Janina Välimaa

TIETOJENKALASTELUHYÖKKÄYKSET SUOMESSA – HYÖKKÄÄJÄN NÄKÖKULMA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Välimaa, Janina
Tietojenkalasteluhyökkäykset Suomessa – Hyökkääjän näkökulma
Jyväskylä: Jyväskylän yliopisto, 2023, 72 s.
Tietojärjestelmätiede, pro gradu –tutkielma
Ohjaaja: Siponen, Mikko

Tietojenkalastelu on yksi suurista kyberuhista jokapäiväisessä elämässä. Koska tietoturvan heikoin lenkki ei usein niinkään ole järjestelmä vaan käyttäjä, tietojenkalastelu on vaivattomuutensa vuoksi suosittu tekniikka, joka iskee tietoturvan heikoimpana pidettyyn lenkkiin. Tietojenkalastelu on noussut merkittäväksi tutkimusaiheeksi verkkopohjaisten palveluiden yleistyessä ja sitä on tutkittu yleisellä tasolla paljon. Tietojenkalastelun tutkimuskentällä on kuitenkin aukko, sillä tietojenkalastelua ei ole tutkittu hyökkääjän näkökulmasta kattavasti esimerkiksi peilaten hyökkäysten taustatekijöitä tai jälkipuintia. Tässä tutkimuksessa tietojenkalastelua tutkittiin hyökkääjän näkökulmasta tavoitteena selvittää mitkä taustatekijät motivoivat hyökkääjää toteuttamaan hyökkäyksiä, miten tekniikka mahdollisesti ajan saatossa kehittyi ja miten hyökkääjät kävivät läpi hyökkäystä toteutettuaan sen. Tutkimus toteutettiin empiirisenä laadullisena tutkimuksena, jonka aineisto kerättiin osittain strukturoitujen haastatteluiden avulla. Tutkimustuloksille tehtiin sisällönanalyysi yksinkertaistamalla haastatteluaineistoa ja lopulta ryhmittelemällä ne. Tutkimustuloksia verrattiin aiempaan tieteelliseen kirjallisuuteen. Tutkimuksessa huomattiin, että hyökkäyksiin johtavat taustatekijät olivat erilaisia, joskin myös yhteisiä tekijöitä, kuten raha, osin havaittiin. Tutkimuksen otannan perusteella tietojenkalastelun hyökkäystekniikat myös kehittyivät hieman. Hyökkääjät kuitenkin jälkipuivat hyökkäyksiään ja pyrkivät neutralisoimaan niitä. Tulosten perusteella todettiin, että tietojenkalastelun prosessi noudattaa usein samaa kaavaa kuin aiemmissa tutkimuksissa, yhtä poikkeusta lukuun ottamatta.

Asiasanat: tietojenkalastelu, tietoturva, tietojenkalasteluhyökkäykset, hyökkääjä

ABSTRACT

Välimaa, Janina
Phishing attacks in Finland – Attackers' viewpoint
Jyväskylä: University of Jyväskylä, 2023, 72 pp.
Information Systems Science, Master's Thesis
Supervisor: Siponen, Mikko

Phishing is a significant threat in everyday life. Because the weakest link in cybersecurity is often not the system but the user, phishing, due to its technical effortlessness, is a popular method that targets this weakness. Due to the rise of web-based services, phishing has become a significant topic of research and has been generally well researched. Despite this, there is still a gap in the research, for phishing has not yet been sufficiently researched from the perspective of the attacker, taking into account the background and aftermath of the attacker. In this study, phishing was observed from the perspective of the attacker in order to shed light on what factors motivate attackers to perform phishing, how phishing techniques may have evolved over time and how attackers may have reflected on their actions. This study was carried out as an empirical qualitative study with data collected from semi-structured interviews. The results were analyzed by simplifying the interview data and then categorizing it. The results were compared with previous studies on the subject. In this study we concluded that the background factors of attackers were varying, but that certain shared motivators, such as money, were observed. Techniques used in phishing have slightly evolved according to our observations. Attackers reported aftermath and attempted to neutralize the consequences of their attacks. Based on our results we state that the process of phishing still adheres to the same principles that have been previously documented in the scientific literature, excluding one case.

Keywords: phishing, information security, phishing attacks, attacker

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Informaatioteknologian tutkimuksessa nousee esiin tietojenkalastelu usein joko siitä näkökulmasta miksi kohteet lankeavat tietojenkalasteluun tai tietojenkalastelun prosessin ja tyyppien näkökulmasta. Hyvin vähän tutkimusta kuitenkin löytyy tietojenkalastelijan näkökulmasta.

Suomen kyberturvallisuuskeskuksen (2022) raportissa todettiin, että yksistään pankkitunnuksiin kohdistuneista tietojenkalasteluhyökkäyksistä koitui Suomessa yli kahdeksan miljoonan euron menetykset. Tietojenkalastelu on siis merkittävä uhka kyberturvallisuuden kentällä, mutta mitä tietojenkalastelu sitten oikeastaan on? Yangin, Zhaon ja Zengin (2019) mukaan tietojenkalastelu on kriittinen kasvava uhka kybermaailmassa, jonka tavoitteena on varastaa sensitiivistä informaatiota hyökkäyksen kohteilta. Tutkijoiden mukaan tietojenkalastelu on myös yksi yleisimmistä metodeista verkkohyökkäyksissä ja se pyrkii aiheuttamaan tietoturvavuotoja, identiteettivarkauksia ja taloudellisia menetyksiä. Tietojenkalastelu kehittyy jatkuvasti eikä rajoitu enää vain sähköpostin kautta tehtyihin tietojenkalasteluihin vaan esimerkiksi myös QR-koodeihin pohjautuvaa tietojenkalastelua, kohdennettua tietojenkalastelua ja mobiiliapplikaatiohuijauksia esiintyy. (Yang ym., 2019).

Yhä suurempi osa vuorovaikutuksesta ja palveluista on verkkopohjaisia, jonka vuoksi yhä suurempi osa ihmisistä hyödyntää verkkopalveluja yhä useammin. Tietojenkalastelua on tutkittu paljon sen tekniikoiden ja kohteiden näkökulmasta, muttei niinkään hyökkääjän näkökulmasta. Tutkimuskentällä on siis selkeä tutkimusaukko. Tämän tutkimuksen tavoitteena on tutkia tietojenkalastelua Suomessa hyökkääjän näkökulmasta rajaten aihe hyökkäyksen taustatekijöihin, tekniikkaan sekä jälkipuintiin, jotta ymmärrys hyökkääjän näkökulmasta lisääntyisi ja tulevaisuudessa tietojenkalastelua voisi ennaltaehkäistä tehokkaammin. Tutkimuksen tavoitteen saavuttamiseksi on asetettu kolme tutkimuskysymystä, jotka antavat tutkimukselle rajauksen:

1. Mitkä taustatekijät johtivat siihen, että tietojenkalasteluhyökkäyksiä ryhdyttiin toteuttamaan?
2. Mitä tekniikkaa hyökkääjät käyttivät ja miten se kehittyi ajan saatossa?

3. Tekivätkö hyökkääjät jälkipuintia hyökkäyksistään eli reflektoivatko he omia toimiaan?

Tutkielman teoreettinen pohja luotiin kirjallisuuskatsauksen kautta, jonka tavoitteena on syventyä tutkimusaiheeseen ja johdatella lukija varsinaiseen tutkimukseen. Kirjallisuuskatsauksessa etsittiin osin myös vastausta toiseen tutkimuskysymykseen, sillä tietojenkalastelutekniikoita on tutkittu aiemmassa tieteellisessä kirjallisuudessa paljon. Kirjallisuuskatsauksessa käsitelty lähdeaineisto koostuu pääosin vertaisarvioiduista artikkeleista sekä kirjoista, joihin on viitattu tutkimuksen aihealueella yleisesti paljon, mutta kirjallisuuskatsauksessa hyödynnettiin myös muutaman organisaation tilastollisia aineistoja. Aineiston keräämiseen hyödynnettiin Jyväskylän yliopiston tarjoamaa JYKDOK-palvelua, johon on koostettu kansainvälisiä artikkeleita ja kirjoja sekä Google Scholar-palvelua. Kirjallisuuskatsauksessa käytetyn aineiston laatua arvioitiin hyödyntäen teosten tieteellistä tasoa arvostelevaa Julkaisufoorumia (*https://www.tsv.fi/julkaisufoorumi/haku.php*).

Tutkielma pitää sisällään tiivistelmän suomeksi ja englanniksi, johdannon ja yhteenvedon, kolme sisältölukua pohjautuen aiempaan tieteelliseen kirjallisuuteen sekä tutkimusta ja sen tuloksia käsittelevät pääluvut. Kolmessa ensimmäisessä sisältöluvussa käsitellään aiheen tausta, joka johdattelee varsinaiseen tutkimukseen pyrkien antamaan teoreettisen pohjan tutkimuksen aiheeseen. Ensimmäinen sisältöluku käsittelee kyberhyökkäyksiä sivuten hieman myös kyberrikollisuutta. Toisessa sisältöluvussa käsitellään tietojenkalastelua ja kolmannessa kriminologiaa profiloinnin ja teorian näkökulmasta. Tutkimusta ja sen tuloksia käsittelevät pääluvut jakautuvat tutkimusmenetelmien, tutkimustulosten sekä tulosten tulkinnan ja pohdinnan esittelyyn.

Tutkimus toteutettiin empiirisenä laadullisena case- eli tapaustutkimuksena ja tutkimuksen aineisto analysoitiin sisällönanalyysin mukaisesti. Tutkimuksen aineisto kerättiin neljän haastattelun avulla. Haastattelut toteutettiin osittain strukturoituina haastatteluina, joissa etukäteen asetettiin vain muutamia haastattelua tukevia haastattelukysymyksiä. Haastatteluaineistolle tehtiin laadullinen sisällönanalyysi, jossa haastatteluaineisto yksinkertaistettiin ja aineistoissa esiin nousseita tutkimuskysymyksiin liittyviä seikkoja ryhmiteltiin.

Tutkimuksessa havaittiin, että tietojenkalasteluhyökkäyksiin johtavat taustatekijät ovat moninaiset. Tietojenkalasteluhyökkäystekniikat puolestaan noudattivat pitkälti samaa kaavaa yleisellä tasolla kuin aiemmassa tieteellisessä tutkimuksessa on havaittu. Jälkipuinnin osalta havaittiin, että hyökkääjät reflektoivat yleisellä tasolla hyökkäyksiä saman kaltaisesti, mutta toki sisältöerojakin löytyi.

2 KYBERHYÖKKÄYKSET

Digitaalisten teknologioiden laajan käyttöönoton myötä monet yhteiskunnan toiminnot ovat siirtyneet verkkoon. Digiyhteiskunnassa eläessä voidaan pohtia digitaalisten teknologioiden merkityksellisyyttä siitä näkökulmasta, kuinka paljon aikaa vietetään verkossa ja mihin digitaalisia teknologioita hyödynnetään. Esimerkiksi sosiaalisen vuorovaikutuksen, ostosten teon sekä laskujen maksamisen lisäksi myös liiketoiminnat ja teollisuus ovat siirtyneet hyödyntämään digitaalista teknologiaa, joka tarjoaa osaltaan mahdollisuuden digitaalisen teknologian hyödyntämiseen myös haitallisiin tarkoituksiin.

Kyberrikollisuus kattaa alleen monenlaista rikollisuutta eikä tarkkaa kuvausta ole todennäköisesti helppo luoda universaalisti. Huntonin (2009) mukaan onkin haastavaa määritellä raja kyberrikollisuuden ja perinteisen rikollisuuden välille, sillä tekniikoita voidaan kombinoida monella eri tapaa sisällyttäen sekä perinteiseksi miellettyä rikollisuuden muotoa, että kyberrikollisuudeksi miellettyä rikollisuuden muotoa. Hunton (2009) nostaa esiin, että Yarin (2006) mukaan kyberrikollisuus myös voi kattaa alleen selvän rikollisuuden lisäksi ei-toivottua käytöstä, jota toteutetaan verkkopohjaisilla teknologioilla. Toisaalta voisi myös pohtia onko enää tarpeen vetää rajaa perinteisen rikollisuuden ja kyberrikollisuuden välille, sillä kybermaailma on ollut ympärillämme jo kauan ja käynyt todennäköisesti hyvin arkiseksi asiaksi monen silmissä.

Hiscoxin vuoden 2023 kybervalmiuden raportin mukaan 48 % raportin kohdemaiden, Belgian, Saksan, Alankomaiden, Iso-Britannian, Ranskan, Irlannin, Espanjan ja Yhdysvaltojen, liiketoiminnoista on kohdannut kyberhyökkäyksiä. Seitsemän kahdeksasta kohdemaasta määrittelivät kyberhyökkäysten olevan maan liiketoiminnoille suurin uhka. Raportin perusteella pilvipalvelimet olivat kyberhyökkäysten suurin väylä, jota seuraa toisella sijalla sähköpostin välityksellä tehdyt hyökkäykset. Raportissa korostui erityisesti yksinkertaisten tietojenkalastelusähköpostien aiheuttamat vuodot, joiden määrän oletetaan lisääntyvän. (Hiscox, 2023). Tietojenkalastelu on siis yksi suurista kyberhyökkäyksen keinoista ja tämän myötä myös yksi merkittävistä tietoturvauhista.

Kyberrikollisuutta voidaan kuvata monella tapaa. Moon, McCluskey J. ja McCluskey C. (2010) kuvaavat kyberrikoksia jatkuvasti kasvavana globaalina

ongelmana, jolla on innovatiivisia, ilmiömäisiä sekä nykyajan mukaisia piirteitä ja joissa hyödynnetään verkkoa laittomiin tarkoituksiin toteuttaen monia eri rikollisia toimenpiteitä kuten käyttäjän manipulaatiota, tietojenkalastelua, petoksia ja palvelunestohyökkäyksiä. Bada ja Nurse (2021) nostavat kyberrikollisuuden myös yhdeksi yhteiskunnan suurista uhista ja niiden aiheuttamien merkittävien turvallisuushaasteiden vuoksi on tärkeää ymmärtää niiden toimintaperiaatteita ja taustoja.

Kyberhyökkäyksen uhriksi joutuminen voi aiheuttaa uhrille psykologista stressiä mahdollisten taloudellisten menetysten ja fyysisen vaaran ohella hyökkääjän usein saadessa myös uhrin henkilökohtaista dataa (Kuroki, 2021). Naquinin, Kurtzbergin ja Belkinin (2010) mukaan yksilöt, jotka ovat joutuneet aiemmin kyberhyökkäyksen uhreiksi voivat kokea kontrollin puutetta ja epäreiluuden kokemuksia, sillä rikollisia on vaikea jäljittää ilman ajallisia ja maantieteellisiä rajoitteita. Myös DeTardo-Bora ja Bora (2016) kuvasivat kyberrikosten aiheuttavan uhrille enemmän avuttomuuden tunnetta kuin perinteiset rikoksen muodot johtuen kyberrikosten mahdollisesti aiheuttaman kontrollin puutteen tunteen ja epäreiluuden tunteen vuoksi. Lisäksi kyberrikos voi potentiaalisesti aiheuttaa uhrissa pelkoa, jonka vuoksi kyberrikosten uhreiksi joutuneilla yksilöillä on taipumusta kokea matalampaa hyvinvointia subjektiivisella tasolla (Diener, 2013).

3 TIETOJENKALASTELU

Tietojenkalastelun nimi pohjautuu yleismaailman kalastus -verbiin, sillä tietojenkalastelija pyrkii houkuttelemaan kohteen tarttumaan syöttiin, joka voi olla esimerkiksi huijaussivustolle ohjaava sähköposti, jonka avulla hyökkääjä voi ”kalastella” kohteen henkilökohtaisia tai luottamuksellisia tietoja (Chiew, Yong, & Tan, 2018). Tietojenkalastelu terminä on siis hyvinkin ymmärrettävä kohteen ollessa saalis, hyökkääjän ollessa saalistaja ja esimerkiksi yleisesti käytetyn tekniikan, tietojenkalastelusähköpostin, ollessa syötti.

Vishwanath, Harrison ja Ng (2018) puoltavat ajatusta, että tietojenkalastelu olisi yksi pääasiallisista uhista kyberturvallisuuden kentällä. Hongin (2012) mukaan tietojenkalastelu voidaan kuvata hyökkäyksenä, jossa rikolliset käyttävät esimerkiksi huijaussähköposteja hyökkäyksen välineenä tavoitteenaan saada potentiaaliset uhrit jakamaan sensitiivistä informaatiota hyökkääjälle tai lataamaan haittaohjelman laitteelleen, jota hyökkääjä pyrkii hyödyntämään omiin, usein kohteelle vahingollisiin, tarkoitusperiin. Khonji, Iraqi ja Jones (2013) puolestaan kuvaavat tietojenkalastelun olevan yksi käyttäjän manipulointihyökkäyksen välineistä, joissa pyritään käyttämään järjestelmän käyttäjien heikkouksia pyrkien keräämään kohteelle kriittistä ja sensitiivistä informaatioita, jota hyödynnetään vahingollisiin tarkoituksiin. Yhtenä esimerkkinä tutkijat nostavat esiin tietojenkalastelusähköpostien hyödyntämisen hyökkäysvälineenä, joiden lähettämisen tavoitteena on saada kohde esimerkiksi vuotamaan salasanansa tai muun kriittisen tiedon hyökkääjän käyttöön, vaikka järjestelmä itsessään olisikin turvallinen. Tutkijoiden mukaan on hyvin hankalaa pienentää tietojenkalastelun riskiä, koska tietoturvan heikoin lenkki on useimmiten kohteeksi valittu käyttäjä eikä niinkään itse järjestelmä. (Khonji ym., 2013). Gutierrezin, Kimin, Corten, Averyn, Goldwasserin, Cinquen ja Bagchin (2018) mukaan tietojenkalasteluhyökkäykset ovat usein myös muodostamassa ensimmäisen tason moniportaisissa kyberhyökkäyksissä. Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple ja Bellekens (2021) tutkivat kyberhyökkäyksiä koronapandemian aikaan ja totesivat monien kyberhyökkäysten alkavan juuri tietojenkalastelukampanjalla, jonka tarkoituksena oli ohjata kohteet menemään tietojenkalaste-

luviestissä olevalle nettisivulle tai lataamaan tietojenkalasteluviestin sisältämän dokumentin. Tutkimuksessa analysoiduista hyökkäyksistä 86% sisälsi tietojenkalastelua (Lallie ym., 2021).

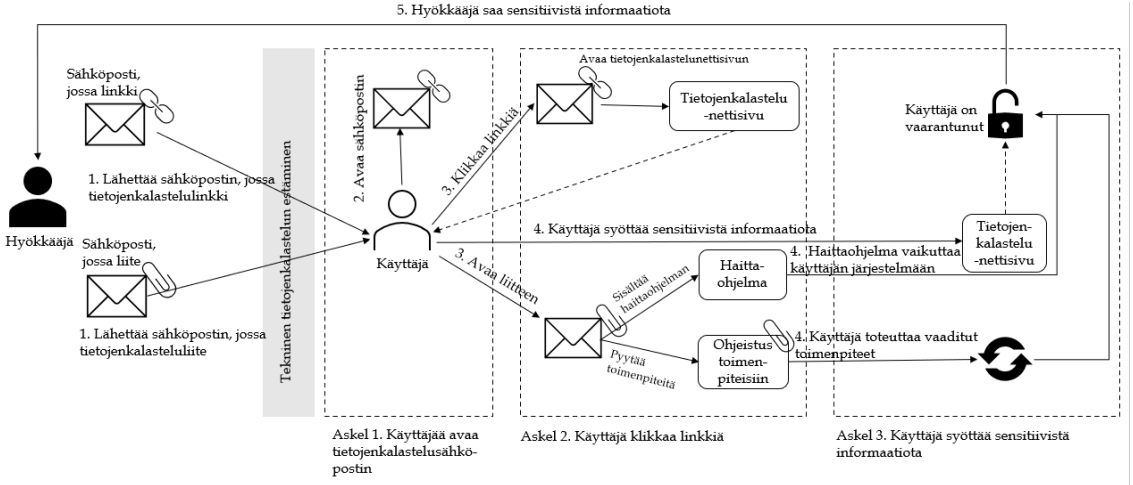
Tietojenkalastelu on siis hyvin relevantti aihe kyberturvallisuuden kentällä. Group-IB:n (2020) tutkimuksen mukaan valmiiden tietojenkalastelupakkausten hinnat nousivat tuplaten vuodesta 2018 vuoteen 2019 mennessä, josta voi päätellä pakkausten olevan erittäin suosittuja pimeillä markkinoilla. Tietojenkalastelupakkaukset tarjoavat valmiin kokonaisuuden usein sisältäen aitona esitettävän tietojenkalasteluun valjastetun nettisivun, jota mainostetaan kohteille esimerkiksi sosiaalisissa verkostoissa ja sähköpostitse (Han, Kheir & Balzarotti, 2016). Tietojenkalastelu on ollut ympärillämme siis pitkään, mutta sen merkitystä ei voi vähätellä vaan se on edelleen erittäin relevantti kyberuhka.

Suomen kyberturvallisuuskeskuksen raportissa (2022) todettiin, että pankkitunnuksiin kohdistuvien tietojenkalasteluhyökkäysten seurauksena tulleet menetykset arvioidaan yksittäin olevan vuoden 2021 aikana yli kahdeksan miljoonaa euroa. Ilmoituksia tehtiin poliisille yli 800 ja Kyberturvallisuuskeskukselle tuli tietoturvailmoituksia yli 1800 tietojenkalasteluhyökkäyksiin liittyen. Vuoden 2021 aikana pankkitunnusten tietojenkalastelussa hyödynnettiin pankkiasiointiin kohdistuvien huijauksien ohella myös viranomaispalveluihin liittyviä huijauksia esimerkiksi viranomaispalveluiden verkkosivustoja esittävien väärennettyjen sivujen avulla. (Kyberturvallisuuskeskus, 2022). Kyberturvallisuuskeskus (2023) julkaisee myös viikkokatsauksia ja esimerkiksi 7/2023 viikkokatsauksessa nostettiin esiin Microsoftin PowerApps-portaalia hyödyntävä aktiivinen tietojenkalastelukampanja, jossa lähetettiin tuhansia tietojenkalasteluviestejä monille eri toimijoille.

Tietojenkalastelijat ovat kehittäneet vuosien saatossa entistä luovempia tietojenkalasteluhyökkäyksiä muokkaamalla ja hienosäätämällä toimintaansa esimerkiksi hyökkäyksen toteuttamistapojen tai sisällön suhteen (Chiew, Yong & Tan, 2018). Kuten aiemmin mainittu, on yleisesti tiedossa, että käyttäjä on usein tietoturvan heikoin lenkki ja juuri tämän vuoksi tietojenkalastelu saattaakin olla kohtuullisen suosittu kyberhyökkäyksissä hyödynnetty tekniikka sen mahdollisesti ollessa hyökkääjälle vaivattomampi tapa saavuttaa tavoitteensa kuin esimerkiksi löytää järjestelmästä heikkouksia ja päästä hyötymään sitä kautta hyökkäyksen tuloksesta.

Abroshan, Devos, Poels ja Laermns (2021) ovat kuvanneet yleistasolla tietojenkalasteluhyökkäyksiä seuraavalla tavalla (Kuvio 1). Ensimmäisessä vaiheessa hyökkääjä lähettää kohteelle esimerkiksi sähköpostiviestin, jossa on tietojenkalastelulinkki, -liite tai molemmat edellä mainituista ohjatakseen kohdetta luovuttamaan sensitiivistä informaatiota hyökkääjän hyödynnettäväksi. Tämän ehkäisemiseksi voidaan ottaa käyttöön erilaisia teknisiä tietojenkalastelua ehkäiseviä ratkaisuja kuten tietojenkalastelun torjumiseen tarkoitettuja suodattimia (Abroshan ym., 2021). Esimerkiksi Gmail ohjaa selkeät tietojenkalastelusähköpostit usein roskapostikansioon, joka ehkäisee osaltaan käyttäjää tarttumasta hyökkääjän asettamaan syöttiin.

Abroshanin ja kollegoiden (2021) mukaan, mikäli tietojenkalastelusähköposti pystyy ohittamaan sitä estävät tekniset ratkaisut, kohde saa hyökkääjän lähettämän tietojenkalastelusähköpostiviestin ja mahdollisesti päätyy avaamaan viestin (Askel 1., Kuvio 1). Mikäli prosessi etenee seuraavaan askeleeseen (Askel 2., Kuvio 1) ja käyttäjä päättää avata linkin tai liitteen, joka saamassaan tietojenkalastelusähköpostissa on. Tiedosto voi sisältää joko itsessään haittaohjelman, joka vaikuttaa käyttäjän järjestelmään tai ohjeistaa käyttäjää tekemään hyökkääjää hyödyttäviä toimenpiteitä kohteen sisäistämättä huijausta. Ohjeistus voi pitää sisällään esimerkiksi sisältöä, joka tarjoaa potentiaaliselle kohteelle nopeasti saavutettavan palkinnon. Nopeasti saavutettava palkinto voi osaltaan hämärtää kohteen päätöksentekokykyä, sillä hyökkäyksen kohde voi palkintoa tavoitellessaan sivuuttaa sen seikan, että sähköposti on mahdollisesti ollut epäilyttävä. Mikäli käyttäjä taas päätyy avaamaan linkin, ohjaa linkki hänet useimmiten tietojenkalastelunettisivulle, jossa tietojenkalastelija pyrkii eri tekniikoita käyttäen houkuttelemaan potentiaalista kohdetta antamaan sensitiivistä informaatiota nettisivun kautta hyökkääjälle. Sensitiivistä informaatiota on esimerkiksi käyttäjän pankkitiedot ja henkilötiedot. Mikäli käyttäjä jatkaa edelleen toimintaansa tietojenkalastelua tekevän hyökkääjän eduksi, prosessin seuraavassa vaiheessa (Askel 3., Kuvio 1) käyttäjä päättää syöttää sensitiivistä informaatiota itse tai haittaohjelma vaarantaa osaltaan potentiaalisen kohteen laitteen tai käyttäjän. Tämän seurauksena hyökkääjä potentiaalisesti saavuttaa tavoitteensa keräten sensitiivistä informaatiota onnistuneesti. (Abroshan ym., 2021).

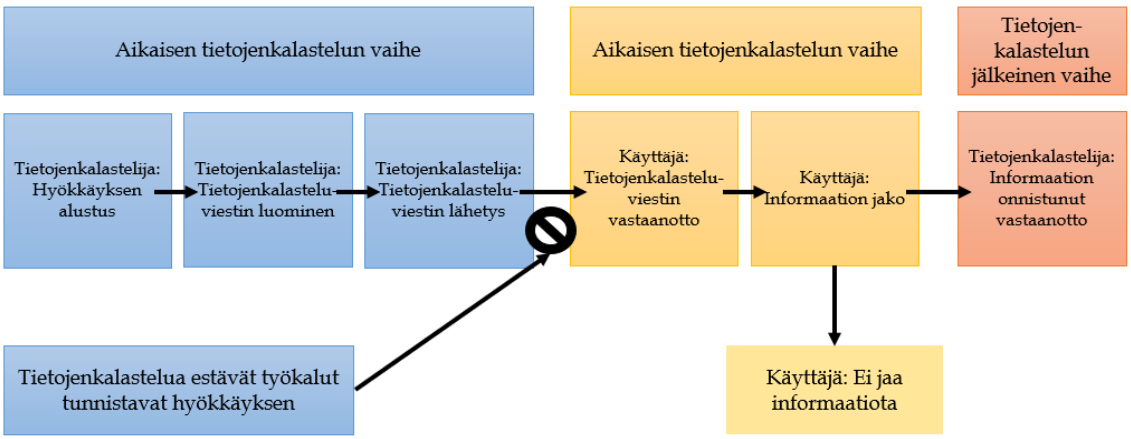


KUVIO 1 Tietojenkalasteluhyökkäyksen prosessi (Abroshan ym., 2021)

Abroshanin ja kollegoiden (2021) yleistä tietojenkalasteluhyökkäyksen prosessikuvausta tukee myös Abdelhamidin, Ayeshin ja Tabtahin (2014) tietojenkalasteluprosessin kuvaus (Kuvio 2), jossa on hyvin saman kaltaisia elementtejä kuin Abroshanin ja kollegoiden (2021) kuvauksessa. Abdelhamidin ja kollegoiden (2014) mukaan tietojenkalasteluhyökkäys perustuu siihen, että hyökkääjät lähettävät autenttisen organisaation lähettämältä sähköpostilta näyttävän viestin pyytäen kohdetta esimerkiksi päivittämään tietoja sähköpostin sisältämän lin-

kin kautta. Prosessi on siis loppujen lopuksi todella yksinkertainen sekä kohtuullisen vaivattomalta vaikuttava ja ehkäpä juuri tämän vuoksi tietojenkalastelu on yleinen kyberrikollisuuden muoto.

Abdelhamidin kollgoineen (2014) muodostama tietojenkalasteluprosessi sisältää kolme eri vaihetta (Kuvio 2.), jotka on havainnollistettu kuviossa 2. Ensimmäisessä vaiheessa, jota nimitetään aikaisen tietojenkalastelun vaiheeksi, tietojen kalastelija ryhtyy alustamaan tulevaa tietojenkalasteluhyökkäystä luoden tietojenkalasteluviestin ja lähettämällä sen kohteille. Aikaisen tietojenkalastelun vaiheen jälkeen tietojenkalastelua vastaan kehitetyt työkalut, kuten tietojenkalastelua torjumaan kehitetyt suodattimet, voivat estää tietojenkalasteluhyökkäyksen läpipääsyn kohteelle. Mikäli työkalu kuitenkin epäonnistuu tietojenkalasteluhyökkäyksen torjumisessa alkaa tietojenkalastelun keskivaihe, jolloin kohde saa viestin ja tekee ratkaisevan päätöksen jakaako informaatiotaan vai ei. Jälkimmäinen tietojenkalasteluvaihe alkaa, mikäli kohde jakaa informaation ja tietojenkalastelija saa haluamansa informaation käyttöön omiin tarkoitusperiinsä. (Abdehamid, Ayesh ja Tabtah, 2014).



KUVIO 2 Tietojenkalasteluprosessin vaiheet (Abdelhamid ym., 2014)

Qabajeh, Thabtah ja Chiclana (2018) ovat määrittäneet tietojenkalastelun elinkaaren, joka sisältää seuraavat askeleet, jotka tukevat osaltaan myös aiemmin mainitun Abroshanin ja kollegoiden kuvausta (2021):

1. Hyökkääjä pyrkii tavoittamaan potentiaaliset uhrit lähettämällä linkin sisältämän viestin käyttäen sähköistä kanavaa kuten esimerkiksi sähköpostin tai sosiaalisen median kanavan kautta.
2. Potentiaalinen uhri valitsee mennä viestin sisältämän linkin johdattamalle sivulle, joka voi olla valjastettu ilkivaltaisiin tarkoitusperiin.
3. Mikäli uhri edelleen päättää jatkaa viestin sisältämien ohjeiden mukaan, hän syöttää sivulle tunnuksensa ja tulee näin haavoittuvaiseksi
4. Ilkivaltainen nettisivu kerää uhrin syöttämät tunnukset siirtäen ne rikollisen palvelimelle tai asentaa vakoiluohjelman uhrin laittelle.
5. Uhrin antamia tunnuksia voidaan hyödyntää kyberrikollisuuden toimissa. (Qabajeh ym., 2018).

3.1 Käyttäjän manipulointi

Tietojenkalastelu on yksi käyttäjän manipuloinnin keinoista. Käyttäjän manipulointi on yksi virtuaalisen maailman uhista Krombholzin, Hobelin, Huberin ja Weippln (2015) mukaan, jota edesauttaa bring your own device-käytännöt sekä verkossa hyödynnettävät kommunikaatio- ja yhteistyötyökalut. Esimerkiksi organisaatioiden sisällä hyödynnetään usein erilaisia digitaalisia kommunikaatiovälineitä kuten sähköpostia, joka osaltaan tarjoaa alustan käyttäjän manipulaatiolle ja on yhä pahempi uhka tietoturvalle. (Aburrous, Hossain, Dahal ja Tabtah., 2010). Myös Konradt, Chilling ja Werners (2016) nostavat käyttäjän manipuloinnin suureksi uhaksi organisaatioiden nojautuessa elektroniseen kommunikaatioon, sillä kohteena olevien käyttäjien haavoittuvuus heihin kohdistuvalle manipulaatiolle voi uhata organisaatioiden tietoturvaa.

Curtisin, Rajivanin, Jonesin ja Gonzalesin (2018) mukaan verrattuna muihin käyttäjän manipulaation muotoihin, tietojenkalastelu on paljon yleisempää ja kehittyneempää. Rajivan ja Gonzales (2018) väittävät, että käyttäjän manipulaatiota yhdistettäessä yleisellä tasolla tietojenkalasteluun, prosessi toimii niin, että rikolliset esiintyvät kolmannen tahon luotettavana tekijänä johdattaen käyttäjiä päätymään lataamaan ilkivaltaisia liitteitä tai menemään petoksellisille nettisivuille. Peltier (2006) kuvaa käyttäjän manipulointia psykologisena hyökkäyksenä, joka pyrkii hyödyntämään kohteelta kerättyä sensitiivistä informaatiota uhrille haitallisiin tarkoitusperiin hyödyntäen yksilölle spesifejä piirteitä kuten taipumusta avuliaisuuteen, luottamukseen sekä ongelmiin joutumisen pelkoon. Myös Abrin, Zhengin, Namin ja Jonesin (2022) tutkimus tukee aiempaa käsitystä väittäen käyttäjän manipuloinnin tavoitteena olevan kerätä sensitiivistä informaatiota eri tekniikoiden kuten tietojenkalastelunettisivujen ja -sähköpostien avulla yksinkertaisimmillaan pyrkien saamaan tietoja suoraan uhrilta vastuksena tietojenkalasteluhyökkäykseen. Myös Gray ja Hovav (2008) tunnistavat kohteena olevien käyttäjien haavoittuvuuden hyödyntämisen käyttäjän manipulaatiossa etenkin tietojenkalastelun osalta hyödyllisenä hyökkääjälle.

Käyttäjän manipulaatioon tähtäävät hyökkäykset voidaan jakaa suoran ja epäsuoran kommunikaation tekniikoihin, joista suorassa kommunikaatiossa käytetään usein tietojenkalastelua (Mouton, Leenen, Malan & Venter, 2014). Tutkijoiden mukaan käyttäjän manipulaation piirissä tietojenkalastelu on suosittu tekniikka suoran kommunikaation käyttäjän manipuloinnin mallissa. Suoran kommunikaation mallissa käyttäjän manipulaatiossa hyödynnetään yleisesti tietojenkalastelua ja hyökkäys käsitetään sellaisena, jossa vähintään kaksi yksilöä kommunikoi toisiensa kanssa suorasti ilman välikäsiä (Mouton ym., 2014). Mouton kollegoineen (2014) ovat luoneet ontologisen käyttäjän manipulaatiota

kuvaavan hyökkäysmallin, jossa käyttäjän manipulaatiohyökkäys koostuu seuraavista vaiheista (Kuvio 3), jossa valitaan tekniikka, myöntyväisyyden periaatteet, hyökkäyksen kohde, hyökkääjät, kommunikointiväline ja tavoite. Tekniikat sisältävät tietojenkalastelun, sosiaalisen tiedustelun, syötin asettamisen ja vastalahjan. (Mouton ym. 2014). Myöntyväisyyden periaatteet sisältävät ystävyyssuhteen tai miellyttävyyden, tarjotusta sitoutumisesta pitämisen tai yhtenäisyyden, niukkuuden, oppineisuuden, sosiaalisen validaation ja auktoriteetin, joilla kohteeseen pyritään vaikuttamaan niin, että hän toimisi hyökkääjän toivomalla tavalla. Kohteena käyttäjän manipulaatioon tähtäävässä hyökkäyksessä toimii yksilö tai organisaatio ja hyökkäyksen toteuttaa yksilö tai joukko yksilöitä. Kommunikaatioväline voi olla:

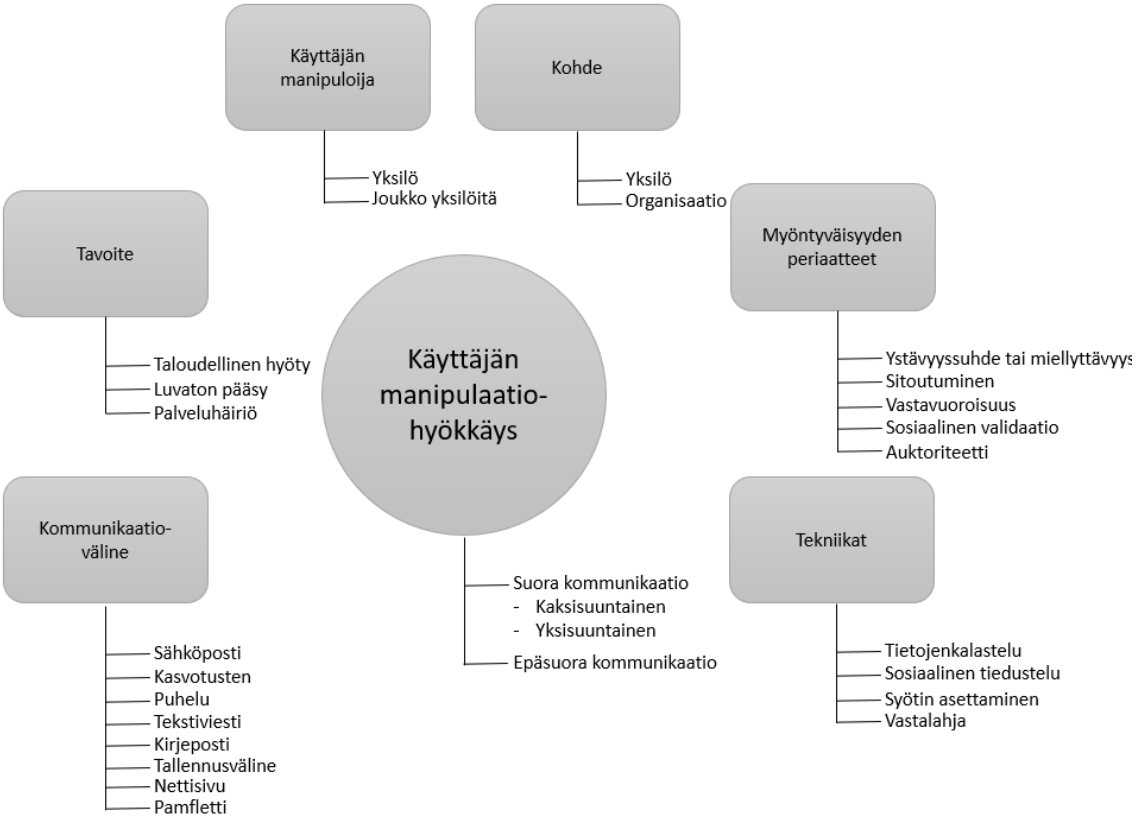
1. Sähköposti
2. Kasvotusten tapahtuva kommunikointi
3. Puhelimitse toteutettava kommunikaatio
4. Tekstiviesti
5. Kirje
6. Tallennusväline
7. Nettisivu
8. Pamfletti.

(Mouton, Leenen & Venter, 2016).

Suora kommunikaatio voidaan kuitenkin osaltaan myös jakaa kahdeksi pienemmäksi osa-alueeksi, jotka ovat kaksisuuntainen ja yksisuuntainen kommunikaatio, joista kaksisuuntainen kommunikaatio kuvastaa tilannetta, jossa kumpikin osapuoli osallistuu keskusteluun. Yksisuuntaisessa kommunikaatiossa puolestaan vain hyökkääjä kommunikoi kohteen suuntaan, mutta kohde ei kommunikoi hyökkääjän suuntaan. (Mouton ym., 2016).

Epäsuorassa kommunikaatiossa varsinaista vuorovaikutusta hyökkäyksen kohteen ja hyökkääjän välillä ei ole vaan kommunikaatio tapahtuu kolmannen osapuolen kommunikaatiovälineen välityksellä kuten esimerkiksi siinä tapauksessa, jos hyökkääjä saastuttaa USB-muistitikun ja jättää sen satunnaisen kohteen löydettäväksi. Näin ollen suoraa kommunikaatiota hyökkääjän ja kohteen välillä ei ole. (Mouton ym., 2016).

Komponentteja ovat Moutonin ja kollegoiden (2016) esittelemässä ontologisessa mallissa siis tavoite, kommunikaatioväline, hyökkääjä, kohde, myöntyväisyyden periaatteet ja tekniikat. Tekniikoiden, myöntyväisyyden periaatteiden ja kommunikaatiovälineen valitsemisen jälkeen hyökkääjä voi jatkaa prosessissa hyökkäysvaiheeseen. Ontologisessa mallissa hyökkääjän tavoitteet voivat pitää sisällään esimerkiksi taloudellisen hyödyn, luvattoman pääsyn ja palveluhäiriön. Kommunikaatioväline kuvastaa puolestaan tapaa, jolla hyökkääjä kommunikoi kohteensa kanssa ja näitä voivat olla esimerkiksi kasvotusten, sähköpostitse tai puhelun kautta tapahtuva kommunikaatio. Tekniikat puolestaan kuvastavat sitä, miten hyökkäys toteutetaan.



KUVIO 3 Käyttäjän manipulaation ontologinen malli (Mouton ym., 2016)

Myöntyväisyyden periaatteet (Taulukko 1), joita ovat ystävyyssuhde tai miellyttävyys, sitoutuminen, niukkuus, vastavuoroisuus, sosiaalinen validaatio sekä auktoriteetti, kuvaavat kohteen motiivia toimia hyökkääjän pyynnön mukaisesti. Periaatteiden tarkoituksena on seuraava: Ystävyyssuhteen tai pitämisen periaate hyödyttää yksilöiden taipumusta noudattaa paremmin pyyntöjä, mikäli pyyntö näyttää tulevan sellaiselta taholta, josta he pitävät tai henkilöltä, jonka kanssa heillä on ystävyyssuhde. Sitoutumisen ja yhtenäisyyden periaatteen taustalla toimii se, että yksilöillä on tapana toimia pyyntöjen osoittamalla tavalla, jos he ovat jo aiemmin toimineet pyydetyn kaltaisesti. Niukkuuden periaatetta hyökkäyksessä hyödyntäessä hyökkääjä pyrkii houkuttelemaan kohdetta pyynnöillä, joiden keskeisen sisällön niukkuus tai vähäinen mahdollisuus hyödyttää kohdetta. (Mouton ym., 2016). Myös Cialdini ja Cialdini (2007) tunnistivat niukkuuden tehostavan yksilön lankeamista hyökkäykseen. Vastavuoroisuuden periaate nojautuu siihen, että yksilöille on tyypillistä noudattaa pyyntöjä, jotka näyttäisivät tulevan taholta, joka on kohdellut heitä suotuisasti menneisyydessä (Mouton ym., 2016. Tämän vuoksi potentiaalinen uhri voi olla helpommin houkuteltavissa toimimaan hyökkääjän haluamalla tavalla tuntiessaan vastavuoroisuuden tarvetta aiemman suotuisan kohtelun vuoksi. Sosiaalisen validaation periaate nojautuu puolestaan siihen, että yksilöillä on taipumus noudattaa pyyntöjä, joiden mukaisen toiminnan he näkevät sosiaalisesti korrektina toimena. Viimeinen periaate on auktoriteetti, jossa hyödynnetään yksilöiden haluna toimia pyyntöjen mukaisesti, mikäli pyyntö näyttäisi tulevan tahol-

ta tai henkilöltä, jolla on kohteen suhteen auktoriteettiasema (Mouton ym., 2016).

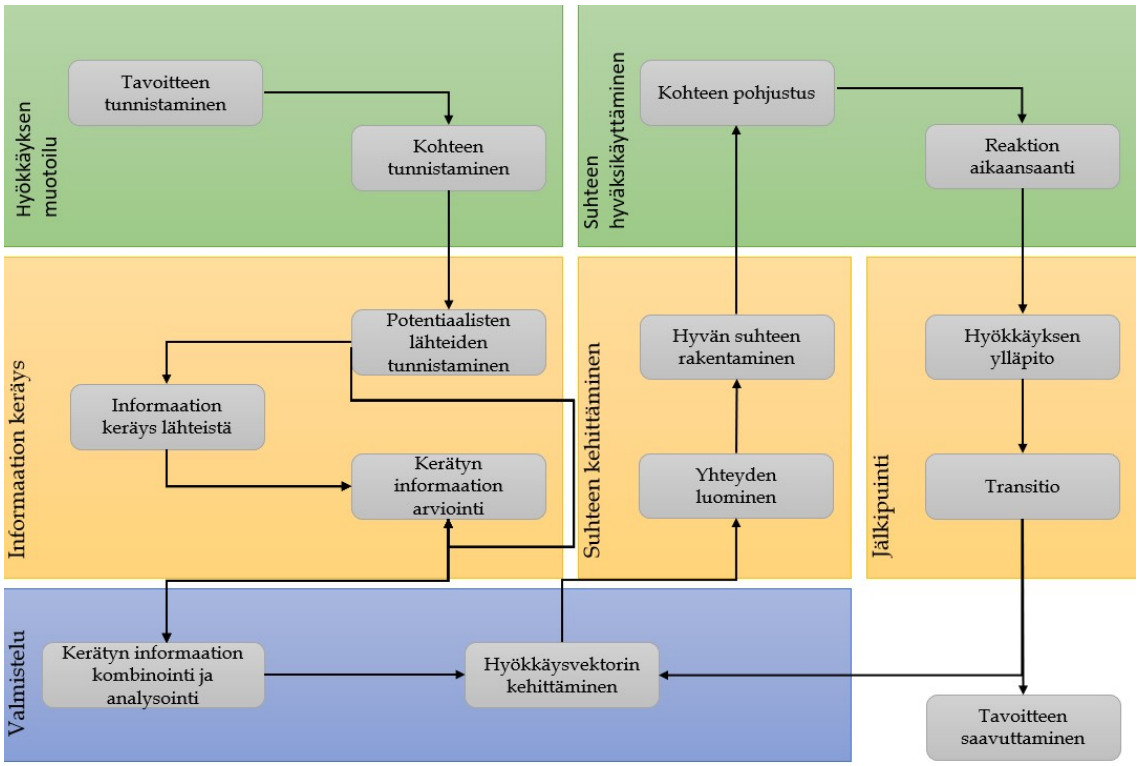
TAULUKKO 1 Myöntyväisyyden periaatteet (Mouton ym., 2016)

Myöntyväisyyden periaate	Selitys
Ystävyyssuhde tai miellyttävyys	Pyyntö tulee väitetysti henkilöltä, jolla on ystävyyssuhde yksilön kanssa tai henkilö on miellyttävä kohteen silmissä.
Sitoutuminen ja yhtenäisyys	Pyyntö tulee väitetysti lähteestä, johon yksilö on sitoutunut.
Niukkuus	Pyynnön sisältö on saatavuudeltaan niukka ja/tai mahdollisuus vähäinen.
Vastavuoroisuus	Pyyntö tulee väitetysti lähteestä, joka on kohdellut yksilöä aiemmin suotuisasti.
Sosiaalinen validaatio	Pyyntö näyttää sosiaalisesti korrektilta toteuttaa.
Auktoriteetti	Pyyntö tulee väitetysti taholta, jolla on enemmän auktoriteettia kuin yksilöllä.

Mouton kollegoineen (2016) kuvaa käyttäjän manipulaatiohyökkäyksen prosessia (Kuvio 4) jakaen sen kuuteen eri vaiheeseen. Hyökkäyksen prosessi alkaa tyypillisesti hyökkäyksen muotoilulla, jonka jälkeen hyökkääjä aloittaa tiedon keräyksen ja hyökkäyksen valmistelun. Tämän jälkeen hyökkääjä pyrkii luomaan yhteyden potentiaaliseen uhriin, jonka jälkeen hyökkääjä pyrkii hyväksikäyttämään muodostamaansa yhteyttä potentiaalisen uhrin kanssa ja hyökkäyksen jälkipuintiin. Vaiheiden sisältämät askeleet on kuvattu tarkemmin alla etenemisjärjestyksessä:

1. Hyökkäyksen muotoilussa hyökkääjä tunnistaa tavoitteen ja kohteensa.
2. Informaation keräämisen vaiheessa hyökkääjä tunnistaa potentiaaliset tiedonlähteet ja kerää niiden kautta informaatiota. Tämän jälkeen hyökkääjä arvioi keräämänsä informaation ja päättää onko sen taso riittävä. Mikäli kerätty informaatio ei ole hyökkääjän mielestä riittävällä tasolla, hyökkääjä toistaa tämän vaiheen keräten lisää informaatiota.
3. Kolmannessa vaiheessa hyökkääjä valmistelee hyökkäystään kombinoimalla ja analysoimalla saatua informaatiota ja kehittää hyökkäysvektorin, jolla pyrkii luomaan yhteyden kohteeseen.
4. Hyökkäyksen neljännessä vaiheessa hyökkääjä pyrkii kehittämään kohteeseen luottamuksellisen kommunikaatioyhteyden, jonka avulla pyrkii luomaan hyvän suhteen kohteeseen.
5. Viidennessä vaiheessa hyökkääjä pohjustaa kohdetta ja pyrkii saamaan aikaan reaktion, jossa kohde toteuttaa hyökkääjän pyytämän toimen tai pyynnön.

6. Tämän jälkeen hyökkääjä ylläpitää toteuttamaansa hyökkäystä ja joko tyytyy hyökkäyksen toteutumiseen tai pyrkii toteuttamaan hyökkäyksen uudelleen. (Mouton ym., 2016)



KUVIO 4 Käyttäjän manipulaatiohyökkäyksen prosessi (Mouton ym., 2016)

3.2 Kohdennettu tietojenkalastelu

Yksi tietojenkalastelutekniikoista on kohdennettu tietojenkalastelu. Krombholz kollegoineen (2015) ovat tunnistaneet kohdennetun tietojenkalasteluhyökkäyksen tehokkaana tekniikkana ja Kwakin, Leen, Damianon ja Vishwnathin (2020) mukaan kohdennettu tietojenkalasteluhyökkäys on yksi kybermaailman vakavista uhista, sillä viime aikoina on havaittu myös hyökkäyksiä teollisuuden ohjausjärjestelmiin ja sen on huomattu olleen valjastettu myös terroristien käyttötarkoituksiin.

Kohdennettu tietojenkalasteluhyökkäys on Hongin (2012) mukaan käyttäjän manipulaatiota hyödyntävien hyökkääjien toteuttama hyökkäys, joka eroaa perinteisemmäksi mielletyistä massana lähetetyistä sähköposteista sen selektiivisellä luonteella. Kohdennetussa tietojenkalastelussa siis käytetään paljon kontekstiltaan spesifimpää ja relevantimpaa kohdennettua informaatiota pyrkimyksenä saada tietyt ennalta spesifisti määritetyt kohteet lankeamaan tietojenkalasteluhyökkäykseen hyödyntäen yksilökohtaisia ominaisuuksia (Hong, 2012). Usein kohdennetussa tietojenkalasteluhyökkäyksessä esimerkiksi viitataan kohteeseen hänen nimellään (Lin, Capecci, Ellis, Rocha, Dommaraju, Oli-

veira & Ebner, 2019). Myös Laszka, Vorobeychik ja Koutsoukos (2015) tukevat Hongin (2012) käsitystä kuvatessaan kohdennettua tietojenkalastelua tekniikkana, joka keskittyy kohdistamaan hyökkäykset tiettyihin ja huolellisesti valittuihin yksilöihin pyrkien rikkomaan tietoturvan heikoimmaksi mielletyn lenkin eli käyttäjän. Tutkijat nostavat esiin myös sen, että kohdennetun tietojenkalasteluhyökkäyksen yritys ei välttämättä myöskään jää kiinni hyökkäyksen alkuvaiheessa yhtä helposti kuin massoittain lähetettävät saman sisällön omaavat sähköpostit, jotka voivat aiheuttaa tietoturvahälytyksen esimerkiksi organisaatiotasolla (Laszka ym., 2015). Kohdennetussa tietojenkalasteluhyökkäyksessä kohde siis valitaan tarkemmin, jotta pääsy haluttuun informaatioon saataisiin helpommin (Burns, Johnson & Caputo, 2019). Im ja Baskerville (2005) väittävät, että tietoturvariskien yksi suurista ongelmista on käyttäjien inhimilliset virheet, joten hyökkääjät pyrkivät hyödyntämään käyttäjän rajoitteita ja taipumuksia, jota voidaan soveltaa myös kohdennettuun tietojenkalasteluun.

Tietojenkalasteluhyökkäyksen prosessissa hyökkäyksiä tekevät henkilöt joutuvat arvioimaan kohteen arvon ja tasapainottamaan sen resurssien kanssa, joita hyökkäykseen vaaditaan, sillä mitä potentiaalisempi onnistuneen hyökkäyksen arvo on, sitä enemmän yleisesti siihen vaaditaan resursseja. Kohdennettua tietojenkalasteluhyökkäystä suorittaessa, kohde on tyypillisesti valittu tarkemmin, joka osaltaan johtaa siihen, että niillä on kapeampi menestyssäde ja toisaalta myös korkeampi onnistumistaso. (Burns ym., 2019).

Mikäli tietojenkalastelun kohdennuksen taso on hyvin matala ei sen lasketa noudattavan kohdennetun tietojenkalasteluhyökkäyksen tekniikkaa vaan se määritellään tietojenkalasteluksi, sillä hyökkääjä ei kyseisessä tapauksessa tee toimia räätälöidäkseen hyökkäystä sen kohteen perusteella eikä useinkaan tiedä kohteesta eli potentiaalisesta uhrista juuri mitään. Tietojenkalasteluhyökkäys voi olla myös todella korkeasti kohdennettu, jonka ominaispiirteitä on perusteellinen tiedustelu ja räätälöity käyttäjän manipulointi, jossa saadaan tietoja lisäämään aiempaa luottamussuhdetta ja hyödyntämään sitä, mikä luo pohjan tehokkaammille hyökkäyksille, jossa valitaan kohteet usein heidän hyödyttävän asemansa ja arvokkaan tiedonsaannin mahdollisuuden perusteella. Korkeatasoisen kohdentamisen hyökkäykset ovat kohdennettuja tietojenkalasteluhyökkäyksiä ja korreloivat resurssien kanssa kasvavasti. (Burns ym., 2019).

Kohdentamista voidaan Burnsin ja kollegoiden (2019) mukaan tehdä mediaa hyödyntäen, esimerkiksi keräämällä yksityiskohtaisia tietoja kohteesta kohteen henkilökohtaisen sosiaalisen median kautta. Sosiaalinen media voikin toimia hyvänä lähteenä kohdennukseen, koska sieltä voi saada merkittävästi tietoa esimerkiksi henkilöiden koulutuksesta, aiemmista työpaikoista ja ihmissuhteista. Tämän seikan vuoksi jokaisen sosiaalista mediaa käyttävän henkilön olisi hyödyllistä pohtia mitä kaikkea informaatiota itsestään jakaa ja mihin sen jakaminen voi altistaa.

3.3 Tietojenkalastelun tyypit

Tietojenkalastelulle on kehittynyt aikojen saatossa erilaisia juuri sille tyypillisiä tapoja tehdä hyökkäyksiä. Hyökkääjät pyrkivät monin eri tekniikoin saamaan käyttäjän niin vakuuttuneeksi, että he lopulta toimivat hyökkääjän pyynnön mukaisesti esimerkiksi avaamalla sähköpostitse saamansa viestissä olevan linkin tai saastuneen liitetiedoston (Mansfield-Devine, 2018).

Tietojenkalastelun tyypit voidaan erotella niiden hyökkäyksen toteutustavan avulla, jotka voivat olla yhteydessä myös toisiinsa samassa hyökkäyksessä. Hyökkäyksen toteutustapoina voi toimia esimerkiksi tietojenkalasteluviestit, tietojenkalastelunettisivut, puhelut sekä QR-koodit.

3.3.1 Tietojenkalasteluviestit

Tietojenkalasteluviesti, joka voidaan lähettää esimerkiksi sähköpostitse tai tekstiviestitse, pyritään usein suunnittelemaan ja toteuttamaan niin, että se vaikuttaa mahdollisimman uskottavalta. Esimerkiksi tietojenkalastelusähköposteissa voidaan esiintyä luotettavana tahona, jolloin käytetään usein samaa fonttia kuin tietojenkalastelussa mahdollisesti esitettävä luotettava taho oikeastikin käyttää, jotta viesti ei herättäisi kohteessa epäilyksiä (Abroshan ym., 2021). Tietojenkalastelusähköpostien avaaminen etenkin pelkkänä tekstinä tai HTML:nä avatessa on useimmiten kuitenkin lähtökohtaisesti turvallista, mutta joissain tapauksissa jo pelkkä sähköpostin avaaminen voi saastuttaa laitteen (CISA Department of Homeland Security, 2023). Tietojenkalasteluhyökkäyksen kohdistuessa organisaation työntekijöihin, työntekijät saattavat matalammalla kynnyksellä avata sähköpostin, jossa lähettäjänä näkyy heille tuttu nimi kuten esimerkiksi heidän esihenkilönsä tai organisaation toimitusjohtaja (Abroshan ym., 2021). Abroshanin ja kollegoiden (2021) mukaan tutkimuksessa ei ollut näyttöä riskinottokäyttäytymisen ja päätöksenteon tyylin vaikutuksesta tietojenkalastelusähköpostien avaamiseen. Kuitenkin Abroshan ja kollegat (2021) tunnistivat, että esimerkiksi miellyttävä sähköpostin aihe, joka käyttää vaistoihin perustuvaa taktiikkaa, sähköposti tunnetulta henkilöltä tai tunne sähköpostin kiireellisyydestä ovat keinoja, joilla pyritään häiritsemään kohteen päätöksentekokykyä. Tietojenkalastelusähköpostin aukaiseminen voi olla ongelmallista ja aiheuttaa kohteelle riskin hyökkääjän voidessa käyttää esimerkiksi erilaisia sähköpostin jäljittämistekniikoita ja selvittää sähköpostin kuuluvan tietylle henkilölle ja hyödyntää tätä esimerkiksi kohdennetun tietojenkalastelun tekniikoissa tehdäkseen tehokkaamman hyökkäyksen (Abroshan ym., 2021) Vaistoihin vaikuttavan taktiikka pyrkii kääntämään kohteen huomion toiminnon aitoudesta toimintoihin, jotka voivat tyydyttää käyttäjän vaistoihin perustuvat tarpeet (Abroshan ym., 2021)

Tietojenkalastelusähköposteille tyypillistä on lyhyt ja tarttuva otsikko, jonka avulla hyökkääjä pyrkii saamaan sähköpostin vaikuttamaan houkuttelevalta ja tämän seurauksena kohteen avaamaan sen (Workman, 2008). Tietojenkalastelusähköpostin otsikkokenttä voidaan myös jättää täysin tyhjäksi. Sapple-

tonin ja Lourençon (2016) tutkimuksen perusteella itseasiassa tyhjäksi jätetty otsikkokenttä tietojenkalastelusähköpostissa saa kohteet avaamaan sähköpostin todennäköisemmin, mutta vastausprosentti tietojenkalasteluun jää kuitenkin alhaiseksi sähköpostin avaamisesta huolimatta (Sappleton & Lourenço, 2016). Tietojenkalastelusähköpostien sisällössä voidaan hyödyntää myös Graggin psykologisia faktoreita, joita ovat palkkio, kiireellisyys auktoriteetti ja luottamus (Stojnic, Vatasalan, Arachchilage, 2021). Stojnicin ja kollegoiden mukaan (2021) tietojenkalastelusähköpostin luomista ja sen toimintalogiikkaa voidaan kuvata kolmella askeleella. Ensimmäisellä askeleella hyökkääjä pyrkii saamaan kohteen avaamaan sähköpostin lyhyellä ja tarttuvalla otsikolla, joka luo tunnetta kiireellisyydestä ja kiehtovuudesta. Toisena askeleena on saada kohde luottamaan ja pitämään huomionsa edelleen tietojenkalastelusähköpostissa esimerkiksi esiintymällä auktoriteettina ja tarjoamalla kohteelle palkinnon. Kolmannessa vaiheessa pyritään saamaan kohde ryhtymään toimiin sähköpostin perusteella esimerkiksi vuotamalla sensitiivistä informaatiota luvattua palkkiota vastaan. (Stojnic ym., 2021).

Sähköposti ei ole kuitenkaan ainoa keino lähettää tietojenkalastelua vaan tietojenkalasteluviestejä voi tulla missä tahansa viestipalvelussa. Yksi suosittu tietojenkalasteluviestien lähettämistapa on tekstiviestit, joihin pätee yleisellä tasolla samat periaatteet kuin sähköpostiviesteillä. Jakobssonin (2018) mukaan tietojenkalastelu tekstiviestitse onkin tehokas tapa, sillä suurin osa käyttäjistä ei oleta tietojenkalastelun tulevan tekstiviestitse vaan useimmiten sähköpostitse, jonka vuoksi tietojenkalastelu tekstiviestitse voikin olla tehokkaampaa. Esimerkiksi Siadati, Nguyen, Gupta, Jakobsson ja Memon (2017) tekivät tutkimuksen tietojenkalastelutekstiviestien tehokkuudessa, jossa he kokeilivat yhdeksää eri tietojenkalastelutekstiviestityyppiä, joista parhaassa 60% kohteista lankesi tietojenkalasteluun. Sidatin ja kollegoiden (2017) kehittämän viestin sisältö oli vapaasti suomennettuna seuraava ”Pyysitkö salasanan nollaamista Gmail-käyttäjällesi? Poista tämä viesti, mikäli pyysit. Muussa tapauksessa lähetä ”peruuta” ja verifiointikoodi, jonka juuri lähetimme sinulle”, jonka seurauksena 60 % kohteista mahdollistivat verifiointikoodin avulla pääsyn käyttäjälleen.

3.3.2 Tietojenkalastelunettisivut

Yangin ja kollegoiden (2019) mukaan tietojenkalastelu ei rajoitu enää pelkästään sähköposti- tai tekstiviestien lähettelyyn ja pop-up ikkunoihin, vaan heidän mukaansa tietojenkalasteluhyökkäyksistä monet tapahtuvat nykyisin nettisivujen kautta, jotka käyttävät suojattua HTTPS:ää ja johdattavat käyttäjän uskomaan, että sivu on aito johtuen HTTPS:n käytöstä ja näin lankeamaan tietojenkalasteluhyökkäyksen uhriksi. Jo pelkkä linkin avaaminen voi johtaa käyttäjän laitteen saastumiseen esimerkiksi haittaohjelmalla, mutta toisaalta myös potentiaalisen uhrin saaman liitetiedoston avaaminen voi saastuttaa käyttäjän tietokoneen (Popoola, Iyekekpolo Ojewande, Sweetwilliams & Atayero, 2017). Abroshanin ja kollegoiden (2021) mukaan nettisivulle mennyttä käyttäjää kuitenkin pääsääntöisesti yritetään saada luovuttamaan sensitiivistä informaatiota, jota hyökkääjä pyrkii hyödyntämään omiin tarkoitusperiinsä.

Hyökkääjät voivat käyttää myös URL:n lyhennysmekanismia huijatakseen potentiaalista uhria, jonka avulla nettisivun osoite voidaan saada vaikuttamaan muulta kuin mitä se todellisuudessa on (Mavroeidis & Nicho, 2017). Sahingozin, Buberin, Demirin ja Dirin (2019) mukaan petolliset tietojenkalastelussa käytetyt nettisivut pyrkivät imitoimaan aitoja suosittuja ja laillisia nettisivuja luoden vilpillisten nettisivujen muotoilun täysin saman kaltaiseksi käyttöliittymiltään aitojen sivujen kanssa johdattaakseen kohdetta harhaan. Kuitenkin URL-osoite poikkeaa aitojen nettisivujen vastaavasta, jonka takia käyttäjällä on mahdollisuus erottaa tietojenkalastelunettisivu aidosta nettisivusta. Vaikka URL-osoite poikkeaakin aidon sivun URL-osoitteesta, se voi jäädä potentiaaliselta uhrilta huomaamatta esimerkiksi siirtyessä eri sivustolta toiselle tai kohde voi jättää muutoin katsomatta URL-osoitteen kokonaisuudessaan varmentuakseen sivun aitoudesta. (Sahingoz ym., 2019).

3.3.3 Äänitietojenkalastelu

Choin, Leen ja Chunin (2017) mukaan äänitietojenkalastelu on kasvava tietojenkalastelurikoksen tyyppi, jossa kohteille soitetaan ja vakuutetaan antamaan tietoja. Tutkijoiden mukaan Etelä-Koreassa jo vuoden 2013 tammikuun ja lokakuun välillä ilmeni 4022 äänitietojenkalastelutapausta. Rikoksissa pyritään saamaan sensitiivistä informaatiota kuten esimerkiksi nimi, osoite, pankkikortin numero, puhelinnumero tai henkilötunnus, jotka voidaan myydä eteenpäin rikoksen tekijän toimesta ja niitä voidaan käyttää rikolliseen toimintaan. (Choi, Lee & Chun, 2017). Esimerkiksi Suomessa on uutisoitu äänitietojenkalastelu-vyyhdistä, jossa puhelinsoitossa tietojenkalastelijat esiintyivät poliisina ja kalastelivat kohteiltaan verkkopankkitunnuksia onnistuneesti (Yle, 2023).

Kangin, Kimin, Limin, Kimin ja Seon (2022) mukaan äänitietojenkalastelussa voidaan käyttää myös deep fake -ääntä, joka tuottaa ääntä synteettisesti. Synteettisellä äänellä tietojenkalastelua tekevät hyökkääjät voivat hyödyntää deep voicea keräämällä esimerkiksi sosiaalisesta mediasta jonkun spesifin henkilön ääninäyte ja deep voicen avulla luoda ääninauhan kyseisen henkilön äänellä ja esiintyä hänenä pyrkien kohdetta saamaan luovuttamaan sensitiivistä informaatiota.

3.3.4 QR-koodilla tapahtuva tietojenkalastelu

QR-koodi (Quick Response-koodi) on kaksiulotteinen matriisi, joka koostuu mustista ja valkoisista pikseleistä ja sitä hyödynnetään tietojen tallettamiseen optisesti skannattavassa ja kompaktissa muodossa (Kumaraguru, Sheng, Acquisti, Cranor & Hong, 2010). QR-koodin hyötyjä on myös sen korkea vaurionkestävyys ja luontainen datakapasiteetti (Lin & Chen, 2017) sen pystyessä varastoimaan 2 953 binääristä tavua, 1 817 japanilaista Kanji tai Kana-symbolia, 7 089 numeerista merkkiä tai vaihtoehtoisesti 4 296 aakkosnumeerista merkkiä (Rouillard, 2008).

Tietojenkalastelu on yksi yleisimmistä QR-koodien kautta tapahtuvista hyökkäyksistä, joissa pyritään saamaan kohde luovuttamaan sensitiivistä in-

formaatiota hyökkääjälle (Kharraz, Kirda, Robertson, Balzarotti & Francillon, 2014). QR-koodien kautta tietojenkalastelu tapahtuu niin, että käyttäjät lukevat koodin laitteellaan ja koodi johtaa verkkosivulle, joihin uhrin mahdollisesti syöttämää tietoa käytetään ilkivaltaisiin tarkoitusperiin. QR-koodia voidaan hyödyntää hyökkäysvektorina kohteelle vahingollisiin tarkoituksiin, kun esimerkiksi käyttäjän manipulaatiota harjoittavat hyökkääjät kehittävät petokselista koodia, joka toimeenpannaan QR-koodin ohjaamalta tietojenkalastelunettisivulta (Krombholz, Frühwirt, Kieseberg, Kapsalis, Huber & Weippl, 2014). QR-koodit ovat tietojenkalastelua tekeville hyökkääjille houkutteleva tapa toteuttaa hyökkäys, koska esimerkiksi älypuhelinten näytön rajallinen koko ei välttämättä näytä koko tietojenkalastelunettisivun URL:ää, jolloin hyökkääjä pystyy huijaamaan kohdetta paremmin URL:n jäädessä osittain näkymättömiin (Mavroeidis & Nicho, 2017) ellei potentiaalinen uhri varta vasten mene sitä katsomaan.

Käyttäjän kynnys skannata QR-koodeja puhelimellaan on kohtuullisen matala, sillä Vidasin, Owusun, Wangin, Zengin, Cranorin ja Chritinin (2013) tutkimuksen perusteella, jossa asetettiin 139 QR-koodin sisältävää julistetta julkiselle paikalle, suurin osa käyttäjistä skannasivat QR-koodin uteliaisuuttaan tai huvin vuoksi. Myös suurin osa käyttäjistä, jotka skannasivat QR-koodin, vierailivat koodin ohjaamalla sivustolla, vaikka sivusto käytti lyhennettyä URL:ää ja he eivät tunnistaneet kyseistä sivustoa (Vidas ym., 2013)

Mavroeidisin ja Nichon (2017) mukaan etenkin mobiililaitteiden käyttäjät ovat hyvä kohde pahansuoville hyökkäyksille, sillä mobiililaitteiden käyttäjät käyttävät laitteita yleisesti päivittäisessä elämässä niin puhelinsoittoihin, viestittelyyn, sosiaalisiin verkkoihin pääsyyn, informaation tallettamiseen kuin myös mahdollisesti työnkuvan mukaan yritysmaailman tietojen käyttämiseen. Yksi mobiilikäyttäjiin kohdistuvista uhista on siis myös QR-koodin avulla tapahtuva tietojenkalastelu.

3.4 Miksi tietojenkalastelu toimii

Chengin, Chanin ja Chaun (2020) mukaan yksilöillä on taipumus luottaa esimerkiksi sosiaalisen median palveluihin ja näin jakaa henkilökohtaista informaatiotaan, joka voi altistaa kyberrikoksen uhriksi joutumiselle. Rajivanin ja Gonzalesin (2018) mukaan tietojenkalasteluhyökkäyksissä pyritään hyödyntämään kohteen heikkouksia, jonka seurauksena käyttäjä mahdollisesti vastaa tietojenkalasteluhyökkäykseen tehden tietojenkalastelusta menestyksekästä.

Yksi piirre, joka voi vaikuttaa tietojenkalasteluun on käyttäjien keskittymisen kohde. Alsharnoubyn, Alacan ja Chiassonin (2015) mukaan käyttäjät eivät mahdollisesti huomaa turvallisuusindikaattoreita, joista osa on näkyvillä vain turvallisilla nettisivuilla verkossa vuorovaikuttaessaan. Volkamer, Renaud, Reinheimer ja Kunz (2017) mukaan tietojenkalastelun onnistumiseen vaikuttavat seuraavat seikat:

1. Käyttäjät tekevät päätöksen väärän signaalin perusteella, sillä heillä ei välttämättä ole tietämystä URL:n olevan tärkeä signaali tietojenkalastelunettisivujen erottamisessa aidosta.
2. Käyttäjät eivät mahdollisesti tiedosta mihin näkyvillä oleviin URL-osoitteisiin voi luottaa.
3. Käyttäjällä ei välttämättä ole mahdollisuutta tarkastella koko URL-osoitetta esimerkiksi uudelleenohjauksen tai piilotetun URL:n vuoksi.
4. Käyttäjä ei välttämättä tarkasta URL-osoitetta riittävän perusteellisesti ennen kuin tekee päätöksen mennä sivustolle tai päätyy sivustolle vahingossa eikä toisaalta välttämättä osata erottaa tietojenkalastelunettisivun URL:ää aidon sivuston URL:stä. (Volkamer ym., 2017).

Viestin sisällöllä on myös paljon merkitystä siinä, miksi tietojenkalastelu toimii. Mikäli hyökkääjä onnistuu luomaan hyvän ensivaikutelman esimerkiksi tunnistettavalla logolla (Naidoo, 2015), aiheuttamaan huomion herpaantumisen (Blythe, Petrie & Clark, 2011) tai sisällyttämällä viestiin väitetyn yrityksen yhteystiedot (Jakobsson, Tsow, Shah, Belvis & Lim, 2007), kohteet ovat taipuvaisempia luottamaan viestiin. Naidoon (2015) mukaan myös viestissä olevat luottamusta herättävät indikaattorit kuten kirjoitusasun ja kieliopin laadukkuus tai viestin sisällöstä kohteelle välittyvä kiireellisyyden tunne, voivat lisätä kohteiden luottamusta tietojenkalasteluviestiä kohtaan. Tietojenkalasteluviestin sisällössä kohteelle mahdollisesti aiheutettu innokkuuden, pelon tai ahdistuksen tunteita osaltaan voi nostaa todennäköisyyksiä kohteen huomion herpaantumiseen (Blythe ym., 2011)

Hawdonin (2021) mukaan sosiaalisen median käyttö on vahvasti liitoksissa kyberrikosten uhriksi joutumisen kanssa. Myös Cheng kollegoineen (2020) tunnistavat tutkimuksessaan kyberrikosten uhriksi joutumisen ja yleisesti informaatioteknologian käytön, älypuhelinten ja tietokoneiden käytön olevan positiivisesti yhteydessä toisiinsa.

Kuroki (2012) on tunnistanut, että mikäli yksilöllä on aiemmin ollut kokemuksia kyberrikoksista yleisesti, on yksilöllä taipumus luottaa vähemmän palveluntarjoajiin ja luovuttaa vähemmän henkilökohtaista dataa kuin yksilöillä, joilla ei aiemmin ole ollut kokemuksia kyberrikoksiin liittyen. Riekin, Böhmen ja Mooren (2014) mukaan yksilöt, jotka eivät ajattele olevansa alttiita kyberrikoksen uhriksi joutumiseksi käyttävät omatoimisemmin informaatioteknologiaa, ovat parempia omaksumaan online-palveluita ja kokevat enemmän turvallisuuden tunnetta internetissä, mutta toisaalta taas yksilöt, jotka kokevat olevansa enemmän haavoittuvaisia kyberrikoksille kuten tietojenkalastelulle välttävät internetin ja online-palveluiden käyttämistä riskin pienentämiseksi. Tämä voi paradoksaalisesti johtaa siihen, että ne, jotka eivät koe olevansa niin haavoittuvaisia kyberrikoksille, voivat helpommin joutua uhreiksi.

3.4.1 Kohteiden persoonallisuus- ja käyttäytymistekijät

Abroshan kollegoineen (2021) löysi tutkimuksessaan yhteyttä käyttäjän riskinottokäyttäytymisessä ja heidän todennäköisyydessään vastata tietojenkalaste-

luun, sillä henkilöt, joilla on taipumusta korkeaan riskinottoon, voivat avata tietojenkalastelulinkin todennäköisemmin. Tutkijat tunnistivat, että riskinottokäyttäytymisen tyypillä on vaikutusta, sillä esimerkiksi henkilöillä, joilla on taipumusta ottaa spesifisti taloudellisia riskejä tai sosiaalisia riskejä, ei ole korkeampaa todennäköisyyttä joutua tietojenkalastelun uhriksi, mutta henkilöt, joilla on yleisesti taipumusta riskejä ottavaan käyttäytymiseen, on korkeampi todennäköisyys avata tietojenkalastelulinkki. Riskinottokäyttäytymisellä ei kuitenkaan ollut vaikutusta siihen, avaako henkilö tietojenkalasteluviestiä tai antaako informaatiota tietojenkalastelijalle. (Abroshan ym., 2021).

Chon, Camin ja Oltramarin (2016) mukaan tietojenkalasteluun lankeamiseen vaikuttaa persoonallisuuspiirteet, sillä tietojenkalastelun yritykset voivat herättää kohteessa epäitsekkyyttä tietojenkalastelijan vedotessa mahdollisen uhrin tunteisiin pyytämällä rahaa huonoon taloudelliseen tilanteeseen tai aiheuttamalla pelkoa. Tupes ja Christal (1992) ovat luoneet viiden suuren persoonallisuuden mallin (The big five personality model), jossa on viisi eri persoonallisuuden dimensiota;

1. Avoimuus kokemukselle
2. Tunnollisuus
3. Ulospäinsuuntautuneisuus
4. Suostuvuus
5. Neuroottisuus

Tietojenkalastelun uhriksi joutumiseen altistavia persoonallisuuspiirteitä ovat tutkimuksen mukaan suostuvaisuus ja neuroottisuus, jotka korreloivat positiivisesti koetun luottamuksen ja riskinottohalukkuuden kanssa (Cho, Cam & Oltramari, 2016). Adalin ja Goldbeckin (2014) mukaan yksilöt, jotka ovat avoimia kokemuksille, ovat älykkäitä ja heillä on vilkas mielikuvitus sekä monipuolisia ideoita ja näkökulmia. Yksilöt, jotka ovat tunnollisia puolestaan ovat usein organisoituneita, uskollisia, pitkäjänteisiä ja vastuullisia, jonka seurauksena he ovat hyviä saavuttamaan asioita esimerkiksi työssä ja heillä on hyvät suunnittelutaidot. Ulospäinsuuntautuneet yksilöt ovat ekstroverttejä, seurallisia ja energisiä. Suostuvaisilla yksilöillä puolestaan on taipumus olla enemmän yhteistyökykyisiä, avuliaita, optimistisia ja luottavaisempia muita kohtaan. Neuroottiset yksilöt ovat tyypillisesti ahdistuneita, ailahtelevia, kireitä ja kokevat usein helposti negatiivisia tunteita. (Adali & Goldbeck, 2014). Cho ja kollegat (2016) tekivät tutkimuksen persoonallisuustyyppien vaikutuksesta loppukäyttäjän taipumukseen olla haavoittuvainen tietojenkalasteluhyökkäyksissä ja tunnistivat yhteyden suostuvan ja neuroottisen persoonallisuustyypin korrelaation tietojenkalasteluhyökkäyksessä haavoittuvuudelle.

Neurokehitykselliset häiriöt voivat vaikuttaa tietojenkalastelun uhriksi joutumiseen. Neurokehityksellisten häiriöiden luokka sisältää älylliset vaikeudet, kommunikaation vaikeudet, autismin kirjon, ADHD:n ja spesifejä oppimishäiriöitä (American Psychiatric Association, 2015, s. 1). Johtuen neurokehityksellisiin häiriöihin liittyvistä mahdollisista kriittisen ajattelun ja harkitsemisen ongelmista yksilöt (Good & Fang, 2015), joilla on neurokehityksellisiä häiriöitä,

voi ilmentää huonosti internetiin sopivaa käytöstä (Carli, Durkee, Wasserman D, Hadlaczky, Despalins, Kramarz, Wasserman C, Sarchiapone, Hoven, Brunner & Kaess, 2013). Tämä puolestaan voi johtaa siihen, että yksilöt päätyvät helpommin kyberrikoksen kuten käyttäjä manipuloinnin uhriksi (Woods, 2022), joka voidaan toteuttaa tietojenkalasteluhyökkäyksen avulla. Esimerkiksi yksilöt, joilla on tiettyjä oppimisen häiriöitä kuten dysleksia, voivat tehdä virheitä lukiessaan huijausviestejä päätyen viestissä mahdollisesti olevan linkin kautta huijaussivustolle ja jakaa henkilökohtaista informaatiota (Woods, 2022). Tämän perusteella heillä voi olla myös suurempi mahdollisuus joutua tietojenkalastelun uhriksi.

Myös yksilöt, joilla on psykoottisia häiriöitä voivat paljastaa herkemmin henkilökohtaista informaatiota itsestään ja muista sekä olla taipuvaisempia käymään epäilyttävillä nettisivuilla avaten epäilyttäviä linkkejä (Woods, 2022). Tämä voi johtaa kohonneeseen tietojenkalastelun uhriksi joutumisen mahdollisuuteen, koska yksilöt jakavat helpommin henkilökohtaista informaatiota, jota tietojenkalastelijat voivat hyödyntää ja osaltaan myös voivat mennä helpommin tietojenkalastelunettisivuille.

Yksilöt, joilla on kaksisuuntainen mielialahäiriö, voivat jakaa omasta aloitteestaan matalammalla kynnyksellä henkilökohtaista informaatiota ja toisaalta myös olla helpommin manipuloitavissa jakaa henkilökohtaista informaatiotaan lisää. Etenkin maanisessa vaiheessa yksilö voi myös olla helpommin johdateltavissa haitallisille nettisivuille heidän kohonneen riskikäytöksensä vuoksi heidän esimerkiksi klikatessa sähköpostitse saatua pahantahtoista linkkiä. (Woods, 2022). Tästä voi päätellä, että myös kaksisuuntaisesta persoonallisuushäiriöstä kärsivät yksilöt voivat olla alttiimpia joutua tietojenkalastelun uhriksi.

Yksilöt, joilla on depressiivinen häiriö voivat myös häiriöstä johtuvan mahdollisen kognitiivisen prosessoinnin heikkenemisen seurauksena olla alttiimpia tekemään päätöksiä heikentyneesti, jolloin yksilöt voivat päätyä menemään epäilyttäville nettisivuille linkkien kautta (Donalds & Osei-Bryson, 2020). Tämän johdosta myös depressiivisestä häiriöstä kärsivät voisivat olla alttiimpia tietojenkalastelun uhriksi joutumiseen, koska he eivät välttämättä tunnista niin herkästi tietojenkalastelussa usein hyödynnettäviä epäilyttäviä nettisivuja heikentyneen päätöksentekokyvyn vuoksi.

Ahdistuneisuushäiriöstä kärsivillä yksilöillä voi olla taipumusta olla henkisesti kuormittuneita ja poissaolevia, jonka vuoksi yksilöiden päätöksentekokyky voi olla heikentynyt ja he eivät välttämättä ajattele kyberturvallisuutta paljoa, mikä osaltaan voi johtaa esimerkiksi heidän käyvän epäilyttävillä nettisivuilla, joihin sähköpostiviesti ohjaa (Woods, 2022). Myös tästä voi vetää johtopäätöksen siihen, että yksilöt voivat olla alttiimpia tietojenkalasteluhyökkäysten uhriksi joutumiseen, mikäli he kärsivät ahdistuneisuushäiriöstä.

Obsessiivis-kompulsiivisesta häiriöstä ja siihen liittyvistä häiriöistä kärsivät yksilöt voivat olla alttiimpia käyttäjän manipuloinnille johtuen tyypillisesti toimia motivoivasta kompulsiosta. Tämän vuoksi käyttäjän manipuloijan mahdollista hyödyntää esimerkiksi ahdistuneisuutta tai tiettyä obsessiivista käytöstä manipuloidessaan kohdetta. Myös epärationaaliset ajatukset voivat johtaa

uhriksi joutumiseen. (Woods, 2022). Obsessiivis-kompulsiivinen häiriö voi siis altistaa yksilöiden joutumista tietojenkalastelun uhriksi.

Yksilöt, joilla on neurokognitiivisia häiriöitä, jotka voivat johtaa esimerkiksi tarkkaavaisuuden heikentymiseen, epäloogiseen ajatteluun, hämmentymiseen siinä kehen voi luottaa ja muistin häiriöihin, voi olla suurempi todennäköisyys joutua käyttäjän manipulaation uhriksi avaamalla herkemmin sähköpostitse tulleita epäilyttäviä linkkejä (Woods, 2022).

Skitsotyyppisestä persoonallisuushäiriöstä kärsivät yksilöt voivat olla käyttäjän manipulaatiolle alttiimpia, sillä heidän käytöksensä voi olla omalaatuista, oudon kielenkäytön ja ajattelun sekä epätyypillisen hahmottamiskokemusten kanssa (Black & Grant, 2014, s. 398). Toisaalta myös on viitteitä siitä, että skitsotyyppisestä persoonallisuushäiriöstä kärsivät yksilöt oireistaan huolimatta saattava olla vähemmän sosiaalisen median alustoilla ja olla vähemmän sitoutuneita sosiaaliseen interaktioon sekä taipuvaisia epäilevyyteen ja vainoharhaisuuteen (Woods, 2022), jonka myötä heidän riskinsä joutua uhriksi voi olla pienempi riippuen siitä, mikä piirre häiriössä dominoi.

Epävakaasta persoonallisuushäiriöstä kärsivät yksilöt voivat kärsiä intensiivisestä hylkäämisenpelosta, jonka vuoksi heihin kohdistetut käyttäjän manipulointiin perustuvat hyökkäykset (Woods, 2022), kuten tietojenkalastelu, voivat onnistua korkeammalla todennäköisyydellä.

Histrionisesta persoonallisuushäiriöstä kärsivillä yksilöillä voi olla myös alttiutta joutua tietojenkalastelun uhriksi. Yksilöt, joilla on histrioninen persoonallisuushäiriö, voivat olla taipuvaisia jakamaan henkilökohtaista informaatiota itsestään sekä muista ympärillään (Nurse, 2019) sekä käyttäytyä huomionhakuisesti (Black & Grant, 2014, s. 399). Tämä voi näyttäytyä avoimuutena ja ylenpalttisena luottamisena muihin (Nurse, 2019), jotka piirteinä voivat altistaa yksilön päätymään herkemmin käyttäjän manipuloinnin uhriksi (Woods, 2022).

Yksilöt, joilla on narsistinen persoonallisuushäiriö voivat olla alttiimpia käyttäjän manipuloinnin uhriksi joutumiselle, koska heillä on taipumus olla esillä ja haluta ihailua, mikä voi johtaa informaation ylenpalttiseen jakamiseen ja postaamiseen sekä toisaalta pelkoon heidät negatiiviseen valoon saattavan informaation leviämisestä, jota manipuloijat voivat hyödyntää (Woods, 2022). Myös Curtis kollegoineen (2018) on todennut korkeiden narsististen piirteiden altistavan tietojenkalasteluhyökkäyksen uhriksi joutumiselle, mikä osaksi voi johtua heillä mahdollisesti ilmenevästä suuresta itseluottamuksesta (Campbell, Goodie & Foster, 2004) sekä epärealistisesta optimismista toimia menestyksekkäästi haastavissa tilanteissa pohjautuen omaan ylivertaisuuteen (Farwell & Wohlwend-Lloyd, 1998).

Riippuvaisesta persoonallisuushäiriöstä kärsivät yksilöt voivat myös olla alttiimpia tietojenkalastelulle käyttäjän manipuloinnin keinona. Yksilöt, joilla on riippuvainen persoonallisuushäiriö kokevat tarvitsevansa tukea esimerkiksi emotionaalisella tasolla ja päätöksenteossa (Woods, 2022) ja toisaalta myös he voivat kokea arvottomuutta perustuen kritiikkiin ja paheksuntaan (Black & Grant, 2014, s. 402). Tämä voi altistaa yksilöt helpoksi manipulaation kohteeksi heidän ollessa mahdollisesti taipuvaisempia piirteidensä vuoksi avaamaan

epäilyttäviä sähköpostiviestejä ja toimimaan niiden pyytämällä tavalla (Woods, 2022).

3.4.2 Uhrien demografia

Choin (2008) mukaan on yleisesti tunnistettu demografisten tekijöiden vaikuttavan siihen, ketkä joutuvat kyberrikoksen uhriksi. Abroshan kollegoineen (2021) ovat tunnistaneet uhrien luottamuksen saavuttamisen olevan usein liitoksissa askel askeleelta etenevään strategiaan tarkoituksena saada uhri lankeamaan tietojenkalasteluun. Mutta mitkä demografiset tekijät oikein vaikuttavat ihmisen todennäköisyyteen langeta tietojenkalasteluun?

Abroshan ja kollegat (2021) ovat tunnistaneet, että ikä, sukupuoli ja koulutus voivat vaikuttaa suorasti tai epäsuorasti siihen, miten potentiaalinen uhri vastaa tietojenkalasteluhyökkäyksen yritykseen. Abroshan ja kollegat (2021) löysivät tutkimuksessaan sukupuolten välisiä eroja, sillä tutkimuksessa selvisi, että naiset saattavat olla hieman herkempiä klikkaamaan tietojenkalastelulinkkiä ja sukupuoli onkin heidän mukaansa merkittävä, mutta ei kuitenkaan vahva ennustaja. Sarno, Lewis, Bohil, Shoss ja Neider (2017) tunnistivat iän ja sukupuolen suhdetta roskapostin, aidon sähköpostin ja vaarallisen sähköpostin identifiointia koskevassa tutkimuksessaan, että keski-ikäisillä aikuisilla on pienempi riski ei-autenttisen sähköpostin tunnistamiseen kuin nuoremmilla aikuisilla, mutta mitään suurta eroa kuitenkaan ei löytynyt sukupuolien välillä tämän näkökulman osalta. Myös Shengin, Holbrookin, Kumaragurun, Cranorin ja Downsin (2010) mukaan sukupuolella on merkitystä siihen, klikkaako käyttäjä tietojenkalastelulinkkiä vai ei ja tutkimuksessa ilmeni naisten olevan todennäköisemmin klikkaamassa tietojenkalastelulinkkiä kuin miesten. Shengin ja kollegoiden (2010) tutkimuksessa sukupuolella oli epäsuora vaikutus teknisen tietämyksen ja käyttäjään harjoituksen puutteen seurauksena ja myös tässä tutkimuksessa naisten tunnistettiin olevan alttiimpia tietojenkalastelulle kuin miesten. Sheng kollegoineen (2010) myös tunnisti, että tutkimukseen osallistuvista 18–25-vuotiaat olivat alttiimpia tietojenkalastelulle kuin verrokkinsa.

Lin kollegoineen (2019) tunnisti tutkimuksessaan, että vanhemmat naiset olivat alttiimpia tietojenkalastelulle ja toisaalta nuoret miehet olivat alttiimpia tietojenkalastelulle kuin vanhemmat miehet. Lin ja kollegat (2019) myös tunnistivat, että nuoremmat olivat alttiita niukkuuden, auktoriteetin sekä havaitun kontrastin eli yksilön kokemus asioista erilaisena, kun ne tapahtuvat peräkkäin ja sosiaalisen todisteen eli esimerkiksi arvostelun ja trendien parissa. Vanhempien henkilöiden osalta tietojenkalastelut, jotka hyödynsivät sitoutumisen, pitämisen ja vastavuoroisuuden periaatteita, ennustivat alttiutta tietojenkalasteluun lankeamiseen. Vanhemmat ihmiset olivat erityisen alttiita vastavuoroisuuden periaatteelle ja nuoremmat taas niukkuuden periaatteelle. (Lin ym., 2019).

3.4.3 Miksi tietoja kalastellaan

Tietojenkalastelun taustatekijöitä ei ole tutkittu aiemmassa tieteellisessä kirjallisuudessa spesifisti. Voisi kuitenkin luulla tietojenkalasteluhyökkäysten kumpuavan rahan tarpeesta tai yhteiskunnan ongelmista kuten korruption korkeasta tasosta, mutta miksi ihmiset länsimaisissa hyvinvointivaltioissa kuten Suomessa tekevät tietojenkalasteluhyökkäyksiä, vaikka Suomessa sosiaaliturva lähtökohtaisesti pyrkii tarjoamaan elämän perustarpeet ja korruptio koetaan yleisellä tasolla vähäiseksi? Tämä kysymys loi pohjan tutkimukselleni. Mikäli jätetään huomiotta ulkopuoliset tekijät, yksilön persoonallisuus voi osaltaan vaikuttaa tietojenkalasteluhyökkäyksien harjoittamiseen yleisesti.

Vaikka tietojenkalasteluun ei aina varsinaisesti liity rikollisuutta tai sen kautta saavutettua hyötyä, on otettava huomioon myös rikollisen toiminnan aspekti. Rikollisuutta yleisesti tarkasteltaessa psykopatia on tärkeä huomioonotettava tekijä, sillä esimerkiksi Polaschek ja Daly (2013) väittävät psykopatian ja rikollisen käyttäytymisen välillä olevan yhteyden olevan voimakas. Tätä voi selittää se, että Seigfried-Spellarin Villacís-Vukadinovićin ja Lynamin (2017) mukaan psykopaattisia piirteitä omaavat ihmiset korreloivat positiivisesti narsismin kanssa ja puolestaan negatiivisesti tunnollisuuden ja suostuvaisuuden kanssa. Seigfried-Spellar ja kollegat (2017) kuvaavat psykopatiaa persoonallisuuden piirteenä, joka voi koostua esimerkiksi epäsosiaalisesta ja väkivaltaisesta käytöksestä, egosentrisyydestä, impulsiivisuudesta sekä vastuuttomuudesta ja psykopatia on Polaschekin ja Dalyn (2013) mukaan vahvasti liitoksissa antisosiaaliseen persoonallisuushäiriöön. Tutkijat havaitsivat myös psykopatialla olevan yhteyden kyberrikolliseen käyttäytymiseen, jonka vuoksi psykopaattisia piirteitä omaavilla henkilöillä on taipumusta tehdä normaalia enemmän kyberrikoksia kuten identiteettivarkauksia ja tietojenkalastelua (Seigfried-Spellar ym., 2017). Moor ja Anderson (2019) tunnistivat myös, että psykopaattisia piirteitä omaavilla yksilöillä on taipumusta ylipäätään kyberhuijauksiin ja kyberaggressioon. Vahingollista online-käyttäytymistä ennustaa erityisesti psykopatia ja miessukupuoli, joiden välillä on löydetty korrelaatiota (Bogolyubova, Panicheva, Tikhonov, Ivanov & Ledovaya, 2018).

Histrionisen persoonallisuushäiriöön taipuvaiset henkilöt voivat todennäköisemmin harjoittaa käyttäjän manipulaatiota (Woods, 2022), jonka yksi keino tietojenkalastelu on (Khonji ym., 2013). Myös narsistinen persoonallisuushäiriö, paranoidi persoonallisuushäiriö, epävakaa persoonallisuushäiriö ja obsessiivis-kompulsiivinen persoonallisuushäiriö ovat yhteydessä kyberrikolliseen käytökseen, mutta tutkimuksessa ei noussut esiin ensisijaisesti taipumusta tietojenkalasteluun tai käyttäjän manipulaatiota (Woods, 2022).

Antisosiaalinen persoonallisuushäiriö voi altistaa henkilön tekemään kyberrikoksia. Antisosiaalisen persoonallisuushäiriön tyypillisiä persoonallisuuspiirteitä on petollisuus ja manipulointi sekä impulsiivisuus ja sosiaalisten normien noudattamisen heikkous (Black & Grant, 2014, s. 397–298) Koska antisosiaalisesta persoonallisuushäiriöstä kärsivät yksilöt eivät koe välttämättä suurissa määrin vastuuntuntoa, voivat yksilöt ryhtyä rikollisiin toimenpiteisiin matalammalla kynnyksellä (Black & Grant, 2014, s. 397). Manipulaatioon taipuvuu-

den vuoksi antisosiaalisesta persoonallisuushäiriöstä kärsivät yksilöt voivat herkemmin harjoittaa käyttäjän manipulointia (Woods, 2022). Tietojenkalastelu on yksi käyttäjän manipuloinnin keinoista, joten antisosiaalisesta persoonallisuushäiriöstä kärsivät yksilöt voivat olla herkempiä tekemään tietojenkalastelua kuin yksilöt, joilla ei persoonallisuushäiriötä ole.

Dark triadin persoonallisuuspiirteet voivat myös olla yhteydessä tietojenkalasteluun. Paulhus ja Williams (2002) kuvaavat persoonallisuuspiirteiden Dark triadin koostuvan häikäilemättömyydestä, narsismista ja psykopatiasta. Häikäilemättömyyden voidaan kuvata liittyvän strategisen petoksen ja joustavan moraalisen taktiikan avulla maksimoidun henkilökohtaisen hyödyn tavoitteluun manipulatiivisella käyttäytymisellä (Bereczkei, 2015). Narsismi puolestaan nähdään valta-aseman tavoitteluun sekä muiden hyväksikäytön oikeuttamiseen ja halukkuuteen liittyvänä piirteenä (McHoskey, 1995). Psykopatiaa kuvataan piirteenä, jossa yksilöllä ei ole taipumusta tuntea empatiaa, ja he ovat taipuvaisia aggressiivisuuteen ja petokseen (Azizli, Atkinson, Baughman, Chin, Vernon, Harris & Veselka, 2016). Dark triadiin määriteltyjä piirteitä pidetään usein yhteiskunnallisesti epämiellyttävinä, mutta ne eivät kuitenkaan poikkea normaalista subkliinisestä vaihteluvälistä, joten näin ollen ne voidaan luokitella ominaisuuspohjaisella spektrillä yhteiskunnassa eikä niinkään varsinaisina persoonallisuushäiriöinä (Vernon, Villani, Vickers & Harris, 2008), jonka vuoksi yksilöt, joilla luokitellaan olevan korkeat Dark triadin piirteet ovat tyypillisesti yhteiskunnan toimivia jäseniä (Furnham, Richards & Paulhus, 2013). Dark triadin persoonallisuuspiirteille yhteistä on niiden taipumus matalaan miellyttämisenhaluun (Jakobwitz & Egan, 2016), joka on yksi tietojenkalasteluhyökkäysten altistavista piirteistä (Cho, Cam & Oltamari, 2016).

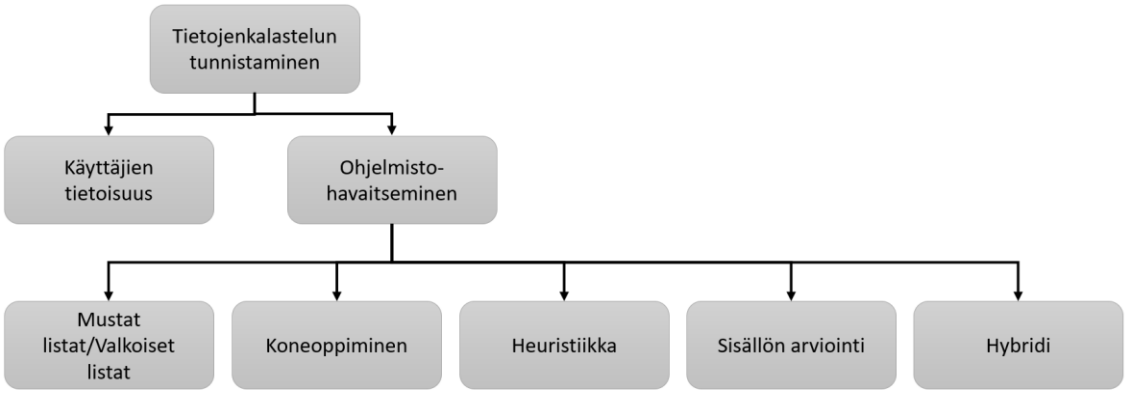
Curtis kollegoineen (2018) tutkivat Dark triadin yhteyttä tietojenkalasteluun, jossa todettiin, etteivät hyökkääjän Dark triadin mukaiset piirteet kuitenkaan ennusta tietojenkalasteluhyökkäyksessä hyödynnettyjen tietojenkalastelusähköpostien tehokkuutta. Tutkimuksessa tutkittiin kuinka paljon muutoksia Dark triadin piirteiden osalta korkeat pisteet saaneet yksilöt tekevät sähköpostipohjaan. Korkeat pisteet psykopatiassa saaneiden yksilöiden toiminta korreloi negatiivisesti muutosten teon suhteen, narsistisista piirteistä korkeat pisteet saaneet tekivät vähemmän muutoksia ja häikäilemättömyydestä korkeat pisteet saaneet tekivät enemmän muutoksia. (Curtis ym., 2018).

Yksilöt, jotka olivat siis saaneet korkeat pisteet häikäilemättömyydessä, todettiin panostavan tietojenkalastelusähköpostiin enemmän kuin yksilöiden, joilla todettiin häikäilemättömiä piirteitä, näkevän enemmän vaivaa tietojenkalastelusähköpostien kirjoittamiseen. Yksilön saamat korkeat narsistiset piirteet ennustivat puolestaan vähempää panosta tietojenkalastelusähköpostien kirjoittamisessa, joka voi olla yhteydessä heillä tyypillisesti ilmenevään korkeaan itseluottamukseen. Korkeat pisteet psykopatian osalta saaneet yksilöt saattavat puolestaan vain toivoa osan potentiaalisista uhreista toimivan hyökkääjän osoittamalla tavalla ja kiirehtien pyrkiä lähettämään tietojenkalastelusähköpostin mahdollisimman monelle. (Curtis ym. 2018).

3.5 Tietojenkalastelun torjuminen

Tässä kappaleessa käsitellään, miten tietojenkalasteluhyökkäyksiä on mahdollista torjua. Gutierrez kollegoineen (2018) nostaa esiin, että tietojenkalastelun torjumisessa, esimerkiksi sähköpostitse tietojenkalastelua torjuvat suositut ohjelmat kuten SpamAssassin, ongelmana voi olla ollut niiden perustuminen vain viestin pintapuoliseen tekstiin lingvististen kaavojen ja tyypillisten ”temppujen” sijasta. Edellä mainituista esimerkkejä voi olla viesteissä erilaisten lauserakenteiden käyttö (Gutierrez ym., 2018). Gutierrezin ja kollegoiden mukaan tietojenkalastelun torjuntaan pyrkivät mekanismit voidaan jakaa kolmeen luokkaan, jotka ovat luokitteluun perustuva, sääntöihin perustuva ja manuaaliseen työhön perustuvat mekanismit. Lin kollegoineen (2021) klassifioi tietojenkalasteluverkkosivujen ehkäisytekniikoiden torjuntaan perustuviin ja identifikaatioon perustuviin lähestymistapoihin. Torjuntaratkaisut käsittävät mustat listat ja koneoppimiseen perustuvat mallit, jotka ehkäisevät tietojenkalastelua perustuen niiden tietoaineiston avulla toteutettuun harjoitteluun. Tietojenkalastelun identifiointiin perustuvat ratkaisut puolestaan hyödyntävät mallia tietojenkalastelun torjunnassa, joka luodaan perustuen aiempiin tietojenkalasteluhyökkäyksiin kohdistettuihin eri brandeihin ja niiden verkkosivuihin. Näiden mallien tavoitteena on tunnistaa ja havaita tietojenkalastelun kohteita. (Lin ym., 2021).

Sahingoz kollegoineen (Kuvio 5, 2019) sekä Jain ja Gupta (2017) jakavat tietojenkalastelun torjunnan kahteen eri teemaan pohjautuviin menetelmiin, jotka ovat käyttäjien tietoisuus sekä ohjelmistohavaitseminen. Ohjelmistohavaitseminen jakautuu lisäksi heidän viiteen eri osa-alueeseen, joita ovat mustat ja valkoiset listat, heuristiikka, visuaalinen samankaltaisuus, koneoppiminen ja hybridinäkökulmat (Sahingoz ym. 2019).



KUVIO 5 Tietojenkalastelun torjuntatyypit (Sahingoz ym., 2019)

3.5.1 Mustat listat/Valkoiset listat

Listoihin perustuvat tietojenkalasteluhyökkäyksien estämiseen tarkoitetut järjestelmät perustuvat luokittelemaan nettisivut aitoihin ja vilpillisiin valkoisten

listojen ja mustien listojen avulla (Sahingoz ym. 2018). Jainin ja Guptan (2016) kehittämä metodi sisältää kaksi vaihetta, jotka perustuvat käyttäjän varoittamiseen automaattisesti päivittyvän valkoisten listojen avulla. Metodin ensimmäinen vaihe on moduuli, jossa IP-osoitteet täsmäytetään valkoiselta listalta löytyvän moduulin kanssa ja toinen, jossa poistetaan linkkien piirteet lähdekoodissa. (Jain & Gupta, 2016).

Guptan, Arachchilagen ja Psannisin (2018) mukaan tietojenkalastelua ehkäisevät mustat listat toimivat siten, että on olemassa lista epäluotettavista URL-osoitteista ja IP-osoitteista, jotka on tunnistettu aiemmin tietojenkalastelua suorittaviksi. Ongelmana tietojenkalastelua ehkäisevien mustien listojen käytössä on se, ettei niihin voi luottaa täysin, sillä ne vaativat jatkuvaa päivittämistä ja verkkoliikenteen monitorointia palveluntarjoajalta uusien tietojenkalastelua tekevien IP- ja URL-osoitteiden vuoksi (Gupta ym., 2018). Yang, Zhao ja Zeng (2019) väittävät myös, että yksi yleisistä tekniikoista tietojenkalastelunettisivujen estämiseksi on mustat listat ja heidän mukaansa esimerkiksi Google tarjoaa pahamaineisista nettisivuista koostuvan blacklistin, jota päivitetään jatkuvasti. Oestin, Safaein, Doupén, Ahnin, Wardmanin ja Tyersin (2019) mukaan nykyisin sekä suurimmat verkkoselaimet työpöydällä, että mobiilissa ovat ottaneet käyttöön tietojenkalastelusivustoja ehkäiseviä alustoja, jotka pyrkivät varoittamaan käyttäjää tunnetusta haitallisesta nettisivusta.

Kuten aiemmin mainittiin, tietojenkalastelua ehkäiseviä mustia listoja tulee myös päivittää. Päivittämisen voi tehdä vertaamalla URL:ää aidon ja turvallisen sivun URL:ään tai esimerkiksi hyödyntämällä koneoppimista (Vayansky ja Kumar, 2018). Gupta ja kollegat (2018) väittävät, että väärän nettisivun URL voi kuitenkin näyttää aidolta ensimmäisellä vilkaisulla, jonka seurauksena käyttäjät voivat joutua tietojenkalasteluhyökkäyksen kohteeksi huomaamattaan. Lin ja kollegat (2011) tutkivat verkkotunnuksen korostamisen tehokkuutta, joka on nykyisin osana useampia selaimia, mutta tutkimuksessaan havaitsivat vain marginaalisen onnistumisen esimerkiksi tietojenkalastelusivuston tunnistamisessa, kun käyttäjän huomio vietiin eksplisiittisesti osoiteriville.

Vaikka mustien listojen käyttö tekee mahdottomaksi hyökkääjän toteuttaa hyökkäys samaa URL- tai IP-osoitetta käyttäen, niiden ei ole mahdollista torjua varsinaista tietojenkalasteluhyökkäystä (Sahingoz ym., 2016) esimerkiksi 0-tunti -tietojenkalasteluhyökkäyksen ollessa kyseessä, jolloin sivustoa ei ole vielä tunnistettu tietojenkalastelusivustoksi ja lisätty mustalle listalle (Khonji, Iraqi & Jones, 2013). Shengin, Wardmanin, Warnerin, Cranorin, Hongin ja Zhangin (2009) mukaan mustiin listoihin perustuva tietojenkalasteluhyökkäyksen torjunta onnistuu noin 20% todennäköisyydellä 0-tunnin tietojenkalasteluhyökkäyksen ollessa kyseessä.

3.5.2 Koneoppiminen

Koneoppimisen hyödyntäminen on yksi tietojenkalasteluhyökkäysten torjuntamuodoista (Sahingoz ym., 2019). Chiewin ja kollegoiden (2019) mukaan koneoppimiseen perustuva tietojenkalastelun estämisen ratkaisu on tuottanut lupaavia tuloksia, joka perustuu siihen, että kapitalisoidaan suuri määrä indikaat-

toreita ja niiden perusteella tunnistetaan uusia tietojenkalastelunettisivuja. Indikaattorien valinta voidaan tehdä kahdella tavalla, joita ovat wrapper- ja suodatinmetodit, joissa ensimmäinen metodi ajetaan iteratiivisesti ja jokaisessa ajossa luodaan ominaisuusosajoukko ja se arvioidaan luokittelun avulla. Wrapper-metodin ongelmana on se, että arvioidessa suurempaa joukkoa ominaisuuksia, iteraatioiden määrä kasvaa eksponentiaalisesti ja on laskennallisesti epäkäytännöllistä. (Chiew ym., 2019)

Gutierrezin ja kollegoiden (2018) mukaan koneoppimisessa sääntöihin perustuvat tietojenkalastelua torjumaan pyrkivät mekanismit toimivat suodattimina, jotka hyödyntävät toiminnassaan erilaisia variaatioita. Nämä variaatioita voivat muodostua muun muassa syntaksitarkastukset, lähettäjän osoitteeseen liittyvät tarkastukset, URL:n tarkastukset sekä erilaisten avainsanojen tarkastamisesta sääntöihin perustuen (Gutierrez ym., 2018). Vayanskyn ja Kumarin (2018) mukaan tietojenkalastelua voidaan ehkäistä suodattimilla, jotka estävät käyttäjää saamasta tietojenkalastelusähköpostia tai muuta tietojenkalasteluyritystä edes tietoonsa. Gupta ja kollegat (2018) nostavat esiin tietojenkalastelun suodattamiseen kehitetyn tekniikan, joka perustuu verkkotasolla tapahtumaan suojaukseen käyttäen roskapostia ehkäiseviä suodattimia, jotka havaitsevat tietojenkalasteluhyökkäyksiä ja pyrkivät vähentämään niiden määrää. Ongelmana on kuitenkin se, että hyökkääjät voivat suodattimia välttääkseen tehdä rakenteellisia tai sisällöllisiä muutoksia tietojenkalasteluviestiin, jolloin suodattimet eivät välttämättä havaitse sitä. Tietojenkalastelun torjuminen suodattimien avulla ei siis ole kovin varmaa niiden ollessa herkkiä muutosten suhteen ja toisaalta myös ongelmana on tietojenkalastelusisältöä ylläpitävien verkkotunnusten taipumus olla tilapäisiä, jolloin on epävarmaa turvautua säännöllisiä URL-skannauksia tekeviin torjuntatekniikoihin. (Gutierrez ym., 2018).

Gutierrezin ja kollegoiden (2018) mukaan tietojenkalasteluja tehtailevat rikolliset löytävät kuitenkin jatkuvasti uusia tapoja ohittaa suodattimet. Yksi tapa, joilla rikolliset pyrkivät ohittamaan suodattimet on kohdennettu tietojenkalasteluhyökkäys, jolloin rikollinen lähettää hyvin kehittyneitä ja personoituja viestejä (Curtis ym., 2018). Laszka, Vorobeychik and Koutsoukos (2015) väittävät, että kuitenkin myös kohdennettuja tietojenkalasteluhyökkäyksiä voidaan pyrkiä torjumaan käyttämällä sähköpostissa tietojenkalastelusuodattimia, mutta toisaalta se voi myös suodattaa oikeita ja turvallisia sähköposteja, jonka vuoksi se ei välttämättä ole kovin tehokasta. Kohdennettujen tietojenkalasteluhyökkäyksien torjunta voi olla ongelmallista, sillä niiden hienostuneiden ominaisuuksien vuoksi niitä ei välttämättä tunnisteta vahingollisiksi niin helposti kuin esimerkiksi massoittain lähetetyt kohdentamattomat tietojenkalasteluhyökkäykset sähköpostitse (Laszka ym., 2015). Tietojenkalasteluviestit voivat yksinkertaisten semanttisten ja rakenteellisten muutosten myötä kuitenkin välttää niiden ehkäisyyn tarkoitettuja suodattimia, mikä voi lisätä hyökkäyksen onnistumista (Gutierrez ym., 2018).

3.5.3 Heuristiikka

Heuristiikkaan perustuvat tietojenkalasteluhyökkäysten torjuntaan tähtäävät tekniikat hyödyntävät tietojenkalastelusivuilta poimittuja piirteitä tietojenkalasteluhyökkäyksen havaitsemiseen (Silva, Feitosa & Garcia, 2020). Silvan, Feitosan ja Garcian (2020) mukaan heuristiikkaan perustuvissa ratkaisuissa tietojenkalastelusivuja identifioidaan piirteitä yleisimmin siis joko sivuston URL:n tai sivuston sisällön perusteella

Raon ja Paisin (2019) mukaan nykyään pyritään hyödyntämään heuristiikan nettisivuilta poimittuja piirteitä yhdessä koneoppimisen algoritmien kanssa. Heuristiikkaan perustuvat tekniikat poimivat uniikkeja piirteitä tietojenkalastelunettisivuilta, jonka perusteella ne yleistetään parametreiksi tietojenkalastelunettisivujen torjuntaan. Heuristiikkaan perustuvat tekniikat onnistuvat yleisellä tasolla 0-päivän hyökkäysten torjunnassa paremmin kuin esimerkiksi listoihin perustuvat tekniikat. (Khonji, Iraqi & Jones, 2013).

3.5.4 Sisällön arviointi

Jainin ja Guptan (2017) mukaan tietojenkalasteluhyökkäys voi onnistua luomalla tietojenkalastelunettisivun, joka imitoi korkealla tasolla aitoa luotettua nettisivua esimerkiksi sivun kuvien, asettelun, sisällön ja tekstifontin avulla luoden sivustosta aidon näköisen esimerkiksi kopioimalla aidon sivun HTML lähdekoodin, sillä käyttäjät eivät aina huolellisesti tarkasta sivuston URL-osoitteen olevan oikea. Hyökkääjä pyrkii harhauttamaan kohdetta myös osoitteen avulla, sillä hyökkääjä voi peittää URL:n kuvalla tai skriptillä (Jain & Gupta, 2017). Chen, Ma ja Huang (2020) jakavat visuaalisen samankaltaisuuden tietojenkalastelunettisivuilla todella samankaltaiseen, paikalliseen samankaltaiseen ja eiimitoivaan luokkaan, joita verrataan aitoihin nettisivuihin, joita tietojenkalastelunettisivut imitoivat. Todella samankaltaisten tietojenkalastelunettisivujen ollessa kyseessä torjunnassa joudutaan arvioimaan näyttökuvia nettisivuista kokonaisuudessaan esimerkiksi värihistogrammien avulla (Chen ym., 2020).

Jainin ja Guptan (2017) mukaan tietojenkalastelusivusto perustuu usein siihen, että hyökkääjä valitsee kohdenettisivun tunnettujen organisaatioiden nettisivuista, jonka jälkeen kerää nettisivusta informaatiota käyttäen sitä luodakseen aidon nettisivun kaltaisen väärennetyn nettisivun. Jain ja Gupta (2017) nostavat esiin kaksi etua, joita visuaalisen samankaltaisuuteen pohjautuvien tietojenkalastelun tunnistustekniikoiden hyödyntämisellä on; ne voivat nopeasti jäljittää upotetut objektit, joita tietojenkalastelijat hyödyntävät välttääkseen tietojenkalastelun tunnistuksen käyttämällä sivustoilla esimerkiksi kuvia suoran HTML-formaattisen tekstin sijaan. Toisekseen visuaaliseen samankaltaisuuteen pohjautuvat tunnistustekniikat käyttävät tunnusmerkkejä, jotka luodaan ottamalla yleisiä piirteitä koko nettisivulta useista eri näkymistä, jonka vuoksi yksi tunnusmerkki on riittävä useiden eri näkymien tai eri versioiden havaitsemiseen tietojenkalastelunettisivujen jäljittämisessä. Tekstejä vertaavissa tietojenkalastelun jäljittämisessä hyödynnettävissä näkökulmissa on se, että ne eivät toimi, jos hyökkääjä korvaa varsinaisen tekstin kuvalla, vaikkakin se on nopeas-

ti toteutettava jäljitys. Kuvien tunnistamiseen perustuvissa näkökulmissa ongelmana on se, että ne vievät aikaa ja ovat komplekseja, vaikkakin ne ovat tarkkoja. (Jain & Gupta, 2017).

3.5.5 Hybridi

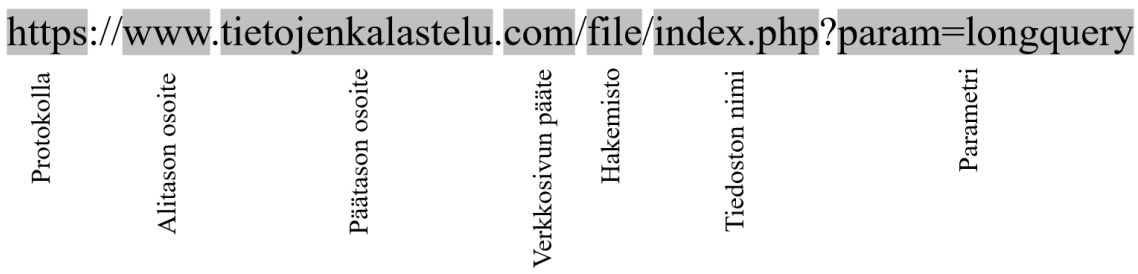
Hybriditekniikoihin perustuvat tietojenkalastelun torjuntaan pyrkivät ratkaisut yhdistelevät eri tietojenkalastelun torjuntatyyppejä. Hybriditekniikoihin perustuvia tietojenkalastelun tunnistamiseen ja sitä kautta estämiseen tähtääviä kombinaatioita on lukuisia, joista esittelen muutaman. Esimerkiksi Tan, Chiew, Yong, Sebastian, Than ja Tiong (2023) ehdottivat visuaalisten ja tekstillisten identiteetin löytämiseen pyrkiviin komponentteihin perustuvaa hybridiä identiteettipohjaista tietojenkalastelun havaitsemiseen tarkoitettua ratkaisua. Tanin ja kollegoiden (2023) ratkaisussa ensimmäisenä vaiheena on tekstinsyöttökenttien tunnistaminen, sillä mikäli nettisivulle voi syöttää tietoja, voi se kerätä käyttäjältä informaatiota. Mikäli tekstinsyöttökentät puuttuvat, luokitellaan sivusto tietojenkalastelun osalta turvalliseksi. Tämän jälkeen ratkaisu hyödyntää visuaalisen identiteetin sekä tekstillisen identiteetin etsimistä, joista visuaalisen identiteetin löydön avulla pyritään tunnistamaan ja erottamaan nettisivun logo, jota myöhemmin haetaan käänteisellä kuvalla hakukoneista pyrkien löytämään kohdeidentiteetti eli mahdollinen vastaava aito sivusto. (Tan ym., 2023)

Tekstillisen identiteetin löytämiseen pyrkivän komponentin avulla puolestaan pyritään poimimaan verkkosivuilta avainsanoja, joiden avulla pyritään löytämään kohdeidentiteetti (Tan ym., 2023). Lähestymistapana Tan kollegoineen (2023) käytti laskennallista lähestymistapaa, jossa erotellaan URL-osoitteiden rakennetta, josta puolestaan poimitaan avainsanoja. Visuaalisen ja tekstillisen identiteetin löytämiseen pyrkivillä yhdistelmillä toteutetaan siis identiteettikyselyt verkkosivun identiteetin löytämiseksi eli onko se mahdollisesti tietojenkalastelusivusto. Tutkijoiden esittelemässä hybriditekniikassa saavutettiin lupaava tulos sen onnistuessa identifioimaan nettisivuja 98.6 % tarkkuudella väärien positiivisten määrän ollessa vain 3.4%.

Krokmaz, Kocyigit, Sahingoz ja Diri (2022) ehdottavat tietojenkalasteluyritysten tunnistamiseen ja torjuntaan hybridinäkökulmaa, jossa yhdistetään sisältöperusteisia ja URL-perusteisia lähestymistapoja tunnistamisen ja torjunnan tehostamiseksi. Tutkijat valitsivat URL-perusteisen lähestymistavan (Kuvio 6), jossa analysoidaan sivuston URL:n protokolla, alitason osoite, päätason osoite, verkkosivun pääte, hakemisto, tiedoston nimi ja parametri piirteiden erottamisen ja koneoppimisen avulla ja mahdollisesti varoitetaan käyttäjää, mikäli URL tunnistetaan tietojenkalasteluksi luokittelun avulla. Sisältöperusteisessa tietojenkalastelun tunnistustekniikassa arvioidaan sivuston sisältöä esimerkiksi tekstin koko, kentät tietojen syötölle, tekstin pituus, otsikon pituus. (Krokmaz ym., 2022).

URL perusteinen tietojenkalastelun tunnistus on nopeampaa. Hybridimallissa mikäli tekniikka tunnistaa URL-pohjaiseen analyysiin perustuen sivuston tietojenkalasteluksi, ei sisältöperusteista arviota tehdä, mikä säästää aikaa. Jos kuitenkin URL tunnistetaan aidoksi, sivuston sisältö analysoidaan sisältöperus-

teisella lähestymistavalla. Ongelmana tässä on kuitenkin väärät positiiviset tulokset, jonka vuoksi tietojenkalastelu URL tunnistetaan väärin aidoksi ja sisältöperusteista arviota ei tehdä. Hybridimallin tarkkuus oli kuitenkin 98,37% tutkimuksen perusteella. (Krokmaz ym., 2022).



KUVIO 6 URL-perusteinen lähestymistapa (Krokmaz ym., 2022)

3.5.6 Käyttäjien tietoisuus

Arachchilage ja Love (2014) toteavat käyttäjän olevan tietoturvan heikoin lenkki ja käyttäjien koulutus ja tietoisuus voi olla puutteellista ja altistaa tietojenkalastelusta huonosti selviämiseen. Guptan ja kollegoiden (2018) mukaan loppukäyttäjän tietoisuus onkin yksi tärkeistä keinoista onnistuneiden tietojenkalasteluhyökkäysten ehkäisemisessä. Tämän vuoksi tietojenkalasteluhyökkäysten onnistumisen ehkäisemiseen keskittyvä loppukäyttäjille kohdistettu koulutus vaatii huomiota. Myös Kwakin ja kollegoiden (2020) mukaan yksi merkittävistä torjumiskeinoista on siis käyttäjien tietoisuuteen keskittyminen, jotta käyttäjät tunnistaisivat tietojenkalasteluhyökkäykset eivätkä toimisi hyökkääjän haluamalla tavalla. Downsin, Holbrookin ja Cranorin (2007) aiemman tutkimuksen mukaan käyttäjien tekninen tietämys lisäsi tietojenkalasteluhyökkäyksien torjumisen onnistumisen todennäköisyyttä ja näin ollen tukee näkemystä, joka korostaa tietojenkalasteluhyökkäysten torjunnassa koulutusta. Toisaalta Downs kollegoineen (2007) tunnistivat myös sen, että ylipäätään verkkoympäristön tunteminen osaltaan nostaa mahdollisuuksia siihen, että yksilö toimii paremmin kohdatessaan tietojenkalasteluhyökkäyksiä ilman, että se vaikuttaa esimerkiksi aitojen sähköpostien vastausmäärään.

Kwakin ja kollegoiden (2020) mukaan yksilöiden harjoittelulla on merkitystä nousseen turvallisuustietoisuuden kanssa ja toisaalta se myös osaltaan on todettu nostavan aktiivisuutta raportoida tietojenkalasteluhyökkäyksiä organisaatiossa, jossa yksilöt vaikuttavat. Yksilöiden rohkaiseminen ilmoittamaan havaitessaan tietojenkalasteluhyökkäyksiä huomatessaan vie eteenpäin pyrkimystä informoimaan muita tietojenkalasteluhyökkäyksen ollessa aktiivisena sekä luoda mahdollisuus aikaisen vaiheen tietojenkalasteluhyökkäyksen ehkäisemiseen (Kwak ym., 2020).

Arachchilage ja Love (2014) tekivät tutkimuksen, jossa pyrittiin selvittämän käyttäjien tietoisuuden vaikutusta omatoimiseen tietojenkalasteluhyök-

käysten torjumisen tehokkuuteen. Tutkimuksessa käsiteltiin konseptuaalista ja prosessuaalista käyttäjien tietoisuutta ja niiden todettiin vaikuttavan positiivisesti tietojenkalastelu-uhkien tunnistamiseen ja toisaalta tietoisuuden puutteen nähtiin olevan yksi pääasiallisista syistä tietojenkalastelun uhriksi joutumiselle (Arachchilage & Love, 2014).

4 KRIMINOLOGIA

Tietojenkalastelua ei välttämättä hyödynnetä rikollisiin tarkastusperiin. Tässä kappaleessa kuitenkin käsitellään kriminologinen teoria ja kriminologinen profilointi, joita voidaan soveltaa tietojenkalasteluhyökkäyksiin niiden ollessa valjastettuna rikollisiin tarkoitusperiin.

4.1 Profilointi

Rikollisia voidaan profiloida. Bada ja Nurse (2021) kuvaavat rikollisten profilointia mallien tutkimiseen perustuen oletuksiin ja yksityiskohtiin rikoksentekijästä ja rikoksista. Kyberrikollisten profilointi on tärkeä työkalu myös kyberrikosten kuten tietojenkalastelun ehkäisemisessä ja sen vuoksi on tärkeää tunnistaa niiden tunnuspiirteitä ja rikollista käyttäytymistä, jotta kyberrikoksia voidaan ehkäistä. Kyberrikollisten profilointi tähtää siis tutkimaan käyttäytymisen malleja ja piirteitä tieteellisen metodiikan avulla, jotta voidaan tunnistaa, kuka syyllistyy tietyn tyyppiseen rikokseen tai on todennäköinen tekemään tietyn tyyppisen rikoksen (Kirwan & Power, 2011 s. 4). Kyberrikollisen profilointi perustuu johdonmukaisuuden oletukseen, jossa oletetaan rikosten toteuttamisen yhteydessä esiintyvän käytöksen olevan samankaltaista kaikissa rikoksissa ja samankaltaisuuden oletukseen, jossa oletetaan rikosten suorittamisen tapa, voidaan yhdistää samankaltaisiin ominaisuuksiin tekijän taustalla. Ongelmana on kuitenkin mahdollisuus siihen, että tekijä saattaa vaihtaa metodia esimerkiksi huomatessaan, ettei kyseisellä metodilla saa tarpeeksi rahaa (jatkuvuus) eivätkä yksilöt välttämättä käyttäydy kaikissa tilanteissa saman kaavan mukaan (samankaltaisuus). (Kirwan & Power, 2011 s. 5). Warikoo (2014) puolestaan arvioi kyberrikollisia kuudella mittarilla (Taulukko 2), joita ovat hyökkäyksen tunnusmerkit, hyökkäyksen metodi, motivaation taso, kyvykkyys, hyökkäyksen vakavuus ja demografia, joilla pyritään kuvaamaan rikollisen käyttäytymistä, menettelytapaa ja psykologisia piirteitä. Warikoon (2014) ehdottama meto-

dologia hyödyntää edellä mainittua kuutta mittaria ja profiloi kyberrikoksen neljän prosessin kautta:

1. Ensimmäisenä prosessina on uhrin profilointi, jossa päätellään, miksi uhri on valittu ja miten uhri on kohdennettu (Warikoo, 2014).
2. Toisessa prosessissa identifioidaan hyökkäyksen taustalla oleva motivaatio, jossa tutkitaan uhrin ja hyökkääjän suhdetta sekä tehdään riskiarvio ja analysoidaan forensiikan tuottamia todisteita sekä todennetaan lähestymistavan ja hyökkäyksen metodi sekä tehdään johtopäätöksiä mahdollisista hyökkäyksen piirteistä (Warikoo, 2014).
3. Kolmannessa prosessissa suoritetaan tilastollinen analyysi, jossa identifioidaan hyökkäyksien kaava/pattern ja korrelaatio datan kanssa. Tämän jälkeen vertaillaan mahdollisia toisen prosessin aikana tunnistettuja piirteitä suhteessa tilastollisessa analyysissa mahdollisesti tunnistettuihin kaavoihin ja luodaan lopullinen lista hyökkäyksen piirteistä. (Warikoo, 2014).
4. Neljännessä profiloinnin prosessissa luodaan varsinainen kyberrikollisen profiili perustuen aiemmissa vaiheissa tunnistettuihin piirteisiin (Warikoo, 2014).

Warikoo (2014) on profiloinut tietojenkalasteluhyökkäyksen olevan rakenteeltaan organisoimaton, motivaatiotasoltaan korkea, hyökkääjän taitotason olevan perustasolla tai edistynyt sekä hyökkäyksen vaikutuksen olevan matala tai keskiverto.

TAULUKKO 2 Kyberrikollisen profiloinnin mittarit (Warikoo, 2014).

Mittari	**Kuvaus**
Hyökkäyksen tunnusmerkki	Hyökkäykseen käytetyt välineet kuten tunnettu koodi
Hyökkäyksen metodi	Hyökkäyksessä käytetty metodi kuten esimerkiksi käyttäjän manipulointi ja tietojenkalastelu
Motivaation taso	Hyökkääjän motivaation taso kuten hyökkäyksen kompleksisuus
Kyvykkyys	Kyvykkyys käyttää välineitä ja tekniikoita hyökkäyksissä
Hyökkäyksen vakavuus	Hyökkäyksen vakavuus sen vaikuttavuuden perusteella
Demografia	Hyökkäyksen demografiset tekijät kuten maantieteellinen sijainti

4.2 Neutralisaatioteoria

Yksi kriminologisista teorioista, joka selittää rikollisen toimintaa on neutralisaatioteoria. Gresham Sykesin ja David Matzan (1957) esittelivät neutralisaatioteo-

rian selittävänä viitekehyksenä väärinkäytösten selittämiselle. Sykesin ja Matzan mukaan, vaikka rikolliset olisivat rikollismaailmaan yhteydessä niin he silti sisäistävät monia tavanomaisen maailman sosiaalisia normeja tehdessään lainvastaista toimintaa. He siis tiedostavat käyttäytymisensä olevan sosiaalisien normien mukaan väärin, jonka seurauksena he käyttävät neutralisaatiotekniikoita. Neutralisaatiotekniikoiden käyttäminen siis auttaa heitä sovittamaan rikoksen heidän haluamaansa minäkuvaan esimerkiksi säilyttämään ei-rikollinen minäkuva rikollisesta toiminnasta huolimatta.

Sykes ja Matza (1957) tunnistivat viisi neutralisaatiotekniikkaa (Taulukko 3), jotka ovat vastuun kieltäminen, vahingon kieltäminen, uhrin kieltäminen, tuomitsijan tuomitseminen sekä vetoaminen korkeampaan lojaliteettiin.

TAULUKKO 3 Neutralisaatiotekniikat (Sykes & Matza, 1957)

Tekniikka	Kuvaus
1. Vastuun kieltäminen	Rikollinen ei koe olevansa henkilökohtaisesti vastuussa laittomista tai sosiaalisten normien vastaisesta toimistaan.
2. Vahingon kieltäminen	Rikollinen kieltää toimintansa aiheuttaneen vahinkoa tai vahinko on kestettävissä.
3. Uhrin kieltäminen	Rikollinen ajattelee, että uhri ansaitsi hänen toteuttaman toimintansa, vaikka se olisi vahingollista uhrille.
4. Tuomitsijan tuomitseminen	Rikollinen keskittyy heidän toimiaan tuomitsevien tahojen kuten esimerkiksi poliisien ja lainhaltijoiden motiiveihin tai käyttäytmiseen.
5. Vetoomus korkeampaan lojaliteettiin	Rikollinen pyrkii täyttämään pienempien ryhmien kuten esimerkiksi jengin, johon hän mahdollisesti kuuluu, vaatimukset lain rikkomisen ja sosiaalisten normien kustannuksella.

Vastuun kieltäminen tekniikkana on, että rikollinen ei koe olevansa henkilökohtaisesti vastuussa laittomista tai sosiaalisten normien vastaisesta toimistaan tai kokea ne vain sattumana. Toisaalta myös rikollinen voi kokea, ettei hänen toimintansa johdu vain hänestä itsestään vaan myös ulkopuolisista voimista ja asioista, kuten huonoon seuraan ajautumisesta eikä näe voivansa vaikuttaa tilanteeseen. (Sykes & Matza, 1957). Tätä voisi toisaalta myös soveltaa jollain asteella yhteiskunnasta syrjäytymisen ollessa kyseessä.

Vahingon kieltäminen on toinen Sykesin ja Matzan (1975) esittelemistä neutralisaatiotekniikoista, joka perustuu rikollisen päättelyyn satuttaako rikollinen toiminta selvästi jotakuta. Rikollinen voi esimerkiksi väittää, ettei toiminta vahingoittanut ketään tai uhri pystyy kestämään vahingon (Sykes & Matza).

Tämä on toisaalta myös hyvin erilaisesti tulkittavissa rikoksen tekijän toimesta. Esimerkiksi omassa tutkimuksessani eräs haastateltavista koki, ettei uhreille oikeasti tullut taloudellista haittaa.

Sykesin ja Matzan (1975) kolmas tunnistama tekniikka tarkoittaa sitä, että vaikka rikoksen tekijä myöntää rikollisen toimintansa aiheuttavan vahinkoa, rikollinen voi neutralisoida omien tekojensa moralisoimisen olosuhteiden varjolla. Vahinko voidaan myös neutralisoida ajattelemalla, että vahinko on oikeutettu koston tai rangaistuksen varjolla eli kääntää uhrin väärintekijäksi. Uhrin olemassaolo siis kielletään ajattelemalla, että hän ansaitsi vahingon, vaikkakin se on äärimmäinen muoto tekniikasta. (Sykes & Matza, 1957).

Tuomitsijan tuomitsemiseen liittyvän tekniikan perustana on se, että rikollinen kääntää huomion omista toimistaan hänen tekojaan paheksuviin henkilöihin ja heidän motiiveihin ja käyttäytymiseen pitämällä heitä esimerkiksi tekopyhänä. Tämän tekniikan osalta voi esiintyä kyynisyyttä yhteiskuntaa kohtaan ja esimerkiksi kokea virkavallan korruptoituneena ja typeränä. (Sykes & Matza, 1957).

Vetoomus korkampaan lojaliteettiin toimii siten, että vallassa olevan yhteskunnan vaatimukset ohitetaan ja vastataan pienemmän sosiaalisen ryhmän, kuten jengin, jonka jäsen ollaan, vaatimuksiin. Tässä neutralisaatiotekniikassa rikollinen ei välttämättä kuitenkaan aktiivisesti kiellä tai halua torjua vallitsevia yhteiskunnan normeja tai vaatimuksia, mutta kokee ajautuneensa pulmaan, joka vain on ratkaistava keinoilla, jotka rikkovat lakia. (Sykes & Matza, 1957).

Siponen, Vance ja Willison (2012) nostavat myös esiin artikkelissaan, että hyökkääjät ovat usein taipuvaisia rationalisoimaan toimintaansa sen oikeuttamiseksi erilaisten neutralisaatiotekniikoiden avulla. Näiden tekniikoiden hyödyntäminen auttaa hyökkääjää vähentämään rikollisesta toiminnasta johtuvaa mahdollista syyllisyyttä ja häpeää (Siponen ym., 2012).

5 TUTKIMUSMENETELMÄT

Tämä luku käsittelee tutkielman empiirisen tutkimuksen toteutusta, tutkimuksen taustaa ja rajausta sekä aineistonkeruumenetelmää ja aineiston analyysia.

5.1 Tutkimuksen tausta ja rajaus

Tutkielma käsittelee tietojenkalasteluhyökkäyksiä Suomessa hyökkääjän näkökulmasta. Edeltävissä sisältöluvuissa on käsitelty aihepiiriin liittyvä olennainen käsitteistö ja tausta aiempien tieteellisten tutkimusten perusteella sekä luotu kirjallisuuskatsauksen avulla tutkimukselle teoreettinen pohja.

Aiempaan tutkimukseen perustuvan teoreettisen pohjan luomisen avulla pyrittiin löytämään vastauksia tutkimuksen tutkimuskysymyksiin. Sisältölukujen edetessä huomattiin, että tietojenkalastelua on tutkittu hyökkäystekniikoiden ja -prosessien näkökulmasta, mutta hyökkäysten taustatekijöihin tai jälkipuintiin liittyvä tutkimus oli vähäistä, jonka vuoksi aihepiirien tutkiminen on tarpeellista. Myös tutkimus hyökkäyksen kohteiden näkökulmasta oli laaja-alaista, mikä osaltaan loi suuren kontrastin sille, ettei aihepiiriä ole hyökkääjän näkökulmasta muutoin kuin tekniikan osalta juurikaan tutkittu. Tutkimuksen aihepiiri rajattiin kolmen tutkimuskysymyksen avulla, jotka on esitetty alla:

1. Mitkä taustatekijät johtivat siihen, että tietojenkalasteluhyökkäyksiä ryhdyttiin toteuttamaan?
2. Mitä tekniikkaa hyökkääjät käyttivät ja miten se kehittyi ajan saatossa?
3. Tekivätkö hyökkääjät jälkipuintia hyökkäyksistään eli reflektoivatko he omia toimiaan?

5.2 Metodologia

Tutkimus toteutettiin empiirisenä laadullisena case-tutkimuksena. Williamsin (2007) mukaan empiirisen tutkimuksen perustana on tutkimuksen kohteena

olevan yksilön tai joukon yksilöitä havainnointi, mittaaminen ja analysointi, jonka avulla kerätty tutkimusaineisto luo lähtökohdan varsinaiselle tutkimukselle. Case- eli tapaustutkimus toteutettiin neljän haastattelun avulla, jossa tapauksina toimivat haastateltavien toteuttamien tietojenkalasteluhyökkäysten tai hyökkäyssarjojen elinkaari sisältäen taustatekijät, tekniikan ja jälkipuinnin haastateltavakohtaisesti.

Kvalitatiivinen tutkimus pitää sisällään case-tutkimuksen, jossa tutkitaan syvällisesti tiettyä aktiviteettia, josta halutaan saada syvällistä tietoa (Creswell, 2003 s. 15) eikä aihetta ole välttämättä aiemmin tutkittu syvällisesti (Leedy & Ormrod, 2001 s.149). Koska tutkimuksen aihepiiriä ei ole kattavasti tutkittu, kvalitatiivinen case-tutkimus sopii tutkimuksen tarkoitukseen hyvin. Kvalitatiivinen eli laadullinen tutkimusmenetelmä pyrkii tutkimaan ilmiötä osallistujan näkökulmasta (Williams, 2007) ja perustuu yksinkertaisimmillaan tutkimuksen aikana järjestetyistä haastatteluista saatuun tekstiaineistoon (Eskola & Suoranta, 1998, s.12). Tuomen ja Sarajärven (2018 s.73) mukaan kvalitatiivisessa tutkimuksessa tutkija päättää tutkimusasetelman perustuen omaan ymmärrykseensä, jonka takia saatu tieto on aina jossain määrin subjektiivista puhtaan objektiivisen tiedon sijaan. Tuomen ja Sarajärven (2018 s.73) mukaan laadullisen tutkimuksen pyrkimys ei niinkään ole osoittaa tilastollisia yleistyksiä vaan muun muassa pyrkiä kuvaamaan ja ymmärtämään ilmiötä tai toimintaa.

Koska tutkimuksen aihepiiriä ei ole vielä kaikilta osin kattavasti aiemmin tutkittu, sopii kvalitatiivinen sisällönanalyysi tutkimuksen tarkoitukseen hyvin. Kvalitatiivinen sisällönanalyysi lähtee liikkeelle aiheen rajauksesta tutkimuksen tarkoitukseen perustuen, jonka jälkeen aineisto puhtaaksikirjoitetaan ja laadullinen aineisto ryhmitellään aihepiireihin perustuen (Tuomi & Sarajärvi, 2018 s. 79). Sisällönanalyysin avulla analysoidaan aineiston sisältöä kuten haastattelua systemaattisesti ja objektiivisesti (Tuomi & Sarajärvi, 2018, s.86).

5.3 Aineistonkeruumenetelmä

Tutkimuksen aineisto kerättiin neljän haastattelun avulla, joiden tarkoituksena oli vastata asetettuihin tutkimuskysymyksiin. Tutkimus perustuu osittain strukturoituihin haastatteluihin, joissa oli vain muutama etukäteen muotoiltu kysymys, joiden perusteella haastateltavat lähtivät esittämään vastauksia ja loput kysymykset muotoutuivat haastattelun edetessä. Osittain strukturoiduissa haastatteluissa ei siis ole varsinaista valmista rakennetta haastatteluille vaan haastattelija voi valmistella muutamia kysymyksiä etukäteen, jonka jälkeen haastattelukysymyksiä improvisoidaan (Myers & Newman, 2007). Osittain strukturoiduissa haastatteluissa haasteena voi olla esimerkiksi luottamuksen puute haastattelijan ollessa mahdollisesti täysin tuntematon, jolloin haastateltava voi jäädä pohtimaan kuinka paljon haastattelijaan voi luottaa tai Hawthorne-efekti, jolloin haastattelija voi struktuurin puuttuessa muuttaa haastattelutilannetta. Lisäksi haastateltava ei välttämättä käsitä kysymyksiä oikein. (Myers & Newman, 2007). Haastateltavina tutkimuksessa toimivat tietojenkalasteluhyök-

käyksiä tehneet Suomessa asuvat henkilöt. Haastattelut toteutettiin joko internetin viestipalvelujen välityksellä (Discord, Zoom, Facebook Messenger) tai kasvotusten.

Tutkimuksen aiheen ollessa arkaluontoinen siihen liittyessä mahdollisesti rikollista toimintaa ja tarkka maantieteellinen rajoite, haastateltavien löytäminen oli haastavaa. Haastateltavia pyrittiin löytämään kontaktoimalla satunnaisesti joko poliisin dokumenteista löytyneitä henkilöitä tai Tor-verkon keskustelupalstalla anonymiteetin suojassa tietojenkalastelusta kirjoitelleita henkilöitä sekä satunnaisesti kyselemällä. Haastateltavien löytymiseksi otin yhteyttä Suomen eri poliisilaitoksiin ja pyysin asiakirjoja, joista ilmenisi henkilöiden nimiä, jotka tietojenkalastelua ovat tehneet. Tor-verkon kautta haastateltavia ei löytynyt, sillä luontaisesti he eivät luottaneet täysin anonyymiin haastatteluun tutkimustarkoituksiin vaan epäilivät tarkoitusperien olevan heitä vastaan. Otin yhteyttä kuuteen henkilöön, joiden nimet löytyivät poliisin toimittamasta dokumentaatiosta sosiaalisen median kautta, joista kaksi ei vastannut mitään ja kaksi kieltäytyi suoraan haastattelusta. Mikäli sain yhteyden henkilöön joka oli tehnyt tietojenkalastelua, pyysin myös heitä informoimaan minua, mikäli tunsivat jonkun, joka oli tietojenkalastelua tehnyt. Kaksi suostui haastatteluun. Kaksi kontaktoimistani ihmisistä, joiden kanssa sain keskusteluyhteyden kertoivat tuntevansa jonkun, joka oli myös harjoittanut tietojenkalastelua ja lupasivat pyynnöstäni kysyä tuntemansa henkilön kiinnostusta osallistua haastatteluun, mutta kukaan ei lupautunut haastatteluun.

Koska haastateltavien löytäminen oli hyvin hankalaa, tämän seurauksena haastattelut ajoittuvat 2021 loppuvuoden ja 2023 alkuvuoden välille. Haastateltavia, jotka suostuivat osallistumaan, löytyi neljä kappaletta pitkästä etsintäajasta huolimatta, mikä ei ole tutkimuksen otannan kannalta optimaalisin määrä. Haastattelut rakentuivat kolmen eri teeman ympärille:

- Taustatekijät
- Tekniikka
- Jälkipuinti

Haastatteluissa keskityttiin perehtymään siihen, miksi henkilöt olivat ryhtyneet kalastelemaan tietoja, millaisia tietojenkalasteluhyökkäyksiä henkilöt olivat tehneet ja kehittyikö tekniikka sekä hyökkäysten jälkipuintiin hyökkääjän toimesta. Yksi haastatteluista toteutettiin kasvotusten ja kolme muuta internetin välityksellä.

Osittain strukturoitu haastattelu loi mahdollisuuden keskustelun kautta ymmärtää tausta miksi Suomen kaltaisessa hyvinvointivaltiossa asuva henkilö ylipäätään ryhtyy kalastelemaan tietoja ja toisaalta myös mahdollisesti millä tavoin tekniikka on kehittynyt tietojenkalastelun myötä. Haastattelun aluksi haastateltava suostui antamaan haastattelun tuoman tiedon anonyymisti tutkimustarkoitukseen sekä käytiin läpi tutkimuksen tausta ja tarkoitus. Haastattelut lähtivät etenemään ensin siten, että haastateltava kertoi vapaamuotoisesti millainen ensimmäinen tietojenkalastelutapaus oli. Tämän jälkeen kysyttiin tarkempia kuvauksia prosessista ja sen mahdollisesta kehittymisestä. Yksi haasta-

teltavista oli tehnyt vain kertaluontoisesti tietojenkalastelua. Haastateltavien taustatekijöitä, jotka motivoivat tietojenkalasteluhyökkäyksien tekoon kartoitettiin myös niin tarkasti kuin mahdollista ja sitä, mikä sai jatkamaan tietojenkalastelua eikä esimerkiksi lopettamaan sitä. Lopulta haastateltavien pyydettiin kuvaamaan hyökkäysten jälkeistä mahdollista jälkipuintia eli reflektiota.

Guestin, Buncen ja Johnsonin (2006) mukaan tutkimuksessa voidaan löytää teemat jo kuuden haastattelun avulla. Dworkinin (2012) mukaan kuitenkin suositeltu otannan määrä vaihtelee 5-50 osallistujan välillä, mutta toisaalta tutkimuksen osallistujien sopiva määrä riippuu myös tilanteesta eikä suositukset kosketa esimerkiksi case-tutkimuksia. Myös Eskola ja Suoranta (1998 s.14) laadullisessa tutkimuksessa voidaan keskittyä määrällisesti pieneenkin otantaan ja arvioida otannan tapauksia mahdollisimman kattavasti, jolloin tieteellisyyden kriteeristö ei perustu niinkään määrään vaan laatuun. Näin ollen tutkimuksen otannan kattaessa neljä osallistujaa, on määrä riittävä, joskaan ei täysin optimaalinen.

Otannasta pyrittiin saamaan mahdollisimman kattava, mutta aiheen arkaluontoisuuden vuoksi, haastateltaviksi valikoitui kaikki ne henkilöt, jotka olivat suostuvaisia haastatteluun. Kriteeristönä otannalle toimi se, että henkilö asui Suomessa ja oli tehnyt tietojenkalasteluhyökkäyksiä. Siinä, oliko mahdollinen haastateltava jäänyt tietojenkalastelusta kiinni virkavallalle tai saanut esimerkiksi taloudellista hyötyä, ei ollut merkitystä. Eskolan ja Suorannan (1998, s. 42-43) mukaan etenkin arkaluontoisien asioiden ympärillä toimiminen tutkijana edellyttää erityistä pohdintaa, mitä tietoja on tarkoituksenmukaista kerätä ja henkilöiden anonymiteettia suojata tiukasti. Tämän vuoksi haastateltavista ei kerätty demografisia tietoja kuin tarpeellisilta osin.

5.4 Data-analyysi

Tutkimuksen datan analysointityyliksi valikoitui aineistolähtöinen sisällönanalyysi, sillä aihepiiristä ei ole vielä tuotettu laajalti jäsenneltyä tietoa. Tutkimusaineiston sisällönanalyysillä pyrittiin saamaan tutkittavasta ilmiöstä teoreettinen kuvaus. Bengtssonin (2016) mukaan sisällönanalyysin lähtökohtana on kerätä tekstiä, identifioida ja ryhmitellä kategorioita ja luoda ymmärrys tutkimusaiheesta tämän perusteella. Laadullisessa sisällönanalyysissä pyritään ryhmittelemään data sanojen ja teemojen perusteella. Aineistolähtöisen sisällönanalyysin prosessi etenee haastatteluiden litteroinnista, sisältöön perehtymisen kautta aineiston pelkistämiseen, jolloin aineisto voidaan pilkkoa osiin ja etsiä samaa aihetta kuvaavia ilmaisuja, jotka ryhmitellään ja tämän jälkeen aineisto käsitteellistetään. Yksinkertaisuudessaan siis yhdistellään käsitteitä vastaamaan asetettuun tutkimusongelmaan. (Tuomi & Sarajärvi, 2018 s. 91-94). Tuomen ja Sarajärven (2018 s. 94) mukaan sisällönanalyysia on kuitenkin myös kritisoitu jäävän alkuvaiheen analyysiin sen luokittelevan luonteen vuoksi.

Haastatteluaineiston analyysi aloitettiin tekstin puhtaaksikirjoituksella. Tutkimuskysymyksillä rajattiin aineiston puhtaaksikirjoituksen taso perustuen

analyysitapaan, joka tässä tapauksessa oli sisällönanalyysi. Tutkimuskysymyksillä pyrittiin selvittämään taustatekijät, jotka johtivat tietojenkalasteluhyökkäyksien totetuttamiseen, hyökkäystekniikat ja niiden kehittyminen sekä miten hyökkääjät jälkipuivat hyökkäyksiään. Koska haastatteluja ei aiheen arkaluontoisuuden vuoksi nauhoitettu, haastatteludatan työstäminen aloitettiin haastattelumuistiinpanojen puhtaaksikirjoituksella mahdollisimman pian kunkin haastattelun jälkeen. Haastattelujen puhtaaksikirjoituksen jälkeen haastatteluaineisto pelkistettiin ja ryhmiteltiin pyrkien luomaan teoreettista käsitteistöä. Ryhmittelyssä puhtaaksikirjoitetusta aineistosta pyrittiin ryhmittelemään samaa ilmiötä kuvaavat käsitteet, joiden avulla pyrittiin erottelemaan olennainen tieto tutkimuksen kannalta. Puhtaaksikirjoitettu aineisto luettiin useaan otteeseen läpi luoden ryhmittelyä mahdollisimman tarkalla tasolla, jonka jälkeen ryhmiä yhdistettiin luokaksi, jotka vastasivat tutkimuskysymyksiin.

6 TUTKIMUSTULOKSET

Tässä luvussa esitellään tutkimuksen tulokset. Tutkimuksessa haastateltiin neljää henkilöä, jotka asuvat Suomessa ja ovat harjoittaneet tietojenkalastelua. Kaikki haastateltavat olivat miehiä.

6.1 Taustatekijät

Tutkimuksessa taustatekijöiksi tunnistettiin sekä ulkoisia, että sisäisiä motivattoreita. Haastatteluissa nousi esiin esimerkiksi aiempi rikostausta, huono elämäntilanne kuten huumeidenkäyttö sekä syrjäytyminen yhteiskunnasta kuten myös toiselta henkilöltä tullut toimeksianto. Motivaattoreina toimi raha, sosiaalinen validaatio, kostonhalu yhteiskunnalle, oman paremmuuden tavoittelu, itsensä kehittäminen ja uteliaisuus.

Kahdella haastateltavista (Tapaus 1 & 2) taustalla oli elämäntilanteeseen liittyvät seikat ja motivaattorina raha. Toisen haastateltavan (Tapaus 1) motiivina toimi raha hänen elättäessään itsensä talousrikoksilla ja koska aiempaa taustaa erilaisista petoksista löytyi, tietojenkalastelu valikoitui yhdeksi tekniikaksi sattumanvaraisesta ideasta sen osoittautuen siihenastisista petoksista tuottoisimmaksi. Hän koki olevansa hyvä tekemään talousrikoksia. Toisen haastateltavan (Tapaus 2) elämäntilanne oli huono esimerkiksi huumeidenkäytön ja yhteiskunnasta syrjäytymisen vuoksi. Haastateltava (Tapaus 2) koki muiden pitävän häntä tyhmänä ja sen seurauksena syntyi halu kostaa yhteiskunnalle, jonka lisäksi raha motivoi häntä. Rahan kautta hän koki saavansa sosiaalista validaatiota ja omaa paremmuudentunnetta.

Kahden muun haastateltavan taustalla tietojenkalastelun harjoittamisessa ei toiminut motivaattorina raha. Molemmille oli yhteistä, että aluksi tietojenkalastelun idea syntyi toisen aloitteesta. Toinen haastateltavista (Tapaus 3) törmäsi ideaan tietojenkalastelusta eräällä foorumilla, jossa toinen henkilö oli ehdottanut tätä ja tunsi uteliaisuutta testata, toimiiko tietojenkalastelu oikeasti. Toinen haastateltavista (Tapaus 4), jonka motivaattorina ei toiminut raha, ryhtyi

ensimmäistä kertaa kalastelemaan tietoja toisen henkilön aloitteesta, jolloin motivaattorina toimi toinen henkilö, joka antoi toimeksiannon tietojenkalastelusta. Myöhemmin haastateltavan (Tapaus 4) motivaattoriksi nousi itsensä kehittäminen.

6.2 Tekniikka

Tutkimuksessa havaittiin, että tietojenkalastelussa potentiaalisten uhrien tavoittamisen tekniikoita olivat sähköposti (Tapaus 1 & 3), tekstiviesti (Tapaus 1 & 2) sekä sosiaalisen median viestintäpalvelut (Tapaus 4). Sähköposteissa ja tekstiviesteissä hyödynnettiin sisältönä linkkejä, jotka ohjasivat potentiaalisen uhrin vilpilliselle nettisivulle, jonne syötettiin sensitiivistä informaatiota kuten käyttäjätunnuksia eri palveluihin. Potentiaalisten uhrien tietoja löydettiin tutkimuksen perusteella Tor-verkosta tai spesifiltä foorumilta. Sosiaalisen median viestintäpalveluissa ei käytetty linkkejä, jotka olisivat vieneet vilpilliselle nettisivulle, vaan keskustelun kautta kalasteltiin potentiaalisen uhrin henkilökohtaisia tietoja sosiaalisen median feikkiprofiilin avulla.

Vilpillisten nettisivujen luominen on tutkimuksen perusteella helppoa. Tutkimuksessa havaittiin, että nettisivujen tekoon löytyi helpot ohjeet yksinkertaisesti vain etsimällä Googlen hakupalvelusta eikä se vienyt kauaa aikaa. Vilpillisistä nettisivuista tehtiin kopioita luotettavista nettisivuista, joiden nimissä lähetettiin tietojenkalasteluviesti.

Tietojenkalastelutekniikkaa tehneet yksilöt myös tutkimuksen perusteella kehittivät tekniikoitaan, pois lukien yksi haastateltavista (Tapaus 3), joka näki tietojenkalastelun kokeiluna uteliaisuudesta. Kaksi neljästä haastateltavasta (Tapaus 1 & 3) käytti sähköpostia tietojenkalastelussa tavoittaakseen potentiaaliset uhrit, toinen kuitenkin siirtyi jälkeenpäin tekstiviesteihin (Tapaus 1). Yksi haastateltavista (Tapaus 2) käytti tietojenkalastelussa potentiaalisten uhrien tavoittamiseen spesifisti tekstiviestiä. Yksi haastateltavista (Tapaus 4) käytti välineenään luomiaan feikkiprofiileja sosiaalisen median alustoilla.

6.2.1 Tapaus 1

Ensimmäisessä tapauksessa kohteita pyrittiin tavoittamaan sähköpostitse ja haastateltava loi netistä löytämillään ohjeilla pankkien nettisivujen näköisiä nettisivuja. Hyökkäyksen kohteita houkuteltiin sivustolle viestillä, joka sisälsi ilmoituksen esimerkiksi väitetystä tullaamattomasta postilähetyksestä tai ilmoituksen perintälaskusta näin houkutellen kohteita vilpilliselle pankkisivustolle, jonne tuli syöttää verkkopankkitunnukset. Haastateltava käytti uhreilta saamaansa sensitiivistä informaatiota, tässä tapauksessa pankkitunnuksia, saadakseen taloudellista hyötyä pääasiassa tunnistautumalla luotonantosivustoille.

Haastateltava kuitenkin päätti vaihtaa viestintäkanavan tekstiviestiksi, joka oli hänen kokemuksensa mukaan tehokkaampi tapa tavoittaa kohteita. Teks-

tiviestejä hän lähetti Skype-palvelun kautta, jossa oli mahdollista muokata lähettäjän nimeksi haluamansa nimi kuten tässä tapauksessa esimerkiksi Posti tai jonkin perintäyrityksen nimi.

6.2.2 Tapaus 2

Toisessa tapauksessa haastateltu henkilö hyödynsi alusta alkaen tekstiviestejä tavoittaakseen kohteita lähtökohtanaan uskotella potentiaalisille uhreille viestin tulleen luotettavalta taholta. Haastateltava löysi Tor-verkkoon vuodetun listan luottopalvelun käyttäjistä käyttäjätunnuksineen, jonka perusteella etsi potentiaalisten uhrien puhelinnumeroita. Haastateltava nosti luottoja vuodetuilla käyttäjätunnuksilla uhrien tilille, jonka jälkeen tekniikkana oli uskotella potentiaalisille uhreille luotonantopalvelun nimissä, että oli tapahtunut virheellinen lainasiirto luotonantajan toimesta, joka tulisi siirtää tilille X, joka oli todellisuudessa haastateltavan tili.

Tekniikka kuitenkin myöhemmin kehittyi ja siirtyi verkkopankkitunnusten kalasteluun, joita saadakseen haastateltava lähetti tekstiviestejä kohteille perintäyrityksen nimissä, jonka sisältö esitti potentiaalisella uhrilla olevan maksamaton lasku ja vetosi siihen, että mikäli maksua ei makseta, luottotiedot menevät. Tekniikan kehittyessä myös kohdennus muuttui ja tietojenkalastelun kohteiksi valittiin nimiä, jotka haastateltava mielsi keski-ikäisiksi, joilla hän oletti olevan luottotiedot. Tekniikkana oli laittaa niin pieni summa, että potentiaaliset uhrit menisivät maksamaan sen matalalla kynnyksellä. Viestissä oli liitettynä linkki, jota ennen ilmaistiin, että kohde voi mennä maksamaan laskun linkin kautta ja linkki ohjasi kohteen tunnistautumaan verkkopankkitunnuksilla vilpilliselle sivustolle, jonka haastateltava oli luonut kopioiden luotettavan sivun. Haastateltavan luomalla tietojenkalastelusivustolla oli tunnistautumisportaali, jonne verkkopankkitunnukset tuli syöttää ja jonka kautta haastateltava sai syötetyt tiedot käyttöönsä.

6.2.3 Tapaus 3

Kolmannessa tapauksessa tietojenkalastelu kohdistui pelin käyttäjätunnuksiin. Sähköpostiosoitteet saatiin haastateltavan mukaan pelifoorumilta eikä kohdennusta näin ollen tehty muutoin.

Sähköpostiviesteissä houkuteltiin kohteita menemään tietojenkalasteluviestin sisältämän linkin ohjaamalle sivustolle tarjoamalla pelintekijä nimissä ilmaista palkintoa. Mikäli potentiaalinen uhri meni linkin ohjaamalle vilpilliselle sivustolle, tuli hänen syöttää käyttäjätunnuksensa ja salasanansa, jonka välityksellä tietojenkalastelija sai uhrin käyttäjätunnukset salasanoineen. Tietojenkalastelu oli kokeilu eikä tekniikkaa kehitetty pidemmälle.

6.2.4 Tapaus 4

Neljännessä tapauksessa tietojenkalastelun tekniikka perustui sosiaalisen median alustojen feikkiprofiilien luomiseen ja kohteiden houkutteluun jakamaan

informaatiota keskustelun kautta. Haastateltava kohdensi tietojenkalastelua pääasiassa miehiin, mutta muutoin hän valitsi uhreja pääasiassa satunnaisesti ja joskus organisaatiokohtaisesti pois lukien ensimmäinen hänen toteuttamansa tietojenkalasteluhyökkäys. Listauksia esimerkiksi Tor-verkosta hän ei ole etsinyt. Ensimmäisessä tapauksessa tietojenkalastelussa hyödynnettiin Facebookiin luotua feikkiprofiilia, jolla haastateltava aloitti keskustelemaan kohteen kanssa ja sai näin kerättyä informaatiota. Tietojenkalastelun tekniikat ja metodit kehittyivät teknologian kehittymisen myötä. Esimerkiksi tietyistä sosiaalisen median palveluista on saatavilla Lynx-versio, jonka avulla palvelussa voi lähettää kuvamateriaalia niin, että se näyttää kyseisestä palvelusta suoraan lähetetyltä, mikä osaltaan auttaa luomaan kohteille kuvaa siitä, että kyseessä olisi aito henkilö tosiasiallisen feikkiprofiilin sijaan. Teknologian kehittyminen haastateltavan mukaan on myös edesauttanut tietojenkalastelutekniikan kehittymistä kohti käyttäjän manipulaatiota luodessaan mahdollisuuden olla vakuuttavampi. Alkuvaiheessa haastateltava käytti verkosta otettuja satunnaisen henkilön kuvia, mutta tietojenkalastelutekniikan kehittyessä yksittäisen feikkiprofiilin, joka sisälsi useita kuvia ja storyja eli rajatun ajan näkyviä tarinoita, tueksi luotiin samalle henkilölle profiileja myös muille sosiaalisen median alustoille luoden digitaalista jalanjälkeä tavoitellen kohteiden silmissä aitouden tunnetta, mikäli kohde etsii verkon hakupalveluilla henkilön, jona haastateltava esiintyy.

Ajan myötä myös toiminta on tehostunut luovan tarinankerronnan kehittymisen myötä ja psykologisia oppeja, kuten antamalla kuvan isosta palveluksesta tai vastavuoroisuudesta, hyödyntämällä. Haastateltava on pyrkinyt myös luomaan kuvaa itsestään nuorena, naiivia tai hieman yksinkertaisena sanojen lyhentämisen ja lausemuotojen kautta. Etenkin seksuaalisella aspektilla keskustelu saa haastateltavan mukaan potentiaalisen uhrin astumaan niin sanotusti suonsilmään. Teknologian kehittymisen myötä myös kohteen vakuuttaminen feikkiprofiilin aitoudesta on kehittynyt haastateltavan hyödyntäessä esimerkiksi kelikameroita. Periaate toimii niin, että mikäli haastateltava on kertonut asuvansa paikassa X, hän säätietojen seuraamisen sijaan katsoo kelikameroista ajantasaisen sään tukeakseen vakuuttamista olevansa henkilö, jona esiintyy. Lisäksi kuvanmuokkaus teknologian kehittymisen myötä edistynyt. Haastateltava on harkinnut myös deep fake-kuvien luomista, mutta ei ole kokenut työpanoksen ja tuottavuuden olevan riittävällä tasolla, sillä pääosassa ei ole niinkään hienot kuvat vaan tarinankerronta ja narratiivi. Haastateltava saattoi hyödyntää uhrin vakuuttelussa myös näyttökuvia väärennetyistä sähköposteista, joissa näytti, että henkilö, jona haastateltava esiintyy, olisi käynyt keskustelua virallisen tahon kanssa, vaikka tosiasiassa haastateltava kävi keskustelua itsensä kanssa. Tarinankerronnan hyödyntämisen vuoksi massaviestin sijaan haastateltavalla on ollut maksimissaan alle 10 kohdetta kolmen eri feikkiprofiilin kesken jaettuna, mutta tyypillisesti haastateltavalla kuitenkin on ollut vain 1-3 kohdetta saman feikkiprofiilin kohteena, mikä on tarinankerronnan kannalta helpompi koordinoida. Keskustelun avaus on haastateltavan mukaan käyttämässään tekniikassa tärkein. Haastateltava on kokenut, että suoraan järkevään keskusteluun ryhtyminen ei ole tehokasta vaan haastateltava naamioi keskuste-

lun joko vahingoksi tai sitten viittaa johonkin kohteen kirjoittamaan verkossa olevaan juttuun tuoden ilmi, että juttu oli kiinnostava, mutta ei ollut tarkoitus häiritä, jolloin kohde usein lähtee mukaan keskusteluun.

6.3 Jälkipuinti

Kuten aiemmin mainittu, vain kahdessa tapauksessa (Tapaus 1 & 2) motivaattorina toimi raha ja rahallista hyötyä myös saavutettiin. Näissä kahdessa tapauksessa toisessa tietojenkalastelija ei avannut jälkipuinnin osuutta. Toisessa tapauksessa (Tapaus 2) haastateltava tiedosti, että rahallinen hyöty ei ole moraalisesti oikein toisen kustannuksella, mutta halu kostaa yhteiskunnalle ja olla kapinallinen sai suorittamaan tietojenkalasteluhyökkäyksiä. Haastateltava (Tapaus 2) myös koki hakevansa omaa paremmuudentunnetta ja tietojenkalastelusta saatu raha toi ympärilleen myös enemmän kavereita rahan mahdollistaessa sen, että pystyi tarjoamaan kavereille asioita. Toisaalta haastateltava (Tapaus 2) koki myös, ettei aiheuttanut suoranaisesti uhrille haittaa vaan pikemminkin luotonantoyhtiölle, sillä yhtiö joutui mitätöimään tietojenkalastelun seurauksena uhrien nimillä nostetut luotot.

Kahdessa muussa tapauksessa (Tapaus 3 & 4) rahallista hyötyä ei tavoiteltu. Toinen haastateltavista (Tapaus 3) ei kokenut tietojenkalastelun uhreja kohtaan sen suurempia tunteita vaan kertoi ajattelevansa, että ovatpa henkilöt tyhmiä, kun menivät niin helppoon huijaukseen. Neljännessä tapauksessa haastateltava kertoi miettineensä paljon seurauksia uhrille ja tunnistaneensa, että uhrit voivat hänen tietojenkalastelunsa seurauksena tuntea emotionaalista tuskaa. Tämän tunnistaessaan haastateltava (Tapaus 4) pyrki toimimaan niin, ettei uhrin kokema emotionaalinen tuska kasva. Haastateltava (Tapaus 4) koki epämukavia tunteita tehdessään tietojenkalastelua, vaikka ei kiristänyt uhreja eikä aiheuttanut heille aktiivisesti mitään pahaa. Haastateltava (Tapaus 4) pyrki myös lopettamaan tietojenkalastelun hienovaraisesti esimerkiksi vetoamalla henkilökohtaisiin seikkoihin, jonka vuoksi keskustelu tulee lopettaa ja välttämällä ghostaamista eli keskustelun lopettamista ilmoittamatta tai ilman syytä. Haastateltava (Tapaus 4) kuitenkin tunnisti myös toisaalta positiivisia seikkoja, kuten dopamiinitason nousu tietojenkalastelun tavoitteiden saavuttamisen yhteydessä. Haastateltava (Tapaus 4) myös koki onnistumisen tunteita ja tunteneensa tyytyväisyyttä kehittymisestään onnistumisten myötä.

7 TULOSTEN TULKINTA JA POHDINTA

Tämä luku pitää sisällään tutkimuksen tulokset ja niiden avulla aiemmin kuvattuihin tutkimuskysymyksiin vastaamisen, jotka esitellään johtopäätöksiä käsittelevässä osiossa. Lisäksi tämä luku sisältää johtopäätöksien käsittelyn sekä tulosten ja tutkimuksen merkityksen tieteellisellä kentällä pohtimisen ja jatkotutkimusehdotukset. Tutkimuksen tuloksia verrataan kirjallisuuskatsauksessa esiteltyyn tieteelliseen tausta-aineistoon. Tutkimuksessa oli myös rajoitteita, joita käsitellään myöhemmin arvioitaessa tutkimuksen luotettavuutta ja rajoitteita.

7.1 Johtopäätökset

Tutkimuksen tavoitteena oli selvittää Suomessa tehtyjen tietojenkalasteluhyökkäysten taustatekijät, tekniikat ja niiden kehittyminen sekä jälkipuinti. Tutkimus rakentui kolmen tutkimusongelmaan liittyvän tutkimuskysymyksen ympärille, jotka olivat seuraavat:

1. Mitkä taustatekijät johtivat siihen, että tietojenkalasteluhyökkäyksiä ryhdyttiin toteuttamaan?
2. Mitä tekniikkaa hyökkääjät käyttivät ja miten se kehittyi ajan saatossa?
3. Tekivätkö hyökkääjät jälkipuintia hyökkäyksistään eli reflektoivatko he omia toimiaan?

Tutkimuskysymyksiin on vastattu kysymyskohtaisesti seuraavissa kappaleissa peilaten tutkimuksen tuloksia aiempaan kirjallisuuteen.

7.1.1 Taustatekijät

Tietojenkalastelun tutkimuskentällä ei ole paneuduttu spesifisti hyökkäysten taustalla toimiviin tekijöihin ja motivaattoreihin, jonka vuoksi tämän tutkielman tutkimustuloksille ei löytynyt täysin sopivaa verrokkia. Aiemmassa kirjal-

lisuudessa paneudutaan esimerkiksi persoonallisuuspiirteisiin, mutta ei oikeastaan pinnallisempiin tekijöihin, jotka motivoivat hyökkääjiä tekemään tietojenkalastelua. Tambe Ebot (2017) tutki internet huijareiden motivaatiota huijausten takana ja löysi internethuijareiden motivoituvan rahasta sosialoidakseen ja nauttiakseen ylellisestä elämäntyylistä ja olemalla taloudellisesti riippumaton. Tutkimuksessa kahdella haastateltavista oli saman kaltaisia motivaattoreita kuin Tambe Ebot (2017) tunnisti tutkimuksessaan, sillä kaksi haastateltavaa (Tapaus 1 & 2) nosti esiin rahan ja elämäntilanteeseen liittyvät seikat motivaattorina. Haastateltava (Tapaus 1) oli elättänyt itsensä jo aiemmin talousrikoksilla ja hyödynsi tietojenkalastelua elättääkseen itsensä kokiessaan olleensa hyvä siinä. Haastateltavalla puolestaan (Tapaus 2) oli huono elämäntilanne, johon liittyi syrjäytymistä yhteiskunnasta, alemmuudentunnetta ja näistä kumpuavaa kostonhalua, jonka lisäksi raha toimi motivaattorina, jonka kautta sai sosiaalista validaatiota ja paremmuudentunnetta. Tambe Ebot (2017) nosti esiin tutkimuksessaan hyökkääjien negatiivisia emootioita, tutkimuksen kohteiden syyttäessä tilanteesta sosioekonomista ympäristöä. Vaikka Tambe Ebotin (2017) tutkimusasetelma poikkeaa maantieteellisesti ja keskittyy internethuijareihin, on tämä osin sovellettavissa myös tutkimukseni haastateltavaan (Tapaus 2) hänen kokiessa negatiivisia emootioita sosioekonomisen ympäristön seurauksena. Myös Ampwartum (2009) on nostanut esiin sosioekonomiset ongelmat, mutta tutkimusasetelma ei sovellu tämän tutkielman tutkimukseen täysin.

Kaksi haastateltavaa (Tapaus 3 & 4) saivat alun alkaen idean tietojenkalasteluun toisen henkilön toimesta. Tähän ei ole aiemmassa tutkimuksessa otettu kantaa. Tambe Ebot (2017) nosti esiin tutkimuksessaan kuitenkin sen, että henkilöt voivat ryhtyä internethuijareiksi ystäviensä harjoittaessa kyseistä toimintaa, mutta se pohjautuu sosiaalisen vuorovaikutuksen ylläpitoon ystävyyssuhteissa, jota tämän tutkielman tutkimuksessa ei puolestaan havaittu. Tutkielman tutkimuksessa ainoastaan idea tietojenkalasteluun saatiin toisen osapuolen toimesta, mutta sen avulla ei ylläpidetty sosiaalista yhteyttä, jonka vuoksi Tambe Ebotin (2017) tutkimus tältä osin ei ole hyvin sovellettavissa tämän tutkielman tutkimukseen.

7.1.2 Tekniikat

Kahdessa tapauksessa (Tapaus 1 & 3) tutkimuksessa hyödynnettiin sähköpostiviestiä tietojenkalastelun potentiaalisten uhrien tavoittamiseksi, jotka noudattivat hyvin Abroshanin ja kollegoiden (2021) kuvaamaa prosessia, joissa pääperiaatteena on yksinkertaisuudessaan se, että hyökkääjä lähettää tietojenkalastelusähköpostin, joka sisältää esimerkiksi tietojenkalastelulinkin, jonka potentiaalinen uhri saa sähköpostiinsa ja mahdollisesti klikkaa linkkiä päätyen vilpilliselle nettisivulle, jossa uhri mahdollisesti syöttää sensitiivistä informaatiota, joka päätyy hyökkääjälle. Tapaus 1 ja 3 noudattivat tätä prosessia hyvin, sillä lähtökohtana oli lähettää tietojenkalastelusähköposti, joka sisälsi linkin vilpilliselle nettisivulle, josta hyökkääjät saivat uhrille sensitiivistä informaatiota hyödynnettäväkseen. Hyvin samankaltaisen prosessin kuvasi myös Abdelhamid (2014) kollegoineen, jossa tietojenkalastelija lähtee liikkeelle hyökkäyksen alustamisel-

la, tietojenkalastelusähköpostin luomisella ja lähettämisellä, jonka jälkeen potentiaaliset uhrit saavat tietojenkalastelusähköpostin, mikäli tietojenkalastelun ehkäisemiseen tehty työkalu ei sitä estä päätymästä potentiaaliselle uhrille. Mikäli uhri saa tietojenkalastelusähköpostin, tekee hän ratkaisevan päätöksen jakaako informaatiota vai ei ja mikäli jakaa, saa tietojenkalastelija hänen informaationsa käsiinsä. (Abdelhamid ym., 2014).

Ensimmäisessä tapauksessa (Tapaus 1) siirryttiin sähköposteista tekstiviesteihin todetessa niiden olevan tehokkaampi tapa tavoittaa uhreja. Toisessa tapauksessa (Tapaus 2) tietojenkalastelu toteutettiin alusta alkaen tekstiviestien välityksellä. Tekstiviestien tehokkuutta puoltaa myös Jakobsson (2018) väittäessään tietojenkalastelun tekstiviestitse olevan tehokas tapa, sillä suurin osa käyttäjistä ei oleta tietojenkalastelun tulevan tekstiviestitse vaan useimmiten sähköpostitse, jonka vuoksi tietojenkalastelu tekstiviestitse voi olla tehokkaampaa. Näihin tapauksiin soveltuu myös Abroshanin ja kollegoiden (2021) ja Abdelhamidin ja kollegoiden (2014) esittämät prosessikuvaukset tietojenkalastelu-hyökkäyksistä, sillä erotuksella, että tutkimuksen tapauksissa käytettiin sähköpostin sijaan tekstiviestejä. Muutoin hyökkäys eteni prosessien mukaisesti viestin luomisesta sen lähettämiseen potentiaaliselle uhrille ja uhrin mennessä linkin kautta vilpilliselle sivustolle syöttämään informaatiota, jonka tietojenkalastelija/hyökkääjä sai käyttöönsä. Toisaalta toisen tapauksen (Tapaus 2) tietojenkalastelun alussa hyökkääjä sai uhrien käyttäjätunnukset haltuunsa Torverkosta ja kontaktoi uhreja vain siirtämään hyökkääjän heidän käyttäjätunnuksillaan lunastaman luoton hyökkääjän omalle tilille esiintyen luotonantajana tekstiviestin välityksellä.

Abroshanin ja kollegoiden (2021) sekä Abdelhamidin ja kollegoiden (2014) esittämät tietojenkalastelun prosessikuvaukset eivät ole kuitenkaan sovellettavissa tutkimuksen neljänteen tapaukseen, sillä neljännessä tapauksessa tietojenkalastelija ei hyödyntänyt vilpillisiä nettisivuja vaan pyrki saamaan informaatiota vain keskustelun kautta. Neljännessä tapauksessa käytetty tyyli on huomattavasti työläämpi kuin pelkkä tietojenkalasteluviestien lähettäminen vilpillisen sivun linkin kera, sillä tietojenkalastelija joutuu sitoutumaan keskusteluun. Neljäs tapaus viittaakin ehkä enemmän käyttäjän manipulaatioon, jonka Abri kollegoineen (2022) kuvaa tavoittelevan sensitiivisen informaation keräämistä kohteelta yksinkertaisimmillaan pyrkien saamaan informaatiota vastauksena hyökkääjän viestiin suoraan kohteelta.

Abroshanin ja kollegoiden (2021) mukaan juurikin tunne sähköpostin kiireellisyydestä toimii yhtenä tietojenkalasteluviestien tekniikkana, jolla kohteen päätöksentekoon pyritään vaikuttamaan ja näin saamaan kohde helpommin toimimaan viestin sisällön pyytämällä tavalla. Myös nopeasti saavutettava palkinto tunnistettiin yhdeksi kohteen päätöksentekokyvyn hämärtämiseen pyrkivistä tekniikoista (Abroshan ym., 2021). Ensimmäisessä ja toisessa tapauksessa vedottiin kiireellisyyteen, sillä ensimmäisessä tapauksessa viestissä nostettiin esiin lähetyksen tullaaminen tai erääntynyt maksu, joka tulisi maksaa tai kohde menettäisi väitetysti luottotietonsa. Toisessa tapauksessa viesti lähetettiin perintätoimiston nimissä ja viestissä nostettiin esiin väitetty maksamaton lasku on

erääntynyt ja se tulee maksaa, mikäli kohde ei halua menettää luottotietojaan. Kolmannessa tapauksessa tietojenkalasteluviesti lähetettiin pelintekijän nimissä pyrkien palkinnon avulla hämärtämään kohteiden päätöksentekokykyä. Neljäs tapaus ei hyödyntänyt edellä mainittuja tekniikoita vaan pyrki luomaan ystävyyssuhteen ja näin saamaan sensitiivistä informaatiota. Mouton kollegoineen (2016) käsitteli käyttäjän manipulaatiota, johon tietojenkalastelukin lukeutuu, tunnistaen myöntyväisyyden periaatteita, joista tämän tutkimuksen kohteet hyödynsivät auktoriteettia ja tietyiltä osin ystävyyssuhdetta. Kolmessa ensimmäisessä tutkimuksen tapauksessa hyödynnettiin auktoriteettiasemaa, joita tutkimuksessa olivat pelintekijä (Tapaus 3), tulli ja perintätoimisto (Tapaus 1) sekä luotonantolaitos (Tapaus 2). Neljännessä tapauksessa hyökkääjä pyrki puolestaan luomaan tietynlaisen ystävyyssuhteen saadakseen kohteelta tietoja. Moutonin ja kollegoiden (2016) ystävyyssuhteen myöntyväisyyden periaatteen lähtökohtana on, että hyökkääjä esiintyy jo hyökkäyksen alussa kohteen ystävänä, mutta neljännessä tapauksessa ystävyyssuhdetta luotiin pienin askelin ja luotua ystävyyssuhdetta hyödynnettiin myöhemmin tietojenkalastelussa, jonka vuoksi ystävyyssuhteen myöntyväisyyden periaate voisi olla sovellettavissa myös tähän tapaukseen. Neljännen tapauksen osalta yhtäläisyyksiä löytyi Tambe Ebotin, Siposen ja Topallin (2023) käyttäjän manipulointiin liittyvän tutkimuksen mukaan sosiaalisen median alustoja hyödyntäessään huijareille on kohtuullisen vaivatonta luoda ja poistaa käyttäjätilejä, käyttää väärennettyjä identiteettejä, valehdella fyysisestä sijainnistaan sekä kehittää tekniikoitaan teknologisen kehityksen myötä. Myös tämän tutkiselman tutkimuksen neljännessä tapauksessa havaittiin tietojenkalastelutekniikan kehittyvän teknologisen kehityksen myötä hyökkääjän tavoitellessa vakuuttavuuttaan kohteen silmissä ja teknologian, kuten sääkameroiden, hyödyntämistä fyysisen sijaintinsa huijaamisen apuna. Niin Tambe Ebotin ja kollegoiden (2023) tutkimuksessa kuin neljännen tapauksen kohdalla teknologiat tarjosivat hyökkääjälle myös mahdollisuuksia luoda ja hyödyntää useampia käyttäjiä ja profiileja sosiaalisen median alustoilla.

Kohdentamisen taso oli tutkimuksessa läpikäydyissä tapauksissa matala, sillä kohteet eivät olleet ennalta spesifisti määriteltyjä eikä tietojenkalastelussa hyödynnetty yksilökohtaisia ominaisuuksia, kuten kohdennetussa tietojenkalastelussa tyypillisesti tehtäisiin (Hong, 2012). Soveltaen Burnsin ja kollegoiden (2019) tekemää tietojenkalastelun kohdennuksen arviointikriteeristöä, tutkimuksessa käsitellyt tapaukset olivat todella matalan kohdennuksen tietojenkalastelua eivätkä näin täytä kohdennetun tietojenkalastelun määritelmiä (Burns ym., 2019).

7.1.3 Jälkipuinti

Aiemmassa tietojenkalasteluun liittyvässä tutkimuksessa ei löytynyt vertailukohdetta spesifisti tietojenkalasteluhyökkäyksen jälkipuintiin ja hyökkääjän itsereflektioon, joka on selkeä tutkimusaukko tieteellisellä kentällä. Tutkimuksessa esiintynyttä tietojenkalastelua ei myöskään voi verrata puhtaasti rikolli-

suuteen liittyviin tutkimuksiin, sillä tämän tutkielman tutkimuksessa ilmeni vain osalla varsinaista rikollista toimintaa.

Ensimmäisessä tapauksessa haastateltava ei ottanut kantaa tietojenkalastelun jälkipuintiin. Toisessa tapauksessa (Tapaus 2) haasteltava tunnisti tietojenkalastelun olevan moraalisesti väärin, mutta neutralisoi aiheuttamaansa vahinkoa sillä, ettei kohteet tosiasiallisesti kärsineet taloudellista haittaa luotonantajan joutuessa mitätöimään rikoksen seurauksena nostetun luoton. Haastateltava (Tapaus 2) myös koki saaneensa tietojenkalastelun avulla enemmän kavereita, sillä tietojenkalastelun avulla saatu rahallinen hyöty mahdollisti kavereille erinäisten asioiden tarjoamisen. Haastateltava (Tapaus 2) haki omaa paremmuudentunnetta ja halusi kostaa yhteiskunnalle tietojenkalastelulla. Tätä voi peilata Sykesin ja Matzan (1975) neutralisaatioteoriaan, jossa tunnistettuja neutralisaation tekniikoita ovat muun muassa vahingon kieltäminen ja uhrin kieltäminen. Haastateltava (Tapaus 2) kielsi vahingon, sillä kohteille ei aiheutunut suoranaisesti taloudellista vahinkoa. Sykesin ja Matzan (1975) neutralisaatioteoriassa uhrin kieltämisen tekniikalla pyritään neutralisoimaan vahinkoa oikeutuksen, koston tai rangaistuksen varjolla, mitä haasteltava (Tapaus 2) ilmaisi myös kostonhaluna yhteiskunnalle kokien muiden pitävän häntä tyhmänä.

Vaikka tutkimuksessa ei tapauksissa 3 ja 4 kohteille ei aiheutettu haittaa eikä ne näin olleet varsinaisesti rikoksia, on niiden jälkipuinnin osalta yhteyksiä myös neutralisaatioteoriaan joissain määrin. Kolmannessa tapauksessa tietojenkalastelua harjoittanut haastateltava ei ajatellut kohteita sen kummemmin kuin, että ovatpa kohteet tyhmiä, kun menevät niin helppoon huijaukseen, mikä voisi kallistua hieman Sykesin ja Matzan (1975) neutralisaatioteorian uhrin kieltämisen tekniikkaan, jossa koetaan kohteen ansaitsevan toteutetun toiminnan. Neljännessä tapauksessa tietojenkalastelija pohti paljon kohteen näkökulmasta ja pyrki aktiivisesti olemaan aiheuttamatta emotionaalista haittaa tunnistaen tekevänsä moraalisesti väärin. Hyökkääjä siis koki, ettei kohteille seurannut toiminnastaan kuin mahdollisesti emotionaalista haittaa, joka voisi mahdollisesti viitata hieman Sykesin ja Matzan (1975) neutralisaatioteorian tekniikoista vahingon kieltämiseen. Toisaalta kolmannessa ja neljännessä tapauksessa kohteille ei selvää vahinkoa aiheutunut, jonka vuoksi neutralisaatioteorian soveltaminen ei ole niiden osalta kaikkein optimaalisinta.

Xu, Hu ja Zhang (2013) tutkivat hakkerointia ilmiönä ja tutkimuksessa ilmeni, että hakkerit olivat yhteydessä hakkerointihistoriansa aikana muihin, joilla oli samoja intressejä ja toisaalta tekijöinä taustalla toimi kyky, houkutteleva kohde ja huoltajiin liittyvät seikat nuorella iällä. Vaikka Xun ja kollegoiden (2013) tutkimus ei ole täysin sovellettavissa tässä tutkielmassa toteutettuun tutkimukseen, myös yhtäläisyyksiä löytyy. Tutkimuksessa haastateltava (Tapaus 2) nosti esiin tuntemuksen siitä, että hän pystyi toteuttamaan tietojenkalastelua ja toisaalta myös ensimmäisen tapauksen haastateltava koki olevansa hyvä tekemään talousrikoksia, joiden osalta yhtäläisyys Xun ja kollegoiden (2013) tunnistamista tekijöistä kykyyn tämä voisi vertautua. Kolmannessa tapauksessa haastateltava keskittyi enemmänkin kohteen toimintaan kuin omiin kykyihinsä, joka ei vertaudu Xun ja kollegoiden (2013) tutkimuksessa tunnistettuun kykyyn

taustalla toimivista tekijöistä. Kohteen houkuttelevuutta puolestaan ei tutkimuksen tapauksissa tullut korostetusti esiin, sillä tietojenkalastelun kohdennuksen taso oli matala.

7.2 Tutkimuksen merkitys

Tietojenkalasteluhyökkäykset ovat relevantti aihe kyberturvallisuuden kentällä, sillä Suomen kyberturvallisuuskeskuksen (2022) raportissa todettiin, että yksistään pankkitunnuksiin kohdistuvien tietojenkalasteluhyökkäysten seurauksena taloudelliset menetykset ovat olleet yli kahdeksan miljoonaa euroa Suomessa. Tietojenkalastelua on tutkittu paljon sen tekniikoiden ja kohteen näkökulmasta, mutta hyökkääjien taustatekijöihin tai jälkipuintiin liittyvä tutkimus on ollut vähäistä. Aiemman tieteellisen tutkimuksen ollessa vähäistä edellä mainittujen näkökulmien osalta, tutkimus tarjoaa tieteellisellä kentällä uutta tietoa hyökkäykseen johtavista taustatekijöistä ja motivaattoreista sekä hyökkääjän oman toiminnan tarkastelusta.

Tietojenkalastelu on siis suuri uhka kybermaailmassa, jonka haittojen torjuminen edellyttää tietämystä hyökkäyksen taustatekijöistä ja jälkipuinnista. Tutkimuksen tavoitteena oli ymmärtää koko tietojenkalastelun prosessia hyökkääjän näkökulmasta ja näin lisätä tieteellistä ymmärrystä tietojenkalastelun taustatekijöistä ja hyökkäyksen jälkipuinnista. Tietojenkalastelutekniikoiden tutkimuksen osalta tavoitteena on lisätä ymmärrystä tietojenkalasteluhyökkäyksen prosessin periaatteiden osalta, jonka tietoisuuden myötä tietojenkalastelua on mahdollista pyrkiä torjumaan tehokkaammin. Hyökkäyksen taustatekijöiden tieteellisen ymmärryksen perusteella voi olla myös mahdollista ennaltaehkäistä tietojenkalasteluhyökkääjäksi päätymistä. Tietojenkalasteluhyökkäyksiin hyökkääjän näkökulmasta pureutuva tutkimus pyrki lisäämään tieteellistä ymmärrystä, miksi tietojenkalastelua tehdään myös länsimaisessa yhteiskunnassa tai tehdäänkö Suomesta käsin edes tietojenkalasteluhyökkäyksiä ja miten.

7.3 Tutkimuksen rajoitteet ja luotettavuus

Tutkimus toteutettiin empiirisenä laadullisena tutkimuksena, jonka vuoksi tutkimuksen rajoitteita tulee pohtia kriittisesti. Tutkimuksen yksi keskeisimmistä rajoitteista oli otannan määrä, joka voi vaikuttaa tutkimuksen luotettavuuden. Dworkinin (2012) mukaan suositeltu otannan määrä vaihtelee 5-50 osallistujan välillä, mutta toisaalta tutkimuksen osallistujien sopiva määrä riippuu myös tilanteesta eikä suositukset kosketa esimerkiksi case-tutkimuksia. Otanta jää siis hieman suositellusta vajaaksi, mutta toisaalta tutkimus oli case-tutkimus, jolloin otannan määrä voi olla myös suositeltua pienempi. Toki tulosten yleistettävyys olisi parempi suuremmalla otannalla.

Oleellista tutkimuksessa on myös pohtia osittain strukturoidun haastattelussa havaittua luotettavuuden rajoitetta. Luotettavuuden rajoite tulee vastaan haastattelijan ollessa haastateltavalle tuntematon ja näin ollen haastateltavan voi olla haasteellista pohtia millä tasolla haastattelijaan voi luottaa (Myers & Newman, 2007) etenkin aiheen ollessa sensitiivinen. Ruusuvuori, Nikander ja Hyvärinen (2010, s.189) nostavat esiin, että yksilöhaastatteluiden analyysissä haastateltavat saattavat vastata tutkijan kysymyksiin sisällöllä, jota he olettavat tutkijan odottavan heiltä etenkin aiheeseen liittyessä moraalisia kysymyksiä, joihin tietyllä tavalla vastaaminen asettaisi haastateltavan tutkijan silmissä epäedulliseen asemaan. Tutkimukseni aihepiiri käsitteli myös moraalisia kysymyksiä, jolloin on ollut vaarana vastaako haastateltava kysymyksiin todenmukaisesti, vaikka olisi toiminut yleisen moraalin mukaisesti väärin.

7.4 Jatkotutkimus

Tämän tutkielman tutkimus olisi mielenkiintoista toistaa laajemmassa mittakaavassa, sillä otanta jäi suppeaksi. Laajemman otannan tutkimus vaatisi kuitenkin todennäköisimmin isompaa ajallista resurssia, sillä tutkimusaiheen ympäriltä oli hyvin hankala löytää haastateltavia. Laajemmalla otannalla voitaisiin tämän tutkimuksen tulosten paikkaansa pitävyyttä perehtyen etenkin taustatekijöihin ja hyökkäyksen jälkipuintiin.

Myös tietojenkalastelijan persoonallisuuspiirteitä olisi mielenkiintoista tutkia psykologisesta näkökulmasta. Psykologinen näkökulma kuitenkin vaatisi huomattavia ajallisia resursseja ja psykologian asiantuntevaa osaamista.

Tässä tutkielmassa esitelty tutkimus käsitteli vain Suomessa tehtyjä tietojenkalasteluhyökkäyksiä hyökkääjän näkökulmasta, mutta tutkimusta voisi laajentaa myös ottamaan mukaan muissa maissa tehdyt tietojenkalasteluhyökkäykset ja tutkia etenkin hyökkääjän taustatekijöitä sekä motivaatiota, sillä eri maiden välillä voi olla eroavaisuuksia esimerkiksi korruption tai sosiaaliturvan välillä, mikä voi osaltaan vaikuttaa hyökkääjien taustatekijöihin ja motivaatioon.

8 YHTEENVETO

Hiscoxin (2023) kybervalmiuden raportin mukaan tietojenkalastelu oli kohdemaiden toiseksi suurin kyberhyökkäysten väylä. Myös Suomen Kyberturvallisuuskeskus (2022) on nostanut esiin vuoden 2021 raportissaan pankkitunnuksiin kohdistuneiden tietojenkalasteluhyökkäysten takia menetyksien olevan yksinään arviolta yli kahdeksan miljoonaa euroa ja tietojenkalastelusta tehtiin poliisille ilmoituksia yli 800 ja Kyberturvallisuuskeskukselle tietojenkalasteluhyökkäyksiin liittyen yli 1800 (Kyberturvallisuuskeskus, 2022). Tietojenkalastelu on siis edelleen yksi merkittävistä kyberuhista, joka koskettaa käyttäjiä universaalisti. Tietojenkalastelua on tutkittu paljon siitä näkökulmasta ketkä joutuvat tietojenkalastelun uhreiksi ja mistä syistä, mutta ei niinkään hyökkääjän näkökulmasta eli mitkä taustatekijät johtivat tietojenkalasteluhyökkäysten tekemiseen, mitä tekniikkaa käytettiin ja miten se kehittyi sekä hyökkäyksen jälkipuintiin. Tässä tutkimuksessa tietojenkalastelun tutkimus rajattiin siis hyökkääjän näkökulmaan, jonka tutkimukselle tarve on merkittävä. Tutkimuksessa pyrittiin selvittämään tietojenkalastelua hyökkääjän näkökulmasta seuraavien tutkimuskysymysten avulla:

1. Mitkä taustatekijät johtivat siihen, että tietojenkalasteluhyökkäyksiä ryhdyttiin toteuttamaan?
2. Mitä tekniikkaa hyökkääjät käyttivät ja miten se kehittyi ajan saatossa?
3. Tekivätkö hyökkääjät jälkipuintia hyökkäyksistään eli reflektoivatko he omia toimiaan?

Tutkielmassa luotiin teoreettinen pohja kirjallisuuskatsauksen avulla, joka pohjautuu aiempaan tieteelliseen kirjallisuuteen tutkimuksen teeman ympärillä. Tämän avulla pyrittiin luomaan ymmärrys erityisesti tietojenkalastelutekniikoista, joihin aiempaa tieteellistä kirjallisuutta oli merkittävästi saatavilla. Taustatekijöitä ja jälkipuintia ei ollut juurikaan aiemmin tieteellisessä kirjallisuudessa käsitelty, joten teoriaa ei ollut näiltä osin suurissa määrin saatavilla.

Tutkimuksen toteuttamistavaksi valikoitui empiirinen laadullinen case- eli tapaustutkimus, joka toteutettiin neljän haastattelun avulla. Tutkimuksessa tapauksina toimivat haastateltavien toteuttamien tietojenkalasteluhyökkäysten

tai hyökkäyssarjojen elinkaari sisältäen taustatekijät, tekniikan ja jälkipuinnin haastateltavakohtaisesti. Haastatteluteknikkana toimi osittain strukturoitu tekniikka, jossa asetettiin haastattelulle muutamia haastattelun rakennetta ylläpitäviä kysymyksiä. Tutkimustuloksia analysoitiin sisällönanalyysin avulla, joka pohjautui haastatteluiden litterointiin ja tekstin ryhmittelyyn.

Tutkimuksessa havaittiin, että taustatekijöinä tietojenkalasteluhyökkäyksille olivat varsin moninaisia, mutta laajemmissa tietojenkelasteluhyökkäyskokonaisuuksissa suuri motivaattori oli raha. Toisaalta myös aiempi rikollinen tausta ja huono elämäntilanne vaikuttivat tietojenkalasteluhyökkäyksiin ryhtymiseen. Laajemmassa tietojenkalasteluhyökkäyskokonaisuudessa hyökkääjä ei kuitenkaan välttämättä tavoitellut taloudellista hyötyä, sillä tutkimuksessa tuli esiin tapaus, jossa hyökkääjä ajatteli hyvinkin eettisesti ja pyrki olemaan aiheuttamatta kohteelleen vahinkoa tai ainakin minimoimaan sen harjoittaessaan tietojenkalasteluhyökkäyksiä itsensä kehittämisen vuoksi. Tutkimuksessa oli myös tapaus, jossa tietojenkalastelu oli vain kertakokeilu mielenkiinnosta, joka syntyi toisen henkilön ehdotuksesta.

Tietojenkalastelutekniikan osalta valtaosassa tapauksista tietojenkalasteluhyökkäyksessä lähetettiin viesti, joka ohjasi tietojenkalastelunettisivulle, jonne kohteen oli mahdollista syöttää sensitiivistä informaatiota. Näissä tapauksissa myös tietojenkalastelutekniikat pääosin kehittyivät. Yhdessä tapauksessa oli kuitenkin poikkeamaa, sillä tietoja kalasteltiin feikkiprofiilin avulla suoraan kohteelta ja tekniikka kehittyi teknologian kehittymisen myötä. Viestien sisällöissä tekniikoina hyödynnettiin kiireellisyyden tunnetta (Tapaus 1 ja tapaus 2) sekä palkintoa (Tapaus 3) hämärtämään kohteen päätöksentekokykyä. Myöntyväisyyden periaatteista hyödynnettiin auktoriteettia (Tapaus 1, Tapaus 2 & Tapaus 3) sekä ystävyyssuhdetta (Tapaus 4).

Hyökkäysten jälkipuinnin näkökulmasta tutkimuksessa havaittiin saman kaltaista toimintaa. Hyökkäysten jälkeen tutkimuksen kohteena olevista hyökkääjistä kaikki neutralisoivat hyökkäystään ainakin jollain tasolla.

Havaitut tutkimustulokset olivat osin linjassa aiemman tutkimuksen kanssa. Koska tietojenkalastelun taustatekijöitä tai jälkipuintia ei ole juurikaan tutkittu, ei aiempaan tutkimukseen perustuvaa spesifiä vertailukohdetta kuitenkaan ollut. Hyökkäyksen jälkipuintia kuitenkin pystyi peilaamaan yleisellä tasolla neutralisaatioteoriaan, joka tuki tutkimuksen tuloksia, vaikka toki kaikissa tutkimuksen tapauksissa toiminta ei ollut rikollista. Tekniikkaa sen sijaan on tutkittu aiemmassa tieteellisessä kirjallisuudessa laajalti ja hyvin pitkälti tutkimuksessa esiin tulleet tietojenkalasteluhyökkäystekniikat olivat linjassa aiempaan tutkimukseen.

Tutkimuksessa on kuitenkin myös rajoitteita. Aihetta on tutkittu tämän tutkimuksen näkökulmasta vähän, joten paikoin tulosten reflektointi aiempaan tieteelliseen kirjallisuuteen oli kevyttä, sillä aiempaa tieteellistä kirjallisuutta ei suurissa määrin ollut saatavilla spesifisti tutkimuksen aiheeseen. Toisekseen aiheen ollessa sensitiivinen sen mahdollisen rikollisen aspektin vuoksi, haastateltavien löytäminen osoittautui haasteelliseksi ja otanta jäi pienehköksi. Suurempi otanta olisi lisännyt tutkimuksen yleistettävyyttä tulosten ollessa katta-

vampia, mutta toisaalta myös vaatinut enemmän resursseja kuin käytettävissä oli.

Tutkimuksen tieteellinen merkitys tietoturvallisuuden kentällä oli lisätä ymmärrystä tietojenkalasteluhyökkäysten taustoista, tekniikoista ja hyökkäyksen jälkipuinnista täyttäen kentällä olevaa tutkimusaukkoa näkökulmasta etenkin hyökkäyksen taustojen ja jälkipuinnin osalta. Tutkimuksen perusteella nousi esiin myös seuraavia jatkotutkimusaiheita tutkimuksen aihealueen ympäriltä:

1. Tutkimuksen toteuttaminen uudelleen laajemmalla otannalla verraten tuloksia nykyiseen tutkimukseen
2. Tutkimuksen laajentaminen käsittelemään psykologisia näkökulmia, jossa tutkittaisiin hyökkääjien persoonallisuustekijöitä
3. Tutkimuksen toistaminen eri kohdemaissa, mikä mahdollistaisi myöhemmin parhaassa tapauksessa maiden välisten erojen analysoinnin.

Hyökkääjän näkökulma erityisesti hyökkäyksen taustojen ja jälkipuinnin osalta on vähän tutkittu aihepiiri, osin varmasti näkökulman hankaluuden vuoksi, jonka vuoksi lisätutkimusta kaivataan.

LÄHTEET

Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection based associative classification data mining. *Expert Systems with Applications*, 41(13), 5948-5959. https://doi.org/10.1016/j.eswa.2014.03.019

Abri, F., Zheng, J., Namin, A. S., & Jones, K. S. (2022). Markov Decision Process for Modeling Social Engineering Attacks and Finding Optimal Attack Strategies. IEEE Access, 10, 109949-109968. https://doi.org/10.1109/ACCESS.2022.3213711

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9, 44928-44949. https://doi.org/10.1109/ACCESS.2021.3066383

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Predicting phishing websites using classification mining techniques. Julkaisussa: *Seventh international conference on information technology*; 2010 (s. 176–181). Las Vegas, Nevada, USA: IEEE. https://doi.org/10.1109/ITNG.2010.117

Adalı, S., & Golbeck, J. (2014). Predicting personality with social behavior: a comparative study. *Social Network Analysis and Mining*, 4, 1-20. https://doi.org/10.1007/s13278-014-0159-7

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

American Psychiatric Association. (2015). Neurodevelopmental disorders: DSM-5 selections. *American Psychiatric Association Publishing*.

Azizli, N., Atkinson, B. E., Baughman, H. M., Chin, K., Vernon, P. A., Harris, E., & Veselka, L. (2016). Lies and crimes: Dark Triad, misconduct, and high-stakes deception. *Personality and Individual Differences*, 89, 34—39. https://doi.org/10.1016/j.paid.2015.09.034

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in human behavior*, 38, 304-312. https://doi.org/10.1016/j.chb.2014.05.046

Bada, M., & Nurse, J. R. (2021, June). Profiling the Cybercriminal: A Systematic Review of Research. Julkaisussa: *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA) (s. 1-8). IEEE. https://doi.org/10.1109/CyberSA52016.2021.9478246

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus open*, 2, 8-14. https://doi.org/10.1016/j.npls.2016.01.001

Bereczkei, T. (2015). The manipulative skill: Cognitive devices and their neural correlates underlying Machiavellian's decision making. *Brain and Cognition*, 99, 24—31. https://doi.org/10.1016/j.bandc.2015.06.007

Black, D. W., & Grant, J. E. (2014). DSM-5 guidebook: The essential companion to the Diagnostic and statistical manual of mental disorders, fifth edition (viides painos). *American Psychiatric Publishing*.

Blythe, M., Petrie, H., & Clark, J. A. (2011). F for fake: four studies on how we fall for phish. Julkaisussa: *Proceedings of the SIGCHI conference on human factors in computing systems* (s. 3469-3478). https://doi.org/10.1145/1978942.1979459

Bogolyubova, O., Panicheva, P., Tikhonov, R., Ivanov, V., & Ledovaya, Y. (2018). Dark personalities on Facebook: Harmful online behaviors and language. *Computers in human Behavior*, 78, 151-159. https://doi.org/10.1016/j.chb.2017.09.032

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, 29(1), 24-39. https://doi.org/10.1080/10919392.2019.1552745

Campbell, W.K., Goodie, A. S., & Foster, J. D. (2004). Narcissism, confidence, and risk attitude. *Journal of Behavioral Decision Making*, 17(4), 297—311. https://doi.org/10.1002/bdm.475

Carli V, Durkee T, Wasserman D, Hadlaczky G, Despalins R, Kramarz E, Wasserman C,Sarchiapone M, Hoven CW, Brunner R, Kaess M (2013) The association between pathological internet use and comorbid psychopathology: a systematic review. *Psychopathology* 46(1):1–13. https://doi.org/10.1159/000337971

Chen, J. L., Ma, Y. W., & Huang, K. L. (2020). Intelligent visual similarity-based phishing websites detection. *Symmetry*, 12(10), 1681. https://doi.org/10.3390/sym12101681

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, 108, 106311. http://dx.doi.org/10.1016/j.chb.2020.106311

Chiew, K. L., Tan, C. L., Wong, K., Yong, K. S., & Tiong, W. K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences*, 484, 153-166. http://dx.doi.org/10.1016/j.ins.2019.01.064

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106, 1-20. http://dx.doi.org/10.1016/j.eswa.2018.03.050

Cho, J. H., Cam, H., & Oltramari, A. (2016, March). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. Julkaisussa: *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support* (CogSIMA) (s. 7-13). IEEE. http://doi.org/10.1109/COGSIMA.2016.7497779

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1).

Choi, K., Lee, J. L., & Chun, Y. T. (2017). Voice phishing fraud and its modus operandi. *Security Journal*, 30(2), 454-466.

Cialdini, R. B., & Cialdini, R. B. (2007). Influence: The psychology of persuasion (Vol. 55, s. 339). New York: Collins.

CISA Department of Homeland Security. (2023). Virus Basics.

Haettu 24.3.2023 osoitteesta https://www.us-cert.gov/

publications/virus-basics

Creswell, J. W. (2003). Research design: Qualitative, quantitative, and mixed methods approaches (2. painos). SAGE.

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, 87, 174-182. http://doi.org/10.1016/j.chb.2018.05.037

DeTardo-Bora, K. A., & Bora, D. J. (2016). Cybercrimes: An overview of contemporary challenges and impending threats. *Digital Forensics*, 119-132. http://doi.org/10.1016/B978-0-12-804526-8.00008-3

Diener, E. (2013). The remarkable changes in the science of subjective well-being. *Perspectives on Psychology*

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. Julkaisussa: *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, 37-44. http://doi.org/10.1145/1299015.1299019

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Archives of sexual behavior*, 41, 1319-1320. http://dx.doi.org/10.1007/s10508-012-0016-6

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.

Farwell, L., & Wohlwend ‐ Lloyd, R. (1998). Narcissistic processes: Optimistic expectations, favorable self ‐ evaluations, and self ‐ enhancing attributions.

Journal of Personality, 66(1), 65—83. https://doi.org/10.1111/1467-6494.00003

Furnham, A., Richards, S. C., & Paulhus, D. L. (2013). The dark triad of personality: A 10 year review. Social and Personality Psychology Compass, 7(3), 199–216. http://doi.org/10.1111/spc3.12018

Good, B., & Fang, L. (2015). Promoting smart and safe internet use among children with neurodevelopmental disorders and their parents. *Clinical Social Work Journal*, 43, 179-188. http://dx.doi.org/10.1007/s10615-015-0519-4

Gray, P., & Hovav, A. (2008). From hindsight to foresight: Applying futures research techniques in information systems. *Communications of the Association for Information Systems*, 22(1), 12.

Group-IB. How much is the phish? Underground market of phishing kits is booming — Group-IB. 2020. Haettu 25.3.2023 osoitteesta https://www.group-ib.com/media-center/press-releases/how-much-is-the-phish/

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.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67, 247-267.

Gutierrez, C. N., Kim, T., Della Corte, R., Avery, J., Goldwasser, D., Cinque, M., & Bagchi, S. (2018). Learning from the ones that got away: Detecting new forms of phishing attacks. *IEEE Transactions on Dependable and Secure Computing*, 15(6), 988-1001.

Han, X., Kheir, N., & Balzarotti, D. (2016). Phisheye: Live monitoring of sandboxed phishing kits. Julkaisussa: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (s. 1402-1413). https://doi.org/10.1145/2976749.2978330

Hawdon, J. (2021). Cybercrime: Victimization, Perpetration, and Techniques. *American Journal of Criminal Justice*, 1-6. http://doi.org/10.1007/s12103-021-09652-7

HISCOX (2023). Cyber Readiness Report 2022. Haettu 17.2.2023 osoitteesta https://www.hiscox.co.uk/cyberreadiness

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

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), 528-535.

Im, G., & Baskerville, R. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database*: the DATABASE for Advances in Information Systems, 36(4), 68-79. https://doi.org/10.1145/1104004.1104010

Jain, A. K., & Gupta, B. B. (2016). A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, 2016, 1-11. https://doi.org/10.1186/s13635-016-0034-3

Jain, A. K., & Gupta, B. B. (2017). Phishing Detection: Analysis of Visual Similarity Based Approaches. *Security and communication networks*, 2017, 1-20. https://doi.org/10.1155/2017/5421046

Jakobsson, M. (2018). Two-factor inauthentication – the rise in SMS phishing attacks. *Computer fraud & security*, 2018(6), 6-8. https://doi.org/10.1016/S1361-3723(18)30052-6

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007). What instills trust? a qualitative study of phishing. Julkaisussa: *Financial Cryptography and Data Security*: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007. Revised Selected Papers 11 (s. 356-361). Springer Berlin Heidelberg.

Jakobwitz, S., & Egan, V. (2006). The Dark Triad and normal personality traits. Personality and Individual Differences, 40(2), 331—339. https://doi.org/10.1016/j.paid.2005.07.006

Kang, Y., Kim, W., Lim, S., Kim, H., & Seo, H. (2022). DeepDetection: Privacy-Enhanced Deep Voice Detection and User Authentication for Preventing Voice Phishing. *Applied Sciences*, 12(21), 11109.

Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D., & Francillon, A. (2014, June). Optical delusions: A study of malicious QR codes in the wild. Julkaisussa: *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (s. 192-203). IEEE.

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091-2121. http://doi.org/10.1109/SURV.2013.032213.00009

Kirwan, G., & Power, A. (2011). The psychology of cyber crime, ensimmäinen painos. IGI Global

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, 58, 39-46. https://doi.org/10.1016/j.cose.2015.12.001

Korkmaz, M., Koçyiğit, E., Şahingöz, Ö., & Diri, B. (2022). A Hybrid Phishing Detection System by Using Deep Learning-Based URL and Content Analysis. *Elektronika ir Elektrotechnika*, 28(5).

Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). QR code security: A survey of attacks and challenges for usable security. Julkaisussa: *Human Aspects of Information Security, Privacy, and Trust:* Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2 (s. 79-90). Springer International Publishing.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.00

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT*), 10(2), 1-31. http://doi.org/10.1145/1754393.1754396

Kuroki, M. (2012). Crime victimization and subjective well-being: Evidence from happiness data. *Journal of Happiness Studies*, 14, 783–794. https://doi.org/10.1007/s10902-012-9355-1.

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, 48, 101343.

Kyberturvallisuuskeskus (2023). Kyberturvallisuuskeskuksen viikkokatsaus – 7/2023. Haettu 17.2.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-72023

Kyberturvallisuuskeskus (2022). Tietoturvan vuosi 2021. Haettu 17.2.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2021.pdf

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

Laszka, A., Vorobeychik, Y., & Koutsoukos, X. (2015). Optimal personalized filtering against spear-phishing attacks. Julkaisussa: *Proceedings of the AAAI Conference on Artificial Intelligence,* , 29(1)

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(5), 1-28. https://doi.org/10.1145/3336141

Lin, P. Y., & Chen, Y. H. (2017). High payload secret hiding technology for QR codes. *EURASIP Journal on Image and Video Processing*, 2017(1), 1-8.

Mansfield-Devine, S. (2018). The ever-changing face of phishing. *Computer Fraud & Security*, 2018(11), 17-19. https://doi.org/10.1016/S1361-3723(18)30111-8

Mavroeidis, V., & Nicho, M. (2017). Quick response code secure: a cryptographically secure anti-phishing tool for QR code attacks. Julkaisussa: *Computer Network Security*: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7 (s. 313-324). Springer International Publishing.

McHoskey, J. (1995). Narcissism and machiavellianism. *Psychological Reports*, 77(3), 755— 759. https://doi.org/10.2466/pr0.1995.77.3.755

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, 38(4), 767-772.

Moor, L., & Anderson, J. R. (2019). A systematic literature review of the relationship between dark personality traits and antisocial online behaviours. *Personality and individual differences*, 144, 40-55. https://doi.org/10.1016/j.paid.2019.02.027

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. Julkaisussa*: 2014 Information Security for South Africa* (s. 1-9). IEEE.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, 17(1), 2-26.

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

Naquin, C. E., Kurtzberg, T. R., & Belkin, L. Y. (2010). The finer points of lying online: E-mail versus pen and paper. *Journal of Applied Psychology*, 95(2), 387. https://doi.org/10.1037/a0018627

Nikander, P., Hyvärinen, M., Ruusuvuori, J., Pöysä, J., Jolanki, O., Nikander, P., & Karhunen, S. (2010). *Haastattelun analyysi*. Vastapaino

Nurse JRC (2019) Cybercrime and you: how criminals attack and the human factors that they seek to exploit. Julkaisussa: Attrill-Smith A, Fullwood C, Keep M, Kuss DJ *The oxford handbook of cyberpsychology*. Oxford University Press, Oxford, s. 663–690

Oest, A., Safaei, Y., Doupé, A., Ahn, G. J., Wardman, B., & Tyers, K. (2019). Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. Julkaisussa: *2019*

IEEE Symposium on Security and Privacy (SP) (s. 1344-1361). IEEE. https://doi.org/10.1109/SP.2019.00049

Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, 36(6), 556—563. https://doi.org/10.1016/S0092-6566(02)00505-6

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Security Journal*, 15(5), 13.

Polaschek, D. L., & Daly, T. E. (2013). Treatment and psychopathy in forensic settings. *Aggression and Violent Behavior*, 18(5), 592-603.

Popoola, S.I., Iyekekpolo, U.B., Ojewande, S.O., Sweetwilliams, F.O., & Atayero (2017). Ransomware: Current Trend, Challenges, and Research Directions. *Proc. of the World Congress on Engineering and Computer Science*, San Francisco, CA, USA, vol. 1, s. 169–174.

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, 29, 44-55. https://doi.org/10.1016/j.cosrev.2018.05.003

Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: a study on adversarial behaviors and strategies in phishing attacks. *Frontiers in psychology*, 9, 135. https://doi.org/10.3389/fpsyg.2018.00135

Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, 31, 3851-3873. https://doi.org/10.1007/s00521-017-3305-0

Riek, M., Böhme, R., & Moore, T. (2014, kesäkuu). Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. Julkaisussa: *13th Workshop on the Economics of Information Security*

Rouillard, J. (2008). Contextual QR codes. Julkaisussa: *Computing in the Global Information Technology*, 2008. ICCGI'08. The Third International Multi-Conference on, IEEE (2008) 50–55

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert systems with applications*, 117, 345-357. https://doi.org/10.1016/j.eswa.2018.09.029

Sappleton, N., & Lourenço, F. (2016). Email subject lines and response rates to invitations to participate in a web survey and a face-to-face interview: the sound of silence. *International Journal of Social Research Methodology*, 19(5), 611-622. https://doi.org/10.1080/13645579.2015.1078596

Sarno, D. M., Lewis, J. E., Bohil, C. J., Shoss, M. K., & Neider, M. B. (2017). Who are phishers luring?: a demographic analysis of those susceptible to fake emails. Julkaisussa: *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 61, No. 1, s. 1735-1739). Sage CA: Los Angeles, CA: SAGE Publications

Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, 51, 67-73. https://doi.org/10.1016/j.jcrimjus.2017.06.003

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Julkaisussa: *Proceedings of the SIGCHI conference on human factors in computing systems* (s. 373-382).

Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J., & Zhang, C. (2009). An empirical analysis of phishing blacklists.

Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & security, 65, 14-28. https://doi.org/10.1016/j.cose.2016.09.009

Silva, C. M. R. d., Feitosa, E. L., & Garcia, V. C. (2020). Heuristic-based strategy for Phishing prediction: A survey of URL-based approach. *Computers & security*, 88, 101613. https://doi.org/10.1016/j.cose.2019.101613

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management*, 49(7-8), 334-341. https://doi.org/10.1016/j.im.2012.06.004

Stojnic, T., Vatsalan, D., & Arachchilage, N. A. G. (2021). Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. *Security and privacy*, 4(5), https://doi.org/10.1002/spy2.165

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, 22(6), 664-670.

Tan, C. C. L., Chiew, K. L., Yong, K. S., Sebastian, Y., Than, J. C. M., & Tiong, W. K. (2023). Hybrid phishing detection using joint visual and textual identity. *Expert systems with applications*, 220. https://doi.org/10.1016/j.eswa.2023.119723

Tambe Ebot, A. C. (2017). Explaining two forms of internet crime from two perspectives: toward stage theories for phishing and internet scamming. *Jyväskylä studies in computing*, (259).

Tambe Ebot, A. C., Siponen, M & Topalli, V. (2023). Towards a cybercontextual transmission model for online scamming. European Journal of Information systems, forthcoming.

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Tupes, E. C., & Christal, R. E. (1992). Recurrent personality factors based on trait ratings. Journal of personality, 60(2), 225-251.

Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. Computer Fraud & Security, 2018(1), 15-20. https://doi.org/10.1016/S1361-3723(18)30007-1

Vernon, P. A., Villani, V. C., Vickers, L. C., & Harris, J. A. (2008). A behavioral genetic investigation of the dark triad and the Big 5. *Personality and Individual Differences*, 44(2), 445–452.

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L.F., Christin, N. (2013). QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. Julkaisussa: *International Conference on Financial Cryptography and Data Security,* Springer (2013) 52–69

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146-1166. https://doi.org/10.1177/0093650215627483

Volkamer, M., Renaud, K., Reinheimer, B., & Kunz, A. (2017). User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers & security*, 71, 100-113. https://doi.org/10.1016/j.cose.2017.02.004

Warikoo, A. (2014). Proposed methodology for cyber criminal profiling. *Information Security Journal*: A Global Perspective, 23(4-6), 172-178. https://doi.org/10.1080/19393555.2014.931491

Williams, C. (2007). Research methods. *Journal of Business & Economics Research* (JBER), 5(3).

Woods, N. (2022). Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior. Julkaisussa: *Cyber Security* (s. 93-134). Springer, Cham.

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

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. Communications of the ACM, 56(4), 64-74. https://doi.org/10.1145/2436256.2436272

Yang, P., Zhao, G., & Zeng, P. (2019). Phishing website detection based on multidimensional features driven by deep learning. *IEEE access*, 7, 15196-15209. https://doi.org/10.1109/ACCESS.2019.2892066

Yle, (2023 12. helmikuuta). Poliisista, päivää. Haettu 25.3.2023 osoitteesta https://yle.fi/a/74-20015999