Justus Uurtimo

TIETOJENKALASTELU JA SIITÄ ILMOITTAMINEN SUOMALAISESSA IT-ALAN ORGANISAATIOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Uurtimo Justus
Tietojenkalastelu ja siitä ilmoittaminen suomalaisessa IT-alan organisaatiossa.
Jyväskylä: Jyväskylän yliopisto, 2023, 55 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaajat: Siponen Mikko, Laatikainen Gabriella

Tämän pro-gradu tutkimuksen tarkoituksena on tutkia sitä miten suomalaisen IT-alan organisaation työntekijät reagoivat saamiinsa tietojenkalasteluviesteihin. Tämän lisäksi tutkimuksessa pyritään selvittämään, onko tietojenkalasteluviestien kehittyneisyydellä vaikutusta siihen, luodaanko kalasteluviestistä ilmoitus ja vaikuttaako tietojenkalastelun onnistumiseen se, avataanko viesti mobiililaitteella. Tutkimus koostuu kirjallisuuskatsauksesta, sekä tutkimusosiosta, joka suoritettiin kenttäkokeena, jota täydennettiin kahden otoksen suhteiden testillä suoritettavalla data-analyysillä, sekä haastatteluilla. Tutkimuksen aineisto koostuu kahdesta tietojenkalasteluaallosta, sekä niiden jälkeen suoritetuista haastatteluista. Tietojenkalasteluaallot suoritettiin osana kohdeorganisaatioon tehtävää tietojenkalastelusimulaatiota. Osana tutkimusta suoritettujen tietojenkalasteluaaltojen, sekä haastatteluiden avulla voitiin saada laadullista ja määrällistä dataa henkilöiden toiminnasta saatuaan tietojenkalasteluviestin. Tässä tutkimuksessa kerätty data on laaja-alaista ja se on kerätty todenmukaisissa olosuhteissa. Osana tutkimusta päästiin myös haastattelemaan henkilöitä, jotka olivat saaneet tutkimuksen simulaatiossa lähetettyjä tietojenkalasteluviestejä. Tutkimuksen tulokset osoittivat, että ihmiset reagoivat monin eri tavoin vastaanottamiinsa tietojenkalasteluviesteihin ja organisaation sisällä kommunikoitiin monipuolisesti tietojenkalasteluviesteistä. Tutkimuksen tulokset osoittivat myös, että tietojenkalasteluviestin kohdentamisella oli vaikutusta siihen, oliko tietojenkalastelu onnistunutta. Tietojenkalastelun kohdentamisella ei tämän tutkimuksen tulosten perusteella ole vaikutusta siihen luodaanko kalasteluviestistä ilmoitus. Mobiililaitteen käyttämisen ja tietojenkalasteluviestin onnistumisen väliltä ei voitu tämän tutkimuksen perusteella vetää suoria johtopäätöksiä, sillä tietojenkalasteluviestejä avattiin hyvin harvoin mobiililaitteella, jonka vuoksi dataa siitä ei kertynyt tarpeeksi. Tätä tutkimusta voidaan soveltaa organisaatioiden sisäisten ilmoituskäytäntöjen, sekä muiden tietoturvamekanismien kehittämiseen. Tutkimusta voidaan myös hyödyntää tulevissa tietojenkalastelusimulaatioissa, sekä tietojenkalasteluun liittyvissä tutkimuksissa.

Asiasanat: tietojenkalastelu, kohdennettu tietojenkalastelu, kalastelusta ilmoittaminen

ABSTRACT

Uurtimo, Justus
Phishing and Reporting in a Finnish IT Industry Organization.
Jyväskylä: University of Jyväskylä, 2023. 55 pp
Cyber Security, Master's Thesis
Supervisors: Siponen Mikko, Laatikainen Gabriella

The purpose of this master's thesis is to investigate how employees of a Finnish IT organization react to phishing emails they receive. Additionally, the study aims to determine whether the sophistication of phishing emails has an impact on whether the phishing is successful and whether a report is generated. The study also aims to determine if the success of phishing is influenced by opening the email on a mobile device. The research consists of a literature review and a research section. The research section was conducted as a field study and it was supplemented by data analysis using a two-sample proportions test, and interviews. The data for the study consists of two phishing waves and interviews conducted after these waves. The phishing waves were conducted as part of a phishing simulation in the target organization. Through the phishing waves and interviews conducted as part of the study, qualitative and quantitative data were collected on how individuals behave when they receive phishing emails. The data collected in this study is comprehensive and was collected under realistic conditions. As part of the research, interviews were conducted with individuals who had received phishing emails sent as part of the research simulation. The results of the study showed that people react in various ways to the phishing emails they receive, and there was diverse communication within the organization regarding phishing emails. The study also found that the sophistication of phishing emails had an impact on whether phishing attempts were successful. Based on the results of this study, the sophistication of phishing did not affect whether a report was generated. Regarding the relationship between using a mobile device to open phishing emails and the success of phishing, no direct conclusions could be drawn from this study because phishing emails were rarely opened on mobile devices, and therefore, there was not enough data. This research can be applied to the development of internal notification practices and other security mechanisms within organizations. It can also be used in future phishing simulation exercises and research related to phishing.

Keywords: phishing, spear-phishing, phishing reporting

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tässä Pro Gradu -tutkielmassa tutkitaan syitä, jotka johtavat tietojenkalasteluviestien onnistumiseen, sekä tietojenkalasteluviesteissä esiintyviä yleisiä rakennemalleja ja miten ne vaikuttavat käyttäjien huijaamisen onnistumiseen. Tutkielmassa tarkastellaan lisäksi sitä, miten työelämässä tietojenkalastelua kohtaavat henkilöt reagoivat saamiinsa tietojenkalasteluviesteihin. Reagoinnilla tarkoitetaan tässä yhteydessä esimerkiksi, tietojenkalasteluviestin käsittelyä, sekä siitä ilmoittamista.

Sähköinen tietojenkalastelu on ollut ihmisten riesana jo lähes 30 vuoden ajan, eikä se todennäköisesti ole katoamassa mihinkään. Tietojenkalastelun englanninkielisen termin ”phishing” alkuperä voidaan jäljittää ainakin vuoteen 1996, jolloin termiä käytettiin viitatessa America Online (AOL) tunnusten kalastelemiseen, käyttäen sähköpostiviestejä eräänlaisina syötteinä. (Ollmann, 2007). Englannin kielisen termin ”ph” alkuliitteen käytön virallinen syy on kadonnut historian hämäriin, mutta se hyvin todennäköisesti on tunnustus ” Phreaking:ille”, eli puhelimiin kohdistuneelle hakkeroinnille (Ollmann, 2007). Tietojenkalasteluilla saaduista ”kaloista” (eng. ”phish”), muodostui jo tuolloin eräänlainen elektroninen valuutta, jota saatettiin vaihtaa esimerkiksi laittomasti kopioituihin ohjelmistoihin (Ollmann, 2007).

Internetin arkipäiväistymisen myötä, käytännössä jokainen yritys voi pyrkiä samoille markkinoille, riippumatta siitä missä yritys fyysisesti sijaitsee. Tämä on johtanut siihen, että monet yritykset ovat, melkein kuin kilpaa, integroineet erilaisia tietojärjestelmiä osaksi yrityksen ansaintalogiikkaa. Yritysten lisäksi, myös verkossa toimivat rikolliset voivat sijaita missä päin maailmaa tahansa, jonka vuoksi yritysten tietojärjestelmien suojaaminen on entistä haastavampaa. Mikäli yritykseen kohdistunut tietomurto aiheuttaa tietovuodon, jossa yksityisten ihmisten henkilökohtaisia tietoja päätyy vääriin käsiin, voi sillä olla yritykselle merkittäviä seurauksia. Yrityksiin voidaan kohdistaa mittavia sakkoja, mikäli tietovuodon seurauksena havaitaan sen johtuneen huonosta tietoturvasta yrityksen sisällä. Laajimmista rikkomuksista sakot voivat olla jopa 20 miljoonaa euroa, tai 4% yrityksen vuosittaisesta liikevaihdosta (Your Europe, 2022).

Yritykselle voidaan lisäksi määrätä kielto prosessoida ihmisten dataa. Tällöin se ei esimerkiksi saisi prosessoida ihmisten luottokorttitietoja (Your Europe, 2022). Pelkästään tämänkaltainen prosessointikielto, olisi käytännössä kuolonisku yritykselle, jonka ensisijainen ansaintamalli perustuu verkkokauppoihin.

Yritysten ja organisaatioiden lisäksi tietojärjestelmät ovat tärkeä osa myös monien yksityishenkilöiden jokapäiväistä elämää. Digi- ja väestötietoviraston julkaiseman digiturvabarometrin mukaan digitaalisten palveluiden käyttö ovat jo tärkeä osa elämää 78 % ihmisistä kaikissa ikäryhmissä. Tämän lisäksi niiden käyttö tulee yhä lisääntymään kaikissa ikäryhmissä. (Digi- ja väestotietovirasto, 2022).

Yhä kiihtyvän digitalisaation myötä organisaatioihin kohdistuu nykyään monia erilaisia kyberuhkia. Euroopan unionin kyberturvallisuusvirasto, ENISAn, mukaan organisaatioiden suurimpia uhkia ovat muun muassa erilaiset kiristysohjelmat (eng. Ransomware), palvelunestohyökkäykset (eng. Denial of Service), erilaiset haittaohjelmat, sekä sähköpostiuhat (European Union Agency for Cybersecurity., 2021). Tässä tutkimuksessa keskitytään tutkimaan tietojenkalastelua (eng. phishing), joka lukeutuu edellä mainittuihin sähköpostiuhkiin.

Tietojenkalastelun määrään vaikuttaakin, se että hyökkääjillä ei tarvitse välttämättä olla teknistä osaamista tietokoneista, tai varsinaisesta hakkeroinnista, tai muusta tietojärjestelmiin murtautumisista, vaan monille riittää tarpeeksi hyvän viestin kehittäminen ja niiden lähettäminen (Warburton & Pompon, 2019). Tietojenkalastelulla hyökkääjät kykenevätkin saavuttamaan merkittäviä tuloja ilman kovin suurta tietoteknistä osaamista, tai merkittävää kiinnijäämisen pelkoa. Pelkästään vuonna 2021 suomalaisilta huijattiin noin 30 miljoonaa euroa, hyödyntämällä erilaisia tietojenkalasteluviestejä (Traficom, 2021, s. 23). Lisäksi Digi- ja väestötietoviraston julkaiseman Digiturvabarometriin vastanneiden mukaan 83% vastanneista oli saanut huijaus- tai tietojenkalastelusähköposteja (Digi- ja väestotietovirasto, 2022).

Tietojenkalasteluviestien merkittävyyttä tietoturvauhkana korostaa se, että viestien muodostamaa uhkaa ei voida täysin torjua pelkästään automatisoiduilla teknisillä keinoilla, sillä tietojenkalatelijat muuttavat jatkuvasti käyttämiään viestejä, pyrkiessään välttelemään teknisiä ja pitkälti automatisoituja turvatoimia (Vishwanath ym., 2011, s. 576). Tämän vuoksi osa tietojenkalasteluun liittyvän tietoturvauhan hallitsemisesta kaatuu väkisinkin viestien vastaanottajien harteille. Aikaisempien tutkimusten perusteella on kuitenkin havainnoitu, että organisaation työntekijät, eli tietojenkalasteluviestien vastaanottajat, ovat usein tietoturvan heikoimpia lenkkejä (Crossler ym., 2013, s. 91). Tähän viittaa myös Digi- ja väestötietoviraston julkaisema Digiturvabarometri, johon vastanneista ihmisistä 75% ei ollut osallistunut tietoturvakoulutukseen vuoteen, tai koskaan (Digi- ja väestotietovirasto, 2022). Lisäksi barometriin vastanneista 30 % koki, ettei tietoturvakoulutukset koske heitä (Digi- ja väestotietovirasto, 2022). Hyvänä esimerkkinä siitä miten ihmiset voivat jopa toimia automatisoituja tietoturvakeinoja vastaan, voidaan käyttää tapausta tietoturvayhtiö RSA:han kohdistuneesta tietojenkalasteluhyökkäyksestä. Hyökkäyksessä yrityksen sähköpostien suodatin oli onnistuneesti suodattanut tietojenkalasteluviestin roskaposteihin, mutta

yrityksen työntekijä oli siitä huolimatta avannut viestin ja sen sisältämän liitteen (Parmar, 2012, s. 9).

RSA:n tapauksesta merkityksellisen tähän tutkimukseen tekee sen, että siinä automaattisen teknologiaan pohjautuvat tietoturvajärjestelmät toimivat moitteettomasti, mutta työntekijöiden toiminnasta löytyi moitittavaa. Tällöin on tärkeää tarkastella myös niitä tietojenkalasteluviestien ominaisuuksia, joiden avulla työntekijöiden toimintaan pyritään vaikuttamaan hyökkääjien toimesta. Lisäksi on tärkeää tarkastella niitä toimia, joita voidaan tehdä sen eteen, että työntekijät osaisivat tunnistaa, sekä raportoida mahdollisimman tarkasti saamansa tietojenkalasteluviestit. RSA:han kohdistunutta hyökkäystä tarkastellaan vielä tarkemmin luvussa 2.4.

1.1 Tutkimuskysymykset

Tässä työssä ensisijainen tutkimuskysymykseni on:

1) ”Miten suomalaisen IT-alan organisaation työntekijät reagoivat heihin kohdistuvaan tietojenkalasteluun?”

2) ”Onko kohdennetun ja geneerisen tietojenkalastelunviestin välillä eroja kalastelun onnistumisessa?”

3) ”Onko kohdennetun ja geneerisen tietojenkalasteluviestien välillä eroa siinä, luodaanko niistä ilmoitusta?”

4) ”Vaikuttaako tietojenkalastelun onnistumiseen se, avataanko viesti mobiililaitteella?”

Tutkimuskysymykset on pyritty muodostamaan siten, että niiden avulla voidaan muodostaa parempi kuva siitä, miten suomalaisessa IT-alan organisaatiossa tietojenkalasteluviesteihin reagoidaan. Tutkimus kysymysten avulla pyritään myös löytämään uutta tietoa siitä, onko tietojenkalasteluviestin kehittyneisyydellä merkitystä sen suhteen, onnistuuko tietojenkalastelu ja luodaanko siitä ilmoitus. Lisäksi tutkimuskysymysten avulla pyritään löytämään uutta tietoa siitä, vaikuttaako mobiililaitteella viestin avaaminen tietojenkalastelun onnistumiseen.

Odotettu tulos ensimmäiseen tutkimuskysymykseen on, että eroja tietojenkalasteluviesteihin reagoinnissa syntyy geneerisen ja kohdennetun tietojenkalasteluviestin välillä. Tämän lisäksi on oletettavaa, että IT-alan organisaation henkilöstöllä on myös tarvittava tietämys tietojenkalasteluviestien ilmoittamisen tärkeydestä. Aikaisemman tutkimuksen mukaan ihmiset eivät kuitenkaan kovin usein ilmoita saamistaan tietojenkalasteluviesteistä eteenpäin (Kwak ym., 2020 s. 2).

Toisen tutkimuskysymyksen odotettu tulos on, että tietojenkalasteluviestin lievälläkin kohdentamisella on merkittävä vaikutus tietojenkalastelun onnistumiseen.

Kolmannen tutkimuskysymyksen odotettu tulos on, että kohdennetusta tietojenkalasteluviestistä luodaan todennäköisemmin ilmoitus, sillä on todennäköisempää, että ihmiset tunnistavat ja vain poistavat tökerömmin luodun geneerisen tietojenkalasteluviestin.

Neljännen tutkimuskysymyksen odotettu tulos on, että mikäli tietojenkalasteluviestin vastaanottaja avaa viestin älylaitteella, kuten puhelimella, niin linkin avaaminen ja sen takana olevalle sivustolle tietojen syöttäminen on todennäköisempää. Älylaitteella pahantahtoisen verkkosoitteen tunnistaminen on todennäköisesti hankalampaa, sillä verkko-osoitteet eivät yleensä näy kokonaisuudessaan mobiililaitteiden näytöiltä. Tämän lisäksi upotettujen linkkien tarkastaminen on mobiililaitteilla huomattavasti hankalampaa, sillä se usein vaatii käyttäjää painamaan linkkiä pitkään sormellaan, joka saattaa johtaa linkin avaamiseen vahingossa.

Tietojenkalastelun onnistumista, riippuen siitä avataanko viesti mobiililaitteella, on tutkittu hyvin vähän. Tämä todennäköisesti johtuu siitä, että tutkimuksen aikana ei voida etukäteen tietää sitä, kuinka moni viestin tulee mobiililaitteella avaamaan. Useimmat mobiililaitteiden käyttöön perustuvat tietojenkalastelututkimukset ovatkin tutkineet lähinnä tekstiviestien välityksellä tapahtuvaa tietojenkalastelua, sekä puheluiden välityksellä tapahtuvaa tietojenkalastelua.

1.1.1 Tutkimuksen aineiston keruu ja tutkimusmenetelmät

Tämä tutkielma on jaettu kahteen osaan. Ensin tutkimuksessa käydään läpi tietojenkalasteluun liittyvää aikaisempaa tutkimusta kirjallisuuskatsauksen muodossa. Tämän jälkeen osana tutkimusta suoritetaan tietojenkalastelukampanja. Tässä tutkimuksessa ei ole kirjallisuuskatsauksessa valittu yhtä teoriaa, johon tutkimus pohjautuu. Sen sijaan kirjallisuuskatsauksessa käsitellään petosteoriaa ja yleisiä käyttäytymisilmiöitä, jotka selittävät miksi ja miten tietojenkalasteluviestintä onnistuu tavoitteessaan.

Kirjallisuuskatsauksessa käytetty lähdekirjallisuus koostuu tieteellisistä artikkelista, kirjoista, sekä aiheeseen liittyvistä uutisista. Lähdekirjallisuuden hakemisessa on hyödynnetty esimerkiksi Google Scholar hakukonetta, sekä Jyväskylän yliopiston JYKDOK kansainvälisten e-aineistojen hakukonetta. Kirjallisuuskatsauksessa pyritään käyttämään mahdollisimman uusia lähteitä, mutta on kuitenkin huomioitava, että sähköistä tietojenkalastelua on tapahtunut jo vuodesta 1996, jolloin osa käytetystä aineistosta saattaa olla vanhempaa.

Kirjallisuuskatsauksen kirjoittamisen jälkeen osana tutkimusta suoritettiin tietojenkalastelukampanja suomalaiseen IT-alan organisaatioon. Tällaisen hyökkäyssimulaation tarkoituksena on lähettää kohde organisaatioon erilaisia tietojenkalasteluviestejä ja seurata sitä, miten ihmiset niihin reagoivat. Tämän kaltaisen simulaation voi ajatella vastaavan monille kouluajoilta tuttua palohälytysharjoitusta. Tässä monille tutussa harjoituksessa palohälyttimet alkavat yhtäkkiä soida, jonka jälkeen oppilaiden tulee siirtyä siistissä järjestyksessä ennalta määriteltyyn tapaamispaikkaan.

Tietojenkalastelusimulaation voi toteuttaa, joko varoittamalla työntekijöitä siitä etukäteen, tai suorittaa tietojenkalastelukampanja varoittamatta. (Hadnagy ym., 2015, s. 107–109) Näistä kahdesta vaihtoehdosta, versio, jossa työntekijöitä ei varoiteta etukäteen tarjoaa todennäköisemmin tuloksen, joka on lähempänä tosielämän tilannetta (Hadnagy ym., 2015, s. 109; Jones ym., 2015). Tämä johtuu siitä, että aikaisempien tutkimuksien mukaan tieto tietojenkalasteluun liittyvästä tutkimuksesta ja tulevasta tietojenkalastelusta saattaisi vaikuttaa huomattavasti osallistujien käyttäytymiseen ja tämän myötä myös tutkimuksesta saataviin tuloksiin (Jones ym., 2015; Mouton ym., 2015, s. 7). Tutkimuksessa suoritetusta tietojenkalastelu kampanjasta kerrotaan tarkemmin luvussa 4.

Tutkimuksessa saatujen tietojen analysoinnissa on hyödynnetty tekoälyä. Käytetty tekoäly oli ChatGPT versio 3.5 ja sitä hyödynnettiin tutkimuksen tuloksista muodostettujen taulukoiden sisältämän numeraalisen datan tulkinnassa. Tämä tapahtui käytännössä siten, että tekoälylle annettiin syöte, jossa pyydettiin tekoälyä analysoimaan annettua taulukkoa ja tämän jälkeen verrattiin, löysikö tekoäly datasta jotain, joka oli jäänyt aiemmin havaitsematta. Tietoturvaan liittyvistä syistä, tekoälylle annettiin ainoastaan hyvin geneeristä numeerista dataa, josta ei voida päätellä mistä data on peräisin.

1.2 Eettiset ongelmat liittyen tietojenkalastelun tutkimiseen

Osana tätä tutkimusta tullaan suorittamaan tietojenkalastelu simulaatio, jossa aidon oloisia tietojenkalasteluviestejä lähetetään työntekijöille. Simulaation tarkoitus on altistaa vastaanottajat tietojenkalastelulle, mahdollisimman todenmukaisessa ympäristössä. Tämän vuoksi, tietojenkalasteluviesteissä tullaan myös käyttämään erilaisia sosiaalisen manipuloinnin keinoja, jotka ovat käytössä myös oikeissa tietojenkalasteluviesteissä. Aikaisempien tutkimusten mukaan tällainen hyökkäyssimulaatio, voi kuitenkin aiheuttaa henkilöissä negatiivisia tunteita (Goel ym., 2017, s. 29).

Tämän vuoksi tietojenkalastelu simulaatiot pyritään tässä tutkimuksessa luomaan siten, että ne eivät loukkaa kenenkään yksityisyyttä, eivätkä suoraan syyllistä ketään yksittäisiä työntekijöitä. Lisäksi tietojenkalastelukampanjassa käytetyt viestit pyritään luomaan niin, että ne eivät aiheuta turhaa epäluottamusta ketään kohtaan. Viestejä ei tulla esimerkiksi luomaan siten, että ne näyttäisivät työkavereiden LinkedIn kutsuilta. Vaikka oikeassa maailmassa hyökkääjät käyttäisivät tällaisia tilaisuuksia häikäilemättä hyväkseen, niin tämän kaltaiset viestit aiheuttaisivat todennäköisesti huomattavaa epäluottamusta muita työyhteisön jäseniä kohtaan, josta seuraisi enemmän haittaa kuin hyötyä.

Ihmiseen kohdistuvan tutkimuksen eettisien periaatteiden mukaan tutkimukseen osallistuvalla henkilöllä on oikeus osallistua vapaaehtoisesti tutkimukseen, sekä kieltäytyä tutkimuksesta (Kohonen ym., 2019). Tämä otettiin tässä tutkimuksessa huomioon, kun tutkimukseen haettiin haastateltavia.

Haastatteluihin kutsuttiin ihmisiä yleisillä ilmoituksilla, jolloin vastaajilla oli täysi vapaus jättää ilmoittautumatta. Tietojenkalasteluaallot kohdistettiin koko organisaatioon, eikä tällöin ketään yksittäisiä työntekijöitä yksilöity viestien vastaanottajiksi.

2 KIRJALLISUUSKATSAUS

Tietojenkalastelulta käyttäjien suojaamista koskevaa aikaisempaa tieteellistä tutkimusta voidaan yleisesti jaotella kahteen erilaiseen lähestymistapaan. Näistä ensimmäinen tutkii käyttäjien suojaamista teknologisilla menetelmillä ja toinen tutkii henkilöiden käyttäytymistä, jotta ymmärtäisimme miksi tietojenkalasteluviestit toimivat. (Vishwanath ym., 2011, s. 1–2) Tässä tutkimuksessa perehdytään lähinnä ihmisten käyttäytymiseen liittyvään tutkimukseen, sillä tutkimuksen tarkoituksena on tutkia sitä, miten ihmiset reagoivat tietojenkalasteluviesteihin.

Tässä kirjallisuuskatsauksessa käsitellään ensin ihmisten manipulointia mahdollistavia käyttäytymisilmiöitä ja petosteoriaa, jonka avulla voidaan selittää miten ihmiset tunnistavat mahdollisen petostilanteen. Tämän jälkeen kirjallisuuskatsauksessa käsitellään tietojenkalasteluviestien yleisiä piirteitä, sekä jaetaan tietojenkalasteluviestit neljään eri tasoon aikaisemman tutkimuksen perusteella.

2.1 Käyttäjien manipulointi

Ihmisten manipulointi, erityisesti sosiaalinen manipulointi (eng. social engineering), muodostaa keskeisen osan tietojenkalastelusta, minkä vuoksi sen käsittely tässä kirjallisuuskatsauksessa on perusteltua. Lisäksi, kun pyritään kehittämään suojamekanismeja tietojenkalastelua vastaan, on äärimmäisen tärkeää ymmärtää niitä ajatteluprosesseja, jotka altistavat ihmiset tietojenkalastelulle.

Tietojenkalastelun lopullisena tavoitteena on yleensä, nimensä mukaisesti, se, että ”kalastelija” saa uhrinsa toimimaan haluamallaan tavalla. Tämä saattaa tarkoittaa esimerkiksi sitä, että uhri päätyy antamaan hyökkääjälle rahaa, tai tietoja kuten käyttäjätunnuksia. (Hadnagy ym., 2015, s. 6) Ihmiset eivät kuitenkaan yleisesti ottaen luovuta omia käyttäjätunnuksiaan, tai muita henkilökohtaisia tietojaan hyökkääjälle tieten tahtoen. Tämän vuoksi on mielekästä tarkastella jonkin verran niitä käyttäytymisilmiöitä, jotka johtavat siihen, että ihmiset päätyvät luovuttamaan omia henkilökohtaisia tietojaan hyökkääjälle. Osana tätä tutkimusta

on myös mielekästä käsitellä hieman petosteoriaa, joka käsittelee menetelmiä, joiden avulla ihmiset pystyvät tunnistamaan mahdollisen tapahtuvan petoksen. Petosteorian käsittely ihmisten manipulointiin pyrkivien keinojen kanssa on mielekästä, sillä teorian mukaan johdonmukaisimmilla huijauksilla on huomattavasti suurempi todennäköisyys onnistua (Vishwanath ym., 2011). Petosteorian käsittämät osa-alueet ovat siis juuri niitä käyttäytymisen malleja, joita tietojenkalasteluviestien lähettäjät pyrkivät toiminnallaan hämäämään.

2.1.1 Käyttäytymisilmiöt

Ihmisten suostutteluun liittyvät periaatteet ovat vahvasti tutkittuja ja tietojenkalasteluun liittyen ne voidaan käytännössä jakaa kolmeen koulukuntaan. Nämä koulukunnat ovat Cialdinin kuusi suostuttelun periaatetta (Cialdini, 2007), Stajanon ja Wilsonin määrittelemät seitsemän huijauksen periaatetta (Stajano & Wilson, 2011) ja Graggin määrittelemät seitsemän psykologista laukaisinta (Gragg, 2003). Näiden kolmen koulukunnan määrittelemät periaatteet voidaan jakaa viiteen yhteiseen periaatteeseen, jotka ovat aktiivisesti esillä tietojenkalasteluviesteissä (Ferreira ym., 2015). Nämä viisi yhteistä periaatetta ovat:

- **Auktoriteetti (eng. Authority)**
  - Ihmisillä on yhteiskunnallisesti taipumus totella auktoriteettisessa asemassa olevia henkilöitä. Esimerkiksi (Gragg, 2003) mukaan ihmisten on haastavaa tarkastaa auktoriteetin todenperäisyys, joka osaltaan mahdollistaa auktorisessa asemassa olevana henkilönä esiintymisen johtavan onnistuneeseen huijaukseen.

- **Sosiaalinen validointi (eng. Social Proof)**
  - Ihmisillä on luontainen taipumus käyttäytyä sosiaalisten normien mukaisesti, jotka yhteiskunta meille määrittelee. Ihmiset siis pyrkivät käyttäytymään siten, miten he olettavat ympäröivän yhteisön haluavan heidän käyttäytyvän (Cialdini, 2001). Kalasteluviestinnässä voidaan antaa henkilön olettaa muiden jo hyväksyneen viestin sisällön, jolloin viestin sanomaa voi olla vaikeampaa pitää epäluotettavana.

- **Pitäminen, samanlaisuus & hämäys (eng. Liking, similarity & Deception)**
  - Ihmisillä on taipumus luottaa tuntemattomiin ihmisiin enemmän, mikäli he kokevat heidän olevan hyvin samanlaisia heidän kanssaan. Esimerkiksi (Gragg, 2003) mukaan hakkerin kannattaa esiintyä mahdollisimman saman kaltaisena ihmisenä kuin hyökkäyksen uhri, voittaakseen uhrin luottamuksen, vaikkei tälle luottamukselle olisi muuten mitään loogista perustetta.

- **Sitoutuneisuus, vastavuoroisuus ja johdonmukaisuus (eng. Commitment, Reciprocation & Consistency)**
    - Ihmiset todennäköisesti toteuttavat lupauksensa jonkin asian tekemisestä, etenkin jos lupaus on annettu julkisesti (Ferreira ym., 2015). Mikäli saatavilla ei ole vahvaa todistusaineistoa siitä, että vastapuoli valehtelee, ihmiset myös hyvin todennäköisesti uskovat vastapuolen kertovan lähtökohtaisesti totuuden siitä mitä he tarvitsevat ja keitä he ovat (Gragg, 2003, s. 9).

- **Harhautus**
    - Ihmisten loogiseen päättelyyn voidaan vaikuttaa käyttämällä jonkinlaista harhautusta. Tällainen harhautus saattaa pyrkiä saamaan uhrin huomion suuntautumaan esimerkiksi mahdollisuuteen saada jotain, minkä saaminen tulisi myöhemmin olemaan lähes mahdotonta (Ferreira ym., 2015). Harhautuksen onnistuessa ihmisten huomio keskittyy täysin tähän lupaukseen jonkin asian, kuten vaikkapa huomattavan omaisuuden, nopeaan saamiseen, jolloin huomio tietojenkalasteluun viittaavista vihjeistä jää uhrilta huomaamatta. Mahdollisen suuren omaisuuden saaminen toimii hyvin harhautuksena, sillä ihmiset luontaisesti tahtovat asioita, joita heillä on vähän tai joidenka hankkiminen ei ole helppoa (Cialdini, 2001). Vastavuoroisesti omaisuuden saamisen lisäksi, hyökkääjät saattavat käyttää harhautuksena, jotain muuta äärimmäistä tunnetta, kuten pelkoa (Hadnagy ym., 2015, s. 110–112). Tämä pelko voidaan kohdistaa esimerkiksi omaisuuden, tai maineen menetykseen.

Näiden viiden periaatteen on havaittu esiintyvän hyvin usein jonkinlaisessa kombinaatiossa ainakin yhden toisen periaatteen kanssa (Ferreira ym., 2015). Näistä kombinaatioista yleisimmäksi osoittautuivat auktoriteetin ja pitämisen, sekä samankaltaisuuden ja hämäyksen kombinaatiot (Ferreira ym., 2015). Tämä on sinänsä hyvin loogista, sillä kukapa työssä ahertava ei pitäisi siitä, että esihenkilö asemassa oleva osoittaa olevansa paitsi samankaltainen, mutta myös pitävänsä alaisestaan. Lisäksi etenkin organisaatiossa aloittavalle uudelle työntekijälle voi olla hyvin vaikeaa kyseenalaistaa auktorisessa asemassa olevaa esihenkilöä.

2.1.2 Petosteoria

Petosteorian mukaan ihmiset havainnoivat petokseen pyrkiviä yrityksiä tulkitsemalla mahdollisia epäjohdonmukaisuuksia kanssakäymisessä ja vertailemalla niitä aikaisempiin kokemuksiin (Wang ym., 2012). Petosteoria on alun perin kehitetty tunnistamaan miten ihmiset tulkitsevat esillä olevaa informaatiota petostilanteissa (Johnson ym., 1992). Petosteoriaa (eng. Theory of Deception) voidaan kuitenkin soveltaa myös tarkastellessa tietojenkalasteluun pyrkiviä sähköposteja (Wang ym., 2012). Tämä johtuu siitä, että siinä missä Interpersonaalinen petosteoria (eng. Interpersonal Decepiton Theory) keskittyy enemmän aktiiviseen, tai ”kasvokkain” tapahtuvaan kommunikaation analysoimiseen, on petosteorian käyttö mielekkäämpää, kun analysoinnin kohteena on epäinteraktiivisempi sähköinen tietojenkalastelu (Wang ym., 2012). Petosteorian mukaan huijauksen huomaaminen voidaan jaotella neljään eri vaiheeseen (Vishwanath ym., 2011; Wang ym., 2012). Nämä neljä vaihetta ovat:

- **Aktivointi (eng. Activation)**
  - Uhri havaitsee mahdollisen petoksen huomaamalla anomalioita esillä olevassa informaatiossa.

- **Petoksen hypoteesin muodostaminen**
  - Uhri vertailee havaitsemaansa mahdollista petollista informaatiota aikaisempiin kokemuksiinsa. Tämän pohjalta uhri muodostaa hypoteesin petoksesta, jolla voisi selittää havaitut anomaliat.

- **Hypoteesin arviointi**
  - Uhri arvioi muodostamaansa petoksen hypoteesia jotain vapaavalintaista kriteeriä vasten. Tämä kriteeri voisi olla esimerkiksi yleinen elämänkokemus, tai tieto siitä miten joku tietty henkilö yleensä käyttäytyy.

- **Kokonaisuuden arviointi**
  - Uhri muodostaa tästä kaikesta kokonaiskuvan, jonka perusteellä hän kykenee päättelemään, onko kyseessä todellakin petos. Kokonaisuuden arviointiin vaikuttaa kuitenkin huomattavasti yksilön ominaisuudet (Vishwanath ym., 2011). Tällaisia yksilön ominaisuuksia voisivat olla esimerkiksi aikaisemmin hankittu tietotaito, tai ympäröivän kulttuurin vaikutus.

2.2 Tietojenkalastelu

Tässä aliluvussa perehdytään aikaisemman tutkimuksen perusteella siihen, minkälaisia elementtejä tietojenkalasteluviestit yleensä sisältävät. Lisäksi viestejä tulkitaan aikaisemmin tässä kirjallisuuskatsauksessa esiteltyjen käyttäytymisperiaatteiden ja petosteorian näkökulmasta. Tarkastelun kohteena ovat erityisesti sähköpostien lähettäjä, sisältö, sekä linkit ja muut mahdolliset liitetiedostot. Kalasteluviestien yleisten piirteiden käsittely on tutkimuksen kannalta mielekästä, sillä tietojenkalasteluviestinnässä hyökkääjä pyrkii saamaan uhrinsa toimimaan haluamallaan tavalla pelkästään sähköisenviestinnän avulla.

Kuten tässä kirjallisuuskatsauksessa on aikaisemmin mainittu, niin tietojenkalastelun lopullisena tavoitteena on usein, että hyökkääjä saa uhrinsa toimimaan haluamallaan tavalla. Tämä voi esimerkiksi olla tilanne, jossa uhri päätyy antamaan rahaa, tai arkaluonteisia tietoja kuten käyttäjätunnuksia, tai salasanoja hyökkääjälle. (Hadnagy ym., 2015) Hyökkääjät pyrkivät myös usein pääsemään käsiksi yksittäisten henkilöiden, sekä organisaatioiden laitteisiin. Mikäli hyökkääjä saa pääsyn henkilöiden, tai organisaation laitteisiin, hyökkääjä kykenee lähettämään viestejä uhrin kontakteille esiintyen täysin toisena henkilönä (Hadnagy ym., 2015).

Tietojenkalastelulla on monia eri muotoja, joiden suurin ero on niiden käyttämä media. Erilaisia käytettyjä medioita ovat esimerkiksi sähköpostit, puhelut, tekstiviestit, sosiaalinen media, sekä tietojenkalastelua varten luodut internetsivut (Alabdan, 2020). Tämän lisäksi hyökkääjät saattavat käyttää hyökkäyksessään jonkinlaista kombinaatiota eri medioista (Hadnagy ym., 2015, s. 6). Tällaisessa kombinaatio hyökkäyksessä hyökkääjä antaa samaa informaatiota uhrille muutamasta eri kanavasta, pyrkimyksenään herättää luottamusta uhrissa. Kombinaatio hyökkäys voisi olla esimerkiksi sähköpostin lähettäminen ja puhelu, jolloin hyökkääjä saattaa lähettää vaikkapa laskun yrityksen maksuvastaavalle ja tämän jälkeen puhelimessa esiintyä yrityksen korkea-arvoisena johtohahmona pyytäen maksuvastaavaa maksamaan laskun pikaisesti. Tässä tutkimuksessa keskitytään kuitenkin lähinnä kahteen sähköpostilla tapahtuvaan tietojenkalasteluun, jotka ovat geneerinen sähköpostilla tapahtuva tietojenkalastelu (eng. ” phishing”) ja kohdennettu sähköpostilla tapahtuva tietojenkalastelu (eng. ”spear phishing).

Sähköpostien käyttäminen tietojenkalastelussa, on hyökkääjälle helppoa, sillä kuka tahansa voi lähettää sähköposteja kenelle tahansa, eikä niiden lähettäminen maksa mitään. Tämän ominaisuuden vuoksi tietojenkalasteluviestejä voi sähköpostin avulla lähettää hyvin suuria määriä hyvin pienessä ajassa, ilman että siitä syntyy hyökkääjälle merkittäviä kuluja. Kalasteluviestit pyritään yleensä luomaan siten, että uhrille syntyy ensivilkaisulla vaikutelma, että viesti on peräisin luotettavasta lähteestä (Hadnagy ym., 2015). Luotettavan lähteen vaikutelma voidaan luoda esimerkiksi väärentämällä lähettäjä (eng. Email spoofing), jolloin lähettäjä näkyy vastaanottajalle olevan joku muu kuin hyökkääjä. Kalasteluviestien yleisistä piirteistä kerrotaan tarkemmin seuraavassa aliluvussa.

2.3 Tietojenkalasteluviestien yleisiä piirteitä

Tässä aliluvussa käsitellään tietojenkalasteluviesteissä esiintyviä yleisiä piirteitä aikaisemman tutkimuksen perusteella. Yleisten piirteiden käsittelyn lisäksi luvussa käsitellään, sitä miten näiden piirteiden avulla voidaan vaikuttaa viestin vastaanottajaan.

2.3.1 Luonnollinen veruke (eng. Pretexting)

Parhaimmillaan hyökkääjä kykenee luomaan viesteillään uhrille sosiaalisia paineita, niin että koko kanssakäyminen tuntuu uhrista hyvin luonnolliselta (Hadnagy ym., 2015, s. 68). Tällaisen luonnollisen kanssakäymisen tunteen hyökkääjä voi luoda käyttämällä jonkinlaista luonnollista veruketta osana tietojenkalasteluviestiä, jotta tietojenkalasteluviestin sanoma herättäisi uhrissa mahdollisimman vähän epäilyksiä (Goel ym., 2017, s. 28).

Kalasteluviestin onnistumiseen vaikuttaa siis vahvasti se, että viesti on sillä hetkellä ajankohtainen viestin vastaanottajalle. Aikaisemmassa tutkimuksessa, esimerkiksi opiskelijat avasivat huijausviestin todennäköisemmin, kun se lähetettiin heille aikana, jolloin oppilaille muutenkin tiedotettiin heidän saamistaan arvosanoista. (Ferguson, 2005). Yleisesti ottaen hyvän verukkeen käyttäminen osana tietojenkalasteluviestiä voidaan jakaa kahteen elementtiin. Nämä elementit ovat hyökkääjän esittämä persoona ja luonnollinen tilanne, tai ongelma, jonka yhteydessä tämä persoona voi esiintyä (Fruhlinger, 2020, s. 1).

Hyvänä esimerkkinä luonnollisen verukkeen käytöstä voidaan ottaa vaikkapa viimevuonna paljon esillä ollut Helsingin kaupungin palkanmaksuongelmat (Marttinen, 2022). Hyökkääjä voisi tällöin esiintyä Helsingin kaupungin palkanlaskentatehtävissä työskentelevänä henkilönä ja lähestyä Helsingin kaupungin työntekijöitä sillä verukkeella, että heidän tulevan palkkansa laskennassa on ilmennyt ongelmia.

Tällä hyökkäyksellä hyökkääjä voisi saada käsiinsä uhrien henkilökohtaista tietoa, kuten henkilötunnuksia, osoitteita ja mahdollisesti jopa pankkitunnuksia. Jo pelkästään nimen, osoitteen ja henkilötunnuksen päätyminen vääriin käsiin voi tuottaa uhrille merkittävää haittaa, sillä niiden avulla hyökkääjä pystyy tehtailemaan esimerkiksi tilauspetoksia, eli tilaamaan uhrin nimissä tavaraa itselleen (Hämäläinen, 2021).

2.3.2 Viestin lähettäjä

Kalasteluviestin keskeisimpiä elementtejä on viestin lähettäjä. Ihmiset kiinnittävät huomiota viesteissä lähettäjään ja tulkitsevat sen perusteella onko lähetetty viesti tarkoitettu juuri heille (Downs ym., 2006). Mikäli lähettäjä ei ole uhrille merkityksellinen, esimerkiksi tilanteessa, jossa vastaanottajalla ei ole aikaisempaa kanssakäymistä lähettäjän kanssa, ei edellä mainittua luonnollista veruketta kanssakäymiseen synny. Aikaisemmissa tutkimuksissa on myös todettu, että mikäli lähettäjä on vastaanottajalle aikaisemmin tuttu, tai auktorisessa asemassa

oleva henkilö, viesti avataan ja siihen reagoidaan todennäköisemmin (Ferguson, 2005). Esimerkiksi (Ferguson, 2005) tuottamassa tutkimuksessa sotilasmaailmassa opiskelevat kadetit avasivat tietojenkalasteluviestin, joka oli lähetetty korkea-arvoisemmassa asemassa olevalta sotilaalta, vaikka he huomasivat sen olevan epäilyttävä. Tämä kadettien toiminta selittyykin sillä, että sotilaskoulutuksessa vallitsevassa kulttuurissa, ylempiarvoisien esihenkilöiden käskyjä täytyy totella kyselemättä. Tämän lisäksi toimintaa vahvistaa jo aikaisemmin tässä kirjallisuuskatsauksessa mainittu ihmisten luontainen haluttomuus tarkastaa auktorisessa asemassa olevan lähettäjän todenmukaisuutta (Gragg, 2003).

Viestin lähettäjän tärkeyden vuoksi, hyökkääjät pyrkivätkin esiintymään luotettavina osapuolina. Luotettavana osapuolena näyttäminen voidaan saavuttaa esimerkiksi väärentämällä viestin lähettäjä. (Hadnagy ym., 2015). Viestin lähettäjä voidaan väärentää luomalla hyvin samankaltainen nimi, kuin oikealla lähettäjällä olisi. Lähettäjän nimestä voidaan korvata kirjaimia toisilla kirjaimilla, jotka näyttävät lähes identtisiltä. Tällaisia vaihdoksia ovat esimerkiksi pienen L kirjaimen (l) korvaaminen isolla i kirjaimelle (I). Väärentämisen onnistumisen mahdollisuutta hyökkääjät voivat parantaa, esimerkiksi tutkimalla kohdeorganisaation käyttämiä palveluita ja niiden palveluntarjoajia (Hadnagy ym., 2015, s. 103). Esiintymällä kohdeorganisaation käyttämänä palvelun tarjoajana, hyökkääjä todennäköisesti vaikuttaa huomattavasti luotettavammalta. Etenkin, jos viesti kohdistetaan henkilöille, jotka todennäköisemmin olisivat muutenkin tekemisissä kyseisen palveluntarjoajan kanssa. Tällöin hyökkääjä voi viesteissään omaksua palvelun tarjoajan roolin, jolloin kanssakäymiseen syntyy luonnollinen veruke. Lisäksi, koska tällöin kyseessä on uhrin näkökulmasta kahden yrityksen työntekijöiden välinen kanssakäyminen, on uhrilla suurempi todennäköisyys toimia sosiaalisten normien mukaisesti, jolloin hyökkääjä saa validoitua itsensä sosiaalisesti.

2.3.3 Viestin sisältö

Lähettäjän lisäksi myös viestin sisältö on keskeisessä asemassa etenkin kohdistettujen tietojenkalasteluviestien onnistumisessa. Etenkin perinteisempien viestien sisällössä viestin otsikko pyritään luomaan mahdollisimman huomiota herättäväksi, jotta uhrin kiinnostus viestiä kohtaan olisi mahdollisimman voimakasta. Tämän lisäksi tietojenkalasteluviestin tekstin sisältöön hyökkääjät saattavat pyrkiä sisällyttämään kiireen tunnetta, jotta viestin lukija ei pysähtyisi miettimään viestin kokonaissanomaa liian tarkasti. (Vishwanath ym., 2011)

Viestin sisältöä tarkastellessa tietojenkalasteluviestit ja kohdennetut tietojenkalasteluviestit eroavat etenkin viestin aloituksessa. Perinteisemmät tietojenkalasteluviestit pyrkivät olemaan hyvin neutraaleja viestin aloituksessa, jotta viesti olisi mahdollisimman luonnollinen mahdollisimman monelle. Tällöin viesti saattaa alkaa esimerkiksi sanoilla: *"Hyvä asiakkaamme…"*. Kohdennettu tietojenkalasteluviesti saattaisi sen sijaan alkaa sanoilla: *"Hei Justus"*. Tällöin viesti tuntuu vastaanottajalta heti huomattavasti henkilökohtaisemmalta, sillä viesti on osoitettu juuri hänelle. Aikaisemmissa tutkimuksissa on havaittu, että mikäli

tietojenkalastelu viesti alkaa henkilökohtaisella aloituksella, nostaa se todennäköisyyttä, että uhri syöttää pyydettyjä tietoja hyökkääjälle (Bullee ym., 2017).

Kalasteluviestiin saatetaan myös sisällyttää linkki, joka johtaa hyökkääjän luomalle väärennetylle sivustolle (Hong, 2012, s. 76). Väärennetty sivusto voi näyttää esimerkiksi jonkinlaiselta palveluun kirjautumiseen käytettävältä sivustolta. Väärennettyjen sivujen etuna hyökkääjälle on se, että niiden avulla voidaan kerätä kirjautumistietoja, ilman suurempaa kanssakäymistä alkuperäisen vastaanottajan kanssa. Edistyneemmissä tietojenkalasteluviesteissä, joissa hyökkääjä esiintyy jonkin palvelun tarjoajana, saattaa olla esillä useampia linkkejä, joista suurin osa vie käyttäjän palvelun oikeille sivuille ja viestin päälinkki vie vastaanottajan väärennetylle tietojenkalastelusivulle (Hadnagy ym., 2015, s. 115-116). Tarjoamalla linkkejä, jotka vievät käyttäjän palvelun oikeille sivuille, hyökkääjän viesti vaikuttaa todennäköisemmin huomattavasti luotettavammalta.

Jotta ihmiset avaisivat linkin, hyökkääjät saattavat yrittää naamioida sen ulkoasua niin, että se vaikuttaisi luotettavammalta. Linkkiä voidaan yrittää naamioida esimerkiksi upottamalla se osaksi viestin tekstiä, esimerkiksi tähän tapaan. Toinen tapa, jolla linkin voi naamioida upottamalla on kirjoittaa tekstillä eri osoite, kuin mihin hyperlinkki johtaa. Hyökkääjä voi esimerkiksi kirjoittaa ”www.bing.com”, mutta asettaa tekstin hyperlinkiksi jotain aivan muuta, esimerkiksi tähän tapaan www.bing.com. Tällöin käyttäjä ei välttämättä huomaa linkin todellisen osoitteen olevan väärennetty. Hyökkääjät saattavat myös rekisteröidä oman verkko-osoitteen, joka pyrkii imitoimaan alkuperäisen palvelun osoitetta mahdollisimman tarkasti. Kuten esimerkiksi voidaan nähdä kuviosta 2, jossa tietojenkalasteluviestin osoitteessa on teksti ”pop-pankkioy.com”, kun taas oikean POP pankin verkkosivuosoite on ”poppankki.fi".

Kalasteluviestiin voi olla myös sisällytettynä jonkinlainen haitallinen liitetiedosto (Hadnagy ym., 2015, s. 2). Liite saattaa näyttää ensisilmäyksellä harmittomalta, mutta todellisuudessa se sisältääkin haittaohjelman, jonka avulla hyökkääjä saa asennettua esimerkiksi takaportin uhrinsa tietokoneelle. Esimerkiksi RSA:han kohdistunut tietojenkalastelukampanja käytti hyväkseen sähköpostissa liitteenä ollutta haitallista Excel tiedostoa (Hadnagy ym., 2015, s. 8; Hyppönen, 2011). Tämä haitallinen Excel tiedosto sisälsi nollapäivä haavoittuvuuden, jonka avulla hyökkääjät kykenivät asentamaan takaportin RSA:n järjestelmiin (Hyppönen, 2011). RSA:han kohdistettua tietojenkalasteluviestiä tarkastellaan tarkemmin seuraavassa luvussa.

2.4 Kalasteluviestien jaottelua

Kuten tutkielmassa on aikaisemmin mainittu, tietojenkalasteluun perustuvia hyökkäyksiä on monia erilaisia, mutta tässä tutkimuksessa keskitytään lähinnä tutkimaan sähköposteilla tapahtuvaa tietojenkalastelua. Vaikka tutkimus rajoitetaankin sähköpostilla tapahtuvaan tietojenkalasteluun ja kohdennettuun tietojenkalasteluun, voidaan näiden kahden pääkategorian sisällä viestejä jakaa eri

tavoilla sen perusteella mihin viestit pyrkivät vaikuttamaan, sekä miten tämänkaltaiseen vaikutukseen pyritään.

Viestien vaikutuksen muotojen mukaan, viestit voidaan jakaa esimerkiksi kahteen kategoriaan sen perusteella, pyrkiikö viesti positiiviseen, vai negatiiviseen viestintään. (Ebot & Claude, 2017, s. 17) (Goel ym., 2017, s. 28) Positiivisella viestinnällä tarkoitetaan tässä sellaisia tietojenkalasteluviestejä, jotka pyrkivät tuottamaan vastaanottajalleen onnen tunnetta, esimerkiksi lupaamalla heille jotain merkittävää hyötyä. Negatiivisella viestinnällä taas tarkoitetaan sellaista viestintää, jolla vastaanottajalle pyritään tuottamaan negatiivisia tunteita, kuten pelkoa. Näille kahdelle jaottelulle on yhteistä se, että näistä molemmat pyrkivät herättämään äärimmäisiä tunteita viestin vastaanottajassa ja niiden avulla harhauttamaan viestin vastaanottajaa, kuten on kuvattu osana luvun 2.1.1 käyttäytymisilmiöitä. Tällä harhautuksella hyökkääjä pyrkii estämään luvussa 2.1.2 esitellyn petosteorian aktivointi vaiheen kokonaan, jolloin uhri ei havaitse esillä olevassa informaatiossa olevia anomalioita, eikä tällöin myöskään jatka mahdollisen petoksen prosessointia.

Viestien jaottelu sen mukaan miten ne pyrkivät vaikuttamaan uhreihinsa voidaan tehdä esimerkiksi jakamalla viestit tasoihin sen perusteella kuinka kehittyneitä ne ovat ja kuinka vaikeita ne on tunnistaa tietojenkalasteluviesteiksi (Hadnagy ym., 2015, s. 110). Tässä tutkimuksessa tullaan ensisijaisesti hyödyntämään jaottelua sen mukaan, miten viestit pyrkivät vaikuttamaan uhreihinsa, sillä se tarjoaa mielekkäämmän asetelman erilaisten tietojenkalasteluviestien erottelulle. Käytettäviä tietojenkalasteluviestejä tullaan myös käsittelemään sen perusteella pyrkivätkö ne vaikuttamaan uhriin myönteisellä, vai kielteisellä viestinnällä, vaikka niitä ei tulla suoraan jakamaan niiden perusteella eri kategorioihin.

Ensimmäisen ja huonoimman tason muodostavat ns. ”nigerialaiskirjeet”, joiden ulkomuodosta ja sananvalinnoista monien vastaanottajien ainakin pitäisi tunnistaa viesti tietojenkalasteluviestiksi (Hadnagy ym., 2015, s. 110). Nämä tietojenkalasteluviestit tulevat yleensä lähettäjiltä, joiden kanssa vastaanottajalla ei ole aikaisempaa kanssakäymistä, jolloin luonnollista veruketta kanssakäymiseen ei synny. Ensimmäisen tason tietojenkalasteluviestit ovat yleensä kielellisesti heikkoja ja niissä saattaa kielen lisäksi esiintyä muita outoja epäloogisuuksia. Tämän tason tietojenkalasteluviestit pyrkivätkin usein peittelemään näitä heikkouksia, esimerkiksi herättämällä vastaanottajassa joitain äärimmäisiä tunteita, kuten pelkoa (Hadnagy ym., 2015, s. 110–112), esimerkiksi maineen tai omaisuuden menetyksellä, tai ahneutta (Ferreira ym., 2015), esimerkiksi omaisuuden saamisen mahdollisuudella.

POLIISI
KAAKKOIS-SUOMI

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

SUOMI

HAASTE TUOMIOISTUIMEEN

Oikeudellista tutkintaa varten
(rikosprosessilain 390-1 §).)

Olen kenraali Seppo Kolehmainen, kansallisen poliisin pääjohtaja ja alaikäisten suojeluyksikön päällikkö.
Otan teihin yhteyttä pian sen jälkeen, kun teihin on
takavarikoitu tietoverkkoon tunkeutuminen (erityisesti lapsipornografian, pornografisten sivustojen ja nettipornografian alalla), ilmoittaakseni teille, että olette useiden oikeudenkäyntien kohteena:

- PORNOGRAFINEN SIVUSTO
- KYBERPORNOGRAFIA
- PEDOFILIA
- EKSHIBITIONISMI

Tiedoksenne, että maaliskuussa 2007 annetussa rikosprosessilain 390-1:ssä kovennetaan rangaistuksia, kun pahoinpitelyt, seksuaalinen väkivalta tai raiskaukset tehdään internetin välityksellä.

Pyydämme teitä ystävällisesti ilmoittamaan mielipiteenne sähköpostitse osoitteeseen sjk.poliisihallituksen@collaborative.li kirjoittamalla meille perustelunne, jotta ne voidaan tutkia ja tarkistaa seuraamusten varalta; tämä tapahtuu tiukan 48 tunnin määräajan kuluessa. Tämän määräajan jälkeen olemme velvollisia toimittamaan raporttimme Helsingin kaupungin tuomioistuimen apulaisvaltakunnansyyttäjälle ja tietokonerikoksiin erikoistuneelle syyttäjälle la, joka laatii teistä pidätysmääräyksen, toimittaa sen asuinpaikkakuntaanne lähimpänä olevalle poliisilaitoksen

Kenraali Seppo Kolehmainen
Kansallisen poliisin pääjohtaja ja nuorten suojeluyksikön päällikkö.

Kenraali Seppo Kolehmainen
Kansallisen poliisin pääjohtaja ja nuorten suojeluyksikön päällikkö.

Europol is the intergovernmental body that facilitates, within the European Union, the exchange of information between national police forces in the areas of drugs, terrorism, international crime and pedophilia. Operational since 1999, Europol is since 2010 a European agency, financed by the Community budget and therefore controlled by the European Parliament.

KUVIO 1 Ensimmäisen tason tietojenkalasteluviesti (Nieminen, 2022)

Yllä oleva esimerkkikuva ensimmäisen tason tietojenkalasteluviestistä on tarkemmin tarkasteltuna monella tapaa kömpelö ja ”viralliseksi” dokumentiksi se olisi hyvin epätavallinen. Kuvasta helpoiten löydettävät epäloogisuudet ovat:

- Suomessa ”pornografinen sivusto” ja ”kyberpornografia” eivät ole rikoksia.
- Suomen poliisin pääjohtaja ei ole kenraali.
- Kuvassa näkyvässä tietojenkalasteluviestissä on pyritty lisäämään todentuntuisuutta käyttämällä viranomaisten logoja, mutta mukana on jostain syystä myös jalkapalloliiton logo.
- Kyseessä on haaste tuomioistuimeen, mutta vastaanottajan nimeä ei mainita missään.
- Kalasteluviestin kieli on selkeästi käännetty jonkinlaisella käännöskoneella, jonka takia se on hyvin kangertelevaa.

Tässä esimerkissä tietojenkalasteluviesti yrittää peittää siitä löytyviä epäloogisuuksia, juuri pelon avulla. Kalasteluviesti antaa ymmärtää, että korkea arvoinen

virkamies, tässä tapauksessa kenraali, lähettää sinulle haasteen tuomioistuimeen, jossa syytteinä esitetään asioita, jotka synnyttävät vastaanottajassa pelon tunteita.

Vaikka ensimmäisen tason tietojenkalasteluviestit ovat tekniseltä toteutukseltaan muita tasoja huomattavasti heikompia, niin niidenkin tarkoitus on tuottaa hyökkääjille rahallista tuottoa. Ensimmäisen tason tietojenkalasteluviestit kääntävätkin yksinkertaisuutensa ja viestien tekniset heikkoudet puolelleen. Kuten luvussa 2.2 on mainittu, viestien lähettäminen ei itsessään vaadi hyökkääjältä merkittävää vaivaa tai rahallista panostusta. Vasta alkuperäisen viestin jälkeinen kanssakäyminen edellyttää hyökkääjän henkilökohtaista panostusta, jonka vuoksi on hyökkääjälle huomattava etu karsia ne ihmiset jotka todennäköisesti eivät lankea huijauksen uhriksi (Herley, 2012, s. 11). Tällöin on hyökkääjälle kannattavaa luoda alkuperäisen viestinsä sisältö siten, että viesti itsessään karsii kaikki muut, paitsi kaikkein hyväuskoisimmat henkilöt.

Toisen tason tietojenkalasteluviestit ovat yleisesti jo hieman edistyneempiä, kuin ensimmäisen tason tietojenkalasteluviestit. Vaikka näissäkin viesteissä on käytännössä paljon samoja virheitä ja epäloogisuuksia, kuin ensimmäisentason viesteissä, niin toisen tason tietojenkalasteluviestit pyrkivät jo esiintymään jonain yrityksenä tai entiteettinä. (Hadnagy ym., 2015, s. 112–114)

KUVIO 2 Toisen tason tietojenkalasteluviesti (Uurtimo, 2022)

Kuten yllä olevasta esimerkkikuvasta voidaan havainnoida, niin tässä toisen tason tietojenkalasteluviestissä, hyökkääjä yrittää jo esiintyä virallisena tahona, joka tässä tapauksessa on pankki. Kuitenkin viestistä on nopeasti havaittavissa, että teksti on jokseenkin kömpelöä.

Esimerkiksi viestin kohdasta

> ”Jos tämä ei ole sinun suorittama toimenpide käy hätäisesti osoitteessa…”

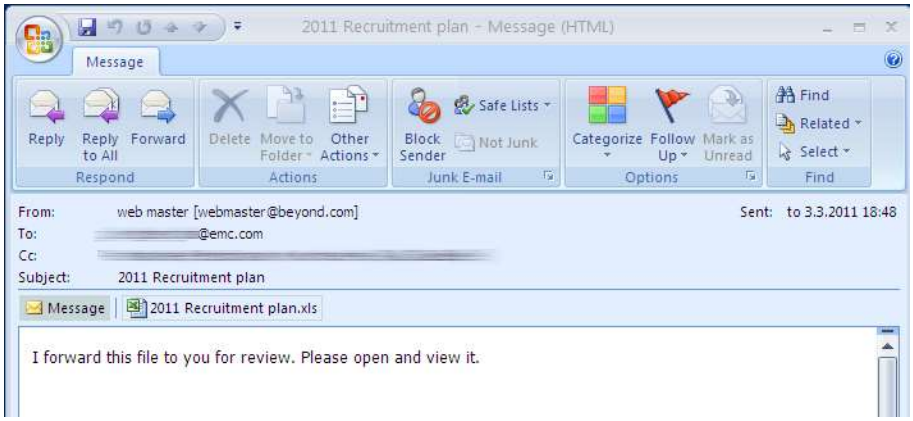
voidaan huomata, että teksti on hyvin todennäköisesti kone käännetty toisesta kielestä suomeksi, sillä se sisältää sanavalintoja, kuten ”suorittama toimenpide”, ja ”hätäisesti”, jotka ovat sanavalintoja, joita oikea pankki tuskin käyttäisi.

Tämän lisäksi, viestissä ei ole vastaanottajan nimeä ja viestissä on outo linkki. Vaikka linkissä onkin HTTPS protokolla käytössä ja ylätason verkkotunnuksena ”.com”, joka on kalliimpi rekisteröidä, kuin vaikkapa ”.info”. Kuitenkin suomalaisissa pankeissa on yleensä käytössä Suomen maakoodi ".fi”. Tämän tietojenkalasteluviestin kömpelyyttä lisää se, että minulla ei ole mitään asiakkuutta POP pankkiin, jolloin luonnollista veruketta kanssakäymiseen ei edes voisi syntyä.

Kolmannen tason tietojenkalasteluviestit ovat jo huomattavasti edistyneempiä aikaisempiin tasoihin verrattuna. Näissä viesteissä hyökkääjä pyrkii jo imitoimaan tarkasti yrityksen viestintää. Tähän imitointiin kuuluu vastaanottajan nimen mainitseminen tervehdyksessä, viestit saattavat imitoida jotain brändiä ja käyttää tämän brändin logoja hyväkseen viesteissä ja tietojenkalasteluviestin teksti on lähtökohtaisesti kieliopillisesti oikein. (Hadnagy ym., 2015, s. 114–117)

Neljännen tason tietojenkalasteluviestit ovat käytännössä täysin kohdennettua tietojenkalastelua. Ennen näiden viestien luontia, hyökkääjät saattavat hyödyntää avointen lähteiden tiedustelua (eng. ”OSINT”), määritellessään kuinka uhria kannattaa sähköpostilla lähestyä (Hadnagy ym., 2015, s. 118). Tällöin viesteihin voidaan sisällyttää teemoja, jotka ovat vastaanottajalle hyvin ajankohtaisia ja merkityksellisiä (Hadnagy ym., 2015, s. 117–119). Neljännen tason viestit eivät yleisesti sisällä kieliopillisesti kankeaa kielenkäyttöä, eikä muitakaan epäloogisuuksia, joita voidaan havaita ensimmäisen ja toisen tason tietojenkalasteluviesteistä.

Hyvänä esimerkkinä neljännen tason tietojenkalasteluviestistä voidaan käyttää viestiä, jonka avulla hyökkääjät onnistuivat käyttämään nollapäivähaavoittuvuutta (eng. ”zero-day vulnerability) tietoturvayhtiö RSA:han. Nollapäivä haavoittuvuus tarkoittaa haavoittuvuutta, johon järjestelmän kehittäjällä on nolla päivää aikaa tehdä päivitys. Toisin sanoen se on haavoittuvuus, jonka olemassaolo havaitaan ensimmäisen kerran silloin, kun sitä hyödynnetään järjestelmää vastaan. On huomioitava, että RSA ei ole julkaissut tietojenkalasteluviestin sisältöä, mutta tietoturvatutkijat ovat löytäneet Virustotal- palveluun ladatun viestin, joka hyvin todennäköisesti on hyökkäyksessä käytetty tietojenkalasteluviesti (Hyppönen, 2011).



KUVIO 3 Todennäköinen viesti, jonka avulla hyökkääjät onnistuivat saamaan nollapäivähaavoittuvuuden RSA:n työntekijän koneelle. (Hyppönen, 2011)

Kuvassa näkyvä tietojenkalasteluviesti on ensisilmäykseltä hyvin yksinkertainen. Viestissä ei ole henkilökohtaista tervehdystä, oikeastaan siinä ei ole tervehdystä lainkaan. Viestissä ei myöskään ole minkäänlaista allekirjoitusta lähettäjältä, ainoastaan Excel tiedosto ja pyyntö arvioida sen sisältämä ”rekrytointi suunnitelma”. Ulkoasultaan viestin voisi arvioida olevan maksimissaan toisen tason tietojenkalasteluviesti. Kalasteluviesti oli kuitenkin kohdennettu tarkkaan RSA:n henkilöstöhallintoon, joiden yhteystiedot hyökkääjä oli löytänyt LinkedIn:stä (Parmar, 2012 s. 9).

Hyökkääjä oli siis käyttänyt avointen lähteiden tiedustelua, valmistellessaan hyökkäystä RSA:han. Hyökkäyksen onnistuminen riippuikin huomattavasti, juuri tästä etukäteen tehdystä tiedustelusta. Kalasteluviestin vastaanottajat olivat kaikki henkilöstöhallinon työntekijöitä, jotka varmasti saavat rekrytointiin liittyviä viestejä päivittäin. Tämän vuoksi viesti onnistui luomaan luonnollisen tekosyyn kanssakäymiseen, joka johti siihen, että työntekijä päätyi avaamaan saastuneen liitetiedoston.

3 TUTKIMUSMETODOLOGIA

Tässä pro-gradu työssä käytetty tutkimusmenetelmä on kenttäkoe, jota täydennetään kahden otoksen suhteiden testillä suoritettavalla data-analyysillä, sekä haastatteluilla. Tutkimuksen aineisto koostuu kahdesta tietojenkalasteluaallosta, sekä niiden jälkeen suoritetuista haastatteluista. Tietojenkalasteluaallot suoritettiin osana kohdeorganisaatioon tehtävää tietojenkalastelusimulaatiota. Tietojenkalasteluaaltojen, sekä haastatteluiden avulla voitiin saada sekä laadullista, että määrällistä dataa siitä miten henkilöt reagoivat saatuaan tietojenkalasteluviestin.

3.1 Tietojenkalastelukampanja

Osana tutkimusta suoritettiin, tutkielman kirjoittajan työnantajan avustuksella, tietojenkalastelukampanja kohdeorganisaatioon, jossa organisaatioon lähetetään erilaisia tietojenkalasteluviestejä. Tässä aliluvussa tullaan esittelemään tietojenkalastelukampanja, sekä tietojenkalastelussa käytettyjä viestejä. Tämän lisäksi aliluvussa tullaan käsittelemään kampanjassa käytettyjä tietojenkalasteluviestejä aikaisemmin tutkimuksessa esitetyn teorian valossa.

3.1.1 Tietojenkalastelukampanjan kuvaus

Tämän pro-gradu tutkielman datan keräystä varten suoritetaan simuloitu tietojenkalastelukampanja tutkielman kirjoittajan työnantajan avustuksella kohdeorganisaatioon. Tietojenkalastelukampanjan kohdeorganisaatio on suomalainen IT-palvelutalo. Kampanjassa on tarkoitus lähettää kohdeorganisaatioon, kirjoittajan työnantajan avustuksella, erilaisia tietojenkalasteluviestejä. Kohdeorganisaation henkilöstöhallinto, sekä kohdeorganisaation tietoturvasta vastaava taho oli tietoinen tulevista tietojenkalasteluviesteistä, mutta muille organisaation työntekijöille simulaatiosta ei informoitu etukäteen.

Vaikka tarkoituksena on simuloida oikeaa kohdeorganisaatioon kohdistettua tietojenkalastelukampanjaa, niin viestit pyritään kuitenkin luomaan siten, että niistä ei ole merkittävää haittaa työntekijöille ja ne ovat hyvän maun

mukaisia. Merkittävän haitan välttäminen tarkoittaa esimerkiksi sitä, että tietojenkalasteluviesteissä ei tulla käyttämään LinkedIn:iä imitoivia viestejä, sillä etenkin keväällä monissa yrityksissä aloittaa paljon uusia työntekijöitä, eikä tämän tutkimuksen tarkoituksena ole pilata heidän verkostoitumismahdollisuuksiaan. Hyvän maun mukaiset tietojenkalasteluviestit tarkoittavat sitä, että viesteihin ei tulla sisällyttämään harhaanjohtavia terveystietoja, kuten väärää tietoa ihmisten sairauksista, tai harhaanjohtavaa tietoa, jonkun läheisen kuolemasta. Lisäksi tietojenkalasteluviesteistä ei tulla tekemään sellaisia, johon vastaanottaja saattaisi syöttää omia terveystietojaan, tai muita työhön liittymätöntä sensitiivistä dataa, kuten henkilötunnuksia.

Todenmukaisimmassa tietojenkalastelusimulaatiossa pyrittäisiin seuraamaan täysin mahdollisen hyökkääjän hyödyntämiä taktiikoita, kuten avointen lähteiden tiedustelua (eng. Open-Source-Intelligence) uhrien etsimisessä, tai mahdollisten hyödynnettävien tietojen hakemisessa. Tässä tutkimuksessa tietojenkalasteluviestejä kohdistetaan kohdeorganisaation työntekijöihin riippumatta siitä, kuinka paljon heistä on esillä tietoa avoimissa lähteissä. Tämä johtuu siitä, että tutkimuksen tarkoituksena on tutkia miten ihmiset yleisesti reagoivat saamiinsa tietojenkalasteluviesteihin ja tällöin vastaanottajien rajaaminen sen mukaan, kuinka paljon heistä on saatavilla tietoa verkossa, saattaisi rajata liikaa tiettyjen työtehtävien henkilöitä pois.

Tietojenkalasteluviestit luotiin niin, että osa viesteistä on ensimmäisen ja toisen tason välimaastossa olevia tietojenkalasteluviestejä ja osa on kolmannen ja neljännen tason välimaastossa olevia tietojenkalasteluviestejä. Tietojenkalasteluviestien tasoista on kerrottu tarkemmin luvussa 2.2.3. Tietojenkalasteluviestit lähetettiin kahdessa eri aallossa, niin että kummassakin aallossa lähetettiin geneerinen tietojenkalasteluviesti puolelle henkilöstöstä ja kohdennettu tietojenkalasteluviesti toiselle puolelle henkilöstöstä. Aallot tullaan muodostamaan siten, että saman liiketoiminta-alueen sisällä kaikki henkilöt eivät saa samaa tietojenkalasteluviestiä viestiä samaan aikaan. Tietojenkalasteluviestien aallot ajoitettiin muutamalle eri kuukaudelle, jolloin aaltojen väliin jäi noin kuukausi aikaa. Tällöin ihmiset todennäköisesti ehtivät unohtaa mahdolliset kahvipöytäkeskustelut muiden saamista tietojenkalasteluviesteistä, joten heillä ei todennäköisesti ole kovin tarkkaa muistikuvaa toisen joukon saamasta viestistä silloin kuin he saavat sen itse.

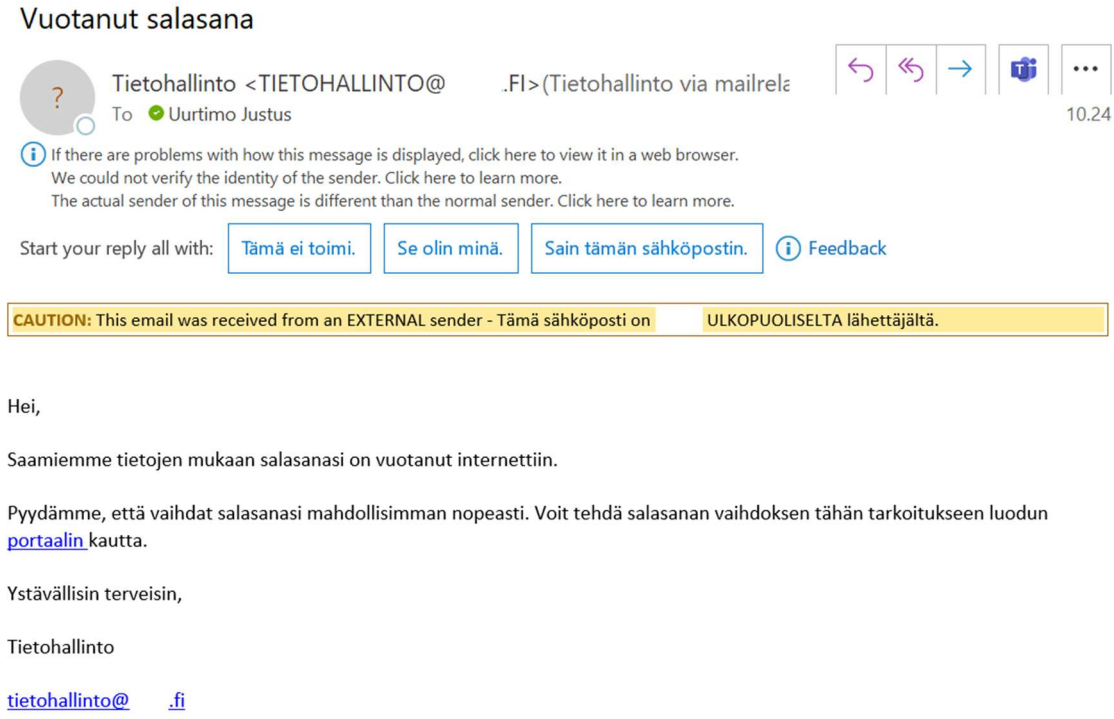
Kalasteluviestien lisäksi kampanjassa hyödynnettiin laskeutumissivuja osana tietojenkalastelua. Tämä tarkoittaa sitä, että henkilön avatessa tietojenkalasteluviestin linkin hän ohjautuu linkkiä varten luodulle laskeutumissivustolle, jossa häntä pyydetään kirjautumaan sisään, tai vaihtamaan salasanansa, riippuen siitä kumman tietojenkalasteluviestin vastaanottaja kulloinkin saa. Kirjautumissivusto ei kuitenkaan luonnollisesti toimi, vaan lomakkeen lähetyksen jälkeen se vain aukeaa uudestaan. Laskeutumissivun funktiona on pitää kirjaa siitä, kuinka moni linkin avannut päätyy syöttämään sensitiivistä dataansa sivustolle. Laskeutumissivustot räätälöitiin siten, että ne vastaavat sekä viestin sanomaa, sekä sen vaikeusastetta. Toisin sanoen geneerisen viestin laskeutumissivusto

sisälsi hieman enemmän vihjeitä mahdollisesta tietojenkalastelusta, kuin kohdennetumman viestin laskeutumissivusto.

3.1.2 Tietojenkalastelukampanjassa käytettävät viestit ja laskeutumissivustot

Tässä simuloidussa tietojenkalastelukampanjassa käytetyt viestit olivat molemmat kirjoitettu hyvällä suomen kielellä. Molemmissa viesteissä päädyttiin käyttämään hyvää suomen kieltä, koska erilaiset käännöskoneet ovat parantuneet huomattavasti viimevuosina. Tämän lisäksi esimerkiksi erilaisilla tekoälyillä, kuten OpenAI:n kehittämä ChatGPT:llä voidaan tuottaa todella hyviä suomenkielisiä viestejä, ilman että alkuperäinen kirjoittaja puhuisi äidinkielenään suomea. Näiden lisäksi tietojenkalastelijat voivat olla myös suomalaisia, jolloin ei voida tuudittautua oletukseen, että tietojenkalasteluviestit pystyttäisiin tunnistamaan pelkän heikon kieliasun perusteella.

Ensimmäinen käytetyistä viesteistä oli hyvin geneerinen, eli sitä ei ollut varsinaisesti kohdistettu kenellekään.



KUVIO 4 Simulaatiossa käytetty geneerinen tietojenkalasteluviesti

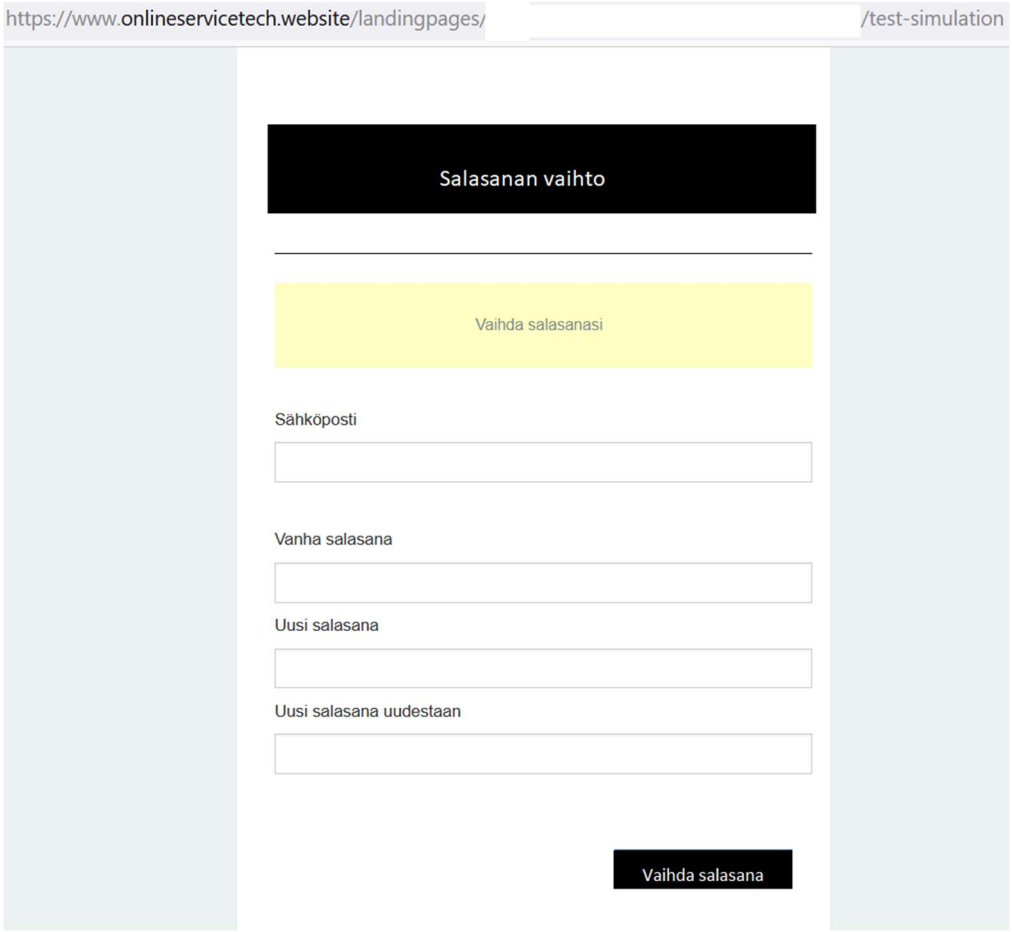
Tietojenkalastelusimulaatiossa käytetty geneerinen viesti on tason 2 tietojenkalasteluviesti. Viesti ei varsinaisesti pyri imitoimaan organisaation viestintää, muuten kuin hyödyntämällä organisaation nimeä lähettäjän osoitteessa. Viesti

on kirjoitettu kohdeorganisaation maan äidinkielellä pyrkimyksenä vähentää viestistä aiheutuvia ennakkoluuloja.
Viestissä on kuitenkin useita vihjeitä, joiden avulla viestin vastaanottaja saattaa havahtua siihen, että kyseessä on tietojenkalasteluviesti.

1. Viestiä ei ole osoitettu kenellekään.
2. Viestissä ei kerrota mikä salasana on vuotanut.
3. Mistä organisaation tietohallinto voisi tietää, että juuri sinun salasanasi on vuotanut internettiin.
4. Viestin sisältämä palautuslinkki on upotettu tekstiin, jotta se ei herättäisi huomiota.
5. Viesti väittää tulevansa organisaation tietohallinnolta, mutta organisaation käytössä oleva sähköpostijärjestelmä ilmoittaa sen tulevan ulkopuoliselta lähettäjältä.
6. Viestin lähettäjän osa, joka ei tietoturvasyistä näy kuvissa, oli kirjoitettu siten että yksi iso ”i” -kirjain oli korvattu pienellä ”l”- kirjaimella.
7. Organisaation käytössä oleva sähköpostijärjestelmä ilmoittaa viestin lähettäjän olevan eri kuin normaalisti
8. Organisaation käyttämä sähköpostijärjestelmä ilmoittaa, että viestin lähettäjää ei pystytty varmentamaan.

Tämä tietojenkalasteluviesti pyrkii vaikuttamaan vastaanottajaansa muutamalla eri tavalla. Viestin lähettäjä vaikuttaa olevan yrityksen tietohallinto, jota voidaan pitää auktorisessa asemassa olevana tahona, etenkin kun puhutaan tietoturvallisuuteen liittyvistä asioista. Kuten aikaisemmin tässä tutkimuksessa on mainittu, niin ihmisillä on luontainen taipumus totella auktorisessa asemassa olevia henkilöitä (Gragg, 2003). Viestin avulla pyritään lisäksi herättämään pelon tunnetta vastaanottajassa, ilmoittamalla mahdollisesta salasanan vuotamisesta internettiin. Pelon tunnetta pyritään viestissä lisäämään viestin sisältämän kiireellisyyden avulla, jossa vastaanottajaa pyritään hoputtamaan viestin linkin avaamiseen. Pelko on äärimmäinen tunne ihmisessä ja sitä voidaan käyttää luvun 2.1.1 mukaisesti harhautuksena, jotta viestin vastaanottajassa ei heräisi petosteorian mukaista petoksen huomaamisen aktivointia.

Geneerisen viestin linkki ohjasi käyttäjän geneerisen viestin laskeutumissivustolle, jossa käyttäjää pyydettiin vaihtamaan salasanansa.



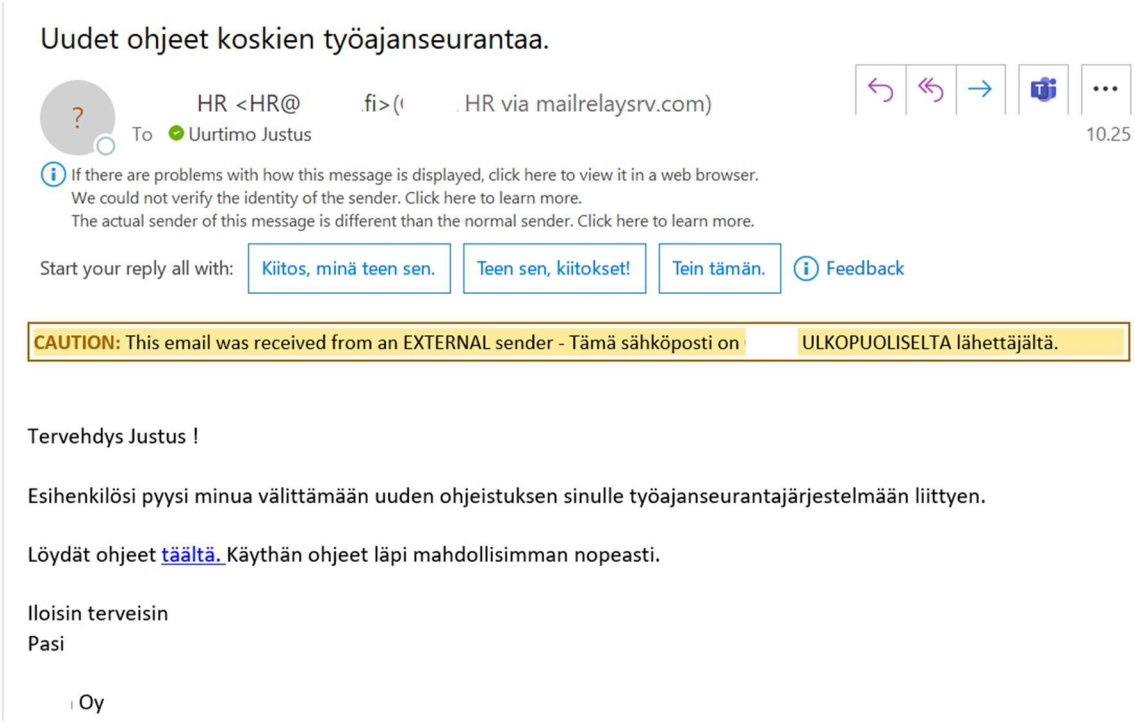
KUVIO 5 Geneerisen viestin laskeutumissivuston näkymä tietokoneella

Geneerisen sivuston laskeutumissivu sisälsi ainoastaan lomakkeen, jossa viestin vastaanottajaa pyydetään antamaan sähköpostinsa, vanha salasanansa, sekä uusi salasana. Laskeutumissivusto ei itsessään vastaa mitään organisaation olemassa olevaa sivua, tai lomaketta. Geneerisen laskeutumissivun lomakkeelle sijoitettiin organisaation logo ja otsikon taustan väriksi asetettiin organisaation väriteeman mukaiseksi (kuvassa logo poistettu ja väri muutettu mustaksi tietoturvallisuussyistä). Geneerisen tietojenkalasteluviestin mukaisesti, myös laskeutumissivusto kirjoitettiin suomeksi. Vaikka laskeutumissivusto vaikuttaa ensinäkemältä suhteellisen oikealta, niin sekin sisältää elementtejä, joiden myötä viestin vastaanottajan pitäisi huomata olevansa väärennetyllä sivulla.

1. Laskeutumissivustolla pyydetään syöttämään vastaanottajan ”vanha” salasana, eli siis nykyinen, jonka antamiseen ei pitäisi olla mitään syytä.
2. Laskeutumissivustolla pyydetään antamaan sähköpostiosoite, vaikkei sille pitäisi olla mitään syytä.

3. Laskeutumissivuston URL: osoite ei ole organisaation käyttämä URL, vaan täysin tekaistu URL, joka ei vastaa organisaation osoitteita millään lailla.

Toinen viesteistä taas oli selkeästi kohdistettu vastaanottajille käyttämällä luontaisena tekosyynä työnajanseurantajärjestelmän uusia ohjeita.



KUVIO 6 Simulaatiossa käytetty kohdennettu tietojenkalasteluviesti

Tässä tietojenkalastelusimulaatiossa käytetty kohdennettu tietojenkalasteluviesti oli tasojen 3 ja 4 välillä oleva tietojenkalasteluviesti. Viestin sävy on itsessään hyvin neutraali ja sen sisältämät sananvalinnat korostavat sitä, että viesti on kirjoitettu omalla äidinkielellä. Näistä sananvalinnoista esimerkiksi *"Esihenkilösi"* käyttäminen kielii siitä, että viestin kirjoittaja on hyvin perillä Suomessa käytävistä yhteiskunnallisista keskusteluista, joissa on pyritty lisäämään sukupuolineutraalien sananmuotojen käyttämistä tehtävänimikkeissä.

Tietojenkalasteluviestin kieli on muotoiltu hyvin rennoksi käyttämällä sananvalintoja kuten: *"Tervehdys"* ja *"Iloisin terveisin"*. Viestissä vastaanottajaa puhutellaan etunimeltä, joka antaa hyvin tutunomaisen vaikutelman viestiin, jonka lisäksi viestin lopetus *"Iloisin terveisin, Pasi"*, pyrkii antamaan läheisemmän vaikutelman viestin vastaanottajan, sekä lähettäjän välillä, kun *"Pasi"* allekirjoittaa viestinsä käyttämällä vain etunimeään.

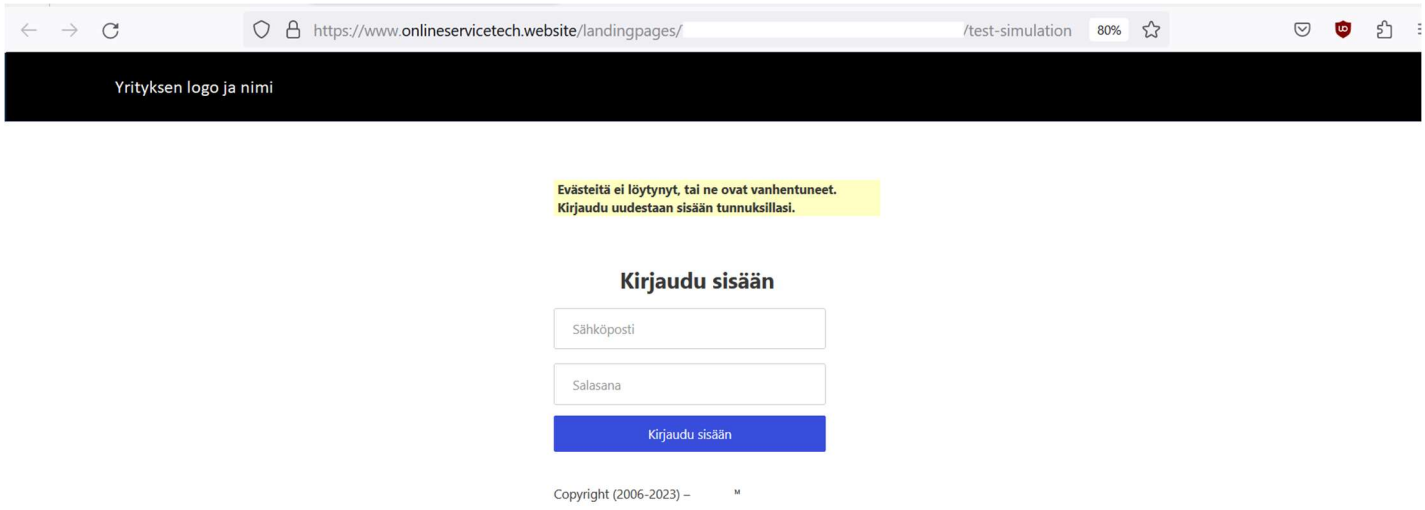
Viesti pyrkii vaikuttamaan vastaanottajaansa myös vetoamalla auktoriteettiin. Viestissä mainitaan, että *"Esihenkilösi pyysi minua"*, jolla viestin lähettäjä pyrkii luomaan mielikuvan, jossa vastaanottajan esihenkilö on jo keskustellut *"Pasin"* kanssa ennen tämän viestin lähettämistä. Tällöin viestin vastaanottajassa herää

hyvin todennäköisesti mielikuva siitä, että viestin lähettäjä on vastaanottajan esihenkilön asialla

Tässäkin tietojenkalasteluviestissä kuitenkin esiintyy muutamia epäkohtia, joiden pohjalta vastaanottaja voisi huomata huijauksen:

1. Viesti väittää tulevansa organisaation henkilöstöhallinnolta, mutta organisaation käytössä oleva sähköpostijärjestelmä ilmoittaa sen tulevan ulkopuoliselta lähettäjältä.
2. Organisaation sähköpostijärjestelmä ilmoittaa näennäisesti sisäisen viestin tulevan *"mailrelaysrv"* kautta.
3. Organisaation käytössä oleva sähköpostijärjestelmä ilmoittaa viestin lähettäjän olevan eri kuin normaalisti
4. Organisaation käyttämä sähköpostijärjestelmä ilmoittaa, että viestin lähettäjää ei pystytty varmentamaan.
5. Organisaation henkilöstöhallinnossa ei työskentele *"Pasia"*.
6. Viestiin upotettu linkki ei johda organisaation sivulle.

Kohdennettu tietojenkalasteluviesti ohjasi käyttäjän laskeutumissivustolle, jossa käyttäjää pyydettiin kirjautumaan sisään käyttäen tunnuksiaan. Kohdennetun tietojenkalasteluviestin laskeutumissivusto erosi geneerisestä siten, että se oli naamioitu esittämään kirjautumissivua. Sivustolla oli näkyvissä yrityksen logo, sekä suomenkielinen ohje, jossa henkilöä pyydettiin kirjautumaan uudestaan sisään, sillä evästeet ovat vanhentuneet.

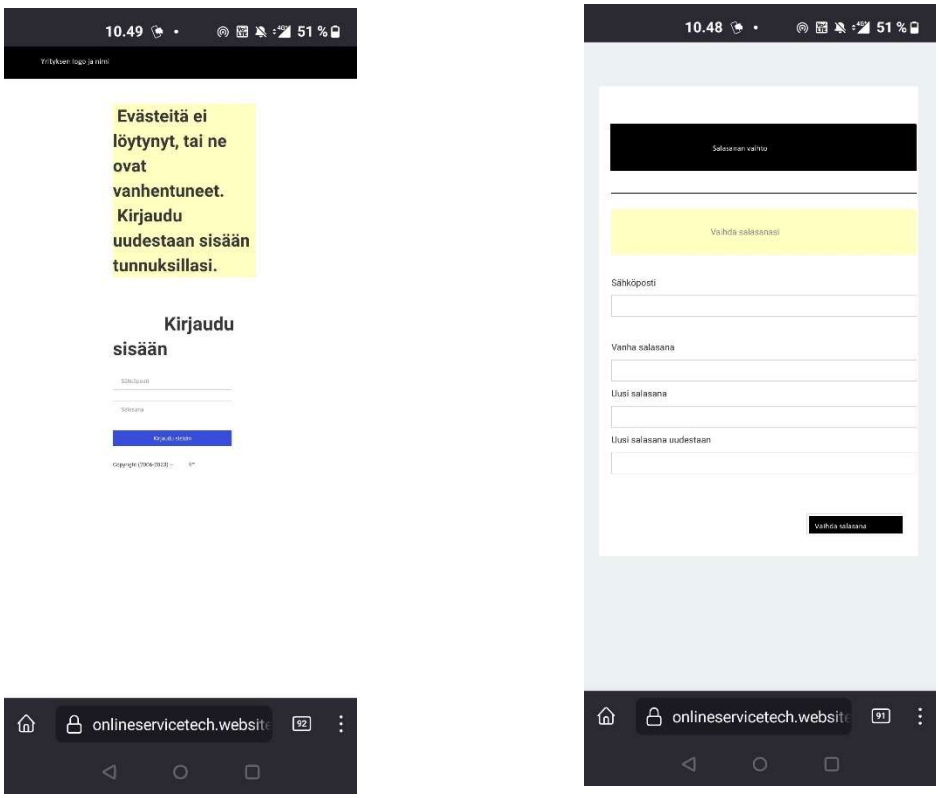


KUVIO 7 Simulaatiossa käytetty kohdennetun tietojenkalasteluviestin laskeutumissivu

Ensisilmäykseltä kohdennetun tietojenkalasteluviestin laskeutumissivu näyttää hyvin normaalilta kirjautumissivulta. Sivun luotettavuutta on pyritty lisäämään sillä, että se on kirjoitettu hyvällä suomen kielellä. Tämän lisäksi sivuston ulkoasu noudattelee jokseenkin samanlaista tyyliä, kuin organisaation omat verkossa näkyvissä olevat sivut ja sivuston vasempaan yläkulmaan sijoitettiin organisaation logo, sekä nimi. Kuvasta nimi ja logo on poistettu, sekä bannerin väriä on muutettu turvallisuussyistä. Myös tällä laskeutumissivulla on muutamia asioita, joista sen voi tunnistaa väärennetyksi ja pahantahtoiseksi kirjautumissivuksi.

- Sivuston URL ei vastaa organisaation sisäisesti käyttämiä URL osoitteita.
- Toisin, kuin organisaation muilla sisäisillä sivuilla, tältä sivulta ei pääse mitenkään organisaation omille sivuille
- Organisaatiolla ei ole tämänkaltaista kirjautumissivustoa olemassa, vaan autentikoitko organisaation intranetin sivustoille, hoituu organisaation oman VPN- yhteyden avulla.

Lisäksi, mikäli viestin vastaanottaja avasi tietojenkalasteluviestien sisältämän linkin mobiililaitteella, niin häntä kohtasi hieman erilainen näkymä.



KUVIO 8 Simulaation laskeutumissivut mobiililla. Kohdennettu vasemmalla ja geneerinen oikealla.

Kuten kuvista voidaan havaita, niin molempien laskeutumissivustojen URL osoite on mobiililaitteella lähes täysin piilossa. Tässä näkyvässä osassa oleva *"onlineservicetech"* saattaakin vastaanottajasta vaikuttaa ensinäkemältä aidoilta. Tällöin on todennäköisempää, että tietojenkalasteluviestin vastaanottaja ei tutki sitä yhtä tarkasti, kuin mikäli laskeutumissivun avaisi tietokoneella.

Molempien tietojenkalasteluviestien laskeutumissivustoille oli yhtenäistä niiden toiminta tietojen syöttämisen jälkeen. Sekä geneerisen, että kohdennetun tietojenkalasteluviestin laskeutumissivu ei tietojen syöttäjän näkökulmasta tehnyt mitään muuta kuin latasi sivun uudestaan, kun viestin vastaanottaja oli syöttänyt tiedot. Laskeutumissivun funktiona oli pitää kirjaa siitä, kuinka moni linkin avannut päätyy syöttämään sensitiivistä dataansa sivustolle. Molemmille laskeutumissivustoilla oli lisäksi yhtenäistä se, että selaimet eivät itsessään hälyttänet niistä. Esimerkiksi yleisesti neuvottu selaimen lukon seuraaminen ei tässä tapauksessa auttaisi, sillä laskeutumissivuston sertifikaatit olivat kunnossa.

3.1.3 Tietojenkalasteluaaltojen jälkeiset haastattelut

Tietojenkalastelukampanjoiden jälkeen suoritettiin haastatteluita. Haastatteluihin pyrittiin saamaan erityötehtävissä työskenteleviä henkilöitä, niin että ainakin osa haastateltavista olisivat sellaisia, jotka olivat tunnistaneet tietojenkalasteluviestin ja osa, jotka eivät olleet tunnistaneet tietojenkalasteluviestiä. Tutkimuksessa suoritetut haastattelut ovat puolirakenteisia, eli haastatteluissa oli joitain valmiita kysymyksiä, mutta vastauksen mukaan haastattelija pystyi esittämään rakenteesta poikkeavia lisäkysymyksiä.

Haastattelut valittiin tähän tutkimukseen sen vuoksi, että niiden avulla on mahdollista saada parempaa dataa etenkin, kun etsitään vastausta siihen mitkä asiat vaikuttivat henkilöiden toimintaan. Pelkän lähetettävän kyselylomakkeen vaarana olisi ollut, että vastaukset olisivat jääneet liian suppeiksi, eivätkä olisi antanut tarvittavia vastauksia haluttuihin kysymyksiin. Esimerkiksi, jos kyselyssä kysyttäisiin: "Mikä asia / asiat viestissä johti siihen, että huomasit sen olevan tietojenkalasteluviesti?", voisi vastaaja vastata vain: "viestin otsikko", jolloin jäisi hyvin epäselväksi mikä otsikosta teki epäluotettavan. Puolirakenteisessa haastattelussa, voidaan haastateltavalle esittää jatkokysymyksiä tarvittaessa, siitä mitkä elementit viestin otsikossa tekivät siitä epäluotettavan. Haastatteluiden käyttämiseen päädyttiin myös aikaisemmissa tutkimuksissa on havaittu, että ihmisten voi olla hyvin vaikeaa myöntää joutuneensa tietojenkalastelun uhriksi, jonka vuoksi kyselytutkimuksista saadut tulokset eivät todennäköisesti ole kovin tarkkoja (Jagatic ym., 2007, s. 7).

Haastatteluihin valikoitui yhteensä neljä henkilöä, jotka ilmoittautuivat vapaaehtoisesti haastatteluihin. Haastatteluihin kutsuttiin ihmisiä yleisillä ilmoituksilla, jotka lähetettiin organisaation käyttämään chat pohjaiseen sovellukseen, sähköpostilla organisaation sisällä, sekä luomalla ilmoituksesta organisaation sisäisenverkon etusivulle blogi kirjoitus. Yleinen ilmoitus valittiin, sillä tutkimuksen kannalta ei ollut merkittävää se, ketkä tietojenkalastelulinkkejä olivat avanneet, eikä heitä haluttu erikseen lähestyä eettisien syiden vuoksi. Haastatteluiden

tavoite pituus oli ~ 15–20 minuuttia. Haastatteluiden päätarkoitus tutkimuksessa oli tuoda syvempää tietoa asioista, jotka vaikuttivat tietojenkalasteluviestin käsittelyyn. Tällaisia käsittelyn tapauksia ovat esimerkiksi

- Syyt, jotka johtivat siihen, että tietojenkalasteluviesti raportoitiin
- Syyt, jotka johtivat siihen, että tietojenkalasteluviestiä ei raportoitu
- Syyt, jotka johtivat siihen, että sensitiivistä dataa syötettiin tietojenkalastelusivustolle.
- Syyt, jotka johtivat siihen, että sensitiivistä dataa ei syötetty tietojenkalastelusivustolle.

Haastattelut suoritettiin puolirakenteisina, eli niitä varten oli valmisteltu kysymyksiä, jotka kohdistuivat etenkin edellä mainittuihin tietojenkalasteluviestien käsittelyihin. Haastattelut nauhoitettiin osallistujien luvalla, jonka jälkeen litteroin aineistoin käyttäen litteroinnin tasona peruslitterointia. Peruslitterointi valikoitui tarvittavaksi litteroinnin tasoksi, sillä ainoastaan puheen asiasisältö oli tutkimuksen kannalta merkittävää. Tämän lisäksi tutkimuksen aiheen vuoksi haastatelluiden litteroinnista on muokattu tietoturvasyistä joitain sanoja, kuten henkilöiden ja käytettyjen sovellusten nimiä niin, ettei niitä voi suoraan tunnistaa. Eettisistä syistä haastateltavat ovat tutkimuksessa anonyymejä ja heihin viitataan ainoastaan pseudonyymeillä H1 – H4.

4 TIETOJENKALASTELUAALTOJEN TULOKSET

Tässä luvussa esitellään tietojenkalastelukampanjoista saadut tulokset. Näitä tuloksia tullaan käsittelemään aikaisemman tutkimuksen pohjalta. Tässä tutkimuksessa otettiin tietojenkalastelun onnistumisen mitaksi se, oliko vastaanottaja avannut linkin. Tämä johtuu siitä, että simulaatio suoritettiin käyttämällä valmista tietojenkalastelusimulaatioihin erikoistunutta ohjelmistoa, joka systemaattisesti aliarvioi kunkin tietojenkalasteluviestin avattuja määriä. Tämä ilmeni esimerkiksi simulaatioiden tulosten perusteella siten, että voitiin havaita useita tapauksia, joissa henkilö oli avannut tietojenkalasteluviestin linkin avaamatta itse viestiä, joka taas on käytännössä mahdotonta. Lisäksi etenkin kohdennettu tietojenkalasteluviesti oli sellainen, että viestin tunnistaminen tietojenkalasteluviestiksi pelkän sähköpostijärjestelmässä näkyvän otsikon perusteella olisi käytännössä mahdotonta, ellei vastaanottajalla ollut valmista tietoa viestin olevan tietojenkalasteluviesti.

Tuloksissa, joissa käsitellään sensitiivisen datan syöttämiseen liittyviä asioita, otettiin onnistumisen mitaksi se, syöttikö henkilö oikean sähköpostinsa laskeutumissivuston lomakkeelle. Tämä johtuu siitä, että teknisistä ja tietoturvallisista syistä ei pystytä todentamaan, oliko syötetty salasana oikea, mutta mikäli lomakkeelle on syötetty oikea käytetty sähköposti, niin voidaan olettaa, että myös oikea salasana on syötetty lomakkeelle.

4.1 Ensimmäisen tietojenkalasteluaallon tulokset

Viesti tyypit	Geneerinen (ryhmä 1)		Kohdennettu (ryhmä 2)	
Viestin saaneet	213	100 %	213	100 %
Viestin linkin avanneet	17	7.9 %	75	35.2 %
Avasivat linkin mobiililaitteella.	12	5.6 %	31	14.5 %
Syöttivät sensitiivistä dataa	6	2.8 %	34	15.9 %
Syöttivät sensitiivisen datan mobiililaitteella	2	0.9 %	6	2.8 %
Ilmoittivat tietojenkalasteluviestin	44 *	20.6 % *	35 *	16.4 % *
Avasivat linkin, sekä loivat ilmoituksen	6 *	2.8 % *	22 *	10.3 % *
Avasivat linkin, mutta eivät ilmoittaneet tietojenkalastelusta	11 *	5.1 % *	52 *	24.4 % *
Eivät avanneet linkkiä, eivätkä ilmoittaneet	158 *	74.1 % *	125 *	58.6 % *
Eivät avanneet linkkiä ja ilmoittivat	38 *	17.8 % *	13 *	6.1 % *
Syöttivät sensitiivistä dataa ja ilmoittivat	2 *	0.9 % *	15 *	7 % *
Syöttivät sensitiivistä dataa ja eivät ilmoittaneet	4 *	1.8 % *	20 *	9.3 % *

TAULUKKO 1 Ensimmäisen aallon tulokset

** Valitettavan tietoteknisen rajoitteen vuoksi, organisaation työntekijöiden Outlookin sisäisen "report phishing" napin avulla luotuja ilmoituksia ei voitu saada. Tämän vuoksi ensimmäisen aallon tulokset ilmoituksista ovat vain suuntaa antavia.*

Ensimmäisen tietojenkalasteluaallon tuloksista voidaan havaita monia mielenkiintoisia asioita. Molempia viestityyppejä lähetettiin 213 vastaanottajalle. Geneerisen viestin avaajista 17 ja kohdennetun viestin vastaanottajista 75 avasi tietojenkalasteluviestin sisältämän haitallisen linkin.

Sensitiivistä dataa, kuten sähköposteja ja salasanoja, laskeutumissivustolle syötti geneerisen viestin vastaanottajista 6. Näistä kuudesta geneerisen viestin vastaanottajista kaikki syöttivät sivustolle työsähköpostinsa. Kohdennetun viestin vastaanottajista 36 syötti laskeutumissivustolle sensitiivistä dataa. Heistä 2

kuitenkin syötti selkeästi väärää dataa sivulle, todennäköisesti testatakseen sen toimintaa, jolloin todellisia sensitiivisen datan syöttäjiä oli 34. Kohdennetun tietojenkalasteluviestin saaneista henkilöistä 4 syötti ilmeisesti työsähköpostinsa sijaan, henkilökohtaisen sähköpostinsa sivustolle.

Tämän lisäksi ensimmäisessä tietojenkalasteluaallossa geneerisen viestin vastaanottajista 12 ja kohdennetun viestin vastaanottajista 31 avasi viestin mobiililaitteella. Kuitenkin näistä vain kaksi geneerisen viestin vastaanottajaa ja kuusi kohdennetun viestin vastaanottajaa syöttivät laskeutumissivustolle sensitiivistä dataa mobiililaitteella.

Molempien viestien kohdalla esiintyi myös tapauksia, jossa viestin vastaanottaja syötti tietonsa useaan kertaan tietojenkalasteluviestin laskeutumissivustolle. Näistä henkilöistä, jotka syöttivät tietojaan useasti laskeutumissivustoille, osa lisäksi syötti tietoja useammalla eri laitteella. Geneerisen viestin vastaanottajista 2 syötti tietojaan vähintään kahdesti ja näistä kahdesta toinen syötti tietoja ensin matkapuhelimella ja tämän jälkeen tietokoneellaan. Kohdennetun tietojenkalasteluviestin vastaanottaneista 25 syötti tietojaan vähintään kahdesti. Näistä 25 henkilöstä 3 syötti sensitiivistä dataa sekä mobiililaitteella, että tietokoneella.

Oletettavasti henkilöt, jotka syöttivät tietojaan useaan kertaan laskeutumissivustoille, tekivät sen laskeutumissivustojen käyttäytymisen vuoksi. Kuten luvussa 4.2 on mainittu, niin laskeutumissivustot eivät antaneet mitään palautetta tietojen syöttämisen jälkeen, vaan ainoastaan päivittyivät. Tällöin on todennäköistä, että monet, jotka syöttivät tietojaan useasti ovat tulkinneet, että sivusto ei jostain syystä toiminut, tai että he olivat itse kirjottaneet jotain väärin. On myös todennäköistä, että samasta syystä jotkut vastaanottajat olivat syöttäneet tietoja useammalla eri laitteella, olettaen, että sivusto ei jostain syystä olisi toiminut mobiililaitteella.

4.1.1 Organisaation luomat ilmoitukset ensimmäisessä tietojenkalasteluaallossa

Organisaation työntekijät tekivät ilmoituksia tietojenkalastelusta käyttämällä kolmea eri kanavaa: Outlookin sisäistä ”report phishing” – nappia, tekemällä ilmoituksen organisaation portaalin kautta, sekä lähettämällä sähköpostia johonkin organisaation hallinnolliseen osoitteeseen. Valitettavien tietoteknisten rajoitteiden vuoksi ensimmäisen tietojenkalasteluaallon tulokset Outlookin sisäisellä napilla tehdyistä ilmoituksista olivat kuitenkin kadonneet, jolloin niitä ei voida tarkastella.

Suurin osa tietojenkalasteluviestin vastaanottaneista ei reagoinut siihen millään tavalla. Geneerisen tietojenkalasteluviestin saaneista 158 henkilöä ei avannut viestiä, eivätkä tehneet siitä ilmoitusta. Kohdennetun tietojenkalastelu viestin saaneista 125 henkilöä ei avannut, eikä tehnyt ilmoitusta viestistä.

Kohdennetusta, sekä geneerisestä tietojenkalasteluviestistä tehtiin yhteensä 80 ilmoitusta. Näistä ilmoituksista 16 tehtiin luomalla tiketti organisaation sisäisen portaalin kautta ja 64 tehtiin lähettämällä sähköpostia johonkin organisaation sisäiseen hallinnolliseen osoitteeseen.

Organisaatiolla ei vaikuttanut olevan mitään yhtä tiettyä paikkaa, johon saadun tietojenkalasteluviestin olisi voinut ilmoittaa, sillä esimerkiksi sähköposteja lähetettiin kaiken kaikkiaan viiteen eri osoitteeseen, joista organisaation tietohallinnon ja tietoturvan sähköposteihin lähetettiin suurin osa viesteistä. Organisaation tietoturvalle lähetettiin 53 ilmoitusta ja organisaation tietohallinnolle lähetettiin 21 ilmoitusta.

Sisäisen portaalinkautta lähetetyistä raportoinneista seitsemän raportoi geneerisen tietojenkalasteluviestin. Näistä seitsemästä kaksi oli avannut viestin sisältämän linkin ja yksi oli syöttänyt laskeutumissivuston kautta sensitiivistä dataa. Tällöin viisi raportoijaa ei ollut avannut viestin sisältämää linkkiä ja olivat raportoineet viestin tietohallinnolle. Kohdennettua tietojenkalasteluviestiä raportoitiin sisäisen portaalin kautta yhdeksän kertaa. Näistä yhdeksästä viisi oli avannut viestin sisältämän linkin ja näistä viidestä neljä oli syöttänyt laskeutumissivustolle sensitiivistä dataa. Tällöin vain neljä henkilöä oli nähnyt tietojenkalasteluviestin, tunnistanut sen ja raportoinut sen eteenpäin.

Sisäisen portaalin kautta ilmoituksen tehneistä kahdeksan henkilöä oli laittanut ilmoitukseensa tietoa tietojenkalasteluviestin sisällöstä. Ilmoitettu sisältö vaihteli koko viestistä, viestin sisältämiin yksittäisiin merkittäviin tietoihin kuten viestin lähettäjään. Sähköpostin kautta tehdyissä ilmoituksissa 54 oli joko kuva saadusta tietojenkalasteluviestistä, tai viesti oli liitetty liitteenä ilmoitukseen.

Sisäisen portaalin kautta ilmoituksen tehneistä kaiken kaikkiaan viisi oli syöttänyt sensitiivistä dataa laskeutumissivustolle. Näistä viidestä, neljä ilmoitti ilmoituksessaan syöttäneensä dataa sivustolle. Sähköpostin välityksellä ilmoituksen tehneistä 13 oli syöttänyt sensitiivistä dataa laskeutumissivustolle. Näistä 13 kuitenkin 10 kertoi ilmoituksessaan syöttäneensä sensitiivistä dataa laskeutumissivustolle.

Ensimmäisessä tietojenkalasteluaallossa neljä geneerisen tietojenkalasteluviestin saanutta ja 20 kohdennetun tietojenkalasteluviestin saanutta ei ollut luonut ilmoitusta viestistä, vaikka he olivat syöttäneet sensitiivisistä dataa laskeutumissivustolle. Kuitenkin aikaisemmin mainittujen teknisten ongelmien vuoksi, ensimmäisessä aallosta ei voitu saata dataa siitä, kuinka moni oli luonut ilmoituksen Outlookin sisäisen *"report phishing"*- napin kautta, jonka vuoksi tarkkaa lukemaa henkilöistä, jotka eivät ilmoittaneet tietojenkalasteluviestistä ollenkaan ei voida tehdä.

4.1.2 Organisaation sisäinen tiedonkulku ensimmäisessä tietojenkalasteluaallossa

Ensimmäisestä tietojenkalastelukampanjasta tiedotettiin virallisesti ainakin organisaation sisäisellä blogi postauksella. Kyseinen blogi postaus näkyi organisaation intrawebin etusivulla kohdassa *"ajankohtaista"*. Blogi postaukseen oli kirjoitettu tietoja tietojenkalasteluviesteistä, jonka lisäksi se sisälsi kuvat sekä geneerisestä, että kohdennetusta tietojenkalasteluviestistä. Tietojenkalasteluviesteihin liittyvien tietojen lisäksi blogissa oli ohjeita siihen miten saatuihin viesteihin kuuluisi reagoida. Näissä ohjeissa pyydettiin välittämään saatu tietojenkalasteluviesti organisaation tietoturvan sähköpostiin.

Organisaation sisällä tapahtuneesta virallisesta tiedotuksesta on huomioitava, että intran *"ajankohtaista"* alaisuudessa olevat postaukset, eivät näy kovin hyvin käyttäjille ilman että he rullaavat sivua alaspäin. Tämän lisäksi *"ajankohtaista"* osion syöte liikkuu alaspäin, mikäli sille lisätään muuta sisältöä. Tällöin tiedote aktiivisesta tietojenkalastelusta saattaa nopeasti hukkua muun sisällön joukkoon, eivätkä työntekijät välttämättä saa tarvittavaa tietoa käynnissä olevasta tietojenkalastelu hyökkäyksestä. On lisäksi huomioitava, että organisaation henkilöstöhallinto oli tietoinen tulevista tietojenkalasteluviesteistä, joten henkilöstöhallinnon reaktiota tietojenkalasteluun ei ole muuten mielekästä tarkastella.

Ensimmäisen tietojenkalasteluaallon kohdalla viesteistä tiedottava artikkeli julkaistiin klo 09:28, mutta tietoja syötettiin tämän jälkeen vielä 34 kertaa. Artikkelia oltiin julkaisupäivänä, maanantaina, luettu 101 kertaa, jolloin tapahtui myös suurin osa sensitiivisen datan syötöistä. Seuraavien päivien lukumäärät olivat huomattavasti pienempiä ja tiistaina artikkelia oli luettu 32 kertaa, keskiviikkona 13 kertaa ja torstaina, sekä perjantaina 2 kertaa. On toki huomioitava, että näissä 34 kerrassa on laskettu mukaan myös toistuvat tiedon syötöt. Toistuvien tietojensyöttöjen mukana laskeminen johtuu siitä, että jokaisen tietojen syötön välissä oli mahdollista, että luvun 2.1.2 Petosteorian mukainen aktivointi olisi tapahtunut, kun laskeutumissivu ei teekään sitä mitä henkilö sen olettaa tekevän.

Virallisten tiedotuskanavien lisäksi tietojenkalastelusta käytiin keskustelua myös organisaation sisäisessä pikaviestintäsovelluksessa. Pikaviestintäsovelluksen keskustelua käytiin ainakin organisaation yleisellä keskustelukanavalla, jossa jaettiin kuva kohdennetusta tietojenkalasteluviestistä. Tässä keskustelussa mainittiin geneerinen tietojenkalasteluviesti, mutta siitä ei liitetty kuvaa. Tämän lisäksi keskustelussa neuvottiin ihmisiä, miten viestin voi raportoida eteenpäin.

4.2 Toisen tietojenkalasteluaallon tulokset

Viesti tyypit	Geneerinen (ryhmä 2)		Kohdennettu (ryhmä 1)	
Viestin saaneet	213	100 %	213	100 %
Viestin linkin avanneet	11	5.1 %	66	30.9 %
Avasivat linkin mobiililaitteella.	1	0.46 %	15	7 %
Syöttivät sensitiivistä dataa	2	0.93 %	16	7.5 %
Syöttivät sensitiivisen datan mobiililaitteella	1	0.46 %	2	0.93 %
Ilmoittivat tietojenkalasteluviestin	26	12.2 %	26	12.2 %
Avasivat linkin, sekä loivat ilmoituksen	0	0	9	4.2 %
Avasivat linkin, mutta eivät ilmoittaneet tietojenkalastelusta	11	5.1 %	57	26.7 %
Eivät avanneet linkkiä, eivätkä ilmoittaneet	176	82.6 %	131	61.5 %
Eivät avanneet linkkiä ja ilmoittivat	26	12.2 %	16	7.5 %
Syöttivät sensitiivistä dataa ja ilmoittivat	0	0	9	4.2 %
Syöttivät sensitiivistä dataa ja eivät ilmoittaneet	2	0.93 %	7	3.2 %

TAULUKKO 2 Toisen aallon tulokset

** Valitettavan tietoteknisen rajoitteen vuoksi, organisaation työntekijöiden Outlookin sisäisen "report phishing" napin avulla luotuja ilmoituksia ei suurelta osin voitu saada. Tämän vuoksi toisen aallon tulokset ilmoituksista ovat vain suuntaa antavia.*

Toisen tietojenkalasteluaallon tuloksista voidaan havaita monia mielenkiintoisia asioita. Samoin, kuin ensimmäisessä tietojenkalasteluaallossa, molempia viestityyppejä lähetettiin 213 vastaanottajalle. Viestit lähetettiin siten, että ne henkilöt, jotka saivat ensimmäisessä aallossa geneerisen tietojenkalasteluviestin, saivat nyt kohdennetun tietojenkalasteluviestin. Geneerisen viestin vastaanottajista 11 ja kohdennetun viestin vastaanottajista 60 avasi viestin sisältämän haitallisen linkin.

Toisessa tietojenkalasteluaallossa sensitiivistä dataa, kuten sähköposteja ja salasanoja, laskeutumissivustoille syötti geneerisen viestin vastaanottajista kaksi

ja kohdennetun viestin vastaanottajista 16. Toisin kuin ensimmäisessä aallossa, toisessa tietojenkalasteluaallossa ei esiintynyt selkeästi väärää dataa kummankaan viestityypin tuloksissa. Tämän lisäksi kaikki, jotka olivat syöttäneet dataa, olivat syöttäneet työsähköpostinsa.

Toisessa tietojenkalasteluaallossa vain yksi henkilö oli avannut geneerisen tietojenkalasteluviestin mobiililaitteella, kun taas 15 henkilöä oli avannut kohdennetun tietojenkalasteluviestin mobiililaitteella. Näistä kuitenkin vain yksi geneerisen viestin vastaanottaja ja kaksi kohdennetun viestin vastaanottajaa oli syöttänyt sensitiivistä dataa mobiililaitteellaan.

Myös toisessa tietojenkalasteluaallossa molempien viestien kohdalla esiintyi tapauksia, jossa viestin vastaanottaja syötti tietonsa useaan kertaan tietojenkalasteluviestin laskeutumissivustolle. Toisessa tietojenkalasteluaallossa ei kuitenkaan esiintynyt tapauksia, jossa sensitiivistä dataa olisi syötetty useammalla eri laitteella. Geneerisen viestin vastaanottajista yksi henkilö syötti tietojaan vähintään kahdesti. Kohdennetun tietojenkalasteluviestin vastaanottaneista 11 henkilöä syötti tietojaan vähintään kahdesti. On hyvin todennäköistä, että useampaan kertaan tietojensyöttämiseen vaikuttivat pitkälti samat asiat, kuin ensimmäisessä tietojenkalasteluaallossa.

4.2.1 Organisaation luomat ilmoitukset toisessa tietojenkalasteluaallossa

Organisaation työntekijät tekivät ilmoituksia myös toisessa aallossa käyttämällä kolmea eri kanavaa: Outlookin sisäistä ”report phishing” – nappia, tekemällä ilmoituksen organisaation sisäisen portaalin kautta, sekä lähettämällä sähköpostia johonkin organisaation hallinnolliseen osoitteeseen.

Organisaation sisäisen portaalin kautta tehtyjen ilmoituksien tarkkaa sisältöä ei, päästy lukemaan tarkemmin toisen tietojenkalastelusimulaation osalta. Sisäisen portaalin kautta tehtiin yhteensä 26 ilmoitusta tietojenkalasteluviesteistä. Näistä ilmoituksista 14 oli tehty geneerisestä tietojenkalasteluviestistä ja 12 oli tehty kohdennetusta tietojenkalasteluviestistä. Huomattavaa on, että geneerisestä viesteistä ilmoittaneista kukaan ei ollut avannut tietojenkalastelulinkkiä, tai syöttänyt laskeutumissivustolle sensitiivistä dataa. Kohdennetun tietojenkalasteluviestin ilmoittaneista kolme oli avannut viestin sisältämän linkin ja syöttänyt sensitiivistä dataa.

Sähköpostin välityksellä tehdyistä ilmoituksista 11 oli saanut geneerisen tietojenkalasteluviestin ja 13 oli saanut kohdennetun tietojenkalasteluviestin. Samoin, kuin sisäisen portaalin kautta tehdyissä ilmoituksissa, kukaan geneerisen viestin sähköpostin kautta ilmoittaneista, ei ollut avannut viestin linkkiä, tai syöttänyt sensitiivistä dataa laskeutumissivustolle. Kohdennetun viestin vastaanottaneista ilmoittajista viisi henkilöä oli avannut viestin sisältämän haitallisen linkin ja yksi henkilö oli syöttänyt sensitiivistä dataa laskeutumissivustolle. Kaikissa sähköpostin välityksellä tehdyissä ilmoituksissa oli mukana jonkinlainen tieto tietojenkalasteluviestistä, näistä 19 oli lähettänyt saadun tietojenkalasteluviestin edelleen, joko organisaation tietohallinnolle, tai tietoturvalle. Sähköpostin

kautta tehdyissä ilmoituksissa kolmessa tietojenkalasteluviesti oli liitetty mukaan kuvana itse ilmoitukseen ja neljässä se oli liitetiedostona.

Toisessa tietojenkalasteluaallossa ilmoituksia tehtiin vähemmän, sekä geneerisen, että kohdennetun tietojenkalasteluviestin osalta. Toisessa aallossa molemmista viestityypeistä luotiin ilmoituksia 26 kappaletta. Toisen aallon sähköposti ilmoituksissa kukaan ilmoittajista ei kertonut syöttäneensä dataa, tai avanneensa linkkejä.

4.2.2 Organisaation sisäinen tiedonkulku toisessa tietojenkalasteluaallossa

Toisessa tietojenkalasteluaallossa organisaation sisäisessä pikaviestintäsovelluksessa käytiin huomattavasti vilkkaampaa keskustelua, kuin ensimmäisen tietojenkalasteluaallon kohdalla. Keskustelua sovelluksessa käytiin etenkin tietojenkalastelusta, sekä saaduista tietojenkalasteluviesteistä. Ensimmäinen viesti sovellukseen tuli noin 4 minuuttia aallon alkamisen jälkeen ja siinä ihmeteltiin kohdennetun tietojenkalasteluviestin sisältämän linkin kummallisuutta.

Sisäisen pikaviestintäsovelluksen keskustelussa jaettiin kuva geneerisestä tietojenkalasteluviestistä, mutta ei kohdennetusta viestistä. Keskustelua käytiin paljon tietojenkalasteluviestien sisältämistä indikaattoreista, joista viestit pystyivät tunnistamaan tietojenkalasteluksi. Tällaisia indikaattoreita, joita tuotiin keskustelussa esiin, oli muun muassa se, että viesteissä ilmoitettiin ulkopuolisesta lähettäjästä ja geneerisen viestin lähettäjän tahallisesta väärin kirjoituksesta, jossa iso ”i”-kirjain oli korvattu pienellä ”l”- kirjaimella.

Sisäisen pikaviestintäsovelluksen keskustelussa käytiin myös jonkin verran spekulaatiota, siitä että käynnissä olisi organisaation sisäinen testi tietojenkalasteluun liittyen. Tällä spekulaatiolla on voinut olla vaikutusta ilmoitusten määriin, sillä mikäli ihmiset ajattelevat kyseessä olevan testi, niin on todennäköisempää, että he eivät tee ilmoitusta tietojenkalastelusta, vaikka olisivatkin syöttäneet sensitiivistä dataa tietojenkalasteluviestien laskeutumissivustolle.

Vaikka keskustelua tietojenkalastelusta käytiin ahkerasti organisaation sisäisessä pikaviestintäsovelluksessa, niin kuitenkin käytännössä jokainen linkin avaus ja sensitiivisen datan syöttäminen tapahtui joko samaan aikaan keskustelun kanssa tai sen jälkeen. Tällöin voidaan tehdä johtopäätös, ettei keskustelukanavalla jaettu informaatio saavuttanut suurta osaa organisaation työntekijöistä riittävällä nopeudella.

4.3 Haastatteluiden tulokset

Kukaan haastatteluihin osallistuneista ei ollut avannut geneerisen tietojenkalasteluviestin sisältämää linkkiä, mutta kaksi haastatteluista oli avannut kohdennetun tietojenkalasteluviestin linkin. Molemmat linkin avaukset olivat tapahtuneet huolimattomuuden takia, tai puhtaasti vahingossa.

”Se haiskahti vaaralliselta koko viesti, eikä mun ollut tarkoitus avata sitä, vaan hoverata siinä nähdäkseni sen URL:in mihinkä se linkki ohjaa. Mutta sormi oli nopeampi kuin aivot sillä kertaa, niin mä naksautin sen auki.” -H2

” Se tuli hetkellä, jolloin mulla oli juuri ollut pitkä palaveriputki, jonka aikana oli tullut kymmeniä viestejä sähköpostiin, joista useimmat olivat sellaisia, että ne pystyi merkkaamaan suoraan luetuiksi. Sitten mä vaan kliksuttelin niitä auki. En lukenut tarkasti otsikkoa, enkä tarkasti sisältöä.” -H4

Tämän lisäksi H4 oli sattumalta käynyt esihenkilönsä kanssa keskustelua työajan seurantaan liittyen juuri ennen kohdennetun tietojenkalasteluviestin, jonka aiheena oli myös työnajan seuranta, saamista. Tällöin tietojenkalasteluviestille oli syntynyt luonnollinen veruke, joka täytti molemmat hyvän verukkeen elementeistä (Fruhlinger, 2020, s. 1).:

- Hyökkääjän esittämä persoona
    - Hyökkääjä esiintyi organisaation henkilöstöhallintona, joka saattaa joissain tilanteissa hyvinkin ottaa kantaa, tai välittää ohjeita työnajan seurannasta.
- Luonnollinen tilanne, tai ongelma, jonka yhteydessä tämä persoona voi esiintyä
    - Tässä luonnollinen tilanne syntyi saman aihepiirin keskustelusta, jonka H4 oli hiljattain käynyt esihenkilönsä kanssa.

Vaikka osa haastatteluihin osallistuneista oli avannut tietojenkalasteluviestin linkin, niin yksikään haastatelluista ei ollut syöttänyt avautuneelle laskeutumissivustolle sensitiivistä dataa, kuten salasanoja. Laskeutumissivustolla epäilyksen oli herättänyt mm. organisaation brändien vastaisen ulkoasun huomaaminen.

” En muista tarkkaan, että mikä siinä oli, oudolta tai silleen näyttänyt. Mutta tosiaan se viesti itsessään oli jo laittanut hälytyskellot soimaan niin ei ollut hetkeäkään semmoista tilannetta, että olisin ryhtynyt. Täyttämään sinne tietojani muutenkaan.

Mut mulla on joku semmoinen muistikuva että siinä oli jäi häiritsemään joku siinä ulkoasussa että se ei näyttänyt uskottavalta, ainakaan niinku meidän firman brändien mukaan. Eikä nyt ehkä muutenkaan modernia webbi työkalua muistuttava. ”-H2

Henkilöt, jotka eivät olleet avanneet kohdennetun tietojenkalasteluviestin linkkiä kertoivat epäilyksensä heränneen siitä, että esihenkilön käytös, työajanseurannasta kertomisen delegointi, ei vastannut sitä, miten esihenkilö oli aikaisemmin käyttäytynyt. Tällöin vastaanottajilla on petosteorian mukaisesti kokonaisuuden arvioinnissa yksilöiden ominaisuuksien avulla herännyt vahva

epäilys siitä, että vastaanotettu viesti on huijausta. Petosteoriaa on käsitelty aikaisemmin luvussa 2.1.2.

> ”Tiesin, että mun esihenkilö ei tuollaista viestiä laittaisi. Työssäni tilanne on sellainen, että ei kukaan tällaista viestiä laittaisi” -H1

> ” No just tää että esihenkilö sanoisi mulle itse. Että, olikohan mä siinä toimistolla, kun mä sain sen ja NIMI oli täällä. Niin tai joku tämmöinen niinku että tunnen hänet ja hän kyllä tulisi mulle sanomaan tai laittaisi viestin siitä itsekin, että hän ei pyydä mitään epämääräistä henkilöstöhallintoa delegoimaan mulle jotain. Kun se oli vissiin kyse jostain työaikakirjanpito hommasta tai jostain tämmöisestä. Mikä kuuluu hänen tontilleen, niin miksi hän sen delegoisi toiselle, eikä sanoisi sitä suoraan?” -H3

Haastatteluihin osallistuneista kaksi kertoi, että oli lukenut keskustelua organisaatioon saapuneista tietojenkalasteluviesteistä organisaation pikaviestintäsovelluksen kautta. Heistä ainakin yhdelle pikaviestintäsovelluksessa käyty keskustelu oli ainakin osittain vaikuttanut siihen, että oli saman tien tunnistanut saamansa tietojenkalasteluviestin tietojenkalasteluksi.

> ”Luin pikaviestintäsovelluksesta ensin, kun jotkut ihmettelivät sitä ja vasta tämän jälkeen näin sen viestin. Mä en osaa sanoa, että mikä mulla olisi siinä hälytyskellot soittanut, mutta pikaviestintäsovelluksessa oli muilla jo hälytyskellot soineet.” – H3

> ” Olisikohan se eka ollut sellainen, että siitä käytiin keskustelua tuolla pikaviestintäsovelluksen puolellakin. Se, että oliko siitä jo ehtinyt jotain keskusteluakin olla, sitä en muista.” -H1

Haastatteluihin osallistuneet olivat tehneet vaihtelevasti ilmoituksia saamistaan tietojenkalasteluviesteistä ja osa oli huomannut, tai päätellyt kyseessä olevan simulaatio. Huomattuaan, että kyseessä on simulaatio, monet haastatelluista oli päättänyt priorisoida aikaansa ja jättäneet ilmoituksen tekemättä. Osa haastatteluihin osallistuneista kertoi myös kokeneensa tietojenkalastelusta ilmoittamisen hankalaksi, mikä on osaltaan voinut vaikuttaa ilmoittamatta jättämiseen, vaikka sitä ei haastatteluissa suoraan mainittu.

> ” Tiesin, että niin pitäisi tehdä, mutta mulle oli myöskin aika selvää, että nää oli vaan tällaisia kokeiluja ja oli aika paljon kaikkea muutakin tekemistä, niin priorisoin ajan käyttöä. Tiedän, että olisi varmaan pitänyt tehdä näin, mutta jos on ihan itsestään selvää, että täällä ei ole mitään vaikutusta muuta kuin että joku tilasto saadaan nyt, että miten ihmiset reagoi, niin ehkä se oma motivaatio sitten toimia ei ehkä ole kauhean hyvä” -H1

> ” Tunnollisena työntekijänä ja juuri tietoturvakoulutuksen käyneenä huomasin, että nyt meitä kalastellaan, joten tein siitä sitten sen ihan ilmoituksen organisaation tietohallinnolle. Toisen viestin kohdalla mulla oli ehkä hieman kutina, että tää saattaa kanssa olla koulutukseen liittyvä viesti kun mä törmäsin pikaviestintäsovelluksen kanavalla keskusteluun, jossa oli

muillekin ilmaantunut tämä sama viesti. Mä sitten en tehnyt ihan sitä virallista tietoturvailmoitusta siitä, eli mua vaan laiskotti toisen kohdalla.” -H2

” Mä en sitä nappulaa löytänyt.

Ja sitten että mikä se organisaation tietohallinnosta vastaavan tahon osoite olikaan ja pitikö nyt sinne laittaa sähköpostiin vai pitääkö kaivaa se organisaation sisäinen ilmoitus järjestelmä ja laittaa sinne tikettiä ja mikä sen Urli olikaan ja sitten se on liian monta tämmöistä niinku pohdinta steppiä ja sitten se jää tekemättä.” -H3

4.4 Tilastolliset erot tietojenkalasteluaaltojen välillä

Tutkimuksen tuloksia tarkastellessa suoritettiin kahden otoksen suhteiden testi (eng. *”Two sample proportions test”)* tutkimuksessa saaduille tuloksille. Tämän testin avulla voidaan arvioida, onko ryhmien välinen ero tilastollisesti merkittävä, niin että se ei ole voinut tapahtua pelkästään sattumalta. Kahden otoksen suhteellinen testi valittiin t-testin sijaan, koska tutkimuksessa saatu data on binääristä. Testit suoritettiin ajamalla ne RStudiossa. Kummassakin ryhmässä viestin vastaanottajia oli 213.

Ensimmäinen aalto:

H_0: Ryhmässä 1 asian x tehneiden ihmisten osuus on sama, kuin ryhmässä 2.
H_A: Ryhmässä 1 asian x tehneiden ihmisten osuus on pienempi, kuin ryhmässä 2.

Toinen aalto:
H_0: Ryhmässä 1 asian x tehneiden ihmisten osuus on sama, kuin ryhmässä 2.
H_A: Ryhmässä 1 asian x tehneiden ihmisten osuus on suurempi, kuin ryhmässä 2

	p-arvo: Ensimmäinen aalto H_0	p-arvo: Ensimmäinen aalto H_A	p-arvo: Toinen aalto H_0	p-arvo: Toinen aalto H_A
Viestin linkin avanneet	1.928e-11 **	9.639e-12 **	1.054e-11 **	5.27e-12 **
Avasivat linkin mobiililaitteella.	0.003792 **	0.001896 **	0.0009236 **	0.0004618 **
Syöttivät sensitiivistä dataa	7.298e-06 **	3.649e-06 **	0.001742 **	0.0008711 **
Syöttivät sensitiivisen datan mobiililaitteella	**0.2843**	**0.1421**	**1**	0.002425 **
Ilmoittivat tietojenkalasteluviestin	**0.31**	**0.8407**	**1**	**0.5**
Avasivat linkin, sekä loivat ilmoituksen	0.00336 **	0.00168 **	0.007033 **	0.003516 **
Avasivat linkin, mutta eivät ilmoittaneet tietojenkalastelusta	4.779e-08 **	2.389e-08 **	2.636e-09 **	1.318e-09 **
Eivät avanneet linkkiä, eivätkä ilmoittaneet	0.001026 **	**0.9995**	2.021e-06 **	**1**
Eivät avanneet linkkiä ja ilmoittivat	0.0003411 **	**0.9998**	**0.1435**	**0.9282**
Syöttivät sensitiivistä dataa ja ilmoittivat	0.002975 **	0.001488 **	0.007033 **	0.003516 **
Syöttivät sensitiivistä dataa ja eivät ilmoittaneet	0.001622 **	0.000811 **	**0.1778**	**0.08889**

TAULUKKO 3 Kalastelun kahden otoksen suhteiden testin tulokset
** $p < 0.01$ * $p < 0.05$

Ensimmäisen aallon nollahypoteesin testeistä voidaan havaita, että kaikissa muissa tutkituissa kohdissa, paitsi: *"Syöttivät sensitiivisen datan mobiililaitteella"* ja *"Ilmoittivat tietojenkalasteluviestin"*, oli tilastollisesti merkittävä ero geneerisen ja kohdennetun tietojenkalasteluviestin välillä p-arvon ollessa alle 0.01. Näiden kohtien osalta voidaan siis hylätä nolla hypoteesi.

Mobiililaitteella sensitiivisen datan syöttämisen p-arvoksi saatiin 0.2843 > 0.05. Tällöin, nolla hypoteesia ei voida hylätä tämän kohdan osalta, sillä tulos olisi voinut tapahtua myös sattumalta. Tämän kohdan korkeaa p-arvoa selittää ensimmäisen aallon kohdalla se, että geneerisen tietojenkalasteluviestin vastaanottajista 2 oli syöttänyt sensitiivistä dataa ja kohdennetun tietojenkalasteluviestin vastaanottajista 6 oli syöttänyt sensitiivistä dataa. Tällöin mobiililaitteilla syötettiin kokonaisuudessaan hyvin harvoin sensitiivistä dataa, jolloin viestityyppien välilläkään ei esiinny suuria eroavaisuuksia.

Tietojenkalasteluviestin kaikkien ilmoittamisten osalta saatiin nollahypoteesin p-arvoksi 0.31 > 0.05. Tällöin nollahypoteesia ei voida hylätä, sillä tietojenkalasteluviestin ilmoituksissa ei esiintynyt merkittäviä eroja viestien tyyppien välillä. Tämä on mielenkiintoinen tulos, sillä ensimmäisen toissijaisen tutkimuskysymyksenkin oletettuna tuloksena oli, että kohdennetun

tietojenkalasteluviestin kohdalla esiintyisi aktiivisempaa ilmoituksien luomista, kuin geneerisemmän tietojenkalasteluviestin.

Ensimmäisen aallon vaihtoehtoisen hypoteesin osalta voidaan havaita tilastollisesti merkittäviä eroja, joissa p-arvo oli alle 0.01, kaikissa testatuissa kohdissa, paitsi: *"Syöttivät sensitiivisen datan mobiililaitteella"*, *"Ilmoittivat tietojenkalasteluviestin"*, *"Eivät avanneet linkkiä, eivätkä ilmoittaneet" ja "Eivät avanneet linkkiä ja ilmoittivat"*. Tällöin poikkeavia kohtia lukuun ottamatta, voimme hyväksyä vaihtoehtoisen hypoteesin ensimmäisen aallon osalta. *"Syöttivät sensitiivisen datan mobiililaitteella"*-kohdan kohdalla tilastollisesti merkittävien erojen puute selittyy samoilla syillä, kuin ensimmäisen aallon nollahypoteesissäkin. *"Ilmoittivat tietojenkalasteluviestin"* kohdalla ei voitu hylätä nolla hypoteesia, eikä hyväksyä vaihtoehtoista hypoteesia, jonka perusteella vaikuttaa, ettei ensimmäisen aallon kohdalla esiintynyt tilastollisesti merkittävää eroa viestityyppien välillä siinä tehtiinkö niistä ilmoitusta. *"Eivät avanneet linkkiä, eivätkä ilmoittaneet"*- kohdalla ei voida hyväksyä vaihtoehtoista hypoteesia, mutta voitiin hylätä nollahypoteesi. Ensimmäisen aallon kohdalla henkilöiden määrä, jotka eivät avanneet, eivätkä luoneet ilmoitusta geneerisestä viestistä oli suurempi, kuin kohdennetun viestin kohdalla. Tällöin viestien välillä esiintyi kyllä merkittävä tilastollinen ero, mutta toisin päin, kuin hypoteesi. Tämä voidaan selittää ainakin osittain sillä, että geneerinen viesti on todennäköisemmin huomattu tietojenkalasteluksi hyvin nopeasti, jonka jälkeen vastaanottaja on todennäköisesti vain poistanut sen ilman muita toimenpiteitä. *"Eivät avanneet linkkiä ja ilmoittivat"* – kohdan osalta ei myöskään voida hyväksyä vaihtoehtoista hypoteesia, mutta voitiin hylätä nollahypoteesi. Samoin kuin *"Eivät avanneet linkkiä, eivätkä ilmoittaneet"*- kohdalla, niin myös tällä kohdalla linkin avaamattomuus oli määrällisesti suurempi geneerisen viestin vastaanottajilla, joka on myös tämän kohdan kohdalla todennäköisesti aiheutunut siitä, että geneerinen viesti on helpommin tunnistettavissa, kuin kohdennettu tietojenkalasteluviesti.

Toisen aallon nollahypoteesin testeistä voidaan havaita merkittävä tilastollinen ero viestien välillä kaikissa kohdissa, paitsi: *"Syöttivät sensitiivisen datan mobiililaitteella"*, *"Ilmoittivat tietojenkalasteluviestin"*, *"Eivät avanneet linkkiä ja ilmoittivat"*, sekä *"Syöttivät sensitiivistä dataa ja eivät ilmoittaneet"*. Kahden ensimmäisen poikkeavan kohdan kohdalla tilastollisesti merkittävien erojen puute selittyy samoilla syillä, kuin ensimmäisen aallon nollahypoteesissäkin. *"Eivät avanneet linkkiä ja ilmoittivat"*- kohdan poikkeama johtuu jälleen siitä, että geneeristä tietojenkalasteluviestiä avattiin huomattavasti vähemmän, kuin kohdennettua. Lisäksi toisen tietojenkalasteluaallon yhteydessä organisaation pikaviestintäsovelluksessa käytiin paljon keskustelua, jossa monet olivat huomanneet yhtäläisyyksiä edelliseen tietojenkalasteluaaltoon ja tajunneet, että kyseessä hyvin todennäköisesti oli simulaatio. Tällöin on todennäköistä, että keskustelun lukeneet henkilöt ovat myös jättäneet ilmoituksen tekemättä, kun kyseessä ei näennäisesti ollut oikea tietojenkalastelu.

Toisen aallon vaihtoehtoisen hypoteesin testistä voidaan havaita merkittävä tilastollinen ero viestien välillä kaikissa kohdissa, paitsi: *"Ilmoittivat tietojenkalasteluviestin"*, *" Eivät avanneet linkkiä, eivätkä ilmoittaneet"*, *" Eivät avanneet linkkiä ja ilmoittivat" ja " Syöttivät sensitiivistä dataa ja eivät ilmoittaneet"*. Myös toisen

aallon kohdalla esiintyi siis tilanne, jossa ei voitu hylätä nolla hypoteesia, eikä hyväksyä vaihtoehtoista hypoteesia. Tällöin tulokset osoittavat molempien aaltojen puolesta sitä, ettei tietojenkalasteluviestin tasolla ollut vaikutusta siihen, luotiinko siitä ilmoitusta.

Aikaisemmista hypoteeseista poiketen toisen aallon vaihtoehtoisen hypoteesin testissä esiintyi tilastollisesti merkittävä ero viestien välillä siinä, syötettiinkö sensitiivistä dataa mobiililaitteella. On kuitenkin huomioitava, että toisessa aallossa geneerisen viestin vastaanottajista vain yksi syötti sensitiivistä dataa mobiililaitteella ja vain kaksi kohdennetun tietojenkalasteluviestin saaneista syötti sensitiivistä dataa mobiililaitteella. Kohdasta: *"Eivät avanneet linkkiä, eivätkä ilmoittaneet"* saatiin nollahypoteesin p-arvoksi 2.021e-06 ja vaihtoehtoisen hypoteesin p-arvoksi 1. Tällöin tämän kohdan nollahypoteesi voidaan hylätä, mutta vaihtoehtoista hypoteesia ei voida hyväksyä. Samoin, kuin ensimmäisen aallon kohdalla henkilöiden määrä, jotka eivät avanneet, eivätkä luoneet ilmoitusta geneerisestä viestistä oli suurempi, kuin kohdennetun viestin kohdalla. Tällöin viestien välillä esiintyi kyllä merkittävä tilastollinen ero, mutta toisin päin, kuin hypoteesi. Tämä voidaan selittää samoin kuin ensimmäisen aallon kohdalla, eli geneerisen viestin tunnistaminen on todennäköisempää. Lisäksi, samoin kuin toisen tietojenkalasteluaallon nollahypoteesissa, organisaation pikaviestintäsovelluksessa käytiin paljon keskustelua, jossa monet olivat huomanneet yhtäläisyyksiä edelliseen tietojenkalasteluaaltoon ja tajunneet, että kyseessä hyvin todennäköisesti oli simulaatio. Tällöin on todennäköistä, että keskustelun lukeneet henkilöt ovat myös jättäneet ilmoituksen tekemättä, kun kyseessä ei näennäisesti ollut oikea tietojenkalastelu.

5 POHDINTA

Tässä luvussa käydään tarkempaa pohdintaa tutkimuksen tuloksista, sekä vastataan tämän tutkimuksen tutkimuskysymyksiin ja toissijaisiin tutkimuskysymyksiin:

1) ”Miten suomalaisen IT-alan organisaation työntekijät reagoivat heihin kohdistuvaan tietojenkalasteluun?”

2) ”Onko kohdennetun ja geneerisen tietojenkalastelunviestin välillä eroja kalastelun onnistumisessa?”

3) ”Onko kohdennetun ja geneerisen tietojenkalasteluviestien välillä eroa siinä, luodaanko niistä ilmoitusta?”

4) ”Vaikuttaako tietojenkalastelun onnistumiseen se, avataanko viesti mobiililaitteella?”

Molempien tietojenkalasteluaaltojen yhteydessä käytiin aktiivista keskustelua organisaation pikaviestintäsovelluksessa. Sovelluksessa käyty keskustelu oli hyvin vapaamuotoista ja osittain tämän vuoksi kummankaan aallon kohdalla ei jaettu kuvaa molemmista tietojenkalasteluviesteistä, joskin molempia kyllä kuvailtiin sanallisesti. Organisaation käyttäessä pikaviestintäsovellusta, jossa kuvien jakaminen on mahdollista, voisi olla käytännöllistä valtuuttaa yksi tai muutama henkilö tiedottamaan tämän kaltaisista turvallisuusuhista myös käytetyn pikaviestintäsovelluksen kautta. Tiedotuksessa olisi hyvä olla myös mukana kuvat tietojenkalasteluviesteistä, sekä ohjeet siitä miten toimia näiden viestien kohdalla.

Osana tutkimusta tehtyjen haastatteluiden perusteella vaikuttaa, että tietojenkalasteluviestin ilmoittamisen todennäköisyyteen vaikuttaa se, kuinka helpoksi ilmoittaminen koetaan. Mikäli tietojenkalastelun ilmoittaminen ei ollut haastatellulle selkeää, tai se koettiin vaivalloiseksi, niin ilmoittaminen jätettiin yleensä tekemättä. Tämä ilmiö vaikutti korostuneen, mikäli haastateltu oli lukenut tietojenkalasteluviesteistä keskustelua organisaation pikaviestintäsovelluksesta ja todennut että asia on jo hoidossa. Tämä tukee aikaisempia tutkimuksia, joiden mukaan tietojenkalasteluviestien ilmoittamiseen vaikuttaa mm. koettu

minäpystyvyys tietojenkalastelun ilmoittamiseen liittyen (Kwak ym., 2020, s. 10). Osassa keskustelua käytiin lisäksi spekulaatiota siitä, että kyseessä olisi ollut simulaatio. Myös tämä saattaa aikaisemman tutkimuksen mukaan saada henkilöt olemaan tekemättä ilmoituksia, vaikka he olisivat syöttäneet sensitiivistä dataa, sillä he ajattelevat, että asia on jo organisaation tietoturvasta vastaavalla taholla tiedossa (Volkamer ym., 2020).

Molempien tietojenkalasteluaaltojen aikana käytiin organisaation sisällä keskustelua ja jaettiin informaatiota saaduista tietojenkalasteluviesteistä. Organisaatiossa ei kuitenkaan vaikuttanut olevan mitään tiettyä kanavaa, jossa asiasta olisi tiedotettu, tai tahoa, jonka vastuulla tiedottaminen olisi. Voidaan olettaa, että tämän vuoksi tieto tapahtuvasta massiivisesta tietojenkalasteluaallosta ei saavuttanut organisaation henkilöstöä tarpeeksi nopeasti. Ensimmäisen tietojenkalasteluaallon kohdalla organisaation henkilöstöhallinto, oli julkaissut aiheesta blogin, organisaation sisäiselle verkkosivulle. Tätä ratkaisua voisikin johtaa eteenpäin siten, että organisaatiolla voisi olla sisäisen pikaviestintäsovelluksensa sisällä oma kanava, johon kuvia ja tietoja saaduista tietojenkalasteluviesteistä voisi jakaa nopeammin.

Haastatteluiden perusteella vaikutti, että organisaation pikaviestintäsovelluksessa käydyllä keskustelulla oli ollut vaikutusta siihen, miten tietojenkalasteluviesteihin reagoitiin. Haastatelluista ainakin yhdelle pikaviestintäsovelluksessa käyty keskustelu oli vaikuttanut tietojenkalasteluviestin nopeaan tunnistamiseen. Pikaviestintäsovellus onkin todennäköisesti tehokkaampi tapa levittää tietoa tapahtuvasta tietojenkalastelusta, sillä se todennäköisemmin on useammalla henkilöllä auki muutenkin työssä käytettävänä kommunikaatiovälineenä, jolloin he saavat sen kautta ilmoituksia nopeammin myös tietojenkalastelusta.

Molempien tietojenkalasteluaaltojen ilmoituksista kävi ilmi, ettei organisaatiolla ollut mitään yksittäistä kanavaa tietojenkalastelun ilmoittamista varten. Osa ilmoituksista tehtiin lähettämällä sähköposteja ja osa tehtiin organisaation sisäisen portaalin kautta. Tietojenkalasteluaaltojen tulokset osoittivat, että organisaation sisällä ei vaikuta olevan tarkkaa määrittelyä, siitä miten ja mihin tämän kaltaiset tietoturvauhat kuuluisi ilmoittaa. Tarkan tietämyksen puutteen takia, ilmoituksia tietojenkalastelusta tehtiin pääasiallisesti ainakin neljään eri paikkaan:

- Organisaation sisäisen tiketti järjestelmään
- Organisaation tietohallinnon sähköpostiin
    - Tämä kuitenkin aiheuttaa organisaatiolle ylimääräistä vaivaa, sillä tietohallinnon työntekijät joutuivat lähettämään ilmoituksia eteenpäin organisaation sisäiselle tietoturvalle.
- Organisaation tietoturvan sähköpostiin
- Organisaation käyttämän Outlook palvelun ”report phishing”-napin avulla
    - Tästä kuitenkaan ei valitettavasti saatu dataa ensimmäisessä aallossa aikaisemmin mainittujen tietoteknisten ongelmien vuoksi.

Neljän ilmoituskanavan vuoksi, joitain ilmoituksia lähetettiin edelleen kohteesta toiseen vieden enemmän työaikaa, kuin olisi tarpeellista. Hukatun työn lisäksi monet henkilöt olivat välittäneet tietojenkalastelusimulaatiosta saamansa viestin lähettämällä sen edelleen organisaation tietoturvalle, tietohallinnolle, tai muulle ryhmälle, tai jollekin kombinaatiolle näistä kolmesta. Tietojenkalasteluviestin edelleen lähetys useaan eri paikaan on hyvin ongelmallinen tapa reagoida pahantahtoisiin sähköposteihin. Organisaation työntekijöiden todennäköisenä tarkoituksena on ollut levittää tietoa tapahtuvasta tietojenkalastelusta, mutta edelleen lähettämällä tietojenkalasteluviestit sellaisenaan, he myös suurensivat tietojenkalastelun osuma-alaa. Tämän takia, myös muut henkilöt, jotka eivät muulloin olisi välttämättä saaneet tiettyä tietojenkalasteluviestiä, altistuivat nyt tälle tietojenkalasteluviestille.

Parhaimmassa tapauksessa organisaation sisällä olisi yksi tietty paikka, johon saaduista tietojenkalasteluista voitaisiin ilmoittaa. Tämän kaltainen tietty paikka voisi olla esimerkiksi organisaation tietoturvasta vastaavan osaston hallinnoiva sähköpostilaatikko, johon saadut tietojenkalasteluviestit voitaisiin suoraan lähettää (Hadnagy ym., 2015, s. 123). Tämän kaltaisen kohdennetun postilaatikon etuna on se, että vaikka viestejä edelleen lähetetään yhä, niin tämän postilaatikon avaaja tietää varmasti, että kaikki sisältö siellä on todennäköisesti haitallista ja osaa suhtautua siihen asian mukaisesti.

Tutkimuksen tulosten tilastollisia eroja tarkastellessa voitiin huomata, että viestien kohdentamisella vaikutti olevan merkittävä tilastollinen ero siinä, avattiinko kalasteluviestin sisältämä linkki ja syötettiinkö laskeutumissivustolle sensitiivistä dataa. Tässä tutkimuksessa geneerisempi tietojenkalasteluviesti oli viesteistä ainoa, joka sisälsi sisään rakennetun uhan (tunnusten menettämisen) ja kohdennetumpi tietojenkalasteluviesti sisälsi potentiaalisen hyödyn (työajanseurantajärjestelmän uuden ohjeistuksen saaminen). Tällöin tutkimuksen tulokset eivät tue (Goel ym., 2017) viitettä (Kahneman & Tversky, 1979) prospekti teoriaan, jonka mukaan potentiaalinen uhka vaikuttaisi ihmisten toimintaan enemmän, kuin potentiaalinen hyöty myös tietojenkalasteluviesteissä. Tämän tutkimuksen kohdennetumpi tietojenkalasteluviesti oli myös tilannesidonnainen henkilöstön arkeen, sillä työajanseurantajärjestelmä on relevantti kaikille työntekijöille. Tällöin sen todennäköisempi onnistuminen tukee (Goel ym., 2017) tutkimusta, jonka mukaan tietojenkalasteluviestit jotka viittaavat vastaanottajille relevantteihin asioihin lisäävät todennäköisyyttä, että tietojenkalastelu onnistuu.

Tutkimuksen tulosten tilastollisia eroja tarkastellessa voitiin huomata, ettei viestien kohdentamisella vaikuttanut olevan merkittävää tilastollista eroa siinä luotiinko ilmoitus. Tietoturvakoulutuksissa lähtökohtaisesti opetetaan, että mikäli henkilö tunnistaa tietojenkalasteluviestin, niin hänen tulee siitä tehdä ilmoitus tietoturvasta vastaavalle taholle. Tilastollisten erojen puute on kuitenkin mielenkiintoista, sillä tutkimuksen tulosten perusteella kohdennetumman tietojenkalasteluviestin kohdalla esiintyi huomattavasti enemmän vuorovaikutusta, kuin geneerisen viestin kohdalla. Kuten edellisessäkin kappaleessa todettiin, niin organisaation työntekijät avasivat kohdennetumman tietojenkalasteluviestin sisältämiä linkkejä, sekä syöttivät linkin takana olleelle laskeutumissivustolle

sensitiivistä dataa tilastollisesti merkittävästi enemmän, kuin geneerisen viestin kohdalla. Tällöin voitaisiin olettaa, että siitä myös olisi luotu enemmän ilmoituksia etenkin organisaation sisäisen tiketti järjestelmän, tai sähköpostin välityksellä, joissa molemmissa tietojenkalastelu viesteistä ja mahdollisesta linkkien avaamisesta, sekä sensitiivisen datan syöttämisestä voisi kertoa sanallisesti, mutta datan perusteella viestien välillä ei ilmennyt tilastollisesti merkittävää eroa ilmoitusten tekemisessä.

Ensimmäisen tietojenkalasteluaallon pohjalta vaikutti, että tietojenkalasteluviestin sisältämän haitallisen linkin avaamiseen vaikutti se, mikäli viesti oli avattu mobiililaitteella. Ensimmäisessä aallossa kohdennetun tietojenkalasteluviestin linkin oli kaiken kaikkiaan avannut 75 henkilöä. Näistä 75 henkilöstä 31 henkilöä, eli 41 % kaikista linkin avaajista, oli avannut viestin ainakin kerran mobiililaitteella. Geneerisen viestin vastaanottajista oli ensimmäisessä tietojenkalasteluaallossa 17 avannut viestin sisältämän linkin, ja näistä 12, eli 70 % kaikista avaajista, oli tehnyt sen ainakin kerran mobiililaitteella.

Toisaalta toisesta tietojenkalasteluaallosta saadut tulokset poikkesivat ensimmäisen aallon tuloksista. Toisessa tietojenkalasteluaallossa kohdennetun viestin linkin oli avannut 66 henkilöä, joista 15 oli tehnyt sen mobiililaitteella. Tällöin kaikista viestin linkin avanneista 22 % oli avannut linkin ainakin kerran käyttäen mobiililaitetta. Toisen aallon geneerisen viestin vastaanottajista 11 oli avannut viestin sisältämän linkin ja näistä 1, eli 9 % kaikista avaajista, oli avannut sen ainakin kerran mobiililaitteella.

6 JOHTOPÄÄTÖKSET

Tässä luvussa tehdään lyhyt yhteenveto tutkielmasta ja sen löydöksistä. Tämän lisäksi luvussa käsitellään tutkimuksen vahvuuksia ja rajoitteita liittyen tutkimuksen validiteettiin ja reliabiliteettiin, mahdollisia jatkotutkimus aiheita, sekä käytännön sovellutuksia, joihin tätä tutkimusta voidaan hyödyntää.

6.1 Tutkimuksen kontribuutiot

Tässä tutkimuksessa kerätty data on laaja-alaista. Aikaisemman tutkimuksen mukaan tietojenkalastelukampanjoissa kannattaisi mitata ainakin kuutta eri asiaa (Hadnagy ym., 2015, s. 124). Nämä kuusi asiaa ovat:

- Henkilöiden määrä, jotka avasivat tietojenkalastelulinkin
- Henkilöiden määrä, jotka ilmoittivat tietojenkalasteluviestit
- Henkilöiden määrä, jotka avasivat tietojenkalastelulinkin, mutta eivät ilmoittaneet
- Henkilöiden määrä, jotka avasivat tietojenkalastelulinkin ja ilmoittivat siitä
- Henkilöiden määrä, jotka eivät avanneet tietojenkalastelulinkkiä, mutta eivät myöskään ilmoittaneet sitä
- Henkilöiden määrä, jotka eivät avanneet tietojenkalastelulinkkiä ja eivät myöskään ilmoittaneet

Tässä tutkimuksessa kyettiin keräämään dataa kaikista näistä osa-alueista ja käsittelemään sitä. Vaikka teknisistä ongelmista johtuneiden vaikeuksien vuoksi ei tutkimuksessa saatu täyttä tietoa Outlookin ”report phishing”- napin kautta tehdyistä ilmoituksista, niin muu data tehdyistä ilmoituksista antaa hyvän kuvan siitä kuinka aktiivista organisaation sisäinen tietojenkalasteluviestien ilmoittaminen on. Tutkimuksen data on myös kerätty hyvin luonnollisissa olosuhteissa.

Tämä tarkoittaa sitä, että simuloidun tietojenkalastelun uhrit eivät olleet tietoisia tulevasta tietojenkalastelusta, jolloin he myös todennäköisemmin reagoivat luonnollisemmin tietojenkalasteluviesteihin. Tutkimuksessa pystyttiin myös keräämään dataa haastatteluiden avulla henkilöiltä, jotka olivat saaneet tietojenkalasteluviestejä simulaation aikana. Näiden haastatteluiden avulla voitiin löytää selittäviä tekijöitä ihmisten käyttäytymiselle, heidän kohdatessaan tietojenkalasteluviestejä ja syitä miksi ihmiset loivat, tai eivät luoneet ilmoituksia.

Tutkimuksen laajasta datasta pystyttiin löytämään uutta tietoa asioista, jotka vaikuttavat ihmisten käyttäytymiseen heidän kohdatessaan tietojenkalasteluviestejä. Tutkimuksessa löydettiin näyttöä siitä, että pikaviestintäsovelluksissa käydyillä keskusteluilla vaikutti olevan positiivinen vaikutus tietojenkalasteluviestien tunnistamiseen, mutta negatiivinen vaikutus niiden ilmoittamiseen. Tämä negatiivinen vaikutus myös tukee aikaisempaa tutkimusta, jonka mukaan henkilöt saattavat jättää ilmoituksen tekemättä ajatellessaan, että asia on jo tullut ilmi (Volkamer ym., 2020). Tutkimuksen datan perusteella voitiin löytää uutta tietoa siitä, että pikaviestintäsovellukset olivat tehokkaampi tapa välittää tietoa tapahtuvasta tietojenkalastelusta, kuin esimerkiksi sisäisen verkon blogi kirjoitukset.

Tutkimuksen datan analysoinnissa havaittiin tilastollisia eroja, joiden tulokset vahvistivat osaltaan aikaisempien tutkimusten havaintoja. Tämän tutkimuksen datan tilastolliset erot tukevat Goelin ym. (2017) tutkimuksen tuloksia, jonka mukaan vastaanottajalle relevantit tilannesidonnaisuudet lisäävät tietojenkalastelun onnistumista. Lisäksi tämän tutkimuksen datasta ilmeni uusia tuloksia, jotka poikkesivat aikaisemmin havaituista tuloksista. Tämän tutkimuksen tulosten mukaan potentiaalisen hyödyn sisältämä viesti oli huomattavasti tehokkaampi, kuin potentiaalisen menettämisen sisältämä viesti, joka taas poikkeaa Goelin ym. (2017) viitteestä Kahnemanin & Tverskyn (1979) prospekti teoriaan tietojenkalastelussa. Tutkimuksen datan analysoinnista löydettiin myös uutta tietoa siitä, että tietojenkalasteluviestin kohdentamisella ei ollut vaikutusta siihen luotiinko tietojenkalasteluviestistä ilmoitusta.

6.2 Tutkimuksen käytännön sovellutukset

Tämän tutkimuksen pohjalta voidaan tunnistaa muutamia merkittäviä käytännön sovellutuksia. Tämän tutkielman pohjalta organisaatiot voivat ymmärtää paremmin tietojenkalastelun merkittävyyttä yleiselle tietoturvalle. Tutkielman pohjalta organisaatiot voivat lisäksi kehittää organisaation sisäisiä ilmoituskäytäntöjä, sekä kehittää koulutuksia ilmoittamisen tärkeydestä. Tämän lisäksi tutkielmaa voi käyttää apuna tietoturvakoulutuksien sisältöjen, sekä yleisten tietoturva mekanismien suunnittelussa. Tutkimusta voidaan myös hyödyntää tulevissa tietojenkalastelusimulaatioissa, sekä tietojenkalasteluun liittyvissä tutkimuksissa. Tämän tutkimuksen pohjalta voidaan löytää lisätutkimuksiin näkökulmia ja erilaisia lähtökohtia. Jatkotutkimuksiin liittyviä pohdintoja on avattu tarkemmin luvussa 7.2.

6.3 Tutkimuksen rajoitteet ja jatkotutkimus

Tässä tutkimuksessa päästiin kuitenkin haastattelemaan ainoastaan neljää henkilöä, jotka olivat saaneet tietojenkalasteluviestin osana simulaatiota. Nämä haastattelut kuitenkin rajoittuivat vain neljään henkilöön. Aikaisempien tutkimusten perusteella 12 haastattelulla voidaan saavuttaa koodi saturaatio käsiteltävästä datasta ja kuudella haastattelulla voidaan tunnistaa datassa olevia metateemoja (Guest ym., 2006, s. 74). Tällöin pelkästään haastatteluiden perusteella ei täydellisiä johtopäätöksiä voida tehdä, mutta haastatteluiden avulla voidaan tukea tutkimuksen muuta dataa. Tämän lisäksi kukaan haastatelluista ei ollut syöttänyt sensitiivistä dataa tietojenkalasteluviestien laskeutumissivulle. Tällöin haastatteluiden avulla ei voitu myöskään selvittää esimerkiksi syitä, jotka johtivat sensitiivisen datan syöttämiseen.

Tämän tutkimuksen tietojenkalastelusimulaatio kohdistui suomalaiseen IT-palvelutaloon, jonka vuoksi huomattava osa tietojenkalasteluviestin saaneista henkilöistä oli IT- alan ammattilaisia. Tulevissa tutkimuksissa voisikin olla mielekästä valita organisaatio, jonka sisällä olisi suurempaa hajontaa liiketoimintojen välillä. Tällöin saadun datan pohjalta voisi tutkia miten ihmiset eri työtehtävissä ja eri liiketoiminta-aloilla reagoivat tietojenkalasteluviesteihin.

Osana tämän tutkimuksen tietojenkalastelusimulaatiota ei myöskään käytetty tietojenkalasteluviestejä, jotka sisältäisivät liitetiedostoja. Jatkotutkimuksissa voitaisiinkin tutkia henkilöiden käyttäytymistä, kun he vastaanottavat liitetiedostoja sisältävän tietojenkalasteluviestin.

Tämän tutkimuksen rajoitteena on myös se, että tämän tutkimuksen hyökkääjällä on epäluonnollisen paljon tietoa kohteestaan. Toisin sanoen hyökkääjä ei käytä avointen lähteiden tiedustelua hyödykseen kartoittaessaan kohdetta. Tämän takia hyökkäyksen kohteiden määrä on luonnottoman suuri tämän tutkimuksen tietojenkalastelusimulaatiossa. Tulevaisuudessa voisi olla hyvin mielenkiintoista, mikäli tutkimusta olisi mahdollista suorittaa jossakin valtiollisessa organisaatiossa. Valtiolliset organisaatiot ovat lisäksi avainasemassa yleisen turvallisuuden kannalta, jonka vuoksi niiden sisäistä resilienssiä voisi olla mielenkiintoista päästä tutkimaan. Valtiolliseen organisaatioon voisi tässä tutkimustapauksessa myös suorittaa avointen lähteiden tiedustelua, jolla voitaisiin selvittää, kuinka suuri näkyvyys valtiollisilla organisaatioilla on mahdollisille hyökkääjille.

Osana tätä tutkimusta ei myöskään suoritettu koulutusta henkilöstölle. Tulevaisuudessa voisi olla mielenkiintoista suorittaa tietojenkalastelusimulaatiot siten, että niiden välissä olisi aikaa tuottaa jonkin näköinen koulutus liittyen tietojenkalasteluviesteihin. Koulutuksen jälkeen voisi lähettää samat, tai hyvin samantyyliset, tietojenkalasteluviestit uudelleen, jolloin voitaisiin saada hyvin mielenkiintoista tietoa siitä, kuinka hyvin koulutus vaikuttaa tietojenkalasteluviestien onnistumiseen.

Tämän tutkimuksen perusteella tarvitaan myös lisätutkimusta siihen, miten mobiililaitteilla viestien avaaminen vaikuttaa tietojenkalastelun onnistumiseen. Tämän tutkimuksen tulokset antoivat viitteitä sille, että mikäli viesti

avataan mobiililaitteella, niin olisi todennäköisempää, että myös viestin sisältämä linkki avattaisiin. Kuitenkin tämän tutkimuksen osalta mobiililaitteilla viestin avanneiden määrä oli niin pieni, ettei siitä voitu vetää merkittäviä johtopäätöksiä.

LÄHTEET

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*, *25*(5), 593–613. https://doi.org/10.1108/ICS-03-2017-0009

Cialdini, R. B. (2001). Harnessing the Science of Persuasion. (Cover story). *Harvard Business Review*, *79*(9), 72–79.

Cialdini, R. B. (2007). *Influence: The psychology of persuasion* (Vsk. 55). Collins New York.

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

Digi- ja väestotietovirasto. (2022, lokakuuta 10). *Digiturvabarometrin tulokset herättävät huolen suomalaisten digiturvaosaamisen tasosta – "Nyt tarvitaan koulutusta"*. Digi- ja väestötietovirasto. https://dvv.fi/-/digiturvabarometrin-tulokset-herattavat-huolen-suomalaisten-digiturvaosaamisen-tasosta-nyt-tarvitaan-koulutusta

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

Privacy and Security - SOUPS '06, 79. https://doi.org/10.1145/1143120.1143131

Ebot, T., & Claude, A. (2017). *Explaining two forms of Internet crime from two perspectives: Toward stage theories for phishing and Internet scamming*.

European Union Agency for Cybersecurity. (2021). *ENISA threat landscape 2021: April 2020 to mid July 2021.* Publications Office. https://data.europa.eu/doi/10.2824/324797

Ferguson, A. J. (2005). *Fostering E-Mail Security Awareness: The West Point Carronade*. 4.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. Teoksessa T. Tryfonas & I. Askoxylakis (Toim.), *Human Aspects of Information Security, Privacy, and Trust* (ss. 36–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-20376-8_4

Fruhlinger, J. (2020). What is pretexting? Definition, examples and prevention. *CSO (Online)*. http://www.proquest.com/docview/2409429463/abstract/D8169814953F4791PQ/1

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44. https://doi.org/10.17705/1jais.00447

Gragg, D. (2003). *A Multi-Level Defense Against Social Engineering*. 21.

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Hadnagy, C., Fincher, M., & Dreeke, R. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=1895166

Herley, C. (2012). Why do Nigerian Scammers Say They are from Nigeria? *WEIS*.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81. https://doi.org/10.1145/2063176.2063197

Hyppönen, M. (2011, elokuuta 26). *How We Found the File That Was Used to Hack RSA*. https://archive.f-secure.com/weblog/archives/00002226.html

Hämäläinen, V.-P. (2021, tammikuuta 11). *Osta nyt, älä maksa koskaan*. Yle Uutiset. https://yle.fi/uutiset/3-11690670

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Johnson, P. E., Grazioli, S., Jamal, K., & Zualkernan, I. A. (1992). Success and failure in expert reasoning. *Organizational Behavior and Human Decision Processes*, *53*(2), 173–203. https://doi.org/10.1016/0749-5978(92)90061-B

Jones, H. S., Towse, J. N., & Race, N. (2015). Susceptibility to Email Fraud: A Review of Psychological Perspectives, Data-Collection Methods, and

Ethical Considerations. *International Journal of Cyber Behavior, Psychology and Learning*, *5*(3), 13–29. https://doi.org/10.4018/IJCBPL.2015070102

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263. https://doi.org/10.2307/1914185

Kohonen, I., Kuula-Luuml, A., & Spoof, S.-K. (2019). Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa. *Tutkimuseettinen neuvottelukunta*, 26.

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*, 101343. https://doi.org/10.1016/j.tele.2020.101343

Marttinen, V. (2022, syyskuuta 2). *Helsingin palkanmaksuongelmat jatkuvat vielä pitkälle syksyyn – suurin väärin maksettu summa on ollut 280 000 euroa*. Yle Uutiset. https://yle.fi/uutiset/3-12602968

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, *55*, 114–127. https://doi.org/10.1016/j.cose.2015.09.001

Nieminen, P. (2022). *Yksi parhaita mitä on tullut vastaan. Huuhkajien logo, kenraalipääjohtajapäällikkö ja kaikki! Ei puutu enää kun amiraalikenraali Aladin:in allekirjoitus….* https://www.linkedin.com/posts/petenieminen_phishing-kalastelu-cybersecurity-activity-6948530713562382336-8Yii/?trk=public_profile_like_view&originalSubdomain=fi

Ollmann, G. (2007). The Phishing Guide Understanding & Preventing Phishing Attacks. *IBM Internet Security Systems*, 3–4.

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, *54*(3), 70–75. https://doi.org/10.1145/1897852.1897872

Traficom. (2021). *Tietoturvan vuosi 2021*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2021.pdf

Uurtimo, J. (2022). *Pop-pankki kalasteluviesti kuvan kaappaus*.

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*, 12.

Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. Teoksessa I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, & A. Sasse (Toim.), *Computer Security* (Vsk. 12580, ss. 312–328). Springer International Publishing. https://doi.org/10.1007/978-3-030-66504-3_19

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. *IEEE Transactions on Professional Communication*, *55*(4), 345–362. https://doi.org/10.1109/TPC.2012.2208392

Warburton, D., & Pompon, R. (2019). *2019 PHISHING AND FRAUD REPORT*. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

Your Europe. (2022, heinäkuuta 6). *Data protection under GDPR*. Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm