Fincher, 2015). Vaikka käyttäjä veisi hiiren linkin päälle varmistuakseen linkin oikeellisuudesta, haitallinen linkki voi nopeasti tarkasteltuna näyttää aidolta (Hadnagy & Fincher, 2015). Hyökkääjä voi tehdä esimerkiksi Googlesta (google.com) identtisen sivun esimerkiksi osoitteeseen googIe.com, jossa L-kirjain onkin iso I-kirjain, tai google-login.com, ja sivu näyttää ja tuntuu täysin samalta kuin alkuperäinen. Tällaisessa tapauksessa hyökkääjä on ostanut itselleen domainin, joka muistuttaa tahoa, jona hyökkääjä haluaa esiintyä (mm. Hadnagy & Fincher, 2015; Hong, 2012).

Kalasteluviesti voi esimerkiksi pyytää käyttäjää vaihtamaan Googlen salasanansa ja vie käyttäjän googIe.com -linkin kautta kloonatulle sivulle oikean sivun sijaan. Kun käyttäjä luulee vaihtavansa salasanaansa Googleen, hyökkääjä saa käyttäjän käyttäjätunnukset (Hadnagy & Fincher, 2015). Ylläpitääkseen tällaista kloonattua feikkisivua, hyökkääjän tarvitsee vain rekisteröidä uusi domain (Hong, 2012).

Käyttäjää voidaan pyytää lataamaan **haitallinen liite** (Hadnagy & Fincher, 2015)**.** Liite voi sisältää esimerkiksi haittaohjelman, jolla hyökkääjä saa koko koneen haltuunsa ja sitä kautta varastettua tietoa. Esimerkiksi "Francophoning"-kampanjassa assistentille lähetettiin varatoimitusjohtajan nimissä lasku (liite), ja hyökkääjä soitti vielä perään esiintyen varatoimitusjohtajana ja kehotti assistenttia avaamaan liitteen heti. Assistentin ladattua liitteen, hyökkääjä sai haittaohjelman avulla hänen koneensa haltuun. Tässä hyökkäyksessä yhdisteltiin monia eri tekniikoita ja suostuttelun periaatteita, kuten kiireellisyyttä, sukupuolta, auktoriteettia ja soittelua (Hadnagy & Fincher, 2015). Kalastelupuheluilla (eng. **vishing** tai **voice phishing**) voidaan pyrkiä lisäämään viestin luotettavuutta tai saamaan luottamuksellisia tietoja. (Hadnagy & Fincher, 2015)

Joka tapauksessa kalastelu on tehty hyökkääjille helpoksi: suuri osa käyttää valmiita työkaluja, joissa voi määrittää, minkä sivun tahtoo kloonata ja mihin varastettu tieto tallennetaan (Hong, 2012). Dark webistä hyökkäyksen voi todennäköisesti tilata myös ilman, että joutuu itse näkemään asian eteen vaivaa. Markkinoilta voi myös löytyä jo valmiit ja toimivat, varastetut tunnukset rahaa vastaan siihen järjestelmään, johon hyökkääjä haluaa (Hong, 2012).

2.3.3 Kalasteluviestien tunnistaminen

Vihjeet viestin otsikossa ja sisällössä voivat auttaa vastaanottajaa tunnistamaan viestin kalasteluksi (Downs ym., 2006). Hadnagyn & Fincherin (2015) mukaan kalasteluviesti voidaan tunnistaa mm. seuraavista tekijöistä: epäilyksiä herättävä tervehdys ja/tai allekirjoitus, epäilyttävän oloinen tai tuntematon lähettäjä, linkit tuntemattomille tai epäilyttävän oloisille sivustoille, kirjoitusvirheet, lähettäjän tiedot, kiireellisyyteen vetoaminen ja epäuskottavat tai epätodennäköiset väitteet tai tarinat. Myös Wangin ym. (2012) ja Viswanathin ym. (2011) mukaan erityisesti kirjoitusvirheet ja kiireellisyyden elementit ja lähettäjän tiedot ovat yleisiä kalasteluviesteissä. Downsin ym. (2006) mukaan ylipäätään kaikki viestit, jotka sisältävät linkin jollekin sivustolle esimerkiksi tilin päivitystä varten, sekä uhkaavat

viestit, jotka vaativat välittömiä toimia käyttäjältä, tulisi aina luokitella epäilyttäviksi.

Tyypillisesti varsinkin geneeriset, ei-kohdennetut kalasteluviestit pyytävät käyttäjän pankki- tai luottokorttitietoja (mm. Downs, 2006; Hadnagy & Fincher, 2015). Usein viestin aihe liittyy rahaan, ja vastaanottajaa voidaan pyytää esimerkiksi auttamaan taloudellisesti, vastaanottamaan (tai siirtämään) rahaa, tai jokin tuote. Usein vastaanottajaa pyydetään maksamaan esimerkiksi lähetyksen toimituskulut, ja ne maksaessaan uhri antaa luottokorttitietonsa. Viesti voi myös vaikuttaa ”liian hyvältä ollakseen totta”, eli vastaanottajalle voidaan luvata esimerkiksi suuria korvauksia tai ilmaisia tuotteita pientä vaivannäköä vastaan. (Hadnagy & Fincher, 2015)

Hadnagyn ja Fincherin (2015) mukaan viesti voi olla myös kielellisesti kömpelö, ja viestin lähettäjä voi olla vastaanottajalle entuudestaan tuntematon taho (esimerkiksi afrikkalaisen yrityksen toimitusjohtaja). Jos viesti tulee esimerkiksi verotoimiston tai pankin nimissä, vastaanottajaa ei usein puhutella nimellä ja linkit voivat tarkemmin katseltuna näyttää epäilyttäviltä. Viesteissä vedotaan usein kiireellisyyteen ja voidaan esimerkiksi väittää, että käyttäjän tili suljetaan tietyn ajan kuluessa, ellei käyttäjä toimi heti. Lähettäjänä on usein hyökkääjän tekemä (vale)auktoriteetti, jonka mukaan käyttäjä tai hänen tietonsa ovat vaarassa, jolloin viesti aiheuttaa käyttäjässä pelkoa tai hätää. (Hadnagy & Fincher, 2015)

Jakobssonin ym. tutkimuksessa (2007) 17 henkilöä arvioi tutkijoiden tekemien kalasteluviestien ja verkkosivujen autenttisuutta. Kohderyhmäksi valittiin 18-60-vuotiaita yliopiston henkilöä (korkeakouluopiskelijoita, mutta myös henkilöstöä). IT-alan henkilöitä ei hyväksytty mukaan tutkimukseen. Arviointi tehtiin samalla, kun käyttäjille näytettiin lokaalisti erinäköisiä tavallisia ja kalastelusähköpostiviestejä sekä verkkosivuja. Tutkimuksessa selvitettiin, kiinnittyykö käyttäjän huomio autenttisuutta arvioitaessa esim. logoon, domainin kirjoitusasuun, IP-osoitteisiin, kirjoitusvirheisiin ja hyperlinkkeihin (http & https). Käyttäjien toiminnot tietokoneella, sekä suullinen arviointi, nauhoitettiin. Jakobsson ym. (2007) toteavat, että tutkimus osoittaa, mitä käyttäjät tarkkailevat yrittäessään arvioida, onko kyseessä kalasteluyritys, vai ei.

Jakobssonin ym. (2007) tutkimustulokset tukevat edellä mainittuja seikkoja ja osoittavat, että autenttisuuden arviointiin vaikuttavat seuraavat indikaattorit:

- kirjoitusasu ja ulkoasu (huonosti kirjoitetut viestit herättivät epäilyksiä)
- turvallisuuden korostaminen (esim. ”tämä viesti on luotettava”)
- URL-osoitteet (hyvin matkittuja osoitteita ei huomattu kalasteluksi, mutta kömpelömmin tehdyt URL:t ja IP-osoitteet herättivät epäilykset)
- sertifikaatit (vain Verisignin sertifikaatit olivat kohderyhmälle tuttuja, muita pidettiin epäilyttävinä)

- sisältö (pelkät informatiiviset viestit eivät herättäneet epäilyjä, mutta salasanojen kysely tai rahapalkintojen lupaaminen arvioitiin kalasteluksi)
- personointi (mitä personoidumpi viesti, sitä vähemmän oli epäilyjä).
- riippulukkoikonit (ikonit selaimen osoiteikkunassa voivat luoda myös hämmennystä, eivätkä välttämättä luo turvallisuutta)
- mahdollisuus vahvistaa viestin autenttisuus (viestissä on esimerkiksi annettu numero, johon voi soittaa varmistuakseen viestin oikeellisuudesta)

Jakobssonin ym. (2007) tutkimuksen mukaan sähköpostit koetaan yleisesti epäilyttävinä, verkkosivut vähän epäilyttävinä ja puheluita ei lainkaan epäilyttävinä. Käyttäjät esimerkiksi sanoivat, että voisivat todentaa viestin lähettäjän henkilöllisyyden soittamalla henkilölle. Osa käyttäjistä tarkensi, että lähettäjän oikea numero etsitään esimerkiksi verkosta eikä soiteta sähköpostin allekirjoituksessa esitettyyn numeroon, koska se voi olla huijarin numero. Osa myös koki, että sähköposti ei ole kunnollinen väline kiireellisille asioille (esim. käyttäjätilien lukitsemisinen ja salasanavuodot), vaan silloin tulisi aina soittaa käyttäjälle.

2.3.4 Koulutusten merkitys

Näyttää siltä, että koulutuksilla voidaan positiivisesti vaikuttaa petoksen tunnistuskykyyn (mm. Kalbfleisch 1992; Goel ym., 2017; Wang ym., 2012; Wright & Marett, 2010). Henkilöstö voi koulutuksen jälkeen tunnistaa herkemmin viestien kiireellisiä tai muita huolta herättäviä elementtejä, ja parhaassa tapauksessa välttää petoksen uhriksi joutumisen (mm. Wang ym., 2012).

Erään tutkimuksen mukaan, kun vastaanottajien annettiin harjoitella petoksen tunnistamista, petosten tunnistamisen tarkkuus ennen harjoittelua oli 50 %, harjoittelun jälkeen 61 %, ja kun harjoitteluun yhdistettiin palautteen antaminen, tarkkuus oli jopa 70 % (Zuckerman, Koestner & Alton, 1984). Myös DeTruck, Harszlak, Bodhorn & Texter (1990) tutkimuksessa vastaanottajat, jotka saivat koulutusta siitä, millaisista eleistä ja tekijöistä petokset voidaan tunnistaa, petosten tunnistustarkkuus oli 77 %, kun taas kouluttamattomien vastaanottajien tarkkuus oli 63 %. Mitä enemmän käyttäjät tietävät kalasteluhuijauksista, sitä enemmän he todennäköisesti kiinnittävät huomiota tekijöihin, joista petos voidaan tunnistaa, eivätkä vastaa kalasteluviesteihin (Wang ym., 2012).

Olisi tärkeää pysytä vaikuttamaan myös yksilölliseen päätöksentekoprosessiin siten, että käyttäjät eivät ajautuisi toimimaan periferisen tai heuristisen prosessin mukaan (ks. luku 2.2.4), eivätkä he käyttäisi sähköpostia ”tapojen ohjaamana” (Viswanath, 2015), eli ettei esimerkiksi avattaisi kaikkia viestejä vain, koska ”tapana on”. Sähköposteja tulisi käsitellä systemaattisen päätöksentekoprosessin mukaan, jotta todennäköisemmin vältyttäisiin kalastelun uhriksi joutumiselta (Viswanath, 2015). Butavicius ym. (2015) argumentoivat, että on

mahdollista oppia aktivoimaan rationaalinen ajatteluprosessi periferisen sijaan koulutuksen avulla. Silloin vastaanottajat arvioisivat loogisemmin ja rationaalisemmin viestejä, ennen kuin toimisivat niissä pyydetyllä tavalla.

Hadnagyn ja Fincherin (2015) mukaan lyhyiden ja ytimekkäiden tietoturvakoulutusten pitäminen kalastelukampanjoiden yhteydessä on oleellista, jotta henkilöstö saa oikeat eväät siihen, miten tunnistaa ja reagoida kalasteluyrityksiin. Ilman näitä eväitä ei voida olettaa, että organisaation tietoturvakulttuuri voi kehittyä suoritetuista testaamisista huolimatta. Myös nk. ”mikropeleillä”, jotka opettavat esimerkiksi selaimista, domain-nimistä ja kalastelusivuista, on näyttöä siitä, että ne auttavat kalasteluviestien tunnistamiseen oppimisessa (Hong, 2012).

Wrightin ja Marettin (2010) mukaan vastaavat, osallistavat opetusohjelmat antavat käyttäjille lisää kokemusta, sekä lisäävät käyttäjien itseluottamusta arvioidessaan viestien luotettavuutta. Nämä kokemukset taas vähentävät todennäköisyyttä, että kalasteluyritys onnistuu (ks. lisää yksilöiden kokemusten merkityksestä luvussa 2.2.5). Vastaaviin opetusohjelmiin osallistuneet henkilöt eivät ainakaan kohtaa kalasteluviestiä ensi kertaa tosielämässä hyökkäyksen alla, vaan ovat ehtineet tottua kalasteluyrityksiin turvallisessa (opetus)ympäristössä (Wright & Marett, 2010).

Kalasteluviestien avulla annettu koulutus näyttää myös auttavan henkilöitä oppimaan, kuinka kalasteluviestit voi tunnistaa (Hong, 2012). Hong (2012, 80) viittaa Kumaragurun PhishGuru-järjestelmään (2007), joka lähettää kalasteluviestejä käyttäjille ja mikäli käyttäjä tulee huijatuksi, PhishGuru opettaa, kuinka jatkossa käyttäjä voi suojata itsensä. Hongin (2012) mukaan oppimistulokset ovat PhishGurussa olleet rohkaisevia (kuukauden jälkeen kalastelun uhrit ovat vähentyneet 45 prosentilla). Nyt uutena markkinoille on tullut suomalainen HoxHunt, josta organisaatiot voivat tilata pelillisen kalasteluohjelman opetustarkoituksiin.

Kun opetustarkoitukseen tehdyt kalastelukampanjat ovat osana organisaation kehitysprosessia, tulee ne aina suunnitella huolella, jotta ne ovat tavoitteellisia ja organisaatiolla on selkeä kuva siitä, mitä niillä halutaan saavuttaa (Hadnagy & Fincher, 2015). Suunniteltaessa tulee miettiä esimerkiksi mitä työkaluja käytetään (sähköposti, puhelin, sosiaalinen media jne), kuinka usein ja kuinka vaikeasti tunnistettavia viestejä milloinkin lähetetään, millaiset organisaationraportointikäytännöt ovat ja miten kampanjoiden tuloksia voidaan käyttää organisaation koulutuksissa (Hadnagy & Fincher, 2015).

Kalastelukampanjat säännöllisesti toistamalla voidaan arvioida tietoturvakoulutusten tehokuutta (Jagatic ym., 2005). Jagatic ym. (2005) mainitsevat, että koulutuksessa olisi hyvä käydä läpi kalastelun vaarat, raportoinnin tärkeys, spoofauksen helppous ja väärinkäytön mahdollisuudet julkisista lähteistä löytyvien tietojen suhteen.

Hadnagyn ja Fincherin (2015) mukaan hyvä koulutus on a) lyhyt (tehokkainta on, jos koulutus kestää vain minuutista neljään minuuttia), b) tehokas niin, että henkilöstö ymmärtää miten kalasteluviestit voidaan tunnistaa, miten niihin tulee reagoida ja mihin niistä raportoidaan, c) yksinkertaista siten, että

henkilöstö ymmärtää mistä puhutaan ja miksi aihe koskettaa heitä, ja d) ajattelevaista siten, että tavoitteena ei ole lisätä henkilöstön stressiä vaan oppia suojautumaan huijauksilta. Hadnagy ja Fincher (2015) esittävät, että erään organisaation klikkausalttius saatiin laskemaan 89 prosentista 7 prosenttiin ja raportoinnin määrän nousemaan alle 10 prosentista 75 prosenttiin seuraamalla edellä mainittua koulutusmetodia.

Ebotin (2017) mukaan sen sijaan koulutettavat tulisi jakaa ryhmiin heidän osaamistasojensa mukaan ja suunnitella koulutukset siten, että osaamistasot otetaan huomioon. Esimerkiksi henkilöt, jotka eivät osaa tunnistaa kalasteluviestejä, tarvitsevat erilaista koulutusta kuin henkilöt, jotka osaavat tunnistaa kalasteluviestit mutta eivät tiedä, miten toimia (Ebot, 2017).

Viswanath (2015) ehdottaa, että yksilöiden luonteenpiirteitä voisi käyttää arvioinnissa, keillä henkilöistä on esimerkiksi taipumus toimia tapojensa mukaan, ketkä voivat olla herkkiä kalastelulle ja keiden kanssa tarvitsee keskittyä spesifimpiin toimenpiteisiin. Tavallaan tässä on kyse osaamistasosta (Ebot, 2017), mutta Viswanath (2015) käyttää jaottelun periaatteena luonteenpiirteitä.

Myös Goelin ym. (2017) mukaan erilaiset tietoisuutta lisäävät (eng. awareness) kampanjat, joissa huomioidaan kohdeyleisön kognitiiviset ominaisuudet, voivat johtaa parempiin koulutustuloksiin. Goel ym. (2017) siis uskoo, että koulutukset tulisi suunnitella yleisön osaamisen ja kognitiivisten kykyjen mukaan. Ymmärtämällä, mitkä asiat vaikuttavat henkilöiden yksilölliseen tietoturvakäyttäytymiseen, voidaan suunnitella koulutuksia, joiden lopputuloksena henkilöt osaavat vastustaa kalasteluyrityksiä (Butavicius ym., 2015).

Koulutusta suunniteltaessa haasteina on, että a) vihjeet siitä, miten petoksen tunnistaa, vaihtelevat tilanteittain, b) petoksiin liittyvät vihjeet voi olla vaikea tunnistaa käytännössä ja siten luotetaan enemmän lähettäjän yleiseen esitystaitoon, c) jos lähettäjät saavat tietää, miten vastaanottajat ovat koulutettu, he voivat muuttaa käytöstään sitä mukaa (Kalbfleisch, 1992).

2.4 Kiireellisyyden kokeminen ja päätöksenteko

Kiireellisyys on kalasteluviestinnässä hyökkääjien hyvin tuntema metodi, jonka avulla pyritään johtamaan vastaanottajaa harhaan (Hong, 2012; Naidoo, 2015; Wang ym., 2012). Tunnettuja esimerkkejä ovat esimerkiksi järjestelmän pääkäyttäjän lähettämät viestit, joissa kerrotaan, että järjestelmään voi kohdistua uusi hyökkäys, ellei liitteenä olevaa päivitystä asenneta, tai kertoa että henkilön tilillä on lukuisia vääriä kirjautumisyrityksiä ja että henkilön tulee vaihtaa salasanansa pikaisesti (Hong, 2012).

Käyttäytymistieteellisessä ja neuropsykologian tutkimuksissa ajallisen paineen on todettu voivan vaikuttaa henkilön päätöksentekokykyyn (Ben Zur & Brenznitz, 1980), ja yksilölliset kokemukset kiireellisyydestä vaikuttavat yksilön käyttäytymiseen (Ben Zur & Brenznitz, 1980; Waller ym., 2001). Subjektiiviseen kokemukseen ajasta vaikuttaa mm. yksilön kulttuuri, perhe, uskonto

sekä työ- ja koulutushistoria (Waller ym., 2001), joita ei kuitenkaan käsitellä tässä tutkielmassa.

Ben Zur & Brenznitz (1980) esittävät, että päätöksenteko voidaan jakaa neljään eri vaiheeseen: 1. todetaan että päätöksentekoon liittyy haaste ja että tilanne täytyy ratkaista, 2. hankitaan tietoa muista lähteistä, 3. etsitään muita mahdollisuuksia tilanteen ratkaisemiseksi.

Kiireellisyyden kokemusta voi luoda esimerkiksi prosessoitavan tiedon määrä suhteessa aikaan (Ben Zur & Brenznitz, 1980). Tiedon ja muiden vaihtoehtojen puute tai kyvyttömyys prosessoida kaikkea saatavilla olevaa tietoa voi aiheuttaa emotionaalista stressiä, jota kiireellisyys ja aikapaineet voivat lisätä (Ben Zur & Brenznitz, 1980; Wang ym., 2012). Kiireen alla yksilö pelkää epäonnistuvansa, koska aikaa ei välttämättä ole tarpeeksi asian riittävään prosessointiin (Ben Zur & Brenznitz, 1980). Kiireen alla päätöksentekijä voi tuntea myös avuttomuutta, koska tietoa nopeasti prosessoitaessa voi jäädä huomioimatta jotakin tärkeää (Ben Zur & Brenznitz, 1980).

Ben Zurin ja Brenznitzin (1980) sekä Wangin ym. (2012) mukaan kiireellisissä päätöksentekoa vaativissa tilanteissa yksilö voi toimia kiihtyneessä tilassa, jolloin kaikki tieto pyritään prosessoimaan mahdollisimman nopeasti ja virheiden riski kasvaa. Toinen vaihtoehto on päätöksenteon välttäminen ja esimerkiksi muiden vaihtoehtojen etsiminen (Ben Zur & Brenznitz, 1980). Kolmas vaihtoehto on kahden edellisen sekoitus, jossa yksilö subjektiivisesti valitsee mielestään tärkeät tiedot, jonka pohjalta päätös tehdään (Ben Zur & Brenznitz, 1980).

Ben Zur & Brenznitz (1980) tutkivat, miten aikapaine vaikuttaa riskinottohalukkuuteen uhkapeleissä, joissa riskinä on menettää rahaa. Hypoteesi oli, että kiireessä päätöksentekijä ottaisi pienempiä (taloudellisia) riskejä. Tutkimuksen tuloksissa todetaan, että hypoteesi pitää paikkansa ja että kiire on yksilölle stressaava tila, jossa pelätään negatiivisia seurauksia. Kahdesta vaihtoehdosta yksilö kiireessä valitsee todennäköisemmin vähemmän riskialttiin vaihtoehdon, koska se tuntuu turvallisemmalta stressin alla. Aikapaineet myös vähentävät todennäköisyyttä, että päätöksentekijä korvaisi välittömästä käsillä olevan ratkaisun jollakin toisella ratkaisulla. Tutkimuksessa aikapaineen alla päätöksentekoa ei kuitenkaan vältetty, vaan suurin osa koehenkilöistä prosessoi ensimmäisenä sellaiset tiedot, jotka kokivat tärkeimmiksi, ja jatkoivat muun tiedon prosessointia, kunnes päätöksentekoon annettu aika loppui. (Ben Zur & Brenznitz, 1980)

Ben Zur & Brenznitz (1980) esittävät, että stressin alla päätöksentekijän kokemukset onnistumisista ja epäonnistumisista vaikuttavat siten, että epäonnistumisen pelko kasvaa. Epäonnistumisen pelko vaikuttaa siihen, että valitaan vähemmän riskialtis vaihtoehto. (Ben Zur & Brenznitz, 1980)

Naidoo (2015) tutki Etelä-Afrikan pankin arkistoon kerättyjä kalasteluviestejä, joita pahantahtoiset hyökkääjät olivat lähettäneet vuosina 2011-2013. Analyysiin otettiin yhteensä 51 erilaista huijausviestiä, ja tutkimuksessa tarkasteltiin erityisesti viestien lähettäjää, kohdetta, päivämäärää, otsikkoa, sisältöä sekä liitteitä (Naidoo, 2015).

Naidoon (2015) analyysi paljasti, että suurimmassa osassa (94 %) kalasteluviesteistä hyökkääjät olivat käyttäneet kiireellisyyden kokemusta luovia

vihjeitä painostamaan vastaanottajaa toimimaan. Niitä oli huomattavasti enemmän, kuin luottamusta herättäviä vihjeitä (63%). 51 % viesteistä sisälsi jonkin uhkakuvan (esim. ”varoitus tiliäsi koskevasta turvallisuusuhasta”) ja 45 % sisälsi potentiaalisen edun (esim. ”käytä bonuspisteesi joulun aikana”). Tehokeinona ja kiireellisyyden kokemusta lisätäkseen, hyökkääjät olivat usein käyttäneet viesteissä huutomerkkejä. (Naidoo, 2015)

Naidoon (2015) mukaan kiireellisyyden vihjeisiin yhdistyy suostuttelun taktiikkana niukkuuden periaate (ks. luku 2.2.3), jonka tarkoituksena on herättää vastaanottajassa vahvoja tunteita kuten pelkoa esimerkiksi pankin antaman luottoluokituksen menettämisestä. Tällaiset uhkakuvat voivat saada vastaanottajan toimimaan nopeasti ja hätiköidysti (Naidoo, 2015).

Lisäksi hyökkääjät hyödynsivät usein luottamusta, joka on jo syntynyt pankin ja asiakkaan välille, kun kalasteluviestin kohteena oli asiakas (Naidoo, 2015). Kalasteluviesteissä haluttiin herättää vastaanottajassa heuristinen prosessi (ks. 2.2.4), kokemus tuttuudesta ja turvallisuudesta, jonka vuoksi kalasteluviestien täytyy näyttää ja tuntua autenttisilta (Naidoo, 2015).

Naidoo (2015) ehdottaa, että kiireellisyyden kokemuksille herkät käyttäjät välttäisivät toimimasta välittömästi viestin luettuaan, vaan jättäisivät sen odottamaan myöhempää prosessointia varten. Myös teknisissä kontrolleissa, kuten filttereissä, joiden tarkoitus on suojata käyttäjiä kalastelulta, tulisi huomioida ja suodattaa tällaiset kiireellisyyden vihjeitä sisältävät viestit (Naidoo, 2015).

Viswanath ym. (2011) tutkivat otsikon ja kiireellisyyden kokemusta lisäävien vihjeiden vaikutusta kalasteluviestien toimivuuteen. Otsikon tarkoitus oli olla relevantti siten, että se houkuttelee vastaanottajaa avaamaan viesti, ja kiireellisyyden vihjeiden oli tarkoitus herättää uhkaa, pelkoa tai niukkuuden tunnetta ja näitä tuntemuksia hyväksikäyttäen ”oikaista” päätöksentekoprosessia viestin luotettavuudesta (Viswanath ym., 2011). Hypoteeseina oli esimerkiksi, että käyttäjän huomion kiinnittyminen kiireellisyyden kokemusta luoviin vihjeisiin ja/tai otsikkoon korreloi positiivisesti todennäköisyyteen vastata kalasteluviestiin.

Viswanathin ym. (2011) tutkimusaineisto on sama kuin mikä oli käytössä Wangin ym. tutkimuksessa 2012, joka on esitelty jäljempänä tässä alaluvussa. Viswanathin ym. (2011) tutkimustulosten mukaan sähköpostin käyttöön liittyvät tavat ja osittain tiedostamaton sähköpostien tavanomainen selailu lisäsivät todennäköisyyttä sille, että käyttäjä vastaa kalasteluviestiin. Mitä enemmän käyttäjä sai sähköpostiviestejä, sitä todennäköisemmin myös kalasteluviestiin vastattiin (Viswanath ym., 2011). Vastaanottajien huomio kiinnittyi myös erityisesti neljään tekijään: otsikkoon, lähettäjään, kiireellisyyden vihjeisiin ja kirjoitusvirheisiin. Kiireellisyyttä lisäävillä vihjeillä oli suurin vaikutus siihen, että kalasteluviestiin vastattiin, jos käyttäjän huomio kiinnittyi näihin vihjeisiin (Viswanath ym., 2011). Jos vastaanottajan huomio kiinnittyi otsikkoon, kirjoitusvirheisiin tai lähettäjään, kalasteluviestiin olisi vastattu huomattavasti harvemmin (Viswanath ym., 2011). Viswanathin ym. (2011) mukaan kiireellisyyden kokemusta lisäävät elementit ovat tutkimustulosten pohjalta kaikista toimivimpia, petokseen johtavia vihjeitä kalasteluviesteissä.

Wang ym. (2012) tutkivat, kuinka käyttäjät prosessoivat kalasteluviestiä ja päättävät, miten vastata siihen, ja miten vastaanottajan huomio kiinnittyy viestin ulkonäköön ja sisältöön, kuten kiireellisyyttä lisääviin elementteihin, sekä tekijöihin, joista petoksen voisi tunnistaa. Kiireellisyyden elementit toimivat motivaattoreina laukaisemaan kevyemmän päätöksentekoprosessin (ks. luku 2.2.4), jolloin viestiä ei käsitellä syvällisesti (Wang ym., 2012). Muita motivaattoreita ovat esimerkiksi inhimillisiin tarpeisiin ja haluihin vetoaminen (Wang ym., 2012). Nämä motivaattorit edesauttavat, että rationaalisen päätöksentekoprosessin sijaan vastaanottaja tekee virheellisen arvion tilanteesta ja toimii kalasteluviestissä halutulla tavalla (Wang ym. 2012).

Wangin ym. (2012) yhtenä hypoteesina oli, että huomion kiinnittyminen sisällöllisiin seikkoihin kuten vastauksen kiireellisyyteen, vähentää kognitiivisia prosesseja, joita vastaanottaja käy läpi käsitellessään kalasteluviestiä. Toinen hypoteesi oli, että huomion kiinnittyminen esimerkiksi kiireellisyyteen lisää todennäköisyyttä, että vastaanottaja vastaa kalasteluviestiin. (Wang ym., 2012)

Vihjeet siitä, mistä petoksen voisi tunnistaa, ovat mm. kirjoitusvirheet ja lähettäjän osoitteen spoofaus (Wang ym., 2012). Vastaanottajan aiemmat kokemukset vaikuttavat siihen, huomataanko nämä vihjeet (Wang ym. 2012). Tiivistettynä, kalastelun uhrit ovat tehneet virheellisen arvion informaation käsittelyssä ja päätöksentekoprosessissa (Wang ym., 2012).

Wangin ym. (2012) tutkimuksessa lähetettiin anonyymi kyselylomake ja oikean kalasteluviestin kuva yhdysvaltalaisille korkeakouluopiskelijoille, ja kysyttiin todennäköisyyttä, vastaisivatko opiskelijat viestiin. Kuvan kalasteluviesti oli lähetetty vuonna 2008 pahantahtoisen hyökkääjän toimesta koko yliopiston sähköpostin käyttäjille, ja samaa kalasteluviestiä käytettiin myös Viswanathin ym. (2011) tutkimuksessa. Kalasteluviestissä kysyttiin käyttäjätunnuksia ja salasanoja. Kyselyssä pyydettiin opiskelijoita arvioimaan esimerkiksi viestin kiireellisyyttä ja kirjoitusvirheitä. Vastauksia saatiin yhteensä 321, ja vastaajien keski-ikä oli 21. (Wang ym., 2012)

Wangin ym. (2012) mukaan todennäköisyys kalasteluviesteihin vastaamiseen kasvaa, kun huomio kiinnittyy viestin ulkonäköön, mutta laskee, kun huomio kiinnittyy petosta implikoiviin tekijöihin. Tunnettujen kalastelu-uhkien tietäminen (Downs ym., 2006; Wang ym. 2012) lisää huomion kiinnittymistä petosta implikoiviin tekijöihin ja vähentää todennäköisyyttä, että vastaanottaja vastaa viestiin (Wang ym., 2012).

Wangin ym., (2012) tutkimus osoittaa, että petoksen tunnistamiseen liittyvät tekijät, visuaaliset ominaisuudet ja tietämys kalastelusta vaikuttavat petoksen tunnistamiseen. Wangin ym. (2012) mukaan kalasteluviestit johtavat huijauksen onnistumiseen usein silloin, kun vastaanottaja keskittyy viestissä kiireellisyyden elementteihin. Kuitenkin käyttäjät, jotka tietävät kalastelusta enemmän, todennäköisemmin prosessoivat kalasteluyritykset tarkemmin aikapaineista huolimatta ja tunnistavat petoksen (Wang ym., 2012).

Wangin ym. (2012) mukaan vastaanottajan huomion kiinnittyminen viestin kiireellisyyteen voi aiheuttaa ahdinkoa ja stressiä, sekä sitä kautta tarpeen

reagoida ja selviytyä. Käyttäjän päätöksentekoprosessi nopeutuu käyttämällä yksinkertaisempia päätösstrategioita (Wang ym., 2012; Wang, ym. 2016). Näiltä osin tutkimustulokset ovat samankaltaisia, kuin Ben Zurin ja Brenznitzin (1980).

Wang ym. (2012, 348) viittaavat Cowaniin (1986), jonka mukaan yksilöt selvittävät mahdollisia ristiriitoja vain ajan salliessa, ja paineen alla (kiireessä) ristiriitoja ei välttämättä koeta merkityksellisinä. Siten kiireellisyyden kokemusta lisäävät elementit voivat saada vastaanottajan keskeyttämään kalasteluviestin syvällisemmän käsittelyprosessin ja reagoimaan nopeasti (Wang ym., 2012).

Virheiden riski päätöksentekoprosessissa lisääntyy ja huonojen päätösten todennäköisyys kasvaa, kun aikapaineen alla kaikkea saatavilla olevaa informaatiota ei huomioida (Wang ym., 2012; Wang ym., 2016). Esimerkiksi kiireellisiä toimia vaativa, uhkaava (kalastelu)viesti voi sisältää huolimattomasti tehtyjä logoja tai kirjoitusvirheitä, joita vastaanottaja ei rekisteröi. Siten, vastaanottajan huomion kiinnittyminen kiireellisyyden kokemuksen laukaiseviin elementteihin lisäävät huonojen päätösten sekä kalasteluviestiin vastaamisen todennäköisyyttä (Wang ym., 2012).

Wang ym. (2012) ja Viswanath ym. (2011) toteavat, että jatkotutkimusta kaipaavat erityisesti kiireellisyyden kokemuksen vaikutukset ja petosta implikoivat tekijät viestissä, sekä kalasteluhyökkäysten todelliset uhrit. Kiireellisyyden kokemuksen tutkiminen esimerkiksi kokeena voisi lisätä ymmärrystä petosten onnistumisesta (Naidoo, 2015; Wang ym., 2012). Tutkimuksessa voisi olla variaatiota kiireellisyyden kokemuksessa esimerkiksi siten, että lähetetään erilaisia kalasteluviestejä, joihin tulee vastata tiettyjen aikojen kuluessa (Wang ym., 2012).

3 HYÖKKÄYSSIMULAATIO ORGANISAATIOSSA

Tässä luvussa esitellään tutkimuksessa käytetty aineisto. Tutkielman kirjoittajan työnantajan yrityksen asiantuntijat suorittivat kohdeorganisaation tilauksesta kolme kalastelukampanjaa, jonka kohteena oli kohdeorganisaation johtoa ja henkilöstöä. Tavoitteena oli selvittää kohdeorganisaation nykytilaa ja henkilöstön osaamista. Kalastelukampanjat olivat osana laajempaa simuloitua kyberhyökkäystä, jota ei käsitellä tässä tutkimuksessa, koska ne ovat aiheen ulkopuolella ja tämän tutkimuksen kannalta epäoleellisia.

Simuloitu kyberhyökkäys jakautui kalastelun osalta kolmeen eri osa-alueeseen, jotka olivat: 1) sosiaalisen median ja julkisten lähteiden kartoitus, 2) phishing (sähköpostikalastelu) 3) vishing (puhelinkalastelu). Näillä osa-alueilla testattiin, saadaanko tietoa kohdeorganisaatiosta, ja sen henkilöstöstä, tietojärjestelmistä ja testauksen kohteena olevista toimipisteistä, sekä voiko saatua tietoa hyödyntää hyökkäyksessä.

Simuloidussa kyberhyökkäyksessä saatujen löydösten myötä suunniteltiin organisaatiolle räätälöity koulutus sekä turvallisuusriskien hallintaohjelma, joiden avulla voidaan vahvistaa puolustusta mahdollisia tulevia hyökkäyksiä vastaan.

Seuraavissa alaluvuissa kuvataan tarkemmin toteutettujen kalastelukampanjoiden vaiheet ja sisältö. Alaluvuista selviää, miten ja miksi näitä vaiheita käytetään silloin, kun kalastelukampanjoita toteutetaan kohdeorganisaation tilauksesta.

3.1 Julkisten lähteiden kartoitus

Kalastelukampanjoita edeltävässä, hyökkäyssimulaation ensimmäisessä vaiheessa tavoitteena on tehdä julkisiin lähteisiin perustuvaa tiedonkeruuta (OSINT – Open-Source Intelligence). Tiedusteluvaiheen tavoitteena on selvittää kohdeorganisaation näkyvyys julkisissa lähteissä, kuten yrityksen kotisivut, yhteistyökumppanit ja sosiaalinen media, sekä etsiä sellaisia tietoja, joista mahdollinen hyökkääjä voisi olla kiinnostunut.

OSINT-tiedonkeruuta ei tehdä geneerisissä hyökkäyksissä, jolloin hyökkääjä ei ole kiinnostunut siitä, kuka tai millainen kohde on. Geneerinen hyökkäys perustuu opportunismiin eli siihen, että jos lähetetään esimerkiksi miljoona kalasteluviestiä, joku aina klikkaa. Kohdennettu hyökkäys, kuten tämä, usein tavoittelee pääsyä tiettyyn tietoon tai järjestelmään tietyn tavoitteen saavuttamiseksi.

Hyökkäyksen kohteiden valitsemiseksi on saatava tietoa kohdeorganisaation henkilöstöstä (nimet, puhelinnumerot, sähköpostiosoitteet, työtehtävät, organisaatiorakenne). Tämän tiedon avulla valitaan kohdehenkilöt, joilla on

todennäköisimmin hyökkääjän kannalta hyödyllistä tietoa tai pääsy järjestelmiin, joihin hyökkääjä haluaa.

Henkilöstön puhelinnumeroita ja sähköpostiosoitteita tarvitaan kalasteluyritysten suorittamista varten. Tiedon haussa käytetään mm. organisaation omia verkkosivuja, hakukoneita, LinkedIniä ja numerotiedustelua, sekä tähän tarkoitukseen suunniteltuja työkaluja (esim. Maltego).

Hyökkääjä voi monin eri keinoin hyödyntää kohdeorganisaation ostamien palveluiden tai tuotteiden nimiä kalasteluviesteissään tai -puheluissaan. Julkisten lähteiden kartoitusvaiheessa etsitään tietoa palveluntarjoajista ja sidosryhmistä, joiden nimissä potentiaalinen hyökkääjä voi esiintyä. Palveluntarjoajat ja toimittajat saattavat referenssinä mainita kohdeorganisaatiolle toimittamiaan ratkaisuja ja palveluita, mikä on helpoin tapa tunnistaa organisaation kumppaneita.

Usein organisaatioihin liittyen löytyy verkosta myös erilaisia raportteja tai muita dokumentteja, joissa saattaa olla laajemminkin hyökkääjän kannalta hyödyllistä tietoa. Välillä dokumenteista voi löytyä suoraan salassa pidettävää tietoa, mutta myös yksittäisiä tiedon palasia yhdistämällä voidaan toteuttaa hyökkäys. Etenkin 3+1 menetelmässä (ks. luku 2.1.) erilaiset pienetkin tiedon palaset helpottavat hyökkääjää kohdehenkilöiden manipuloinnissa.

Hyökkääjää kiinnostaa, mitä tietojärjestelmiä kohdeorganisaatiolla on käytössä, ja mitä järjestelmiä (nimet, teknologiat) kohdeorganisaatio käyttää mihinkin tarkoitukseen. Tätä tietoa etsitään muun muassa organisaation tietosuojaselosteista, henkilöstön LinkedIn-profiileista, organisaation työpaikkailmoituksista, palveluntarjoajien referenssikuvauksista sekä erilaisilla muilla hakukonehauilla.

Hyökkääjillä on usein käytössään normaalin selaimen lisäksi erilaisia hakukoneita, joilla kohdistaa hakutoimintoja kohteeseensa. Näillä usein ilmaisilla työkaluilla hyökkääjä kykenee selvittämään hyvin pitkälti kohteensa näkyvyyden ulkoverkkoon ja mahdollisesti näkemään alustaversioita, jonka avulla voidaan selvittää, onko kyseisessä versiossa haavoittuvuutta, jota voisi hyödyntää yleisesti löytyvien työkalujen avulla. Tällaisia työkaluja ovat mm. robtex.com, theharvester, recon-ng ja Maltego. Työkaluilla ja selaimen whois-kyselyillä voidaan selvittää yrityksen julkiset IP-osoitteet ja näihin IP-osoitteisiin tehtävillä reverse DNS-kyselyillä muita mahdollisia palveluita, jotka sijaitsevat samassa osoitteessa.

Kohdeorganisaation tapauksessa julkisten lähteiden kartoituksessa löytyi tietoa, jota pystyttiin käyttämään osana hyökkäyksiä. Näitä tietoja voitiin käyttää esimerkiksi 3+1 menetelmässä (Niemelä, 2016), jossa henkilöä huijataan käyttämällä kolmea totuutta rakentamaan luottamusta, jotta henkilö uskoisi yhden valheen. Huijauksissa käytettiin internetistä löytyneiden tietojärjestelmien nimiä, joita työntekijät käyttävät työtehtävissään. Samalla tunnistettiin järjestelmiä, jotka ovat hyökkääjän kannalta kiinnostavimpia kohteita hyökätä.

Julkisista lähteistä löytyneiden tietojen avulla oli mahdollista suunnitella, toteuttaa ja lähettää kalastelusähköposteja, jotka näyttävät henkilöstölle ja kumppaneille lähes identtisiltä oikeiden järjestelmien lähettämien

sähköpostien kanssa. Jos henkilöt ovat aiemmin saaneet ko. järjestelmiltä vastaavia viestejä, he usein eivät osaa epäillä huijaussähköpostien aitoutta, vaan klikkaavat helposti niissä olevaa linkkiä, joka johtaakin haitalliselle sivustolle. Hyökkääjä voi myös kloonata kohteensa käyttämiä verkkosivuja ja käyttää osoitetta, joka muistuttaa hyvin läheisesti alkuperäistä ja näin ollen erehdyttää käyttäjät antamaan tunnuksiaan. Näin tehtiin myös tässä hyökkäyssimulaatiossa.

3.2 Aineiston kuvaus ja testauksen osa-alueet

Sähköpostikalastelun tavoitteena on testata kohdeorganisaation kyvykkyyttä tunnistaa ja puolustautua sähköpostikalastelulta. Koehyökkäyksissä pyritään kalastelemaan tietoa (salassa pidettävä tieto, käyttäjätunnukset, salasanat) sekä saamaan henkilöitä suorittamaan erilaisia toimenpiteitä (esimerkiksi klikkaamaan haitallista linkkiä tai avaamaan haitallisen liitteen). Testin tulokset raportoidaan ja analysoidaan, sekä laaditaan suositukset korjaaviksi toimenpiteiksi.

Puhelinkalastelun tavoitteena on testata kohdeorganisaation kyvykkyyttä tunnistaa ja puolustautua vishing-hyökkäyksiltä eli puhelimitse tapahtuvilta kalasteluyrityksiltä, sekä raportoida ja analysoida testin tulokset laatien suositukset korjaaviksi toimenpiteiksi. Koehyökkäyksissä pyritään kalastelemaan tietoa (salassa pidettävä tieto, käyttäjätunnukset, salasanat) sekä saamaan henkilöitä suorittamaan erilaisia toimenpiteitä (esimerkiksi klikkaamaan sähköpostikampanjaan kuuluvaa haitallista linkkiä).

Simuloitu kyberhyökkäys käynnistyi tiedusteluvaiheella (kuvattu luvussa 3.1), jota seurasivat kalastelusähköpostit ja –puhelut. Ensimmäisessä kalastelukampanjassa lähetettiin geneerinen kalasteluviesti ja soitettiin kalastelupuheluita, jotka eivät liittyneet viestiin. Toisessa kampanjassa lähetettiin kohdennetumpi kalasteluviesti ja jatkettiin kalastelupuheluita. Toisen ja kolmannen kampanjan välissä kyberhyökkäyssimulaation toteuttanut yritys kävi kouluttamassa kohdeorganisaation henkilöstä, jotta kolmannessa kampanjassa voidaan havainnoida, vaikuttavatko koulutukset henkilöstön käyttäytymiseen. Kolmannessa kampanjassa lähetettiin kaksi erilaista kalasteluviestiä ja jatkettiin kohdennettuja kalastelupuheluita, joissa kehotettiin uhria klikkaamaan viestin linkkiä. Kampanjat on avattu tarkemmin luvuissa 3.2.1-3.2.3.

Testausta (hyökkäyssimulaatiota) ei kohdistettu siitä tietäviin henkilöihin (projektiryhmä ja YT-toimikunta), ja eräs yksikkö rajattiin kokonaan testauksen ulkopuolelle arkaluontoisista syistä. Kohdeorganisaation edustajille ei eettisistä syistä johtuen ilmoitettu missään vaiheessa, ketkä kalasteluviestejä tai -puheluita saivat. Hyökkäyssimulaatioiden tulokset luovutettiin ilman kalastelun kohteiden tietoja, koska tarkoituksena on kehittää koko organisaation toimintavalmiutta ja tietoturvakulttuuria. Sitä ei edistä se, kuka (yksittäinen henkilö) on tehnyt tai ollut tekemättä jotakin, vaan aihetta tarkastellaan kokonaisuutena.

Kalastelupuheluita sai soittaa arkisin klo 8-17 välisenä aikana, ennalta sovittuina päivinä. Testauksessa ei esiinnytty ulkoisena sidosryhmänä tai palveluntarjoajana, ja kohdeorganisaation ulkoiset sidosryhmät jätettiin

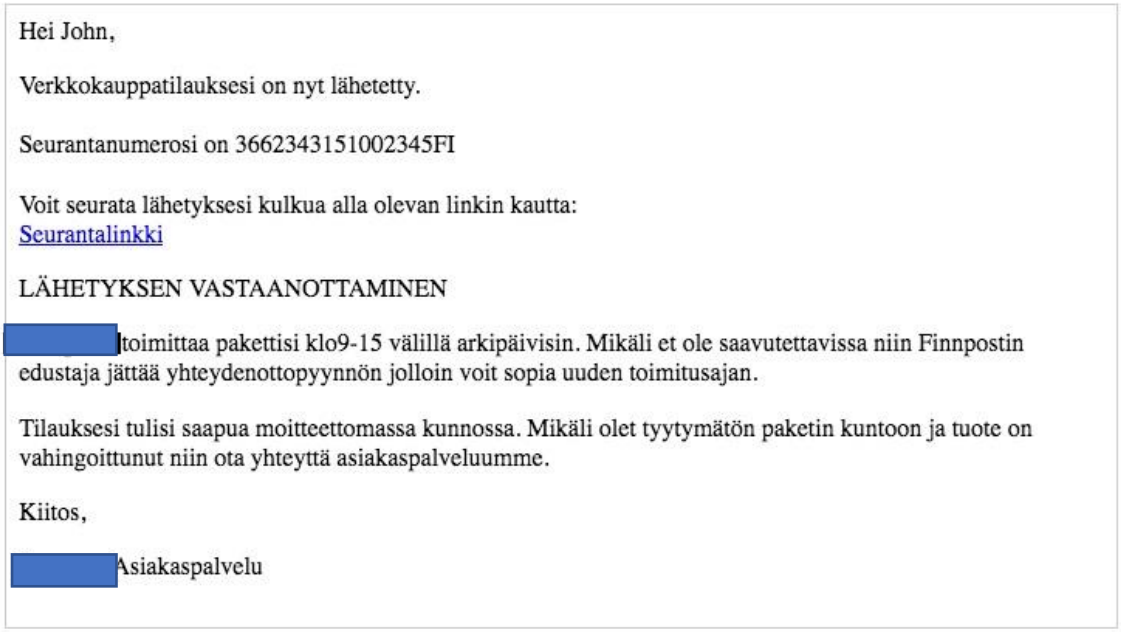
testauksen ulkopuolelle. Todellisen vahingon aiheuttaminen ei ollut osana testausta, ja kalastelun avulla saatuja tietoja käsiteltiin salassapitosopimuksen mukaisesti.

Tässä tutkielmassa ei huomioitu lainkaan niitä vastaanottajia, jotka avasivat viestin, mutta eivät klikanneet viestin sisältämää linkkiä/avanneet liitettä. Luvut viestin avanneista on jätetty pois, koska tulokset eivät sen osalta ole luotettavia. Sähköpostiviestin avaamista seurattiin ”näkymättömällä kuvalla”; mikäli sähköpostiohjelmassa on estetty kuvien automaattinen lataus, niin käyttäjän täytyy erikseen hyväksyä, ladataanko viestissä olevat kuvat. Mikäli käyttäjä ei lataa kuvia, tieto sähköpostin avaamisesta ei välity oikein.

3.2.1 Ensimmäisen kalastelukampanjan kuvaus

Ensimmäisen kalastelukampanjan tarkoituksena oli mitata ainoastaan, kuinka moni kalasteluviestin vastaanottajista avaa viestin ja klikkaa viestissä olevaa linkkiä. Kalasteluviesti suunniteltiin niin, että se on geneerinen ja vetoaa johonkin arkipäiväiseen asiaan, tässä tapauksessa kuriiriviestiin, missä vastaanottaja olisi tilannut jonkin tuotteen verkkokaupasta (kuva 6). Viesti ei sisällä kiireellisyyden kokemusta luovia elementtejä, mikä helpottaa vertailua viestien välillä tässä tutkielmassa. Viestissä olisi voinut olla jokin aikamääre, missä esimerkiksi ilmoitetaan, että vastaanottajan on valittava sopiva toimitusaika paketille tietyn ajan sisällä. Jos käytetään Ebotin (2017) kategorisointia kalasteluviestien kahteen eri ryhmään jaosta, tämä viesti sisältää hyödyn, eikä uhkaa; vastaanottaja on siis saamassa paketin.

Kuriiriviestin käyttö osana tietojen kalastelua on varsin tehokas tekniikka, sillä nykypäivänä suurin osa ostoksista tehdään internetissä. Verkkokaupassa käyttäjällä ei ole aina tietoa siitä, minkä niminen kuriiriyritys paketin toimittaa. Tämän lisäksi on hyvin todennäköistä, että mitä suurempi vastaanottajien lukumäärä on, sitä varmemmin joku vastaanottajista oikeasti odottaa pakettia.



Hei John,

Verkkokauppatilauksesi on nyt lähetetty.

Seurantanumerosi on 3662343151002345FI

Voit seurata lähetyksesi kulkua alla olevan linkin kautta:
Seurantalinkki

LÄHETYKSEN VASTAANOTTAMINEN

[redacted]toimittaa pakettisi klo9-15 välillä arkipäivisin. Mikäli et ole saavutettavissa niin Finnpostin edustaja jättää yhteydenottopyynnön jolloin voit sopia uuden toimitusajan.

Tilauksesi tulisi saapua moitteettomassa kunnossa. Mikäli olet tyytymätön paketin kuntoon ja tuote on vahingoittunut niin ota yhteyttä asiakaspalveluumme.

Kiitos,

[redacted]Asiakaspalvelu

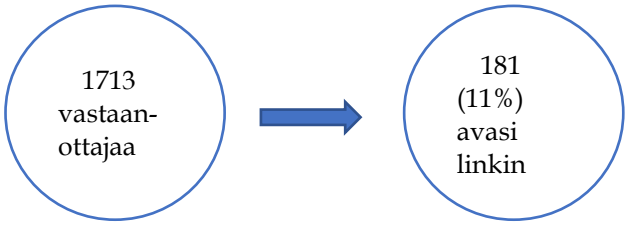
Kuva 5 Malli ensimmäisen kalastelukampanjan viestistä

Alla on listattu muutamia seikkoja, joista viestin voi tunnistaa kalasteluksi:

- Sähköposti liittyy toimintaan, mitä vastaanottaja ei todennäköisesti ole tehnyt
- Verkkokauppatilauksien toimitusviestit tulevat yleensä itse verkkokaupalta, eikä suoraan kuriiriyritykseltä
- Sähköpostiviestin allekirjoitus ei sisällä mitään kontaktitietoja. Luotettavat verkkokaupat ja yritykset useimmiten sisällyttävät kattavat yhteystiedot osaksi viestiä
- Sähköpostiviesti ei sisällä mitään tietoa varsinaisesta tilauksesta

Sähköpostiviesti lähetettiin kokonaisuudessaan 1713 vastaanottajalle kohdeorganisaatiossa. Kohderyhmänä oli koko organisaatio pl. rajoitukset (ks. luku 3.2), ja tästä joukosta valittiin satunnaisesti vastaanottajat, joille viesti lähetettiin. Kohdeorganisaation edustajat projektiryhmässä eivät tienneet, keille viesti lähti, ja ketkä siihen vastasivat. Kohderyhmän (ja organisaation) koko on jätetty pois tästä tutkimuksesta, jotta kohdeorganisaatio pysyy anonyyminä.

Sähköpostiviesti lähetettiin kesälomakauden alussa, mikä on ainakin osittain nähtävissä tuloksissa. Kokonaisuudessaan 181 uniikkia vastaanottajaa avasi sähköpostiviestin ja klikkasi sen sisältämää linkkiä. Oikeassa hyökkäyksessä linkki olisi voinut johtaa käyttäjän haitalliselle sivustolle.



Kuva 6 Ensimmäisen kalastelukampanjan tulokset

Sähköpostin avaaminen ei varsinaisesti aiheuta merkittävää riskiä kohdeorganisaatiolle, sillä viestin avaaminen ei vielä mahdollista työaseman kaappaamista tai tietojen vuotamista. Viestissä olevan haitallisen linkin klikkaamisella voi sen sijaan olla huomattavasti vakavammat seuraukset. Jo pelkkä sähköpostin avaaminen auttaa hyökkääjää saamaan selville, että kyseinen vastaanottajan sähköpostiosoite on validi ja aktiivisesti käytössä sillä hetkellä. Tätä tietoa hyökkääjä voi käyttää myöhemmin kohdentaessaan tietojen kalastelua.

Suuressa organisaatiossa, missä on useita tuhansia työntekijöitä, varsin yksinkertaisellakin tietojen kalasteluviestillä on mahdollista saada huijattua satoja työntekijöitä klikkaamaan haitallista linkkiä sähköpostiviestissä. Tämän sähköpostikalastelukampanjan aikana ei pyritty varastamaan käyttäjiltä tietoa, vaan ainoastaan mittaamaan, kuinka moni työntekijä saattaisi klikata osana huijausviestissä tullutta linkkiä.

3.2.2 Toisen kalastelukampanjan kuvaus

Toisessa kalastelukampanjassa pyrittiin keräämään kohdeorganisaation työntekijöiden käyttäjätunnuksia ja sähköpostiosoitteita. Kohdeorganisaatiolla on julkisessa internetissä saatavilla oleva palvelu, missä organisaation työntekijät voivat vaihtaa salasanansa. Tämä palvelu löytyi julkisia lähteitä tiedustellessa (ks. luku 3.1).

Kampanjaa varten kloonasimme kyseisen palvelun ja lähetimme valitulle kohderyhmälle sähköpostin, missä ilmoitetaan, että kohdeorganisaation työntekijöiden salasanat ovat joutuneet tietovuodon kohteeksi. Kohderyhmästä sovittiin yhdessä projektiryhmän kanssa, ja tästä ryhmästä valittiin vielä satunnaisotos, jolle viesti lähetettiin. Kohdeorganisaation edustajat projektiryhmässä eivät siis tienneet, keille ryhmän sisältä viesti lähti, ja ketkä siihen vastasivat.

Kampanjaa varten varasimme nimiimme id-kohdeorganisaatio.fi -nimisen domainin, joka on lähes identtinen kohdeorganisaation palvelun URL:n kanssa. Alla on esimerkkikuva kohteille lähetetystä sähköpostista. Salasanan vaihtopalvelun kloonattua sivua ei kuvata tässä raportissa salassapitosyistä, ja kalasteluviestin (kuva 8) organisaatiokohtaiset tiedot on editoitu pois.

Käytettäessä Ebotin kategorisointia (2017) tämä viesti sisältää uhkan, ei hyötyä, eli vastaanottajalle ilmoitetaan, että hänen salasanansa on vuotanut, ja se pyydetään vaihtamaan välittömästi. Viestissä sanalla ”välittömästi” halutaan korostaa kiireellisyyttä ja saada vastaanottaja reagoimaan viestiin heti. Viestin sisältöä suunnitellessa oli ajateltu, että vetoamalla kiireeseen ja käyttäjälle tärkeään informaatioon, eli käyttäjätunnukseen ja salasanaan, kasvatettiin mahdollisuuksia saada mahdollisimman moni kirjautumaan kloonatulle sivustolle.

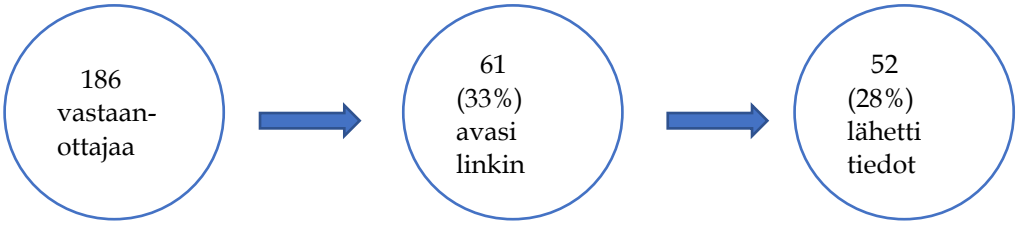
Kuva 7 Malli toisen kalastelukampanjan viestistä

Alla on listattu muutamia seikkoja, joista viestin voi tunnistaa kalasteluksi:

- Lähettäjä on geneerinen noreply, eikä esimerkiksi nimetty henkilö organisaation servicedeskistä
- Sähköpostiviesti ei sisällä mitään kontaktitietoja tai tarkempaa tietoa mahdollisesta tietovuodosta
- Viestiä ei lähetetty organisaation omasta domainista

Mikäli vastaanottaja siirtyi salasanapalveluun linkkiä klikkaamalla ja syötti käyttäjätunnuksensa ja salasanansa kloonatulla sivustolla, hänet uudelleenohjattiin välittömästi kohdeorganisaation omalle salasananvaihtosivustolle. Tässä vaiheessa käyttäjille ei haluttu vielä paljastaa, että kyseessä on hyökkäyssimulaatio, koska tietoisuus testausprojektista olisi voinut vaikuttaa kolmannen kalastelukampanjan tuloksiin.

Sähköpostiviesti lähetettiin kokonaisuudessaan 186 vastaanottajalle. Viestien lähetys oli porrastettu siten, että niitä lähti pitkin päivää (klo 8-16 välillä), jotta kaikki eivät saisi viestiä yhtä aikaa kiinnijäämisriskin pienentämiseksi.



Kuva 8 Toisen kalastelukampanjan tulokset

Kampanjan aikana 52 uniikkia vastaanottajaa kirjautui kloonatulle sivustolle käyttäen mahdollisesti oikeaa käyttäjätunnusta ja salasanaa (kuva 9). Tämän

lisäksi osa käyttäjistä yritti kirjautua tunnuksillaan useaan kertaan. Lukema on korkea ottaen huomioon, että 186 vastaanottajasta lähes kolmannes avasi linkin, ja linkin avanneista 85 % kirjautui kloonatulle sivustolle. Koska kyseessä oli kyberhyökkäyssimulaatio eikä organisaatiolle haluttu missään vaiheessa aiheuttaa todellista haittaa, käyttäjien syöttämiä tietoja ei tallennettu, ja kaikki liikenne väärennetylle palvelimelle kulki salatun HTTPS-yhteyden kautta tietoturvasyistä.

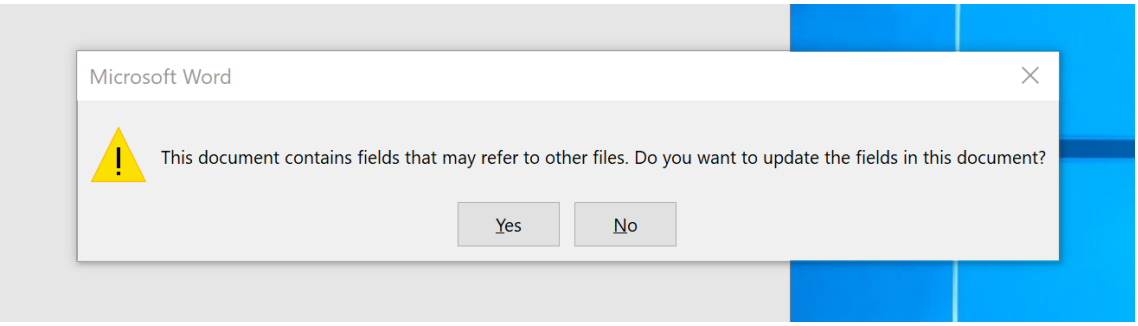
Tuloksista on nähtävissä, että tarkkaan suunnitellulla ja hyvällä suomenkielellä toteutetulla tietojen kalastelulla on mahdollista saada haltuunsa arkaluontoista tietoa organisaatiosta. Tässä tapauksessa kohteena olivat nimenomaan organisaation käyttäjätunnukset ja salasanat. Tunnusten ja salasanojen joutuminen vääriin käsiin voi mahdollistaa hyökkääjää saamaan pääsyn muihinkin, esimerkiksi liiketoimintakriittisiin järjestelmiin, mikäli käyttäjät käyttävät samaa käyttäjätunnusta ja salasanaa useissa sisäisissä tai ulkoisissa palveluissa. Tästä syystä on tärkeää, että käyttäjiä rohkaistaan käyttämään eri salasanoja palveluissa, jolloin on mahdollista minimoida mahdollinen vahinko, mikäli käyttäjätunnus ja salasana joutuvat tietovuodon kohteeksi käyttäjän tietämättä.

3.2.3 Kolmannen kalastelukampanjan kuvaus

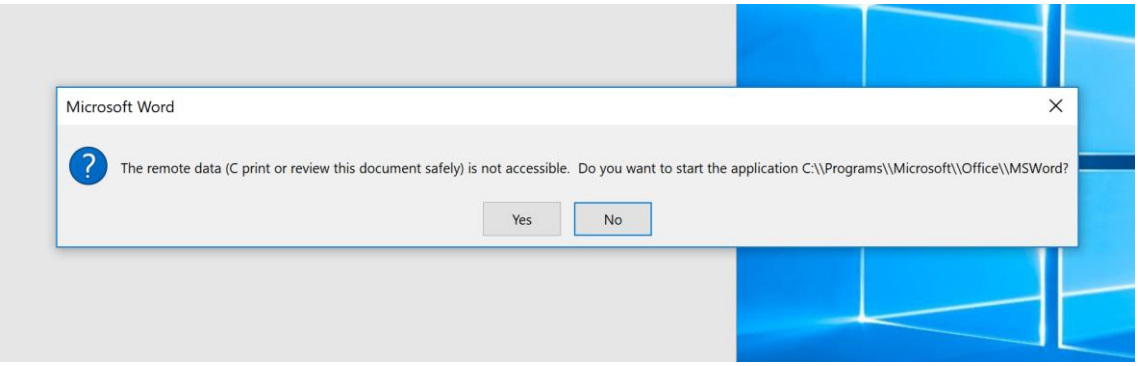
Kolmannessa sähköpostikampanjoissa kalasteluviestissä myytiin toimistotarvikkeita esiintyen ulkopuolisena tahona tekaistun yrityksen nimissä. Viestistä ei tietoturvasyistä ole liitetty tähän raporttiin mallikuvaa. Kalasteluviesti lähetettiin tekaistun toimistotarvikeyrityksen nimissä, joka avajaistarjouksenaan tarjosi edullisia toimistotarvikkeita kohdeorganisaatiolle. Tekaistulle yritykselle oli ostettu domain ja tehty yksinkertaiset verkkosivut epäilysten välttämiseksi. Kyseistä yritystä ei kuitenkaan löydy mistään rekisteristä, koska todellisuudessa sitä ei ollut koskaan olemassa. Viestissä kehotettiin toimimaan nopeasti, koska avajaistarjoukset olivat voimassa vain viikon verran, eli tämäkin kalasteluviesti sisälsi kiireellisyyden kokemisen elementtejä ja hyödyn (edullisia tuotteita), ei uhkaa.

Viesti sisälsi liitteen nimeltä ”Avajaistarjoukset.doc”, jonka vastaanottajan haluttiin avaavan. Kalasteluviestin liite pyrki väärinkäyttämään Microsoft Officessa olevaa toiminnallisuutta, jonka avulla uhri voidaan huijata lataamaan haittaohjelma omalle työasemalleen. Kyseinen toiminnallisuus tunnetaan nimellä Dynamic Data Exchange (DDE) -kentät. Microsoft Office-ohjelmistossa oleva DDE-protokolla mahdollistaa tiedon välittämisen sovellusten välillä.

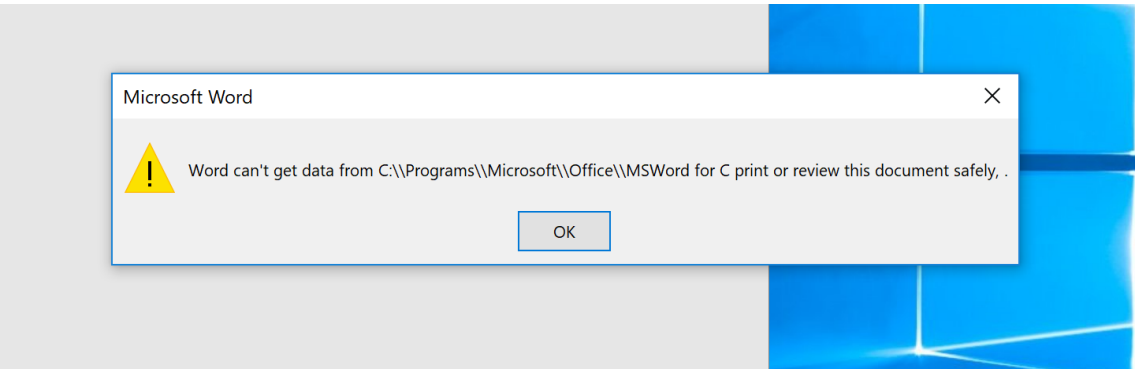
Haasteena on, että vastaanottajan tulee ohittaa varoitusviestejä liitettä avatessa, ennen kuin mahdollinen haittaohjelma voi asentua koneelle. Kyseisen hyökkäysvektorin varoitusviesti on myös hyökkääjän väärennettävissä, mikä saattaa edesauttaa hyökkääjää saamaan kalasteluviestin uhri ohittamaan varoitusviestit. Alla (kuvat 10-12) on kalasteluviestin sisältämän liitteen varoitusviestit, jotka uhrin tuli hyväksyä ennen kuin mahdollinen haittakoodi olisi suorittunut työasemalla.



Kuva 9 DDE-hyökkäysvektorin varoitusviesti



Kuva 10 DDE-hyökkäysvektorin varoitusviesti



Kuva 11 DDE-hyökkäysvektorin varoitusviesti

Kalasteluviesti lähetettiin kaikkiaan 293 vastaanottajalle, joista 20:lle satunnaiselle vastaanottajalle soitettiin erikseen pyrkimällä huijaamaan vastaanottajaa avaamaan sähköpostin mukana tullut liitetiedosto. Kalastelupuheluissa kysyttiin, oliko vastaanottaja saanut avajaistarjoukset, ja kehotettiin avaamaan viestin liite puhelun aikana. Puheluista 3:ssa (15 %) vastaanottaja avasi liitteen puhelun aikana pyydettäessä.

Mahdolliset sähköpostiliitteen avaajat eivät todellisuudessa asentaneet tietämättään mitään haitallista työasemilleen, vaan liitetiedoston avaaminen lähetti ainoastaan tiedon kyberhyökkäyssimulaation toteuttaneen yrityksen palvelimelle, että liitetiedosto on avattu ja varoitusviestit jätetty huomiotta.

Jälkikäteen selvisi, että organisaatiolla oli käytössä sellainen Windowsin versio, jossa DDE-protokollan väärinkäyttö ei toiminut siten, kuin sen oletettiin toimivan. Kampanjan aikana statistiikan mukaan yksikään viestin vastaanottajista ei ohittanut kaikkia varoitusviestejä, mikä olisi avannut potentiaaliselle hyökkääjälle pääsyn organisaation työntekijän työasemaan. Todellisuudessa ei siis tiedetä, kuinka moni vastaanottajista avasi viestin, avasi liitteen ja ohitti varoitukset. Liite oli mahdollista avata myös siten, että vastaanottaja on sulkenut varoitusviestit painamatta ”ohita” -nappia. Näin ollen tiedämme varmaksi vain, että 20 soitetuista puheluista kolmessa liite avattiin.

4 TUTKIMUSMETODOLOGIA

Tutkimus on empiirinen ja laadullinen, perustuen kirjallisuuskatsaukseen. Laadullinen siksi, koska tutkimuksessa pyritään ymmärtämään kalasteluviestintää paremmin ilmiönä. Tavoitteena on syventää ymmärrystä siitä, miksi osa kalasteluviesteistä toimii paremmin kuin muut. Tilastollisen yleistämisen sijaan tavoitteena on ymmärtää paremmin, miksi kalasteluviestit toimivat ja kuinka viestin sisältö vaikuttaa viestin toimivuuteen. Jotakin ilmiötä kuvaileva ja ymmärrystä lisäävä, positivistinen tutkimus on tyypillistä tietoturvallisuuden tutkimuskentässä (esim. (Orlikowski & Baroudi, 1991).

Jos tarkastellaan tutkimusta Nummenmaan (2009) näkökulmasta, jossa tutkimus jaetaan empiiriseksi tai teoreettiseksi, ei tämä tutkimus perustu pelkästään teoreettiseen analyysiin, vaan tutkimuksessa tehdään päätelmiä havaintojen pohjalta. Havainnot perustuvat kirjallisuuskatsauksen lisäksi aineistoon (luku 3).

Aineisto perustuu käytännön toimintaan työelämässä silloin, kun organisaatio on kyberhyökkäyksen kohteena. Kirjallisuuskatsauksella pyritään selittämään organisaation toimintaa hyökkäysten aikana perustuen aiempaan tietoon (teoriat, periaatteet, ammatillinen kirjallisuus), ja sitä arvioidaan suhteessa aineistoon. Tämä tutkimus pyrkii siis löytämään teoriasta selityksen sille, miksi aineistossa tapahtui muutosta eri kalastelukertojen välillä, ja selittämään tätä ilmiötä.

Oleelliseksi näkökulmaksi on otettu kiireellisyyden kokemusta lisäävät elementit viesteissä, koska siitä ei juurikaan löytynyt tieteellistä tutkimusta kalastelukontekstissa, ja koska aineisto mahdollistaa tämän (osassa viesteistä on enemmän kiireellisyyden kokemusta lisääviä elementtejä, kuin toisissa). Alun perin tutkimuksen otsikko oli pelkästään ”kiireellisyyden kokemuksen vaikutukset kalasteluviestinnässä”, mutta koska tutkimuksen edetessä kirjallisuuskatsausta oli vaikea rakentaa pelkän kiireellisyyden näkökulmasta aiemman tieteellisen tutkimuksen puuttuessa, lisättiin Pro Gradu - tutkielman otsikkoon sanat ”Kalasteluviestintä ilmiönä”. Ilmiön kuvailun mukaan ottaminen mahdollisti laajemman kirjallisuuskatsauksen, ja sitä kautta paremman ymmärryksen kalasteluviestinnästä ilmiönä.

Suuri osa käyttäytymistieteellisestä tutkimuksesta tietoon liittyen olettaa, että ihmiset käyttäytyvät tarkoituksellisesti ja vakaasti, sekä toimivat rationaalisesti ja tavanomaisesti (Orlikowski & Baroudi, 1991). Tällaisissa tutkimuksissa tutkija on yleensä objektiivinen tarkkailija, mutta positivistista näkökulmaa kritisoidaan myös sen rajoituksista (Orlikowski & Baroudi, 1991). Tässä Pro Gradu - tutkielmassa kirjoittaja on ollut mukana kohdeorganisaatioon tehdyissä kampanjoissa projektiryhmässä, joten tutkija ei ole ulkopuolinen eikä objektiivinen, eikä kyse ole positivistisesta tutkimuksesta, vaan enemminkin kuvailevasta. Kuvailevan ja selittävän tutkimuksen erona on, että kuvaileva tutkimus

vastaa usein kysymyksiin ”mitä” tai ”millainen”, selittävä sen sijaan vastaa enemmän kysymykseen ”miksi” (KvantiMOTV 2009).

Tämä tutkimus ei perustu mihinkään yksittäiseen teoriaan, eikä luo uutta teoriaa. Tutkimus voidaan ajatella abduktiiviseksi, sillä se on sekoitus induktiivista ja deduktiivista siten, että aineisto tuo uusia näkökulmia teoriaan (kiireellisyyden kokemuksen tarkastelu yksittäisenä elementtinä).

Kyseinen aineisto on valittu tutkimuksen aineistoksi siksi, että aineisto on tuorein saatavilla oleva (vuodelta 2017) ja se on otos oikeassa elämässä toimimisesta. Aineisto poikkeaa aiemmasta alan tutkimuksesta siten, että se perustuu oikeassa työelämässä toteutettuihin kampanjoihin ja vastaanottajat ovat olleet henkilöitä, jotka eivät ole tienneet, että kyseessä on tilattu hyökkäyssimulaatio. Aineistossa kuvattu vastaanottajien toiminta on siis verrattavissa siihen, miten henkilöt todellisuudessa oikeasti toimivat kalastelutilanteissa. Hyökkäyksen kohteena oli myös organisaation henkilöstö, eivätkä opiskelijat, joka on ollut toistuva trendi aiemmassa tutkimuksessa. Aiempia tieteellisiä tutkimuksia käsitellään tarkemmin luvussa 2.

Tutkimuskysymykseen vastaamiseen liittyen vertailukelpoisuutta lisää aineistossa se, että kalastelukampanjoita toteutettiin samaan organisaatioon yhteensä kolme, ja osa kalasteluviesteistä sisälsi kiireellisyyden kokemisen elementtejä ja osa ei. Aineisto mahdollistaa kiireellisyyden kokemisen vaikutuksiin liittyvän tarkemman tarkastelun verrattuna esimerkiksi sellaiseen aineistoon, jossa kalastelukampanjoita olisi toteutettu vain yksi. Koska kampanjoita oli useampi ja viestit olivat erilaisia, mutta kohdeorganisaatio pysyi samana, voidaan pohtia, vaikuttivatko kiireellisyyden kokemisen elementit vastaanottajien toimintaan.

Tutkimuksessa olisi voitu käyttää myös yhden kohdeorganisaation sijaan useita kohdeorganisaatioita. Viestien sisällöt suunnitellaan kuitenkin aina organisaatiokohtaisesti, joten mikäli kohdeorganisaatioita olisi ollut useita, viestit olisivat todennäköisesti silti olleet uniikkeja ja siten ne evät olisi olleet täysin vertailukelpoisia keskenään statistiikan kannalta.

5 LÖYDÖKSET

Tässä luvussa pyritään löytämään teoriasta selitys sille, miksi aineistossa tapahtui muutoksia eri kalastelukertojen välillä, ja kuvailemaan tätä ilmiötä. Statistiikoissa voidaan nähdä toistuvia trendejä, joista voidaan tehdä suuntaa-antavia johtopäätöksiä. Hadnagy ja Fincher (2015) muistuttavat, että kyse ei lopulta ole statistiikoista, vaan tavoite on kouluttaa henkilöstöä suojautumaan kalasteluyrityksiltä (2015). Myös tämän tutkielman tavoitteena on, tieteellisen näkökulman lisäksi, että tuloksia voidaan hyödyntää mm. tietoturvallisuuskoulutuksia suunniteltaessa.

Tässä luvussa pyritään vastaamaan tutkimuskysymykseen ja apukysymyksiin:

- Millaiset seikat vaikuttavat kalasteluviestien toimivuuteen?
- Missä määrin kiireellisyyden kokeminen kalasteluviesteissä vaikuttaa viestin vastaanottajien toimintaan?
- Miksi kalasteluyritykset toimivat?

Kaikissa kalastelukampanjoiden viesteissä pyrittiin herättämään vastaanottajassa periferinen ajatteluprosessi rationaalisen ajatteluprosessin sijaan (luku 2.2.4). Mikäli vastaanottaja alkaa prosessoida syvällisesti viestin sisältöä, petos voi tulla ilmi (mm. Ebot, 2017; Goel ym., 2017). Näin ollen kaikki viestit sisälsivät tekijöitä, joiden tarkoitus oli motivoida vastaanottajaa toimimaan ajattelematta viestiä enempää. Kirjallisuuskatsauksen perusteella voidaan olettaa, että ainakin seuraavilla seikoilla on vaikutusta kalasteluviestien toimivuuteen:

- Vastaanottajan aiemmat kokemukset ja tietotaito
- Viestin herättämät tunnetilat
- Viestin herättämä päätöksentekoprosessi
- Viestissä käytetyt suostuttelun periaatteet
- Viestin ulkonäkö, sisältö ja autenttisuus
- Lähettäjän tuttuus
- Kiireellisyyden kokemusta luovat vihjeet viestissä
- Viestin houkuttelevuus tai uhkaavuus
- Viestin geneerisyys

Alla olevaan taulukkoon 1 on kerätty yhteenveto aineistosta ja siinä käytetyistä elementeistä, joilla on todennäköisesti vaikutusta viestin toimivuuteen. Todettakoon, että kampanjan 3 tuloksiin liittyy validiteettiongelmia (selitetty luvussa 3.2.3), joten tulokset ovat siltä osin lähinnä suuntaa-antavia.

Indikaattori	**Kampanja 1**	**Kampanja 2**	**Kampanja 3**
Vastaanottajat	1713	186	20
Viestin liitteen /linkin avanneet	181 (11%)	61 (33%)	3 (15%)

Tietoja antaneiden määrä	-	52 (28%)	-
Uhka/Hyöty	Hyöty	Uhka	Hyöty
Kohdennettu hyökkäys	Ei	Kyllä	Osittain
Kiireelliset elementit	Ei	Kyllä	Kyllä
Suostuttelun periaatteet		Auktoriteetti	Niukkuus
Tunnetilat, joita vastaanottajassa halutaan herättää	Ahneus Uteliaisuus	Pelko Hätä Kiire	Ahneus Kiire

Taulukko 1 Yhteenveto aineiston kalastelukampanjoista

Ensimmäisessä kampanjassa motivaattorina oli paketin saanti. Vastaanottajalla on mahdollisuus saada jotakin (hyötyä), ja herättää sitä kautta ahneuden tunnetta. Toisaalta, vastaanottaja voi ihmetellä viestiä, koska ei ole tilannut kyseistä pakettia, ja saattaa siksi klikata viestin linkkiä (huolestuneisuudesta tai uteliaisuudesta). Periferiseen prosessiin pyrittiin ohjaamaan uteliaisuuden lisäksi harmittomuudella. Viesti vaikuttaa vilpittömältä, siinä ei kysytä mitään tietoja, ja viesti tulee kuriiriyritykseltä. Vaikka kyseinen yritys ei ole vastaanottajalle tuttu (koska nimi oli tekaistu), todennäköisesti vastaanottaja on ennenkin saanut vastaavia sähköposteja, joten tilanne on tuttu. Siitä syystä vastaanottaja saattaa (tapojensa mukaisesti) sen enempää ajattelematta klikata viestin linkkiä, josta lähetystä voi seurata.

Erityisesti toisessa ja kolmannessa kampanjassa käytettiin kiireellisyyden kokemusta lisääviä elementtejä, jotta vastaanottaja toimisi heti. Toisessa kampanjassa haluttin myös herättää vastaanottajassa pelkoa siitä, että tunnukset ovat vuotaneet. Johnstonin ja Warkentinin (2010) mukaan tietoturvallisuuskirjallisuudessa pelkoa pidetään suosittuna tekijänä motivoimaan henkilöitä suojaamaan omia tietojaan.

Tavoite oli, että vastaanottaja siirtyy kloonatulle tunnustenvaihtosivulle ja syöttää tunnuksensa turvatakseen tietonsa. Tosiasiallisesti hän tekee juuri päinvastaisesti; osaamatta toimia paremminkaan, vastaanottaja luovuttaa tunnuksensa hyökkääjälle vahingossa sen sijaan, että tutkisi tarkemmin viestin alkuperää tai kysyisi asiasta esimerkiksi IT-tuelta. Vastaanottajien päätöksentekoon vaikuttaa koettu riski tai palkinto (Goel ym., 2017). Ebot (2017) toteaa, että vastaanottajat klikkaavat pelkoa herättäviä kalasteluviestejä tarkoituksenaan suojella omia tietojaan. Tällöin vastaanottaja usein ei tiedä, mitä tulisi tehdä, joten hän toimii viestissä käsketyllä tavalla (Ebot, 2017). Voidaankin ajatella, että tässä on kyse tason 2 toiminnasta (Ebotin osaamistasoista lisää luvussa 2.2.5).

Tämän tutkimuksen aineisto tukee pelkoon liittyvää havaintoa sen toimivuudesta motivaattorina, sillä eniten klikkauksia prosentuaalisesti sai tämä 2. kampanjan viesti, jossa vastaanottaja luuli, että hänen tunnuksensa ovat vuotaneet. Klikkausprosentti kyseisessä viestissä on huomattavasti suurempi kampanjan 2 viestissä (32 %), kuin kampanjan 1 viestissä (10 %), joka ei sisältänyt tietoturvauhkaa.

Emme kuitenkaan tiedä, luovuttiko vastaanottaja tunnuksensa 2. kampanjassa kloonatussa portaalissa, koska hän hätääntyi ja reagoi ajattelematta, hän ei osannut huomata URL-osoitteesta, että sivusto ei vie oikeaan osoitteeseen, vai koska vastaanottaja ei tiennyt, miten muutenkaan toimia kuin luovuttaa tunnuksensa, vai koska vastaanottaja luuli viestin olevan aito (vai kaikkia näitä syitä). Kuitenkin, koska prosentuaalisesti kalasteluviesti oli toimivin näistä kolmesta, se tukee Goelin (2017) viitettä prospektiteoriaan, jonka mukaan potentiaalinen uhka vaikuttaa ihmisten toimintaan enemmän kuin potentiaalinen hyöty (ks. luku 2.3.1).

Toisaalta, 2. kampanjan viesti oli tehty huolellisesti. Kalastelu oli kohdennettua; kampanjaa varten oli kloonattu kohdeorganisaation portaali ja ostettu alkuperäistä URL :a muistuttava domain. Goelin ym. (2017) tutkimuksen mukaan tilannesidonnaiset ja sisällöltään kohdennetut kalasteluviestit vaikuttavat viestien toimivuuteen. Varsinkin kohdennettu viesti, joka sisältää riskin menettää jotain vastaanottajalle tärkeää, voi ylikirjoittaa tarpeen arvioida seurauksia ja saada vastaanottajan toimimaan nopeasti hyökkääjän eduksi (Goel ym., 2017). Vastaanottaja voi olla tietoinen kalastelumetodeista ja esimerkiksi etsiä tietoa viestin aitoudesta verkosta ennen klikkausta, mutta epäilyksistä huolimatta vastaanottaja saattaa lopulta klikata kalasteluviestin haitallista linkkiä (Ebot, 2017; Goel ym., 2017). 2. kalastelukampanjan tulokset tukevat edellä mainittuja väitteitä, vaikkemme varmuudella tiedä, ovatko viestit herättäneet epäilyksiä vai eivät.

Klikkausten suurta määrää voi selittää myös se, että viesti on mahdollisesti aktivoinut vastaanottajan päässä periferisen prosessointimallin. Vastaanottajaa pyrittiin ohjaamaan periferiseen päätöksentekoprosessiin hyödyntämällä luottamusta, joka oletettavasti on syntynyt IT-osaston ja henkilöstön välille. Koska viestiä näyttää tulleen IT-tuelta ja ”IT-tukeen voi luottaa” (vrt. Viswanathin ”ystäviin voi luottaa” heuristiikkaesimerkki luvussa 2.2.4). Tämä voi aktivoida periferisen päätöksentekoprosessin, jossa reagoidaan ”tuttuun ja turvalliseen” viestiin niin kuin niihin on ennenkin reagoitu. Toisaalta vastaanottaja on todennäköisesti kokenut viestin ja siihen liittyvän päätöksen (miten toimia) tärkeäksi, jolloin systemaattinen prosessointimalli on voinut aktivoitua. Tässä tilanteessa on mahdotonta arvailla, kumpaan prosessointimalliin vastaanottaja on ajautunut aineistossa esiteltyjen kalastelukampanjoiden viestejä saadessaan.

Aiemmin (luvussa 2.3.1) keskusteltiin myös siitä, täytyykö lähettäjän olla tuttu, nimetty henkilö vai riittääkö tuttu organisaatio/yksikkö/muu ei-luonnollinen henkilö. Goel ym. (2017) argumentoi, että heidän tutkimuksensa mukaan nimellä puhuttelu ei ole tarpeen vaan vähempikin personointi riittää, jotta kalasteluviesti toimii. Tämä 2. kampanjan onnistuneisuus tukee Goelin ym. (2017) näkemystä, koska viesti oli kirjoitettu organisaation IT-tuen nimissä yksittäisen henkilön sijaan.

Näyttää siltä, että Ebotin (2017) tulkinta, että kalasteluviestin koettu tärkeys ja mahdollisuus siitä, että viesti on tosi (eikä huijaus), ylikirjoittaa muut mahdollisuudet (uhka huijauksesta ym), pitää paikkansa varsinkin silloin, kun

viesti sisältää uhkan ja kiirellisyyden kokemuksia lisääviä elementtejä. Aineistoa tarkasteltaessa uhkan ja kiireellisyyden kokemusta lisäävät elementit sisältävät viestit (kampanja 2 ja 3) johtivat kalasteluviestin onnistumiseen (vastaanottaja tuli huijatuksi) todennäköisemmin, kuin viestit, joista kyseiset asiat puuttuivat (kampanja 1). Toisaalta, kyseiset kalasteluviestit sisälsivät uhkan lisäksi myös välittömän ratkaisun ongelmaan (”vaihda tunnuksesi tästä”), joka voi osaltaan tehdä viestistä houkuttelevamman. Havainto tukee myös Wangim ym. (2012) toteamusta, että kun relevantiksi koettu kalasteluviesti sisältää pelon, uhan tai kiireellisyyden elementtejä, petos toimii paremmin.

Suuri osa käyttäjien manipulointiin liittyvistä hyökkäyksistä pyrkii hyödyntämään useita eri tekijöitä ja tekniikoita (Workman, 2008). Kolmannessa kampanjassa haluttiin yhdistää ahneus ja niukkuuden periaate (ks. Suostuttelun periaatteet luvussa 2.2.3) lupauksella toimittaa vastaanottajille ilmaiseksi lamppuja, mikäli he toimivat riittävän nopeasti. Tavoitteena oli herättää vastaanottajassa kiireellisyyden kokemusta. Viesti oli kohdennettu siten, että tiedettiin, että se lähetettiin henkilöille, jotka vastaavat sellaisista hankinnoista, joita tekaistun yrityksen nimissä myytiin avajaistarjouksina.

Kalastelupuheluilla kolmannessa kampanjassa oli tarkoitus vauhdittaa vastaanottajan päätöksentekoa ja saada hänet toimimaan (avaamaan liite) jo puhelun aikana. Puheluissa vedottiin kiireellisyyteen ja niukkuuden periaatteeseen (ks. luku 2.2.3) kertomalla, että sähköpostitse lähetetyt tarjoukset ovat lähetetty nyt vain kohdeorganisaation toimialan yrityksille, ja ne ovat voimassa vain muutaman päivän, joten liite kannattaisi avata heti.

Jakobsson ym. (2007) toteavat, että kalastelua puhelimitse pidetään vähiten epäilyttävänä, ja hyökkääjän on usein helppo hyväksikäyttää tätä uskomusta. Tämän Pro Gradu - tutkielman aineiston pohjalta voidaan todeta, että puhelimitse on helppo saada henkilö tekemään jotain, mitä muuten ehkä ei tekisi (kampanja 3). Lähetimme vastaanottajille kalasteluviestin, jossa mainostettiin tarjouksia, eikä viesti ollut erityisen houkutteleva. Siitä huolimatta puhelimitse henkilöistä osa saatiin houkuteltua avaamaan viesti. Kaikki puhelimeen vastanneet sanoivat, etteivät aiemmin olleet avanneet viestiä, vaikka osa oli noteerannut sen. On mahdollista, ettei kukaan vastaanottajista olisi avannut viestiä tai sen liitettä ilman kalastelusoittoja. Kaikki puhelimitse tavoitetut henkilöt suhtautuivat viestiin varauksella niin, etteivät he olleet heti kehoituksesta huolimatta avaamassa viestiä tai sen liitettä. Puhelimessa suostuttelulla, tarjousten ylivoimaisuuden ja rajoitetun ajan korostamisella, saatiin kuitenkin ainakin 3 henkilä (15%) avaamaan tämä liite.

Luvussa 2.3.1 kuvattiin Goelin ym. (2017) tutkimusta, jonka mukaan kalasteluviestit, joissa luvataan ”ilmaisia hyödykkeitä”, voivat ylikirjoittaa vastaanottajan mahdolliset epäilykset viestin aitoudesta ja koettu potentiaalinen hyöty ohittaa potentiaaliset viestin avaamisen riskit. Kolmannen kampanjan tulokset eivät ainakaan ole ristiriidassa tämän väitteen kanssa. Toisaalta, kolmannen kampanjan viestissä vastaanottajalle ei tarjottu mitään henkilökohtaista hyötyä, vaan tuotteita tarjottiin vastaanottajan edustamalle organisaatiolle. Kenties viestiä ei silloin koeta yhtä houkuttelevana.

Kalasteluviestit ovat kehittyneet niin, että niiden tunnistaminen vaatii usein vaivaa ja huomiota tulee erityisesti kiinnittää viestin otsikkoon, lähettäjän tietoihin ja viestien sisältöön (Viswanath ym., 2011). Vaikuttaa siltä, että kiireellisyyden kokemukset ja uhka esimerkiksi potentiaalisesta tietovuodosta saavat vastaanottajan toimimaan nopeasti, jolloin vaivaa viestin luotettavuuden arviointiin ei ehditä käyttää. Samaan tulokseen tulevat tutkimuksessaan myös Wang ym. (2016), ja ajan puute voi johtaa epäonnistuneeseen arvioon. Kuten Viswanath ym. (2011) ja Wang ym. (2012) totesivat, voidaan tämänkin tutkielman pohjalta tehdä huomio, että kiireellisyyden kokemusta lisäävät elementit näyttävät vaikuttavan positiivisesti siihen, että henkilö tulee huijatuksi. Uhka ja kiireellisyys vaikuttavat toimivan yhdessä hyvinä motivaattoreina kalasteluviestin avaamiselle ja viestin ohjeiden mukaan toimimiselle. Myös kiireellisyys ja niukkuus sekä potentiaalinen hyöty (kampanja 3) vaikuttavat olevan hyvä suostuttelutekniikoiden yhdistelmä.

Jakobsson ym. (2007) pitävät kymmenen vuotta sitten kirjoittamassa julkaisussaan kohdistettuja viestejä ja tiedon louhintaa ”tulevaisuuden riskinä”. Aiemmin kalasteluviestit olivat kömpelömpiä ja vähemmän kohdennettuja. Nyt kymmenen vuotta edellä mainitun julkaisun kirjoituksen jälkeen nämä riskit ovat erittäin ajankohtaisia. Esimerkiksi kohdennetun kalastelun uhrin perheenjäsenten nimet, postinumero ja kiinnostuksen kohteet on suhteellisen helppo selvittää julkisista lähteistä tietoa keräämällä ja yhdistelemällä.

Ensimmäisessä kampanjassa ei viestiä oltu tehty kohdennetusti, eli kohdeorganisaatiosta riippumatta kuka vaan voisi saada ”Sinulle on saapumassa paketti”-viestin. Toisessa kampanjassa viesti taas oli erittäin kohdennettu, ja kolmannessa kampanjassa osittain kohdennettu. Näin ollen, koska viesteissä oli paljonkin eroja sisällöllisesti ja ulkonäöllisesti, ei niitä voi tässä kontekstissa luotattavasti verrata keskenään. Tulokset eivät kuitenkaan ainakaan ole ristiriitaisia aiempien tutkimusten kanssa, joissa kohdennetut viestit ovat ovat olleet tehokkaimpia. Myös tässä tutkielmassa kohdennetut viestit (kampanja 2 ja 3) toimivat paremmin, kuin geneerinen (kampanja 1). Aineiston pohjalta voidaan siis todeta, että ainakin tässä hyökkäyssimulaatiossa parhaiten kohdennetut viestit (kampanja 2) tehosivat myös parhaiten.

Mitä tulee hyökkäyssimulaation suunnitteluun ja toteutukseen, se näyttää olevan sopiva väline nykytilan arivointityökalun lisäksi myös opetustarkoituksiin. Hadnagy ja Fincher (2015, 120) toteavat, että he ovat usein aloittaneet kalastelukampanjat geneerisistä viestiestä, ja siirtyneet niistä pikku hiljaa vaikeammin tunnistettaviin, kohdennetumpiin viesteihin. Vaikeimmista viesteistä ei ole aloitettu, koska kohdeorganisaatioissa usein koetaan, että kampanjoista opitaan ja että niitä tehdään hyvässä hengessä, kun henkilöstöllä on paremmat mahdollisuudet tunnistaa viestit kalasteluksi (Hadnagy & Fincher, 2015). Näin tomittiin myös tämän kohdeorganisaation hyökkäyssimulatiossa. Palaute kalastelukampanjoista oli kohdeorganisaatiolta hyvää ja tulokset johdonmukaisia, joten aineisto tukee Hadnagyn ja Fincherin tapaa aloittaa kampanjat geneerisistä kalasteluviesteistä.

Tämä myös tarkoittaa, että aiemmat viestit ovat saattaneet vaikuttaa seuraavien tuloksiin, jos vastaanottajat ovat ymmärtäneet, että nyt heitä kalastelallaan. Jos viestit olisivat samankaltaisia, niin vastaanottajien pitäisi oppia, jolloin klikkausten määrän tulisi vähentyä ja onnistuneiden kalasteluhyökkäysten määrän laskea jokaisella kerralla. Se, että kyseessä on sarja viestejä, on merkittävää statistiikkaa analysoitaessa.

Henkilöiden osaamistason vaikutuksia kalastelun toimivuuteen arvioitaessa voidaan todeta, että koulutusten merkityksellisyyttä ja hyötyjä on tutkittu liian vähän, jotta niiden todellinen arvo voitaisiin selvittää. Vaikka kalastelua käsittelevässä kirjallisuudessa usein neuvotaan kiinnittämään huomiota kalasteluviestin tiettyihin seikkoihin, kuten otsikkoon, lähettäjään ja viestin sisältöön (Viswanath ym., 2011), niin neuvoja ei välttämättä noudateta, koska niitä ei ole kohdennettu oikean osaamistason oleville henkilöille (Ebot, 2017). Käytännössä tämä tarkoittaa sitä, että yritetään opettaa esimerksiksi internetin käyttöä henkilölle, joka ei osaa käyttää tietokonettakaan.

Hadnagy ja Fincher (2015) toteavat kokemuksiensa pohjalta, että jatkuva (esim. kerran kuukaudessa tai neljä kertaa vuodessa) testaaminen ja lyhyet, ytimekkäät tietoturvakulutukset pienentävät kalasteluviestien klikkausmäärää. Hadnagy ja Fincher (2015) esittävät, että muutoksia tuskin tapahtuu kuukausissa vaan pikemminkin vuosissa. Myös tässä tutkielmassa käytetty aineisto jokseenkin tukee tätä päätelmää, koska vaikka aloitimme helposti tunnistettavista, geneerisistä viesteistä ja siirryimme niistä kohdennetumpiin viesteihin, klikkausten määrä prosentuaalisesti väheni. Klikkausten määrän laskua voidaan selittää myös monilla muilla tässä luvussa mainituilla tekijöillä.

Tämän Pro Gradu -tutkielman aineisto, välissä olevan koulutuksen merkityksellisyyttä pohdittaessa, ei suoraan tue, muttei myöskään ole ristiriidassa koulutuksiin liityvien aiempien väitteiden kanssa. On mahdotonta luotettavasti arvioida, kuinka paljon 2. ja 3. kampanjan välissä pidetty koulutus vaikutti henkilöstön osaamistasoon ja/tai 3. kampanjan tuloksiin. Koska aineistosa ei löydy tähän enempää näkökulmaa, koulutusnäkökulmaa pohditaan lisää luvussa 6.

6 POHDINTA

Tässä luvussa pohditaan kalasteluilmiötä aiempien tutkimusten valossa peilaten niitä tähän tutkielmaan. Tutkielmaa tehdessä esiin nousseita asioita, joihin aineisto ei anna suoraa vastausta, on avattu tässä luvussa.

Aineisto ei kerro, millaisissa mielentiloissa tai ajanhetkellä kalasteluviestejä avattiin. Aiempien tutkimusten pohjalta kuitenkin tiedostamaton ja ”automatisoitu” sähköpostin selailu kasvattaa kalastelun uhriksi joutumisen riskiä. Tiedostamattomaan ja tapojensa orjana suoritettavaan sähköpostin selailuun voisi auttaa se, että päivästä otetaan erikseen aikaa sähköpostien lukuun, eikä sitä suoriteta automaatiotoimintana esimerkiksi autoa ajaessa. Työyhteisöissä organisaatioita voitaisiin kannustaa siihen, ettei sähköpostia selailla puhelimesta esimerkiksi lounastunneilla. On mahdollista jopa estää mobiilisähköpostisovellusten käyttö, mikä voi olla tarpeen, mikäli kalasteluhyökkäykset ovat organisaatiossa todellinen ongelma, ja tietovuotojen seuraukset ovat vakavia tai erittäin vakavia.

Downsin ym. (2006) ja Workmanin (2008) tutkimustulokset näyttävät tukevan Ebotin (2017) tutkimuksia siltä osin, että vaikka käyttäjät tiesivät, että heidän tulee suojella tietojaan, ja vaikka viestit herättivät välillä epäilyksiä, siitä huolimatta käyttäjät toimivat viestissä halutulla tavalla, koska eivät tienneet, miten muutenkaan toimia. Tämän tutkielman aineiston pohjalta ei tiedetä, herättivätkö kalasteluviestit vastaanottajissa epäilyksiä, vai eivät.

Viswanathin ym. (2011) tulokset siitä, että mitä enemmän käyttäjä saa sähköpostia, sitä todennäköisemmin hän tulee huijatuksi ja joutuu kalastelun uhriksi, voi implikoida myös sähköpostin käyttäjän kiireeseen. Sen lisäksi, että kalasteluviestien sisältämät kiireellisyyden kokemusta lisäävät elementit näyttävät lisäävän todennäköisyyttä tulla huijatuksi, voi myös vastaanottajan kokema kiire siitä, että sähköposteja on paljon, vaikuttaa huijatuksi tulemisen todennäköisyyteen. On mahdollista, että ylipäätään kiireellisyyden kokemukset vaikuttavat siihen, kuinka todennäköisesti sähköpostin käyttäjä tulee huijatuksi. Mitä kiireisempi käyttäjä, sitä korkeampi riski. Tämän aineiston pohjalta ei kuitenkaan tiedetä, kuinka kiireisiä vastaanottajat olivat, tai kuinka paljon he saavat päivittäin sähköpostia.

Ebot (2017) toteaa, että välttyäkseen huijatuksi tulemiselta, vastaanottajalla tulisi olla turvallisuusosaamisen ja minäpystyvyyden (eng. self-efficacy) lisäksi olla erityistä tietämystä siitä, kuinka toimia kalastelutilanteessa. Tämä tukee ajatusta siitä, että tietoturvakoulutuksilla, joissa käsitellään kalasteluviestien tunnistamista ja niiltä suojautumista, on vaikutusta siihen, miten vastaanottaja toimii kalasteluviestejä kohdatessaan.

Ebot ehdottaa (2017), että henkilöiden yksilölliset tarpeet ja nk. osaamistaso (ks. luku 2.2.5) tulisi arvioida, jotta suositukset tietoturvallisuuden kehittämiseksi voidaan antaa räätälöidysti. Esimerkiksi enismmäisellä tasolla oleville tulee kouluttaa yleisellä tasolla tietoturvallisuutta, kun taas toisella tasolla oleville voidaan kertoa syvällisemmin, mikä on oikea tapa toimia

huijaustilanteessa ja kuinka huijaus voidaan tunnistaa (Ebot, 2017). Toisella tasolla olevilla on jo ymmärrys turvallisuusongelmista, mutta he eivät välttämättä siitä huolimatta osaa toimia oikein (Ebot, 2017). Toisella osaamistasolla olevia henkilöitä voitaisiin esimerkiksi ohjeistaa olemaan klikkaamatta sellaisia viestejä, jotka aiheuttavat heissä hämmennystä (Ebot, 2017). Lisäksi, turvallisuusasiantuntijoiden tulisi kontrolleja suunnitellessa arvioida, mitä erityisesti henkilöisen toiminnassa halutaan muuttaa, kuten kalasteluviestien liitteiden tai linkkien klikkaaminen (Ebot, 2017).

Mitä valveutuneisuuteen ja koulutuksiin tulee, Wrightin ja Marettin (2010) mukaan kohonnut turvallisuustietoisuus (esimerkiksi turvallisuuspoikkeaman tai koulutuksen seurauksena) saa vastaanottajat varuilleen. Voidaan olettaa, että jo suorittamamme kaksi kalastelukampnjaa sekä tietoturvakoulutus on lisännyt henkilöstön tietoturvatietoisuutta ja se on yksi syy, miksi kolmannessa kampanjassa « klikkausalttius » oli pienempi, eli teknisistä haasteista huolimatta näyttää siltä, että kalasteluviesteillä oli vähemmän uhreja prosentuaalisesti.

Ebot (2017) mainitsee, että emme vielä tiedä, tulevatko käyttäjät huijatuiksi hyödyn sisältävissä viesteissä esimerkiksi ahneuden, alruismin vai toiveajattelun vuoksi. Kalasteluviestinnältä suojautumiseen liittyvä koulutus on todettu usein tehottomaksi ja tulokset ovat olleet huonoja (mm. Goel ym., 2017). Tässäkin Pro Gradu - tutkielmassa on todettu, ettei kalasteluilmiötä ole tarpeeksi tutukittu, eikä sitä vielä täysin ymmärretä. Tämä saattaa osaltaan selittää sitä, miksi kalasteluviesteihin haksahdetaan tietoturvakoulutuksista ja neuvoista huolimatta.

7 JOHTOPÄÄTÖKSET

Tässä luvussa avataan tarkemmin tutkielman vahvuudet ja rajoitukset liittyen validiteettin ja reliabiliteettiin (luku 7.1), sekä esitetään lyhyt yhteenveto tutkielmasta (luku 7.2). Jatkotutkimusaiheita löytyi useita ja ne on avattu luvussa 7.3. Tutkielman sovellettavuutta ja tulosten käytettävyyttä pohditaan viimeisessä luvussa (7.4).

7.1 Tutkimuksen vahvuudet ja rajoitukset

Hadnagy ja Fincher (2015) mainitsevat statistiikan luotettavuutta heikentäviä seikkoja, jotka pätevät myös tämän tutkimuksen aineiston analyysissä. Hadnagy ja Fincher (2015, 124) suosittelevat, että kalastelukampanjoissa kannattaa mitata kuutta asiaa:

1) ihmisten määrä, jotka klikkasivat,
2) ihmisten määrä, joka raportoivat viestin kalasteluksi,
3) ihmisten määrä, jotka klikkasivat mutteivät raportoineet,
4) ihmisten määrä, jotka klikkasivat ja raportivat,
5) ihmisten määrä, jotka eivät klikanneet eivätkä raportoineet, ja
6) ihmisten määrä, jotka eivät klikanneet ja jotka raportoivat.

Tässä tutkimuksessa käytetty aineisto sisälsi vain 1) lähetyttyjen kalasteluviestien määrän ja 2) niiden vastaanottajien määrän, jotka avasivat viestin ja jotka klikkasivat viestin sisältämää haitallista linkkiä tai latasivat haitallisen liitteen. Lisäksi hyökkäyskampanjoiden välisissä tapaamisissa kävimme suullisesti läpi ne kalastelun uhrien IT-tuelle tekemät raportoinnit, jotka olivat kohdeorganisaation projektiryhmän jäsenten tiedossa.

Mikäli statistiikkaa olisi kerätty järjestelmällisesti Hadnagyn ja Fincherin (2015) ehdottamista kuudesta eri asiasta, olisi kalastelukampanjoiden tehokkuutta todennäköisesti voitu arvioida laajemmin. Tavoite on usein organisaation tietoturvalliosuuskulttuurin näkökulmasta, että niiden ihmisten määrä, jotka eivät klikanneet viestiä mutta jotka raportoivat siitä, olisi mahdollisimman suuri. Nyt tätä määrää ei tiedetä.

Arviota siitä, ovatko kalastelukampanjat auttaneet henkilöstöä tunnistamaan kalasteluviestit, auttaisi kenties se, että kalasteluviestit olisivat kaikissa kampanjoissa lähetetty koko henkilöstölle, eikä vain osalle siitä. Nyt ei voida varmuudella tietää, onko yksi yksittäinen henkilö saanut ja avannut kalasteluviestit kaikissa kolmessa kampanjassa, vai vaan osassa niistä (tai ei lainkaan). Organisaatiossa voi siis olla henkilöitä, jotka ovat saaneet kaikki kolme kalasteluviestiä, ja henkilöitä, jotka eivät ole saaneet yhtäkään, joten testaus ei ole ollut tasapuolista. Toisalta tämä riski on aina otettava silloin, kun koeryhmästä valitaan satunnainen otanta, jolle viestit lähetetään. Emme myöskään voi

varmuudella tietää, etteikö henkilöstö olisi keskustellut kalasteluviesteistä sisäisesti, emmekä tiedä, mitkä olivat niiden henkilöiden pohjatiedot ja -taidot, jotka tunnistivat viestit kalasteluiksi.

Hadnagy ja Fincher (2015) väittävät tallaista testaamista, jossa testataan vain osa henkilöstöstä kerrallaan ja mitataan vain klikkausalttiutta, merkityksettömäksi. Argumentti pohjautuu siihen, että mitattavuuden luotettavuus kärsii. Hadnagyn & Fincherin (2015) mielestä kampanjat eivät ole suoraan vertailukelpoisia keskenään, koska viesteistä osa on geneerisiä ja osa kohdennettuja. Toisaalta, jos koko henkilöstö saa kalasteluviestit, niiden kohdennus on vaikeaa, eikä erilaisten viestien toimivuutta voida vertailla. On epätodennäköistä, että esimerkiksi johdolle lähetetään sisällöltään täysin samanlainen kalasteluviesti, kuin työntekijöille. Täytyy myös muistaa, että aineisto perustuu hyökäykseen, jossa haluttiin simuloida tosielämän hyökkäyksiä. Aineisto ei siis oltu kerätty tutkimusta varten.

Statistiikkaa (aineistoa) tarkastellessa on mahdollista, että tulokset ovat sattumaa. Nyt tiedämme vain, että kampanja 2 oli huomattavasti toimivampi kuin kampanja 1, ja kampanjan 3 kalastelupuheluiden avulla saadut tulokset olivat myös huomattavasti paremmat, kuin ensimmäisessä kampanjassa. Viestit olivat kuitenkin sisällöltään hyvin erilaisia ja kiireellisyyden elementtien lisäksi eroja oli suostutteluteknikoissa sekä viestien kohdentamisessa. Emme varmuudella tiedä, mitkä näistä viestien sisällöllisistä ominaisuuksista vaikuttivat tai eivät vaikuttaneet avaamiseen.

Aihetta laajennettiin (ks. luku 4), koska aineisto ei ole riittävän vahvaa, jotta siitä voitaisiin vetää yksiselitteisiä johtopäätöksiä, vaikuttavatko kiireellisyyden kokemusta lisäävät elementit kalasteluviestin toimivuuteen. Aineistossa ei ole näyttöä siitä, kokiko vastaanottaja todellisuudessa kiireellisyyttä, koska vastaanottajia ei haastateltu jälkikäteen. Kalasteluviestien toimivuuteen vaikuttaa aiempien tutkimusten perusteella myös lukuiset muut syyt, kuin pelkästään kiireellisyyden kokeminen. Näitä syitä esitellään luvussa 2. Emme tiedä esimerkiksi vastaanottajan koulutustaustaa, viestien herättämiä tunteita, mihin päätöksentekoprosessiin on päädytty, ja mitkä tekijät vaikuttivat mahdollisesti enemmän, kuin muut.

Viestien avaamiseen voi siis vastaanottajan päässä vaikuttaa moni asia, jota emme tiedä. Esimerkiksi lomakausi (kampanja 1), vastaanottajien ikä, sukupuoli, asema, osaaminen, luonteenpiirteet ja muut yksilölliset erot ja kiire voviat olla asioita, jotka vaikuttavat viestien avaamiseen. Myös kampanjan 2 ja 3 välissä ollut koulutus on voinut vaikuttaa kampanjan 3 tuloksiin. Nämä kaikkki ovat potentialisia korrelaatiotekijöitä, jotka voivat vaikuttaa statistiikkaan sen lisäksi tai siitä huolimatta, että viesti sisälsi kiireellisyyden kokemuksen elementtejä.

Aineistoa ei ole myöskään kerätty siten, että olisi voitu vertailla kahta eri satunniasesti valittua testiryhmää, joissa toiselle ryhmälle lähetetään kiireellisyyden kokemuksen elementtejä sisältävä viesti, ja toiselle ei. Jos tällainen asetelma olisi ollut mahdollinen, oltaisiin voitu vertailla tuloksia luotettavammin.

On siis mahdollista, että heikon aineiston vuoksi analyysissä on tapahtunut 1. tyypin virhe (false positive). On mahdollista, että vaikka näyttää siltä, että kiireellisyyden kokemusta luovien elementtien lisääminen kalasteluviesteihin lisää todennäköisyyttä, että vastaanottaja toimii hyökkääjän haluamalla tavalla, tällaista yhteyttä ei todellisuudessa välttämättä ole. Toisaalta teoria puhuu sen puolesta, että kiireellisyys vaikuttaa päätöksentekoon ja altistaa virheille.

Täytyy myös huomioida, että näyte on pieni. Olisi hyvä, jos kohderyhmässä olisi satoja, jopa tuhansia kalasteluyritysten vastaanottajia. Lähetettyjä viestejä on tässä tutkielmassa suhteellisen vähän. Kampanjassa 1 kohderyhmä oli suhteellisen iso (noin 1700 lähetettyä kalasteluviestiä), mutta esimerkiksi kampanjan 3 aineistosta voimme arvioida vain murto-osaa lähetetyistä viesteistä testauksessa ilmenneiden teknisten haasteiden vuoksi. Kohteena oli myös vain yksi organisatio ja kampanjat jakaantuivat yhden vuoden ajalle, eivät esimerkiksi viiden vuoden ajalle. Näytteen peini koko laskee tutkielman luotettavuutta.

Jos tämä tutkimus toistetaan, ei välttämättä saada samoja tuloksia. Ihmiset ovat oppivia yksilöitä, ja jos hyökkäyssimulaatioita tehdään testaus- ja koulutusmielessä, niin on toivottavaa, että ihmiset muuttavat käyttäytymistään. Tutkimusta ei kuitenkaan sellaisenaan ole toistettu kyseisessä kohdeorganisaatiossa, tai missään muussakaan organisaatiossa.

Tarkoitus on kuitenkin onnistua selittämään kalasteluviestintää ilmiönä. Kyseinen ilmiö ei tule aina esille, esimerkiksi johtuen siitä, että vastaanottajia on koulutettu tai heillä ei ole kiire, joten kiireellisyyden lisääminen kalasteluviesteihin ei välttämättä aina lisää viestien onnistumista.

Tutkielman vahvuutena on, että hyökkäyksen kohteena on ollut työelämän organisaatio. Tutkielma erottuu monista muista aiemmista tutkumuksista sillä, ettei kohdeorganisaatio ole yliopisto, ja hyökkäyksen kohteet eivät ole opiskelijoita. Lähteenä on nk. arkistotieto (eng. arhival data), jossa aineisto kerättiin alun perin organisaation oman tietoturvallisuustason määrittelemiseksi ja haavoittuvuuksien löytämiseksi.

Luotettavuuden arvioinnissa positiivista on, että tutkimusta voidaan tehdä käytännön tasolla (käytännön aineisto), eikä kohde tiennyt olevansa testattavana aineistoa kerätessä (kyseessä ei ole esimerkiksi kyselytutkimus tai laboratorio-olosuhteissa tehty tutkimus). Koska kohdeorganisaation henkilöstö ei tiennyt hyökkäyksestä etukäteen, se lisää tulosten luotettavuutta siitä, kuinka henkilöstö toimisi oikeassa tosielämän hyökkäystilanteessa. Kysely- ja haastattelututkimuksissa on haasteena se, että henkilö voi vastata jotakin muuta, kuin miten todellisuudessa toimisi.

Tutkimustuloksiin ei siis vaikuta koehenkilöiden tietoisuus siitä, että kyseessä on koe tai testi, koska hyökkäyssimulaatiossa havainnointiin toimintaa tositilanteessa (tai henkilö luulee, että kyseessä on tositilanne). Organisaatiolla oli myös intressinä nähdä, vaikuttaako pidetty koulutus (toisen ja kolmannen kampanjan välissä kalasteluviestinnän tuloksiin.

Tämän tutkielman luotettavuutta olisi voitu nostaa huomattavasti, mikäli kalasteluviestin saaneita henkilöitä olisi voitu haastatella, tai heille olisi lähetetty kyselylomake jälkikäteen. Siinä olisi voitu kysyä esimerkiksi

vastaanottajan kokemasta kiireestä, tunnetiloista, osaamistasosta sekä seikoista, joihin hän kiinnitti huomiota kalasteluviestin avattuaan. Olisi ollut kiinnostavaa tietää, mitkä seikat saivat vastaanottajan klikkaamaan viestin linkkiä/liitettä tai siirtämään viestin roskakoriin, ja mitkä seikat saivat vastaanottajan mahdollisesti raportoimaan viestistä eteenpäin. Kyselyitä tai haastatteluita ei tehty, koska kalastelu-uhrien henkilötietoja ei ole tarkoituksella kerätty, jotta heillä on mahdollisuus pysyä anonyyminä. Eettisestä näkökulmasta tällainen jälkihaastattelu on vaikea järjestää.

Tässä alaluvussa avatuista rajoituksista johtuen ei tämän tutkielman pohjalta voida vielä muodostaa teoriaa tai mallia, eikä tutkimuksesta voida vetää suoraa syy-seuraussuhdetta siihen, miksi osa kalasteluviesteistä oli tehokkaampia kuin toiset. Voidaan kuitenkin todeta, että aihetta tulisi tutkia lisää. Tutkielma myös lisää ymmärrystä kalasteluviestinnästä ilmönä.

7.2 Yhteenveto

Vaikuttaa siltä, että vastaanottajan toimintaan kalastelutilanteessa vaikuttaa moni seikka. Näitä ovat mm.

- Vastaanottajan aiemmat kokemukset ja tietotaito
- Viestin herättämät tunnetilat
- Viestin herättämä päätöksentekoprosessi
- Viestissä käytetyt suostuttelun periaatteet
- Viestin ulkonäkö, sisältö ja autenttisuus
- Lähettäjän tuttuus
- Kiireellisyyden kokemusta luovat vihjeet viestissä
- Viestin houkuttelevuus tai uhkaavuus
- Viestin geneerisyys

Aihetta täytyy tutkia lisää, jotta ilmiötä voidaan ymmärtää paremmin. Aiempien tutkimusten sekä tämän tutkielman valossa ei vielä tiedetä, mitkä tekijät vaikuttavat vastaanottajaan eniten tai vähiten, ja ovatko ne esimerkiksi tilannesidonnaisia seikkoja.

Näyttää kuitenkin siltä, että kiireellisyyden kokemusta lisäävillä elementeillä on positiivinen vaikutus kalasteluviestien toimivuuten. Viswanathin ym. (2011) mukaan kiireellisyyden kokemusta lisäävät elementit ovat tutkimustulosten pohjalta kaikista toimivimpia, petokseen johtavia vihjeitä kalasteluviesteissä, mutta tämän aineiston pohjalta yhtä vahvaa väitettä ei voi tehdä.

Tulosten pohjalta etenkin uhkaavilla viesteillä, jotka sisältävät kiireellisyyden kokemusta luovia elementtejä, ja jotka ovat kohdennettuja (eng. spear fishing), on suuri todennäköisyys toimia. Toinen toimivaksi havaittu yhdistelmä on niukkuuden periaatteen, kiireellisyyden kokemusta luovien elementtien ja hyödyn (uhkan sijaan) käyttäminen samassa viestissä.

Kalastelviestien yhteydessä soitetut kalastelupuhelut näyttävät johtavan hyökkääjän kannalta parempiin tuloksiin.

Kalasteluviestintä on organisaatioiden kannalta vakava uhka, ja siltä on mahdotonta suojautua pelkästään teknisin keinoin. Henkilöstön koulutus on yksi niistä kontrolleista, joilla kalasteluviestinnältä suojautumista voidaan edesauttaa. Koulutuksen sisältöä suunnittellessa tulee huomioida koulutukseen osallistuvien osaaminen ja tietotaito.

7.3 Jatkotutkimus

Tutkielmaa tehdessä kiireellisyyden kokemuksen vaikutukset ihmisten verkkokäyttäytymiseen oli aihe, josta oli hyvin vaikeaa löytää tieteellistä tutkimusta. Kiireellisyyden kokemusten vaikutukset (viestien sisällön luoma kokemus, mutta myös vastaanottajan kokema kiire esimerkiksi sähköpostitulvan vuoksi) tarvitsee myös lisää tutkimusta, kyseistä näkökulmaa ei aiemmassa tieteellisessä tutkimuksessa ole löydösten mukaan käsitelty juuri lainkaan.

Kyselytutkimusten ja kokeiden sijaan olisi hyvä, jos voitaisiin tutkia ihmisten toimintaa kyberhyökkäysten, tai kyberhyökkäyssimulaatioiden aikana siten, että tutkimuksen kohteet eivät tiedä, että kyseessä on testi tai tutkimus. Suurin osa aiemmasta tutkimuksesta on tehty niin, että henkilöt ovat tienneet olevansa testattavana. Pelkät kyselyt ja haastattelut eivät ole välttämättä paras menetelmä luotettavien tutkimustulosten saamiseksi. Lisäksi kiinnostavaa olisi tutkia sitä, miten kyberhyökkäyssimulaatioiden aikana ja niiden jälkeen tarjotut palautteenantomahdollisuudet ja -kanavat vaikuttavat simulaation uhrien tuntemuksiin ja kokemuksiin hyökkäyksestä.

Tutkimuksien kohderyhmäksi olisi hyvä valita opiskelijoiden sijaan myös työyhteisöjä. Yksi aihe, mistä ei myöskään löytynyt tätä tutkielmaa tehdessä aiempia tutkimuksia, on kalasteluviestintään liittyvien raportointikäytäntöjen toimivuus työyhteisöissä. Olisi kiinnostavaa tietää, miksi ihmiset raportoivat tai eivät raportoi epäilyistään, liittyykö siihen esimerkiksi käyttäytymistieteellisiä seikkoja. Jätetäänkö raportoimatta, koska sitä ei pidetä tärkeänä, ei osata, ei ole ketään, kenelle raportoida, työntekijää hävettää tai hän pelkää saavansa rangaistuksen, koska avasi kalasteluviestin ja/tai luovutti tietoja? Tutkimusta kaipaa myös se, miten IT-osasto toimii raportteja saadessaan, ja kuinka organisaation sisäiset raportointikäytännöt vaikuttavat kalasteluyrityksiin, varsinaisiin kalasteluhyökkäyksiin ja hyökkäysten seurauksiin.

Lisäksi yksityiskäyttäjänäkökulmaa voisi tuoda tutkimuskentälle lisää siten, että aineistossa olisi erilaisia ihmisiä demografisesti mahdollisimman laajalla otannalla. Kohderyhmien ylipäätään tulisi olla isoja, jotta tutkimustulokset olisivat luotettavampia. Kentien tässä voitaisiin tehdä yhteistyötä jonkin virustentorjuntaohjelman palveluntarjoajan, Viestintäviraston kyberturvallisuuskeskuksen tai jonkun muun tahon kanssa, kenellä on/voisi olla pääsy tietokantoihin, joiden avulla voisi tavoittaa myös hyökkäysten todellisia (oikean elämän) uhreja.

Tutkimuksen kohderyhmänä hakkerit olisivat myös erittäin mielenkiintoinen lähestymistapa aiheeseen, mutta tämä kohderyhmä on tuskin tavoitettavissa tieteellistä tutkimusta varten. Hakkerit haluavat pysyä piilossa ja lähes aina myös anonyymeinä, joten he tuskin antavat esimerkiksi haastatteluita.

7.4 Käytännön sovellukset

Tätä tutkielmaa voidaan hyödyntää työyhteisöissä, joissa kalasteluviestinnältä halutaan oppia suojautumaan paremmin. Tutkielma voi auttaa esimerkiksi organisaation tietoturvaryhmää tai IT-osastoa ymmärtämään kalastelua ilmiönä paremmin, mikä auttanee tietoturvakoulutuksien sisältöjen ja muiden tietoturvakontrollien suunnittelussa.

Tutkielma voi auttaa myös kyberhyökkäyssimulaatioita tuottavia yrityksiä suunnittelemaan ja tekemään parempia simulaatioita. Aineiston validiteettihaasteet osoittivat, että simulaatioita suunnitellessa ja statistiikkoja kerättäessä tulisi kehittää sitä, miten tulokset olisivat vertailukelpoisempia. Vertailukelpoisuus parantaisi tulosten mitattavuutta, mikä taas auttaa organisaatiota mahdollisen turvallisuuskulttuurin kehityksen arvioinnissa. Olisi toivottavaa, että jos organisaatio panostaa työntekijöiden oppimiseen ja hyökkäyssimulaatioita käytetään arvioimaan organisaation osaamista, statistiikat muuttuisivat ajan kuluessa siten, että kalasteluviestien uhreja olisi jatkossa vähemmän ja raportointeja höykkäyksistä olisi enemmän.

Tutkielma toimii tiedeyhteisöissä myös ponnistuslautana uusille tutkimuksille. Tämä tutkielma osoittaa, että kalastelu kaipaa lisätutkimusta monista eri näkökulmista ja lähtökohdista.

LÄHTEET

Ars Technica. (2012). *8 million leaked passwords connecyed to LinkedIn, daring website.* Haettu 1.11.2018 osoitteest https://arstechnica.com/information-technology/2012/06/8-million-leaked-passwords-connected-to-linkedin/

BBC News. (2012). *LinkedIn users targeted in email scam after hack.* Haettu 1.11.2018 osoitteesta https://arstechnica.com/information-technology/2012/06/8-million-leaked-passwords-connected-to-linkedin/

Ben Zur, H. & Breznitz, S.J. (1981). *The effect of time pressure on risky choice behaviour.* Acta Psychologica (47) 2, 89-104.

Buller, J. & Burgoon, J. (1996). *Interpersonal Deception Theory*. Communications Theory. Volume 6, Issue 3, 1 August 1996, 203–242.

Butavicius, M., Parsons, K., Pattinson, M. & McCormac, A. (2015). *Breaching the human firewall: Social engineering in phishing and spear-phishing emails*. Paper presented at the 26th Australasian Conference on Information Systems, Adelaide, Australia.

Bacharach, S.B. (1989). *Organizational theories: Some criteria for evaluation*. The Academy of Management Reviw, 14(4), 496-515.

Buller, D. B., Strzyzewski, K. D. & Comstock, J. (1991). *Interpersonal deception: I. Deceivers' reactions to receivers' suspicions and probing.* Communication Monographs, 58, 1-24.

Cialdini, R. (2001). *Harnessing the Science of Persuasion.* Harvard Business Review, October 2001, 73-39.

Cowan, D. A. (1986). *Developing a process model of problem recognition.* Acad. Manage. Rev., vol. 11, pp. 763–776.

Downs, J. S., Holbrook, M. B. & Cranor, L. F. (2006). *Decision strategies and susceptibility to phishing.* In Proceedings of the Second Symposium on Usable Privacy and Security, 79-90.

Ebot, A. (2017). *Explaining two forms of Internet crime from two perspectives: toward stage theories for phishing and Internet scamming.* Väitöskirja. Informaatioteknologian tiedekunta. Jyväskylän Yliopisto.

Ekman, P. & Friesen, W. (1974). *Detecting deception from the body or face*. Journal of Personality and Social Psychology, 29, 288-298.

Goel, S., Williams, K. & Dincelli, E. (2017). *Got Phished? Internet security and human vulnerability.* Journal of the Association for Information Systems; Atlanta Vol. 18, Iss. 1, january, 22-44.

Hadnagy, C. (2010). *Social Engineering. The Art of Human Hacking.* Wiley.

Hadnagy, C. & Fincher, M. (2015). *Phishing Dark Waters. The Offensive and Defensive sides of Malicious E-mails*. Wiley.

Halevi, T., Memon, N. & Nov, O. (2015). *Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks.*

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). *Social Phishing.* Communications of the ACM, 50(10), 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, 356-361.

Jakobsson, M. (2007). *The human factor in phishing.* Privacy & Security of Consumer Information, 7, 1-19.

Johnson, P. E., Grazioli, S., Jamal, K. & Zualkernan, I. (1992). *A Success and Failure in Expert Reasoning*, Organizational Behavior and Human Decision Processes (53:2), 173-203.

Johnston, A. C. & Warkentin, M. (2010). *Fear appeals and information security behaviors: An empirical study.* MIS Quarterly, 34(3), 549-566.

Kahneman, D. & Tversky, A. (1979). *Prospect theory: An analysis of decision under risk.* Econometrica, 47(2), 263-291.

Kalbfleisch, P. J. (1992). *Deceit, distrust and the social milieu: Application of deception research in a troubled world.* Journal of Applied Communication Research, 20, 308-334.

Knapp, M. L. & Cornadena, M. E. (1979). *Telling it like it isn't: A review of theory and research on deceptive communication.* Human Communication Research, 5.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2007). *Teaching johnny not to fall for phish.* ACM Transactions on Internet Technology (TOIT), 10(2), 7.

KvantiMOTV. (2009). *Tutkimusprosessi.* Haettu 25.11.2018 osoitteesta https://www.fsd.uta.fi/menetelmaopetus/tutkimus/prosessi.html

Langer, E.J., Blank, A. & Chanowitz, B. (1978). *The Mindlessness of Ostensibly Thoughtful Action: The Role of Placebic Information in Interpersonal Interaction.* Journal of Personality and Social Psychology 36, no. 6, 635-2.

Lawrence, P. R., & Nohria, N. (2002). *Driven: How human nature shapes our choices*. San Francisco: Joseey-Bass.

Maier, N. R. F. & Thurber, J.A. (1968). *Accuracy of judgements of deception when an interview is watched, heard and read.* Personnel Psychology, 21, 23-30.

McCroskey, J. C. (1972). *An introduction to rhetorical communication.* Englewood Cliffs, NJ: Prentice-Hall.

McCroskey, J. C. & Young, T. J. (1981). *Ethos and credibility: The construct and its measurement after three decades.* Central States Speech Journal, 32.

Mitchell, R. W. & Thompson, N. S. (1986). *Deception: Perspectives on Human and Non-human Deceit*. SUNY Press, Albany, NY.

Mitnick, K. & Simon, W. (2002). *The art of deception: Controlling the human element of security.* Indianapolis: Wiley Publishing.

Mitnick, K. & Vamosi, R. (2017). *The Art of Invisibility.* Little, Brown and Company.

Naidoo, R. (2015). *Analysing urgency and trust cues exploited in phishing scam designs.* In 10th International Conference on Cyber Warfare and Security, 216.

Nummenmaa, L. (2009). *Käyttäytymistieteiden tilastolliset menetelmät.* Helsinki: Tammi, 22-24.

Orlikowski, W. J. & Baroudi, J. J. (1991). *Studying information technology in organizations: Research approaches and assumptions.* Information Systems Research, 2(1), 1-28.

Petty, R. & Cacioppo, J. (1986). *The elaboration likelihood model of Persuasion.* Advances in experimental social psychology. Vol. 19, 123-205. San Diego: Academic Press.

Riggio, R.E. (1986). *Assessment of basic social skills.* Journal of Personality and Social Psychology, 51, 649-660.

Riggio, R. E. (1993). *Social interaction skills and nonverbal behavior.* Applications of nonverbal behauioral theories and research, Hills- dale, NJ: Erlbaum.

Sanastokeskus TSK. (2004). *Tiivis tietoturvasanasto*. Haettu 21.2.2018 osoitteesta http://www.tsk.fi/tiedostot/pdf/TiivisTietoturvasanasto.pdf

Sanastokeskus TSK. (2016). *Kohdennettu verkkourkinta*. Haettu 21.2.2018 osoitteesta http://www.tsk.fi/tsk/fi/haku-266.html?page=get_id&id=ID468&vocabulary_code=TSKTT

Stiff, J.B., Miller, G.R, Sleight, C., Mongeau, P., Garlick, R. & Rogan, R. (1989). *Explanations for visual cue primacy in judgements of honesty and deceit.* Journal of Personality and Social Psychology, 56, 555-564.

Staudenmayer, N., Tyre, M. & Perlow, L. (2002). "*Time to change: Temporal shifts as enablers of organizational change*". Organization Science (13) 5, 583-597.

Thagard, P. (1992). *Adversarial Problem Solving: Modeling an Opponent Using Explanatory Coherence*. Cognitive Science (16), 123-149.

Vishwanath, A. (2015). *Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack.* Journal of Computer-Mediated Communication, 20(5), 570-584.

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.

Waller, M.J., Conte, J.M., Gibson, C.A. & Carpenter, M.A. (2001). *The effect of individual perceptions of deadlines on team performance.* Academy of Management Review (26) 4, 586-600.

Wang, J., Herath, T., Chen, R., Vishwanath, A. & Rao, H. R. (2012). *Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email.* Professional Communication, IEEE Transactions On, 55(4), 345-362.

Wang, J., Li, Y. & Raghav, R. (2016). *Overconfidence in Phishing Email Detection.* Journal of the Association for Information Systems; Atlanta Vol. 17, Iss. 11, November, 759-783.

Wright, R. T. & Marett, K. (2010). *The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived.* Journal of Management Information Systems, 27(1), 273-303.

Workman, M. (2008). *Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security.* Journal of the American Society for Information Science and Technology, 59(4), 662-674.

Zuckerman, M., Koestner, R. & Alton, A.O. (1984*). Learning to detect deception.* Journal of Personality and Social Psychology, 46, 519-528.