Kia Orpana

KÄYTTÄJIIN KOHDISTUVA TIETOJENKALASTELU JA SEN EHKÄISEMINEN PALVELUNTARJOAJAN SEKÄ KÄYTTÄJÄN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Orpana, Kia
Käyttäjiin kohdistuva tietojenkalastelu ja sen ehkäiseminen palveluntarjoajan sekä käyttäjän näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2024, 37 s.
Tietojärjestelmätiede, Kandidaatin tutkielma
Ohjaaja(t): Vuorinen, Jukka

Tietojenkalastelu on yksi suurimpia uhkia internetissä, joten se aiheuttaa turvallisuusriskin käyttäjille sekä palveluille. Uhkan suuruutta lisää myös erilaisten kalastelumenetelmien olemassaolo, sillä yhden menetelmän ehkäiseminen ei välttämättä suojaa toiselta menetelmältä. Lisäksi kalastelulla voidaan aiheuttaa vahinkoa esimerkiksi arkaluontoisen tiedon päätyessä hyökkääjälle. Vahinkojen vähentämiseksi kalastelun ehkäiseminen sekä käyttäjien ja palveluiden turvallisuuden lisääminen on tärkeää. Kalastelun ehkäisyllä voidaan nostaa palveluiden turvallisuustasoa sekä parantaa arkaluontoisen tiedon suojausta tietojenkalastelua vastaan. Tämän takia tässä kandidaatin tutkielmassa käsitellään erilaisia tietojenkalastelun menetelmiä sekä menetelmiin soveltuvia ehkäisykeinoja. Ehkäisykeinot jaetaan palveluntarjoajalle sekä käyttäjälle soveltuviin keinoihin. Tämän pohjalta suoritetaan vertailu tietojenkalastelun ehkäisemisen eroista palveluntarjoajan ja käyttäjän näkökulmien välillä. Tutkielma on toteutettu kuvailevana kirjallisuuskatsauksena ja tutkimusprosessissa on hyödynnetty tutkielman aiheeseen soveltuvia lähteitä. Tutkielman tuloksissa esitellään tarkasteltuihin tietojenkalastelumenetelmiin soveltuvia ehkäisykeinoja ja ehkäisykeinojen jakautumista palveluntarjoajan sekä käyttäjän näkökulmiin. Tämän pohjalta tuloksista päätellään, miten palveluntarjoajan ja käyttäjän näkökulmat poikkeavat toisistaan kalastelun ehkäisyssä. Tuloksien perusteella keskeisiksi eroiksi näkökulmien kannalta havaitaan kalastelun ehkäisyn takana oleva motiivi, näkökulmiin soveltuvien ehkäisykeinojen tyyppi sekä ehkäisykeinojen hyödyntäminen.

Asiasanat: tietojenkalastelu, käyttäjä, palveluntarjoaja, ehkäisykeinot

ABSTRACT

Orpana, Kia
User focused phishing and its prevention from service provider's and user's perspectives
Jyväskylä: University of Jyväskylä, 2024, 37 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Vuorinen, Jukka

Phishing is one of the biggest threats on the internet and therefore phishing prevention as well as raising internet safety is important. The various existing phishing techniques can be hard to detect as well as prevent and as a result the techniques can cause damage if one falls victim to the phishing. This bachelor's thesis reviews different phishing techniques and prevention methods for the mentioned phishing techniques through a descriptive literature review. The prevention methods are divided into service provider's and user's perspective. Based on this division the perspectives will go through a comparison on how the perspectives differ from each other regarding phishing prevention. The results of the thesis present different prevention methods against phishing and the division of those methods to service provider's and user's perspectives. Based on these results the thesis includes conclusions on how the perspectives differ from each other regarding phishing prevention. The main differences between the perspectives are the motive behind phishing prevention, the suitable phishing prevention methods as well as the use of the prevention methods.

Keywords: phishing, user, service provider, prevention methods

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tietojenkalastelu on yksi yleisimpiä uhkia internetissä (Gupta ym., 2017). Tämän takia myös tietojenkalasteluhyökkäykset ovat entistä yleisempiä. Tietojenkalastelulla tarkoitetaan sosiaalista manipulointia sekä teknisiä ominaisuuksia hyödyntävää hyökkäystä, jossa hyökkääjä pyrkii esimerkiksi aiheuttamaan vahinkoa uhrille (Alkhalil ym., 2021). Hyökkääjän tarkoitus kalasteluyrityksessä on päästä käsiksi uhrin arkaluontoiseen tietoon kuten esimerkiksi pankkitietoihin tai salasanoihin (Ivanov ym., 2021). Arkaluontoisen tiedon kuten kirjautumistunnuksen päätyminen hyökkääjälle mahdollistaa tunnuksen takana olevien tietojen hyödyntämisen hyökkääjän haluamalla tavalla. Hyökkääjä voi hyödyntää tietojenkalasteluhyökkäyksessä varastettua arkaluontoista tietoa laittomasti esimerkiksi myymällä tietoa tai tekemällä ostoja (Alkhalil ym., 2021). Kalastelulla kerättyä tietoa hyödynnetään siis monesti laittomiin tarkoituksiin. Tietojenkalastelu on rikos, joka uhkaa sekä käyttäjää että palveluntarjoajaa (Jeeva & Rajsingh, 2016). Tietojenkalastelun määritelmään syvennytään luvussa kaksi.

Tietojenkalastelun yleistyminen lisää myös tarvetta ymmärtää tietojenkalastelun toimintaa ja tarkoitusta. Kalastelun ymmärtäminen vähentää esimerkiksi käyttäjien alttiutta tietojenkalastelulle (Alkhalil ym., 2021). Lisääntynyt ymmärrys auttaa siis varautumaan tietojenkalasteluun sekä sen mahdollisiin seurauksiin. Lisäksi on hyvä lisätä tietoisuutta erilaisista kalastelumenetelmistä sekä tavoista ehkäistä kalastelun tapahtumista ja onnistumista. Kouluttaminen on yksi tehokkaimpia tapoja ehkäistä tietojenkalastelua ja sen luomaa uhkaa (Bailey, Ph.D. ym., 2008). Esimerkiksi koulutuksen kautta saatu tietoisuus erilaisista tietojenkalastelun keinoista helpottaa siis tunnistamaan tietojenkalastelua ja ehkäisemään sitä. Ehkäisykeinot taas puolestaan auttavat tilanteissa, joissa tietojenkalastelu havaitaan. Kalastelun havaitseminen on oleellista ennen kalastelun ehkäisyä (Apandi ym., 2020). Ehkäisykeinojen tunnistaminen auttaa myös osaltaan vähentämään onnistuneiden kalasteluyritysten määrää, koska kalasteluyritykseen osataan reagoida tilanteeseen soveltuvalla ehkäisykeinolla.

Tässä tutkielmassa on tarkoituksena tutkia, miten tietojenkalastelun ehkäiseminen eroaa palveluntarjoajan ja käyttäjän näkökulmien välillä. Tutkielmassa tarkastellaan tietojenkalastelun määritelmää sekä erilaisia tietojenkalastelun

menetelmiä syvemmällä tasolla. Lisäksi tutkitaan keinoja, joilla tietojenkalastelua voidaan ehkäistä. Ehkäisykeinoista eritellään ne, joita hyödyntämällä palveluntarjoaja voi osaltaan vähentää tai ehkäistä kalastelua palvelussaan sekä ne keinot, joilla käyttäjä voi ehkäistä kalastelua. Käyttäjälle ja palveluntarjoajalle soveltuvien ehkäisykeinojen tutkimisen helpottamiseksi tutkielmassa tarkastellaan myös palveluntarjoajan, käyttäjän ja tietojenkalastelun yhteyttä. Edellä mainituilla tiedoilla pohjustetaan tutkielman tarkoitusta sekä vertailua käyttäjän ja palveluntarjoajan näkökulmista kalastelun ehkäisyssä.

Tutkielmassa esiteltyjä tietojenkalastelun ehkäisykeinoja analysoidaan palveluntarjoajan sekä käyttäjän näkökulmasta. Palveluntarjoajalle oleellisten ehkäisykeinojen etsiminen voi vähentää käyttäjän taakkaa kalasteluhyökkäyksissä. Kalastelun ehkäiseminen palveluntarjoajan toimesta voi mahdollisesti vähentää tietojenkalastelun ilmenemistä palvelun käyttäjille. Käyttäjälle oleellisten ehkäisykeinojen löytäminen taas suojaa käyttäjää kalastelutilanteissa.

Monesti tutkimuksissa keskitytään analysoimaan kalastelun ehkäisyä käyttäjän näkökulmasta. Käyttäjän näkökulmaan keskittyvissä tutkimuksissa esiteltävät ehkäisykeinot on suunnattu erityisesti käyttäjälle kalastelun ehkäisyä varten. Tässä tutkielmassa on päädytty tarkastelemaan aihetta ja ehkäisykeinoja sekä palveluntarjoajan että käyttäjän näkökulmasta, koska on mielenkiintoista selvittää ja vertailla näkökulmiin soveltuvia ehkäisykeinoja.

Tutkielman tavoitteena on selvittää, miten käyttäjänäkökulma eroaa palveluntarjoajan näkökulmasta tietojenkalastelun ehkäisyssä. Tavoitteen kannalta on tärkeää löytää keskeisimmät eroavaisuudet näkökulmien välillä. Tämä pyritään toteuttamaan tutkielmassa käytettävien lähteiden sekä lähteiden pohjalta tehtävien johtopäätösten avulla.

Tutkimuksen toteutustapa on kuvaileva kirjallisuuskatsaus. Tutkielman ideana on toteuttaa kirjallisuuskatsaus, jonka tutkimuskysymykseen löytyviä tuloksia vertaillaan tutkielmassa esiteltyjen näkökulmien kautta. Tutkimuskysymykseen vastataan hyödyntämällä löytyneitä lähteitä sekä omaa pohdintaa lähteiden kautta. Lähteinä on 27 artikkelia, jotka ovat tyypiltään esimerkiksi tutkimusartikkeleita sekä konferenssijulkaisuja. Artikkelien luotettavuutta on tarkasteltu muun muassa Julkaisufoorumin luokituksen avulla. Tutkielmassa käytettävät aineistot on kerätty hyödyntämällä erilaisia tietokantoja kuten Google Scholar, IEEE Xplore Digital Library, ACM ja Scopus. Lisäksi aineistoja on etsitty Jykdokin kautta. Aineistojen haussa on hyödynnetty avainsanoina esimerkiksi ”phishing”, ”user”, ”phishing prevention” ja ”service provider”. Hakuihin on myös tehty rajauksia esimerkiksi vuosiluvun kautta. Käytetyt aineistot ovat pääosin kirjoitettu englannin kielellä. Aineistojen valikoinnissa analysoitiin kriittisesti niiden soveltuvuutta tutkielman sisältöön sekä tutkimuskysymyksen kannalta oleellisiin aiheisiin. Tutkielman tutkimuskysymys on seuraavanlainen:

- Miten käyttäjän ja palveluntarjoajan näkökulmat eroavat toisistaan tietojenkalastelun ehkäisyn kannalta?

Tutkielman toinen luku keskittyy tietojenkalasteluun ja käyttäjään. Luvun alussa esitellään tietojenkalastelun määritelmä, jonka jälkeen tarkastellaan yksitellen valittuja tietojenkalastelun menetelmiä. Tämän jälkeen esitellään käyttäjän määritelmä sekä keskitytään tarkastelemaan käyttäjää ja tietojenkalastelua. Näistä tarkastellaan erityisesti käyttäjän ja tietojenkalastelun välistä suhdetta, vaikutuksia ja kalastelun ilmenemistä käyttäjälle.

Tutkielman kolmas luku tarkastelee palveluntarjoajaa ja tietojenkalastelua. Luvun alussa määritellään palveluntarjoaja käsitteenä. Tämän jälkeen käsitellään palveluntarjoajan ja tietojenkalastelun välistä suhdetta. Suhteesta on olennaista tarkastella esimerkiksi tietojenkalastelun ilmenemistä palveluntarjoajalle sekä kalastelun vaikutuksia palveluntarjoajaan. Palveluntarjoajan ja tietojenkalastelun yhteyden tarkastelemisen jälkeen luvussa siirrytään tarkastelemaan palveluntarjoajan ja käyttäjän yhteyttä. Palveluntarjoajan ja käyttäjän yhteydestä tarkastellaan muun muassa niiden vaikutusta toisiinsa. Lisäksi tuodaan esille palveluntarjoajan ja käyttäjän yhteys tietojenkalasteluun.

Tutkielman neljäs luku käsittelee tietojenkalastelun ehkäisykeinoja ja palveluntarjoajan sekä käyttäjän näkökulmien vertailua. Luvun alussa esitellään tutkimuksen tuloksena löytyneitä tietojenkalastelun ehkäisykeinoja sekä pohditaan niiden soveltuvuutta luvussa kaksi esiteltyjen kalastelumenetelmien ehkäisemiseen. Tämän jälkeen keskitytään tarkastelemaan esitettyjen ehkäisykeinojen olennaisuutta palveluntarjoajalle ja käyttäjälle sekä vertaillaan palveluntarjoajan ja käyttäjän näkökulmia kalastelun ehkäisyssä.

Viides luku on yhteenveto tutkielmasta. Tässä luvussa kootaan yhteen tutkimuksen sisältö sekä kerrataan tutkimuksen tulokset. Lisäksi pohditaan mahdollisia jatkotutkimusaiheita.

2 TIETOJENKALASTELU JA KÄYTTÄJÄ

Tässä luvussa määritellään tietojenkalastelu käsitteenä sekä esitellään erilaisia tietojenkalastelun menetelmiä. Lisäksi kerrotaan käyttäjän määritelmä ja tuodaan esiin käyttäjän sekä tietojenkalastelun välinen suhde.

2.1 Tietojenkalastelun määritelmä

Tietojenkalastelulle löytyy useita toisiaan vastaavia määritelmiä. Kalastelua on määritelty esimerkiksi sosiotekniseksi hyökkäykseksi, jossa hyökkääjä hyödyntää olemassa olevaa heikkoutta ja sen avulla pääsee käsiksi uhrin järjestelmään sekä houkuttelee sosiaalisen manipuloinnin avulla uhrin tekemään halutun toiminnon vahingon aiheuttamiseksi (Alkhalil ym., 2021). Toisen määritelmän mukaan tietojenkalastelu on sosiaalista manipulointia hyödyntävä hyökkäys, jonka tavoitteena on löytää muun muassa käyttäjän aiheuttamia heikkouksia järjestelmäprosesseissa ja hyväksikäyttää niitä (Khonji ym., 2013). Kalastelua on määritelty myös petoksen muodoksi, jossa hyökkääjä esittää luotettavaa entiteettiä ja yrittää saada luottamuksellista tietoa uhrilta (Jagatic ym., 2007). Tietojenkalastelun voidaan siis ajatella olevan jokin tapa huijata uhria lankeamaan kalastelulle ja jakamaan arkaluontoista tai henkilökohtaista tietoa hyökkääjälle. Voidaan myös tulkita, että tietojenkalastelun kannalta olennaisesti vaikuttavia tekijöitä ovat käyttäjään kohdistuva haitta sekä hyökkääjän tavoittelema hyöty.

Määritelmien pohjalta voidaan päätellä, että tietojenkalasteluun liittyy vahvasti sosiaalinen manipulointi. Tietojenkalastelu on myös yksi yleisimpiä sosiaalista manipulointia hyödyntäviä hyökkäyskeinoja (Sumner & Yuan, 2019). Näiden selkeän yhteyden takia on siis hyvä tuoda esiin sosiaalisen manipuloinnin määritelmä. Sosiaalinen manipulointi on yksilön piirteitä kuten esimerkiksi ahneutta, pelkoa tai uteliaisuutta hyväksikäyttävä hyökkäystyyli, jota hyödynnetään tietojenkalastelussa hyökkäyksien suorittamisessa manipuloimalla uhria psykologisesti tekemään haluttu toiminto (Ivanov ym., 2021).

Edellä mainitun perusteella voidaan havaita, että tietojenkalastelulle löytyy useita määritelmiä ja niillä on yhteys sosiaaliseen manipulointiin. Kalastelun määritelmät vastaavat pääpiirteiltään toisiaan sekä antavat samankaltaisen ymmärryksen tietojenkalastelusta. Voidaan siis tulkita, että kalastelu on teknologiaa hyödyntävää, uhriin kohdistuvaa sosiaalista manipulointia, jonka tavoitteena on päästä käsiksi luottamukselliseen tietoon sekä näin aiheuttaa myös vahinkoa.

2.2 Erilaiset tietojenkalastelun menetelmät

Tietojenkalastelulle on olemassa monia menetelmiä, mutta niiden perusperiaate on sama. Kalasteluhyökkäyksille on määritelty vaiheet, joita suurin osa hyökkäyksistä noudattaa. Hyökkäyksessä on ensin tavoitteena kerätä dataa järjestelmän käyttäjistä, jonka jälkeen valmistellaan pohja kalasteluhyökkäykselle esimerkiksi luomalla väärennetty nettisivu (Ivanov ym., 2021). Hyökkäyksen toteuttamiseksi on siis oleellista tehdä pohja, jossa hyökkäys toteutetaan. Seuraavaksi hyökkääjä lähettää esimerkiksi viestin, joka sisältää haittaohjelman tai hyperlinkin ja näiden kautta hyökkääjä saavuttaa tavoitteensa eli muun muassa käyttäjätietojen varastamisen tai taloudellisen hyödyn (Ivanov ym., 2021).

Kalasteluhyökkäysten perusrakenteen lisäksi on tärkeää huomioida erilaisten tietojenkalastelumenetelmien eroavaisuudet. Kalastelumenetelmät voidaan esimerkiksi jakaa sosiaalista manipulointia hyödyntäviin menetelmiin sekä teknologiakeskeisiin menetelmiin (Alkhalil ym., 2021). Myös Guptan ym. (2017) artikkelissa esitetyn käsityksen mukaan kalastelu jaetaan kahteen edellä mainittuun kategoriaan. Sosiaalista manipulointia hyödyntävät kalastelumenetelmät pyrkivät rakentamaan hyökkäykseen soveltuvan psykologisen ympäristön parantaakseen hyökkäyksen onnistumismahdollisuutta (Gupta ym., 2017). Teknologiakeskeiset kalastelumenetelmät taas puolestaan perustuvat haitallisen ohjelman päätymiseen käyttäjän järjestelmiin (Gupta ym., 2017).

Sosiaalista manipulointia hyödyntävät menetelmät ja teknologiakeskeiset menetelmät eroavat siis toisistaan esimerkiksi niiden tavalla vaikuttaa käyttäjään. Sosiaalisessa manipuloinnissa keskeistä on psykologinen vaikuttaminen käyttäjään halutun reaktion ja toiminnan saavuttamiseksi. Teknologiakeskeiset menetelmät taas pyrkivät vaikuttamaan ensisijaisesti käyttäjän laitteisiin. Voidaan kuitenkin havaita, että useat tietojenkalastelun menetelmät saattavat sisältää sekä sosiaalista manipulointia että teknologiakeskeisiä menetelmiä. Yleensä kuitenkin tietojenkalastelun menetelmät sisältävät selkeästi enemmän joko sosiaalista manipulointia tai teknologiakeskeisyyttä, vaikka niissä hyödynnettäisiinkin molempia menetelmiä. Kalastelumenetelmien pääkategorioiden eroavaisuuksien sekä kahtiajaon takia on siis olennaista käydä läpi yleisimmät erilaiset kalastelumenetelmät yksitellen, jotta kokonaiskuva tietojenkalastelusta sekä sen erilaisista menetelmistä rakentuu oikeanlaiseksi.

2.2.1 Tietojenkalastelu sähköposti

Tässä tietojenkalastelumenetelmässä sähköpostien lähettäminen uhrille on pääosassa. Sähköpostihuijauksen vaiheisiin kuuluu huijausviestin muodostaminen, viestin lähettäminen, viestin sisältämän haitallisen linkin tai liitteen avaaminen sekä halutun tiedon kerääminen uhrilta (Alkhalil ym., 2021). Huijauksen onnistuminen riippuu kuitenkin uhrista, sillä sähköpostin laukaisema toiminta vaihtelee yksilöittäin.

Sähköpostihuijauksen tarkoituksena on siis hyödyntää sosiaalista manipulointia, jotta uhri seuraa sähköpostin sisältämiä ohjeita arkaluontoisen tiedon luovuttamiseksi (Alkhalil ym., 2021). Sähköpostihuijauksen sisältämää sosiaalista manipulointia käytetään hyväksi uhrin toiminnan hallitsemisessa, jotta manipuloinnilla saadaan aikaan haluttu reaktio ja toiminta. Huijaussähköpostin tekstisisällöllä ja lähettäjällä yritetään esimerkiksi luoda kiireellisyyden ja uskottavuuden tunnetta sekä tällä tavoin manipuloida uhri reagoimaan mahdollisimman nopeasti viestin sisältöön (Kamruzzaman ym., 2023). Tälle huijaukselle olennaista on siis kiireellisyys, jolloin uhri ei ehdi analysoimaan viestin sisältöä kriittisesti ja on alttiimpi toimimaan hyökkääjän eduksi. Tietojenkalastelu sähköpostien voidaan ajatella olevan sosiaalista manipulointia hyödyntävä menetelmä, koska esimerkiksi kiireellisyys tai muu tunnetilan herätys on tyypillistä kalastelumenetelmälle.

2.2.2 Väärennetty nettisivu

Tämä tietojenkalastelumenetelmä perustuu väärennettyihin nettisivuihin, joiden kautta yritetään kalastella sivustolle päätyneen yksilön tietoja. Väärennetty nettisivu on hyökkääjän rakentama sivu, jonka tarkoitus on näyttää kopiolle alkuperäisestä nettisivusta (Mohammad, 2014). Väärennetyn sivuston tavoite on mukailla oikeaa sivustoa niin tarkasti, että sen tunnistaminen väärennökseksi on uhrille haasteellista. Väärennetyn sivuston tunnistamisen vaikeus lisää myös tietojenkalastelun uhrien määrää, koska käyttäjä saattaa luottaa liikaa sivustojen oikeellisuuteen ja luotettavuuteen.

Väärennetty nettisivu voi ilmetä uhrille muutamallakin eri tavalla. Sivusto voi esimerkiksi tulla linkkinä edellä mainitun huijaussähköpostin mukana tai mainoksen avaamisen yhteydessä (Alkhalil ym., 2021). Keskeistä väärennettyjen nettisivujen toiminnassa sekä kalastelun onnistumisessa on siis käyttäjän toiminta eli esimerkiksi saapuneiden linkkien tai mainosten avaaminen. Tässä kalastelumenetelmässä väärennetyille sivustoille päädytään, kun käyttäjä avaa sivustolle johtavan mainoksen tai linkin. Tällaisella sivulla toimintojen suorittaminen johtaa arkaluontoisen tiedon keräämiseen hyökkääjän toimesta (Alkhalil ym., 2021).

Väärennettyjä nettisivuja hyödyntävän tietojenkalastelun menetelmän voidaan ajatella olevan sosiaalista manipulointia hyödyntävä menetelmä. Väärennetyn nettisivun jäljitellessä oikeaa sivustoa, se herättää uhrissa esimerkiksi luottamuksen tunnetta, koska uhri ei välttämättä osaa ajatella väärennöksen

mahdollisuutta. Tämä luottamuksen tunne mukailee sosiaaliselle manipuloinnille tyypillisiä ominaisuuksia.

2.2.3 Tietojenkalastelu sosiaalisen median kautta

Tietojenkalastelu sosiaalisessa mediassa tapahtuu millä tahansa sosiaalisen median alustalla. Tietojenkalastelu sosiaalisessa mediassa voi ilmetä esimerkiksi alustalla olevissa mainoksissa, yksityisviesteissä tai julkaisuissa (Garcia, 2023). Käyttäjä altistuu kalastelulle olemalla vuorovaikutuksessa muun muassa kalastelujulkaisuissa, -viesteissä tai -mainoksissa olevan sisällön, kuten linkkien, kanssa.

Edellä mainituissa sosiaalisen median tietojenkalastelukeinoissa hyödynnetään myös sosiaalista manipulointia uskottavuuden ja julkisen aseman kautta. Garcian (2023) mukaan kyseisissä kalasteluhyökkäyksissä voidaan esimerkiksi esittää tunnettua henkilöä luomalla vale käyttäjätili ja hankkimalla käyttäjälle useita seuraajia lisäämään tilin uskottavuutta. Tämän jälkeen vale käyttäjätili voi julkaista haitallista sisältöä ja uskottavuutensa avulla houkutella seuraajia lankeamaan julkaisujen kautta tapahtuvalle tietojenkalastelulle (Garcia, 2023).

Sosiaalisen median kautta tapahtuvassa tietojenkalastelussa hyökkäykselle on olemassa useita tavoitteita. Kalasteluhyökkäyksen tavoitteena voi olla esimerkiksi haittaohjelmien jakaminen, huijaukset, toisena yksilönä esiintyminen sekä käyttäjätilien varastaminen (Alkhalil ym., 2021). Voidaan kuitenkin ajatella, että päätavoite edellisten pienien tavoitteiden takana on uhrin arkaluontoisen tiedon kaappaaminen.

Tietojenkalastelu sosiaalisen median kautta hyödyntää sosiaalista manipulointia osana kalasteluhyökkäystä, joten tämä kalastelumenetelmä voidaan luokitella sosiaalista manipulointia sisältäväksi menetelmäksi. Esimerkiksi sosiaalisen median alustalla vale käyttäjätili pyrkii herättämään uskottavuutta sekä luotettavuutta uhreissa. Tämä mukailee sosiaaliselle manipuloinnille olennaisia ominaisuuksia.

2.2.4 Puhelimen kautta tapahtuva kalastelu

Puhelimella tapahtuvassa tietojenkalastelussa hyökkääjä esiintyy luotettavana tai uhrille tuttuna henkilönä viestien tai puheluiden välityksellä (Alkhalil ym., 2021). Tämä menetelmä hyödyntää sosiaalista manipulointia, sillä tavoitteena on luoda uhrille turvallinen ja luotettava kuva. Turvallisuuden tunne taas osaltaan voi kannustaa uhria jakamaan arkaluontoista tietoa hyökkääjälle puhelimen välityksellä. Luottamuksen tunne puolestaan voi vähentää uhrin epäilyksiä tilanteeseen liittyen ja mahdollinen tietojenkalastelu voi onnistua isommalla todennäköisyydellä.

Puhelinkalastelussa yritetään puhelimen välityksellä saada uhri jakamaan arkaluontoista tietoa eli esimerkiksi salasanoja tai koodeja esiintymällä luotettavana henkilönä tai organisaationa, kuten muun muassa uhrin pankkina (Alkhalil ym., 2021). On myös olennaista mainita, että hyökkääjä voi ottaa uhriin yhteyttä soittamalla tai tekstiviestillä.

Alkhalilin ym. (2021) mukaan tekstiviestin kautta tapahtuvassa tietojenkalastelussa tavoitteena on saada uhri avaamaan viestissä oleva linkki tai reagoimaan viestissä mahdollisesti olevaan yhteydenottopyyntöön. Kalastelumenetelmässä huijauksen onnistumisen kannalta on siis oleellista käyttäjän reaktio kalasteluyritykseen.

2.2.5 Haittaohjelmapohjainen tietojenkalastelu

Guptan ym. (2017) mukaan haittaohjelmapohjaisessa kalastelussa käyttäjän laitteella ajetaan jokin useista olemassa olevista haitallisista ohjelmista. Tässä kalastelumenetelmässä uhrin laitteelle siis päätyy haitallinen ohjelma, joka voi esimerkiksi varastaa käyttäjän tietoja laitteelta. Haittaohjelmalla on pääsy uhrin laitteella olevaan dataan ja ohjelman tavoitteena on kerätä haluttu data sekä jakaa se hyökkääjälle (Gupta ym., 2017).

Haittaohjelmapohjaisen kalastelun voi jakaa muutamaan alakategoriaan, jotka sisältävät keskenään pieniä eroavaisuuksia. Eroista huolimatta kategorioissa mainitut menetelmät kuitenkin hyödyntävät haittaohjelmia toiminnassaan. Näitä kategorioita ovat istunnon kaappaus, sisällön lisäys, host-tiedoston manipuloiminen, DNS kalastelu ja näppäinten tai näytön tallentaminen (Gupta ym., 2017). Haittaohjelmapohjainen tietojenkalastelu perustuu pääosin teknologiaan sosiaalisen manipuloinnin sijaan. Haittaohjelma voi kuitenkin päätyä järjestelmään myös sosiaalista manipulointia hyödyntävän tietojenkalastelumenetelmän kautta. Haittaohjelman voi siis saada laitteelleen esimerkiksi sähköpostin tai tekstiviestin välityksellä.

2.2.6 Hakukoneen kautta tapahtuva tietojenkalastelu

Bandayn ja Qadrinin (2011) mukaan tietojenkalastelu hakukoneessa tapahtuu, kun hyökkääjä luo hakukoneella löydettävän kalastelusivuston. Tavoitteena on luoda sivusto, joka tavalla tai toisella houkuttelee käyttäjän avaamaan sivun hakukoneen tuloksista. Kalastelusivustoista tehdään kiinnostavia esimerkiksi hyvillä tarjouksilla (Banday & Qadri, 2011). Tämä tietojenkalastelun menetelmä perustuu siis hakukoneella ilmestyviin houkutteleviin sivustoihin. Kalastelumenetelmä eroaa väärennettyjä nettisivuja hyödyntävästä menetelmästä sivustojen tyylin takia, sillä hakukoneen kautta tapahtuvassa kalastelussa ei välttämättä hyödynnetä kopioita oikeista sivustoista.

Hakukoneen kautta tapahtuvassa tietojenkalastelussa hakukoneoptimointi on myös tärkeässä roolissa. Hakukoneoptimointi (SEO) on nettisivuston näkyvyyttä parantava keino, jossa hakukone tuo halutun sivuston ylemmäs hakutuloksissa (Lu ym., 2011). Tällä keinolla siis saadaan esimerkiksi enemmän suosiota sekä kävijöitä sivustolle. Lu ym. (2011) kertovat, että hakukoneoptimointia voi kuitenkin käyttää väärin, jolloin siitä tulee mustan hatun hakukoneoptimointia (black hat SEO). Mustan hatun hakukoneoptimointi helpottaa tietojenkalastelua, sillä se nostaa kalastelusivustoja ylemmäksi hakutuloksissa.

Mustan hatun hakukoneoptimointi voidaan jakaa haun liioitteluun ja haun myrkyttämiseen (Lu ym., 2011). Haun liioittelulla tarkoitetaan sivuston

näkyvyyden kasvatusta keskittymällä sivustolle olennaisiin avainsanoihin ja houkuttelemalla vain sivustoon liittyviä hakuja tekeviä käyttäjiä (Lu ym., 2011). Haun myrkyttämisellä taas tarkoitetaan sivuston näkyvyyden lisäämistä suosittujen hakutermien kautta, vaikka nämä termit eivät liittyisi sivustoon mitenkään (Lu ym., 2011). Molempien keinojen hyödyntämisessä tavoitteena on siis houkutella hakukoneen hakutuloksien avulla kävijöitä kalastelusivustoille, jotta hyökkääjillä on suurempi mahdollisuus löytää tietojenkalasteluun lankeavia käyttäjiä.

Hakukoneen kautta tapahtuva tietojenkalastelu voidaan luokitella teknologiakeskeiseksi kalastelumenetelmäksi, koska menetelmään liittyy vahvasti esimerkiksi sivustojen luominen sekä hakukoneoptimointi.

2.2.7 Välityshyökkäys (MITM)

Chiew ym. (2018) kertovat, että välityshyökkäys eli Man-in-the-middle (MITM) tietojenkalastelumenetelmässä hyökkääjä on uhrin ja verkkosovelluksen välisen kommunikaation välissä. Kalastelumenetelmässä hyökkääjä kerää salaa verkkosovellukseen syötettyjä uhrin henkilökohtaisia tietoja (Chiew ym., 2018). Kyseisen menetelmän kautta tapahtuva tietojenkalastelu voi siis kaapata luotettavalle sivustolle syötettyjä arkaluontoisia tietoja. Menetelmän toiminnassa ei ole kuitenkaan tarkoituksena hyödyntää väärennettyjä sivuja vaan seurata olemassa olevilla sivustoilla tapahtuvaa kommunikaatiota.

Käyttäjän on vaikea havaita välityshyökkäys kalastelumenetelmää ja näin myös varautuminen menetelmän tietojenkalastelua varten voi jäädä vähäiseksi. Välityshyökkäys on vaikeasti havaittavissa oleva kalastelumenetelmä, koska käyttäjälle lähetetään silti kaikki verkkosovelluksessa tapahtuva tieto eli sivuston toiminta näyttää uhrin silmissä normaalille (Chiew ym., 2018). Käyttäjälle ei siis todennäköisesti ilmene mitään normaalista verkkosovelluksen toiminnasta poikkeavaa, mutta kaikki käyttäjän toiminta on näkyvissä hyökkääjälle.

Välityshyökkäys kalastelumenetelmän voidaan ajatella kuuluvan teknologiakeskeisiin kalastelumenetelmiin, koska menetelmä perustuu uhrin ja verkkosovelluksen kommunikaation seuraamiseen. Menetelmä ei keskity uhrin toimintaan vaikuttamiseen vaan se pyrkii seuraamaan uhrin toimintaa sekä kaappaamaan arkaluontoista tietoa uhrin ja verkkosovelluksen välisestä kommunikaatiosta.

2.3 Käyttäjä ja tietojenkalastelu

Tietojenkalastelussa käyttäjää huijataan jakamaan henkilökohtaista tietoa esimerkiksi sosiaalisen manipuloinnin avulla (Jaswal ym., 2022). Tämän perusteella käyttäjä on olennainen osa tietojenkalastelua ja voidaankin ajatella, että käyttäjä on tietojenkalastelussa tapahtuvan huijauksen kohde. Tietojenkalastelun ja käyttäjän välinen suhde perustuu siihen, että käyttäjään kohdistetaan tietojenkalasteluhyökkäys.

Käyttäjällä tarkoitetaan tässä yhteydessä yksilöä, joka käyttää jotakin verkkopalvelua kuten esimerkiksi hakukoneita, työpaikan tietojärjestelmiä, sähköpostia tai sosiaalisen median alustoja. Monesti käyttäjällä on myös käyttäjätili ja tiliin kuuluva salasana tai muita mahdollisia kirjautumistietoja.

Käyttäjään kohdistuvassa tietojenkalastelussa halutaan saada käyttäjältä arkaluontoisia tietoja hyödyntäen monia olemassa olevia tietojenkalastelun menetelmiä. Tietojenkalasteluhuijauksissa käyttäjä voi esimerkiksi joutua tietämättään luotettavaa sivustoa, kuten pankkia, esittävälle huijaussivustolle, jossa käyttäjää pyydetään syöttämään kirjautumistiedot ja tämän jälkeen sivusto kerää kyseiset tiedot käyttäjältä (Darwish ym., 2012). Tämä tukee ajatusta käyttäjän roolista tietojenkalastelun kohteena.

Khonjin ym. (2013) mukaan kalasteluhyökkäys kohdistuu käyttäjään, koska käyttäjä aiheuttaa heikkouden järjestelmien turvallisuuteen. Esimerkiksi käyttäjän toiminta voi vaikuttaa käyttäjän osuuteen järjestelmän heikkoutena. Kamruzzaman ym. (2023) esittävät taas puolestaan, että ihmisten virheet ovat suurin syy tietojenkalasteluhyökkäyksien tapahtumiseen. Tämäkin väite tukee käyttäjän tekojen vaikutuksen olennaisuutta kalasteluhyökkäyksissä. Hyökkääjät siis näkevät käyttäjän mahdollisena heikkoutena ja pyrkivät hyödyntämään kyseistä heikkoutta kalasteluhyökkäyksissä.

Käyttäjien tuoma heikkous järjestelmien turvallisuuteen liittyy vahvasti tietojenkalastelussa käytettävään sosiaaliseen manipulointiin. Tietojenkalastelu on esimerkiksi sosiaalista manipulointia hyödyntävä hyökkäys (Khonji ym., 2013). Sosiaalisen manipuloinnin ja käyttäjän yhteyttä on siis olennaista tarkastella, sillä molemmat liittyvät vahvasti myös tietojenkalasteluun. Tietojenkalastelussa hyödynnettäviä sosiaalisen manipuloinnin keinoja ovat esimerkiksi pelottelu, auktoriteetit, kiireellisyys ja suostuttelu (Kamruzzaman ym., 2023). Tämä ilmenee käyttäjälle muun muassa kiireellisyyden tunteen luomisena esimerkiksi uhkaavan tai houkuttelevan sähköpostin kautta. Kiireellisyyden tunne puolestaan vähentää käyttäjän arviointikykyä tilanteessa ja saa aikaan nopeita reaktioita, esimerkiksi sähköpostiin tulleen linkin klikkauksen ilman tarkempaa analyysiä tilanteesta. Kyseinen reaktio tilanteeseen voi johtaa onnistuneeseen kalasteluyritykseen.

Sosiaalinen manipulointi voi ilmetä käyttäjälle myös auktoriteettien vaikuttavuuden kautta. Esimerkiksi käyttäjän pankkina esiintyvä hyökkääjä voi tietojenkalastelukeinossaan kehottaa käyttäjää vaihtamaan hyökkääjän mukaan vanhentuvia kirjautumistietojaan hyökkääjän ehdottamassa paikassa kuten huijaussivustolla. Auktoriteettia hyödyntävän tietojenkalastelu huijauksen käsky muokata kirjautumistietoja voi saada käyttäjän reagoimaan herkemmin kalasteluhuijauksen ohjeisiin sekä myös joutumaan herkemmin hyökkäyksen uhriksi.

Esiteltyjen sosiaalisen manipuloinnin keinojen pohjalta voidaan päätellä niiden tarkoituksen keskittyvän esimerkiksi saamaan käyttäjälle vahva tunnereaktio, joka harhauttaa käyttäjän ajattelukykyä ja ajaa käyttäjän toimimaan tietojenkalastelun menetelmän ohjeiden mukaan. Voidaan myös ajatella, että sosiaalista manipulointia hyödynnettäessä pyritään häiritsemään käyttäjän ajatuksen kulkua hyökkääjän eduksi. Käyttäjiin kohdistetaan hyökkäyksen yhteydessä

sosiaalisen manipuloinnin keinoja, joilla pyritään psykologisesti hallitsemaan uhrin eli käyttäjän reaktiota kalasteluhyökkäykseen (Kamruzzaman ym., 2023). Käyttäjä on siis kohteena olemisen lisäksi myös hyökkäyksen uhri.

Darwish ym. (2012) esittävät, että käyttäjän joutumiseen tietojenkalastelun uhriksi vaikuttavat persoonallisuuden piirteet sekä demografiset tekijät, kuten ikä, sukupuoli, koulutustausta ja tietojenkalastelun ehkäisemiseksi saatu koulutus. He esimerkiksi mainitsevat myötäileviä persoonallisuuspiirteitä omaavien olevan helpommin houkuteltavissa kalasteluhuijauksiin ja nuorten käyttäjien joutuvan kalastelun uhreiksi vanhempia käyttäjiä enemmän. Lisäksi he tuovat esiin sukupuolen vaikutuksen, jonka mukaan naispuoliset käyttäjät ovat luottavaisempia omien tietojensa jakamisen suhteen sekä näin myös alttiimpia kalasteluhyökkäyksien uhriksi joutumiselle. Sukupuolen vaikutus kalasteluun riippuu kuitenkin myös uhrin tottumuksista internetin käytöstä (Darwish ym., 2012). Edellä mainitusta voidaan päätellä, että käyttäjän lankeaminen tietojenkalasteluun riippuu monesta tekijästä. Voidaan lisäksi ajatella, että käyttäjän suhde tietojenkalasteluun siis rakentuu myös kalasteluun altistavien tekijöiden ja piirteiden vaikutuksesta. Käyttäjät, jotka omaavat enemmän kalastelun lankeamiseen altistavia ominaisuuksia, omaavat oletettavasti myös vahvemman suhteen tietojenkalasteluun.

Käyttäjän reaktio tietojenkalasteluhyökkäykseen on kuitenkin tärkeä. Jos sosiaalisen manipuloinnin keinot epäonnistuvat vaikuttamaan käyttäjään, myös tietojenkalastelu kyseisellä keinolla epäonnistuu. Eli jos hyökkääjä ei saa aikaan reaktiota käyttäjässä, tietojenkalasteluhyökkäyskään ei onnistu. Käyttäjä pystyy siis esimerkiksi hallitsemaan kalastelun aiheuttaman psykologisen reaktion, joka puolestaan voi mahdollistaa paremman ajattelun sekä näin ehkäistä kalastelun uhriksi joutumista. Tämäkin tukee ajatusta siitä, että käyttäjä on olennaisessa roolissa tietojenkalastelussa.

3 PALVELUNTARJOAJA JA TIETOJENKALASTELU

Tässä luvussa määritellään palveluntarjoaja käsitteenä. Tämän lisäksi esitellään palveluntarjoajan rooli tietojenkalastelussa sekä käsitellään kalastelun ilmenemistä palveluntarjoajalle. Luvussa tarkastellaan myös palveluntarjoajan ja käyttäjän välistä suhdetta.

3.1 Palveluntarjoaja

Altmann (2000) määrittelee palveluntarjoajan tarjoavan palveluita kuluttajille. Palveluntarjoajan palveluissa vaihtelevia tekijöitä ovat palvelun kesto ja tyyppi sekä internetin käyttö palvelussa (Altmann, 2000). Tässä tutkielmassa keskitytään palveluissaan internettiä hyödyntävään palveluntarjoajaan, koska tutkielmassa käsitellyt tietojenkalastelun menetelmät liittyvät vahvasti verkkopalveluihin.

Tutkielman kannalta tärkeä palveluntarjoajan osa-alue on internet palveluntarjoajan käsite. Altmannin (2000) mukaan internet palveluntarjoaja tai toiselta nimeltään informaatio palveluntarjoaja on yksi kolmesta internetin palvelukerroksen rooleista. Hän kertoo, että informaatio palveluntarjoaja toimittaa tietoa asiakkaille sekä käsittelee tietoa. Hän jakaa artikkelissaan tämän roolin viiteen eri alatasoon sen perusteella, mitä tietoa jaetaan. Informaatio palveluntarjoajien roolien alatasoja ovat sovellus, sisältö ja kommunikaatio palveluntarjoajat sekä internet jälleenmyyjät ja markkinapalveluiden tarjoajat (Altmann, 2000). Voidaan siis tulkita informaatio palveluntarjoajan sisältävän verkkopalveluissa sen osuuden tiedoista, joka välittyy palvelun käyttäjälle. On myös olennaista mainita, että tässä tutkielmassa informaatio ja internet palveluntarjoajilla tarkoitetaan samaa käsitettä.

Palveluntarjoajan rooli on siis jakaa tai tarjota palveluaan asiakkaille ja internetissä tämä konkretisoituu internet palveluiden tarjoamisena. Tarjottavia palveluita voi esimerkiksi olla sähköposti, verkkokaupat, sosiaalisen median

palvelut, suoratoistopalvelut ja hakukoneet. Tarjottavien palveluiden ylläpito on palveluntarjoajan vastuulla.

3.2 Tietojenkalastelu ja palveluntarjoaja

Palveluntarjoajalla on selkeä rooli tietojenkalastelussa, koska tietojenkalastelu tapahtuu palveluntarjoajan palvelussa. Voidaan ajatella, että palveluntarjoaja siis toimii alustana tietojenkalastelulle. Edellä mainitun rajauksen mukaan keskitytään erityisesti internet palveluita tarjoaviin palveluntarjoajiin ja tietojenkalasteluun.

Tietojenkalastelun ja palveluntarjoajan yhteyttä voidaan tarkastella seuraavan esimerkin kautta. Valitaan esimerkissä käsiteltäväksi palveluntarjoajaksi sosiaalisen median alusta Instagram ja tietojenkalastelun menetelmäksi aiemmin esitelty sosiaalisen median kautta tapahtuva tietojenkalastelu. Ensin palveluntarjoaja eli Instagram tarjoaa käyttäjälle mahdollisuuden tehdä käyttäjätili palveluun, jonka kautta käyttäjä voi tehdä julkaisuja, mainostaa ja viestitellä. Käyttäjätilin tekijä onkin hyökkääjä, jonka tarkoituksena on kalastella tietoja sosiaalisessa mediassa. Tämä hyökkääjä hyödyntää omaa käyttäjätiliään esimerkiksi haitallisten linkkien jakamiseen julkaisuissa tai yksityisviesteissä. Tässä kuvitetussa tilanteessa palveluntarjoajan palvelua eli Instagramia käytetään alustana tietojenkalasteluun hyökkääjän toimesta. Samaa periaatetta voidaan soveltaa muihin palveluntarjoajiin, jolloin palveluntarjoajan ensisijainen rooli tietojenkalastelun kannalta on kalastelualustana toimiminen.

Palveluntarjoajan ja tietojenkalastelun yhteyden tarkastelussa on olennaista tuoda esiin myös se, miten tietojenkalastelu ilmenee palveluntarjoajalle. Kalastelun havaitseminen jää usein käyttäjän vastuulle, sillä käyttäjän kouluttaminen ja tietoisuus kalastelusta ovat monesti ensimmäinen ratkaisu kalastelua vastaan (Hong, 2012). Edellä mainittu johtaa myös siihen, että palveluntarjoaja saa tiedon palvelussaan tapahtuvasta kalastelusta käyttäjältä. Käyttäjän kautta palveluntarjoajalle tulleet ilmoitukset tietojenkalasteluyrityksistä palveluntarjoajan palvelussa ovat siis olennaisessa osassa kalastelun ilmenemistä palveluntarjoajalle.

Lisäksi palveluntarjoajan on tärkeää huomioida tietojenkalastelun seuraukset palvelussaan. Tietojenkalastelussa hyödynnetään käyttäjän luottamusta palveluntarjoajaan ja onnistuneen kalasteluyrityksen kohdalla uhrin luottamus palveluntarjoajaan, jonka palvelussa kalastelu tapahtui saattaa kärsiä (Riah ym., 2024). Tietojenkalastelu voi siis osaltaan tuhota palveluntarjoajan suhdetta palvelunsa käyttäjiin. Onnistunut tietojenkalasteluyritys voi myös vaikuttaa negatiivisesti palveluntarjoajan maineeseen (Riah ym., 2024). Voidaan tulkita, että tietojenkalastelu voi aiheuttaa vahinkoa palveluntarjoajalle palvelun suosion laskemisen sekä palvelun luotettavuuden alentumisen kautta. Käyttäjien luottamuksen ja palvelun hyvän maineen ylläpitämiseksi tietojenkalastelun ehkäiseminen palveluntarjoajan toimesta on tärkeää (Riah ym., 2024).

Palveluntarjoajan on hyvä varautua tietojenkalasteluun, koska esimerkiksi Gupta ym. (2017) kertovat tietojenkalastelun olevan yksi yleisimpiä uhkia

internetissä. Hyvä varautuminen ja ehkäiseminen lisäävät palveluntarjoajan luotettavuutta. Varautumisen ja ehkäisemisen keinoja käsitellään myöhemmin tutkielmassa.

3.3 Palveluntarjoaja ja käyttäjä

Käyttäjä ja palveluntarjoaja liittyvät vahvasti toisiinsa. Esimerkiksi Altmannin (2000) mukaan kuluttaja on yksilö tai organisaatio, joka käyttää palveluntarjoajien tarjoamia palveluita. Kyseistä määritelmää on mahdollista soveltaa käyttäjään. Voidaan muun muassa tulkita määritelmän kuvastavan käyttäjän ja palveluntarjoajan välistä suhdetta, sillä käyttäjä käyttää palveluntarjoajan tarjoamaa palvelua.

Käyttäjän ja palveluntarjoajan suhde on olennainen myös tarjottavan palvelun kannattavuuden takia. Palveluntarjoaja tarvitsee käyttäjiä palvelulleen, jotta sen ylläpito on kannattavaa. Moni palveluntarjoaja esimerkiksi tarjoaa palvelussaan maksullisia toimintoja. Ilman maksullisten ominaisuuksien käyttäjiä palveluntarjoaja ei välttämättä saa tarvitsemaansa taloudellista hyötyä. Käyttäjän ja palveluntarjoajan suhde tuo myös muita hyötyjä sekä palveluntarjoajalle että käyttäjälle. Päähyödyksi voisi kuitenkin tulkita palveluntarjoajan osalta käyttäjien saamisen tarjotulle palvelulle. Käyttäjän puolesta isoin hyöty taas on käytettäväksi saatu palvelu.

Palveluntarjoajan ja käyttäjän välinen suhde perustuu luottamukselle. Käyttäjille on tärkeää pystyä luottamaan siihen, että palveluntarjoaja toimittaa käyttäjän odotuksia vastaavan palvelun (Coulter & Coulter, 2002). Käyttäjien luottamus mahdollistaa myös pidempiä suhteita palveluntarjoajan ja käyttäjän välille. Käyttäjän ja palveluntarjoajan suhteessa luottamus on olennaista, koska käyttäjän on esimerkiksi luotettava tarjottujen palveluiden toimivuuteen, turvallisuuteen ja käytettävyyteen.

Käyttäjän ja palveluntarjoajan välisen suhteen käsittelyn lisäksi on olennaista tarkastella, miten tietojenkalastelu liittyy käyttäjään ja palveluntarjoajaan. Kuten aikaisemminkin tutkielmassa on mainittu, tietojenkalastelu on käyttäjään kohdistuva teko ja kalastelu tapahtuu palveluntarjoajan tarjoamassa palvelussa.

Sekä käyttäjä että palveluntarjoaja voivat kärsiä tietojenkalastelusta. Kalasteluhyökkäyksissä käytetään hyväksi käyttäjän luottamusta palveluntarjoajiin (Riah ym., 2024). Käyttäjän luottamuksen hyväksi käyttäminen hyökkääjän toimesta voi siis myös vähentää käyttäjän luottamusta palveluun tulevaisuudessa, sillä käyttäjälle saattaa esimerkiksi muodostua käsitys palvelun turvattomuudesta. Kalasteluyritysten tapahtuminen palveluissa vahingoittaa palveluntarjoajan ja palvelun mainetta sekä vähentää käyttäjien luottamusta palveluun (Riah ym., 2024). Palveluntarjoaja siis puolestaan kärsii kalastelusta, kun käyttäjän luottamus palveluun vahingoittuu. Luottamuksen vahingoittumisen seurauksena myös käyttäjän ja palveluntarjoajan välinen suhde kärsii. Voidaan tulkita, että tietojenkalastelu vaikuttaa negatiivisesti sekä käyttäjään että palveluntarjoajaan ja mahdollisesti myös tuhoaa näiden välisiä suhteita.

Käyttäjän ja palveluntarjoajan suhde on hyödyllinen molemmille osapuolille. Suhteen ylläpitäminen hyödyttää molempia, mutta voidaan ajatella osassa tapauksista palveluntarjoajan tarvitsevan suhdetta käyttäjään enemmän kuin käyttäjä palveluntarjoajaan. Tämä koskee esimerkiksi tilanteita, joissa palveluntarjoajan palvelu ei ole käyttäjälle pakollinen tai välttämätön. Tällaisissa tilanteissa palveluntarjoaja oletetusti tarvitsee käyttäjiä palveluunsa enemmän kuin käyttäjä tarvitsee palvelua käyttöönsä.

Käyttäjä on siis esimerkiksi tärkeä sidosryhmä palveluntarjoajalle. Suhteen ylläpitäminen kuitenkin vaatii palveluntarjoajalta toimenpiteitä, joilla on mahdollista maksimoida käyttäjien mielenkiinto palveluun. Esimerkiksi käyttäjien palaute palvelun käyttökokemuksesta auttaa palveluntarjoajaa kehittämään palveluitaan miellyttämään käyttäjiä (Yang ym., 2011). Palveluiden kehittämisen voidaan ajatella olevan tärkeä tekijä palveluntarjoajan ja käyttäjän suhteen kannalta, koska se mahdollisesti auttaa palveluntarjoajia ylläpitämään suhdetta käyttäjiin. Käyttäjien palautteen avulla palveluntarjoaja voi myös kehittää käyttäjäkokemuksen laatua ja vaikuttaa käyttäjätyytyväisyyden tasoon (Yang ym., 2011). Voidaan tulkita, että käyttäjäkokemuksen ja käyttäjätyytyväisyyden huomioiminen palvelun kehittämisessä auttaa myös osaltaan ylläpitämään palveluntarjoajan ja käyttäjän välistä suhdetta.

Palveluntarjoajan ja käyttäjän suhde siis koostuu monesta osa-alueesta ja näillä osa-alueilla voidaan parantaa tai huonontaa suhteen laatua. Tietojenkalastelu taas voidaan ajatella negatiiviseksi tekijäksi käyttäjän ja palveluntarjoajan suhteen kannalta. Suhteeseen vaikuttavia tekijöitä on useita ja niiden huomioiminen tarpeellisella tavalla on olennaista suhteen ylläpidossa. Kokonaisuudessaan käyttäjän ja palveluntarjoajan välisen suhteen ylläpitäminen on hyödyllistä molemmille osapuolille.

4 TIETOJENKALASTELUN EHKÄISYKEINOT JA NÄKÖKULMIEN VERTAILU

Tässä luvussa käsitellään tietojenkalastelun ehkäisykeinoja yleisesti ja pohditaan niiden soveltuvuutta aiemmin tutkielmassa esitellyille tietojenkalastelun menetelmille. Ehkäisykeinojen käsittelyn jälkeen keinoista tarkastellaan niiden soveltuvuutta palveluntarjoajalle ja käyttäjälle. Tämän jälkeen vertaillaan palveluntarjoajan ja käyttäjän näkökulmia tietojenkalastelun ehkäisyn kannalta.

4.1 Tietojenkalastelun ehkäisykeinot

Tietojenkalastelun ehkäisemiseksi on esitetty useita keinoja ja malleja, joita hyödyntämällä kalastelun onnistumista on tarkoitus vähentää. Tässä tutkielmassa on tarkoituksena tarkastella ensin ehkäisykeinoja yleisellä tasolla sekä pohtia niiden hyödyntämistä aiemmin tutkielmassa esitetyille tietojenkalastelun menetelmille. Tietojenkalastelun ehkäisykeinoista esitellään ensin ihmistä ja sosiaalista manipulointia koskettavat ehkäisykeinot, jonka jälkeen tarkastellaan teknisempiä ratkaisuja kalastelun ehkäisemiseksi.

4.1.1 Kouluttamisratkaisut tietojenkalastelun ehkäisykeinona

Ensimmäisenä käsitellään yksilön kouluttamista yhtenä kalastelua ehkäisevänä keinona. Ihmisen kouluttaminen on yksi toimivimmista ehkäisykeinoista ja sillä nostetaan käyttäjien kykyä havaita tietojenkalastelua (Alkhalil ym., 2021). Voidaan siis tulkita, että käyttäjien tietoisuuden lisääminen vähentää onnistuneita kalasteluyrityksiä.

Ihmisten kouluttamiselle on kuitenkin olemassa useampia tapoja. Esimerkiksi Alkhalil ym. (2021) esittävät ihmisten koulutukselle kolme suuntaa, joiden avulla kouluttamista voisi toteuttaa. Heidän mukaansa ensin nostetaan käyttäjien tietoisuutta muun muassa kurssien ja seminaarien kautta. Toiseksi ratkaisuksi he esittelevät tekokalasteluhyökkäykset, jotka auttavat käyttäjiä

arvioimaan omaa osaamistaan kalasteluhyökkäyksissä sekä testaamaan käyttäjien haavoittuvuutta. Kolmas ratkaisu käyttäjien kouluttamisessa on kalasteluhyökkäyksistä opettavat opetuspelit (Alkhalil ym., 2021). Näiden esiteltyjen vaiheiden voidaan tulkita antavan hyvän käsityksen siitä, mitä kalastelun ehkäiseminen ihmisen kouluttamisen kautta tarkoittaa.

Myös Riah ym. (2024) kertovat, että käyttäjän kouluttaminen ja tietoisuuden lisääminen on tärkeää tietojenkalastelun ehkäisemisessä. Heidän mukaansa teknologia tarjoaa instituutioille ja organisaatioille alustan, jossa kouluttaa käyttäjiä ja lisätä tietoisuutta tietojenkalastelun välttämisestä sekä tunnistamisesta. Olennaisiksi koulutustavoiksi ilmenee esimerkiksi interaktiiviset koulutusohjelmat, opetusvideot ja nettisivut (Riah ym., 2024). Tämäkin siis tukee ajatusta siitä, että käyttäjien kouluttaminen on yksi olennainen ehkäisykeino.

Lisäksi Wash ja Cooper (2018) esittävät tutkimuksessaan käyttäjän kouluttamisen hyödyllisenä ehkäisykeinona tietojenkalastelua vastaan. Heidän tutkimuksensa perustuu sulautetun kouluttamisen muotoon, jossa käyttäjien sähköposteihin sisällytetään tekokalastelulinkkejä ja näitä klikatessaan käyttäjälle aukeaa koulutusviesti. Tutkimuksen edetessä kouluttamisen positiivinen vaikutus oli huomattavissa, sillä sähköpostilinkkien avaaminen käyttäjien toimesta väheni jo ensimmäisen tutkimusviikon jälkeen (Wash & Cooper, 2018). Ihmisten kouluttaminen edellä mainitulla menetelmällä on myös hyödyllinen ehkäisykeino tietojenkalastelulle.

Aiemmin mainitut opetuspelit ovat osaltaan hyödyllisiä tukemaan kouluttamista ehkäisykeinona. Esimerkiksi CJ ym. (2018) tutkivat artikkelissaan tietojenkalastelulinkkejä varten muodostettua opetuspeli Phishy:ä ja testasivat pelin toimivuutta työntekijöiden kouluttamisessa. He kertovat, että Phishy opetti pelaajia tunnistamaan kalastelulinkkejä onnistuneesti ja pelaajat kokivat koulutuksen muodon hauskana sekä opettavaisena kokemuksena. Yrityskäyttäjien kouluttaminen opetuspelien avulla on hyödyllinen opetuskeino tietojenkalastelun ehkäisemiseksi (CJ ym., 2018). Opetuspelit voidaan siis nähdä yhtenä kalastelua ehkäisevistä koulutuskeinoista. Voidaan myös päätellä, että opetuspelien hyödyntäminen kouluttamisessa voi olla hyödyllistä käyttäjätyypistä riippumatta.

Kouluttamiseen perustuvasta ehkäisykeinosta ja sen osa-alueista on hyvä pohtia myös niiden soveltuvuutta tutkielmassa aiemmin mainittuihin tietojenkalastelun menetelmiin. Kyseinen ehkäisykeino soveltuu hyvin esimerkiksi tietojenkalastelu sähköpostien ehkäisyyn, koska muun muassa Wash ja Cooper (2018) testasivat yksilön kouluttamista sähköpostikalastelun avulla. Kouluttaminen toimii ehkäisykeinona myös väärennettyjä nettisivuja hyödyntävään kalastelumenetelmään, sillä CJ ym. (2018) kertovat Phishy pelin auttavan tunnistamaan kalastelulinkkejä. Voidaan ajatella kouluttamisen auttavan myös väärennettyjen nettisivujen URL-osoitteiden tarkastelussa, koska esimerkiksi edellä mainittu opetuspeli voi osaltaan helpottaa URL-osoitteiden luotettavuuden analysointia.

Sosiaalisen median kautta tapahtuvaan kalasteluun sekä puhelimen välityksellä tapahtuvaan kalasteluun voi myös olla hyötyä kouluttamisesta sekä tietoisuuden lisäämisestä. Alkhalil ym. (2021) kertovat esimerkiksi ohjeita, joilla varautua sosiaalisen median tai puhelimen kautta tapahtuvaan kalasteluun.

Tärkeänä ohjeena on aiheesta oppiminen, jotta on tietoisempi kaikesta kalasteluun liittyvästä (Alkhalil ym., 2021). Käyttäjän ohjeistamisesta voidaan tulkita yksilön tietoisuuden lisäämisen olevan tärkeää.

Ihmisen kouluttaminen voi luultavasti toimia ehkäisykeinona myös haittaohjelmapohjaiseen kalasteluun, hakukonekalasteluun sekä välityshyökkäykseen, koska näidenkin keinojen ehkäisyssä olennaista on käyttäjän tietämys mahdollisesta kalastelusta. Tietojenkalastelun tunnistaminen kokonaisuudessaan on todennäköisempää käyttäjän ollessa tietoisempi tietojenkalastelusta sekä saatuaan koulutusta aiheesta.

Ihmisen kouluttaminen on siis tehokas keino ehkäistä tietojenkalastelua ja vähentää onnistuneiden kalasteluyrityksien määrää. Kuten myös aiemmin todettiin, kyseinen ehkäisykeino jakautuu useampaan osa-alueeseen, sillä kouluttamisen voi toteuttaa hyödyntämällä eri koulutusmuotoja. On kuitenkin hyvä muistaa, että koulutus on vain osa tietojenkalastelun ehkäisyä. Esimerkiksi Fajarin (2020) mukaan tietojenkalastelun vähentäminen edellyttää käyttäjän kouluttamista teknisten ratkaisujen rinnalla. Voidaan siis tulkita kouluttamisratkaisujen ja teknisten ratkaisujen tukevan toisiaan kalastelun ehkäisyssä. Tämän takia on olennaista käsitellä myös teknisempiä ratkaisuja, joilla tietojenkalastelua voidaan ehkäistä.

4.1.2 Tekniset ratkaisut tietojenkalastelun ehkäisykeinona

Tietojenkalastelulle on esitetty myös monia teknisempiä ehkäisykeinoja. Osa ehkäisykeinoista on tarkoitettu hyödynnettäväksi havaitsemaan tietojenkalasteluhyökkäyksiä tilanteissa, joissa hyökkäys on jo käynnissä (Alkhalil ym., 2021). Eli tällaisessa tilanteessa ehkäisykeinot eivät ehkäise hyökkäyksen julkaisua uhrien näkyville, mutta pyrkivät löytämään ja poistamaan haitallista sisältöä. Esimerkiksi Alkhalilin ym. (2021) mukaan on mahdollista skannata nettisivustoja väärennettyjen sivustojen havaitsemiseksi. Sivuston sisältöön perustuvia tietojenkalastelua havaitsevia ehkäisykeinoja käytetäänkin internetissä paljon (Alkhalil ym., 2021). Esimerkiksi Jeeva ja Rajsingh (2016) esittelevät artikkelissaan kalastelu URL-osoitteita havaitsevan järjestelmän, joka tarkastaa annetun URL-osoitteen aitouden. Jos aitoutta ei voida varmistaa, järjestelmä siirtyy tarkastelemaan osoitteen sivustosta ominaisuuksia, jotka erottavat oikeat sivustot huijaussivustoista varmistuakseen URL-osoitteen aitoudesta. Sivuston ominaisuuksien lisäksi tarkastellaan URL-osoitteen muotoa erilaisten ennalta määriteltyjen sääntöjen perusteella, jotta voidaan selvittää osoitteen luotettavuus (Jeeva & Rajsingh, 2016). Edellä mainittu keino siis soveltuu yhdeksi esimerkiksi huijaussivustojen havaitsemisesta nettisivujen skannauksen avulla ja voi osaltaan auttaa ehkäisemään tietojenkalastelua.

Gupta ym. (2017) taas puolestaan esittelevät käynnissä oleville kalasteluhyökkäyksille ehkäisykeinoksi tietojenkalastelua havaitsevat työkalupalkit sekä lisäosat. Heidän mukaansa nämä työkalupalkit ja lisäosat on suunniteltu havaitsemaan tietojenkalasteluhyökkäyksille tyypillisiä piirteitä eli heuristiikkoja. Heuristiikoista voi olla hyötyä esimerkiksi sivustojen aitouden testaamisessa sekä kalasteluviestien ja -sähköpostien tunnistamisessa (Gupta ym., 2017).

Tämän ehkäisykeinon hyödyntäminen voi olla avuliasta tilanteissa, joissa käyttäjä ei ole tarpeeksi perehtynyt tunnistamaan hyökkäysten heuristiikkoja ilman teknistä apua.

On myös olemassa ehkäisykeinoja, jotka on suunniteltu ehkäisemään tietojenkalasteluhyökkäyksiä jo ennen kuin ne päätyvät käyttäjän järjestelmiin (Alkhalil ym., 2021). Kyseisten ehkäisykeinojen voidaan ajatella pienentävän kalasteluhyökkäyksien ilmenemistä käyttäjille sekä näin myös vähentävän onnistuneiden hyökkäysten määrää. Alkhalil ym. (2021) mainitsevat tietojenkalastelun ehkäisyn ennen hyökkäyksen ilmenemistä käyttäjälle olevan tärkeää, koska käyttäjän ei tarvitse itse käsitellä hyökkäystä. He esittävät, miten esimerkiksi sähköpostikalastelussa erilaiset roskapostia tunnistavat työkalut voivat estää epäilyttävien sähköpostien saamista. Roskapostia tunnistavat työkalut tarkastelevat esimerkiksi kielioppia ja kirjoitusvirheitä sähköposteista voidakseen havaita kalastelusähköpostit sekä estääkseen näiden päätymisen käyttäjälle (Alkhalil ym., 2021). Tässä ehkäisykeinossa minimoidaan hyökkäyksen aiheuttama riski estämällä sen pääsy käyttäjän järjestelmään.

Tietojenkalastelun ehkäisykeinona voi hyödyntää kalastelua korjaavia tekniikoita (Alkhalil ym., 2021). Korjaavat tekniikat voidaan tulkita keinoiksi, joilla käynnissä olevaa tietojenkalasteluhyökkäystä yritetään poistaa käyttäjien ulottuvilta. Mooren ja Claytonin (2007) mukaan korjaava ehkäisykeino voi olla esimerkiksi väärennetyn nettisivun sulkeminen internetistä, jotta sivuston kautta tapahtuva tietojenkalastelu ei pääse jatkumaan. He mainitsevat sulkuprosessin alkavan muun muassa kalastelusähköpostin mukana tulleen linkin tarkastelulla, jotta saadaan selville sen luotettavuus. Jos sivu ilmenee väärennetyksi sivuksi, sen URL-osoite merkitään mustalle listalle. Tämä listaus taas osaltaan helpottaa roskaposteja tunnistavia työkaluja havaitsemaan kyseinen kalastelulinkki saapuneista sähköposteista. Huijaussivuksi määritetty URL-osoite ilmoitetaan palveluntarjoajalle ja sivustosta jätetään sulkupyyntö (Moore & Clayton, 2007). Voidaan siis tulkita, että korjaaviin tekniikoihin perustuvissa ehkäisykeinoissa on tärkeää reagoida sekä korjata ilmennyt uhka esimerkiksi juuri sulkemalla havaittu väärennetty nettisivu.

Alkhalil ym. (2021) kertovat myös erilaisten selaimeen upotettujen turvallisuusilmoitusten sekä varoitustyökalujen hyödyntämisestä tietojenkalastelun ehkäisykeinona. Heidän mukaansa monet ehkäisykeinot perustuvat pääasiassa käyttäjälle ilmeneviin varoituksiin työkalupalkissa. Osan työkalupakeista kuten McAfeen toiminta sisältää epäilyttävien sivujen estämisen jo ennen käyttäjälle ilmenevän varoituksen antamista sivustosta (Alkhalil ym., 2021). Voidaan kuitenkin ajatella, että pelkkiin varoitusilmoituksiin perustuvissa ratkaisuissa käyttäjän on oltava tarkkana huomatakseen varoitukset työkalupalkissa. Työkalupalkkien toiminta perustuu muun muassa siihen, että ne on ohjattu tunnistamaan esimerkiksi väärennettyjen sivustojen URL-osoitteita ja antamaan varoitus käyttäjälle tämän kohdatessa mahdollisen väärennetyn sivuston (Gupta ym., 2017).

Gupta ym. (2017) tukevat myös väitettä, että kalasteluhyökkäyksiä voidaan ehkäistä varoittamalla käyttäjää hyödyntämällä verkkoselaimeen upotettuja turvallisuusominaisuuksia. Verkkoselain ilmoittaa turvallisuusongelmasta

käyttäjälle tämän avatessa haitallisen linkin tai sivuston (Gupta ym., 2017). Voidaan havaita kalasteluhuijauksen tunnistamisen jäävän kyseisessä keinossa turvallisuusominaisuuksien vastuulle. Käyttäjän on siis edes osittain luotettava selaimen turvallisuusilmoituksiin. Mahdollisia ilmoitustyyppejä on kaksi, joista toinen sisältää aktiivisia varoituksia eli sulkee haitallisen sisällön käyttäjän näkyviltä ja toinen taas koostuu passiivisista varoituksista eli käyttäjälle ilmestyvästä varoitusilmoituksesta (Gupta ym., 2017). Nämä ilmoitukset voivat osaltaan ehkäistä tietojenkalastelun onnistumista, sillä varoitusten avulla käyttäjälle välittyy tieto mahdollisesti haitallisesta sisällöstä. Wu ym. (2006) kuitenkin selvittivät tutkimuksessaan aktiivisten varoitusten eli sisällön estämisen tai ponnahdusvaroitusten toimivan paremmin kuin passiiviset varoitukset työkalupalkissa, sillä moni käyttäjä esimerkiksi jättää työkalupalkin varoitukset epähuomiossa lukematta. Tässä ehkäisykeinossa on siis olennaista käyttäjän reaktio työkalupalkissa tai ponnahdusilmoituksena saatuun varoitukseen, koska ehkäisykeino ei välttämättä toimi halutulla tavalla tilanteissa, joissa käyttäjä ei huomioi varoitusta.

Tietojenkalastelua voi ehkäistä myös erilaisilla todennukseen perustuvilla keinoilla. Guptan ym. (2017) mukaan todennukseen perustuvissa ehkäisymenetelmissä varmistetaan, että tapahtuuko kommunikaatio luotettavan vai epäluotettavan verkkotunnuksen ja reitin välityksellä. Kyseistä ehkäisykeinoa voi hyödyntää sekä verkkotunnus- että käyttäjätasolla (Gupta ym., 2017). Todennuksessa tarkoituksena on hyödyntää erilaisia keinoja kommunikaation luotettavuuden arvioimiseksi. Esimerkiksi Alkhalil ym. (2021) esittelevät kolme erilaista keinoa todennuksen toteuttamiseksi. Näitä keinoja ovat yksivaiheinen, kaksivaiheinen ja monivaiheinen todentaminen. Yksivaiheisessa todentamisessa hyödynnetään käyttäjätunnusta ja salasanaa. Kaksivaiheisessa todentamisessa taas puolestaan käytetään käyttäjätunnuksen ja salasanan lisänä kertakäyttöisiä salasanoja, jotka lähetetään esimerkiksi käyttäjän määräämään puhelinnumeroon. Monivaiheinen todentaminen perustuu useamman eri tunnistamistavan hyödyntämiseen todentamisen toteuttamiseksi (Alkhalil ym., 2021). Todentamisen voi siis toteuttaa useammalla eri tyylillä. Voidaan myös ajatella, että valittu tyyli voi osaltaan vaikuttaa todennuksen vahvuuteen. Esimerkiksi pelkän salasanan ja käyttäjätunnuksen varastaminen tietojenkalastelua varten hyökkääjän toimesta voidaan ajatella helpommaksi kuin kaksi- tai monivaiheisen todentamisen vaatimien lisävarmistusten varastaminen.

On oleellista käsitellä edellä mainituista teknisiin ratkaisuihin perustuvista tietojenkalastelun ehkäisykeinoista myös niiden soveltuvuutta tutkielmassa esiteltyihin kalastelumenetelmiin. Esimerkiksi URL-osoitteiden ja nettisivujen skannaamiseen perustuvat menetelmät soveltuvat erityisesti väärennettyjen nettisivujen kalastelumenetelmän ehkäisemiseen. Lisäksi kyseinen ehkäisymenetelmä voisi soveltua tietojenkalastelu sähköpostien, hakukonekalastelun ja puhelimen tekstiviestikalastelun ehkäisyyn, koska näihin kalastelutekniikoihin voi sisältyä linkkejä nettisivustoille. Ehkäisymenetelmä siis auttaisi tarkastelemaan linkkien ja sivustojen luotettavuutta.

Tietojenkalastelua havaitsevat työkalupalkit sekä lisäosat puolestaan soveltuvat esimerkiksi kalastelusähköpostien, -viestien ja väärennettyjen

nettisivustojen tunnistamiseen (Gupta ym., 2017). Työkalupalkit ja lisäosat helpottaisivat sivustojen, viestien ja sähköpostien luotettavuuden arvioinnissa.

Ehkäisymenetelmä, jossa kalasteluhyökkäyksiä pyritään ehkäisemään jo ennen niiden päätymistä käyttäjälle, voisi soveltua jokaiseen mainituista tietojenkalastelutekniikoista. Kalastelun ehkäiseminen tällä tavoin on kuitenkin haasteellista eikä ehkäisymenetelmä välttämättä havaitse kaikkia kalasteluhyökkäyksiä ennen kuin ne ilmenevät käyttäjälle.

Kalastelua korjaavien ehkäisymenetelmien voidaan ajatella olevan hyödyllisiä väärennettyjen sivustojen kautta tapahtuvassa kalastelussa, koska menetelmän tavoite on esimerkiksi havaita ja sulkea kyseiset sivut. Ehkäisymenetelmä voi kuitenkin olla osittain oleellinen myös kalastelusähköpostien, -viesti ja hakukonekalastelun osalta, sillä näiden kautta käyttäjälle ilmenevien haitallisten sivustojen sulkeminen mahdollistuu menetelmää hyödyntämällä.

Turvallisuusilmoituksiin perustuva ehkäisykeino taas puolestaan soveltuu hyvin kaikkiin muihin menetelmiin paitsi välityshyökkäykseen. Kyseisestä kalastelumenetelmästä olisi hyvin epätodennäköistä saada turvallisuusilmoitus, koska välityshyökkäyksen huomaaminen on haasteellista.

Todennuksiin perustuvat ehkäisymenetelmät soveltuvat esimerkiksi sähköpostien kautta tapahtuvan kalastelun ehkäisyyn. Todennuspohjaiset tekniikat vahvistavat sähköpostiviestinnän turvallisuutta (Gupta ym., 2017). Ehkäisymenetelmää voidaan ajatella hyödynnettäväksi myös muiden tietojenkalastelukeinojen ehkäisemiseen, koska erityisesti vahvemmat todentamismenetelmät pitävät palveluihin syötettävän käyttäjätunnuksen ja salasanan turvallisempana lisävahvistuksien avulla.

Teknisiin ratkaisuihin perustuvien ehkäisykeinojen hyödyntäminen on tärkeää, sillä ne mahdollistavat tietojenkalastelun ehkäisyä eri näkökulmasta kuin ihmiseen pohjautuvat ehkäisymenetelmät. Olemassa olevat ehkäisymenetelmät eivät kuitenkaan tarjoa vahvaa suojaa tietojenkalastelumenetelmiä vastaan, sillä ei ole teknologiaa tai ratkaisua ehkäisemään kaikkea mahdollista tietojenkalastelua (Alkhalil ym., 2021). Voidaan kuitenkin ajatella, että ehkäisymenetelmien hyödyntäminen tietojenkalastelua vastaan auttaa vähentämään onnistuneiden kalasteluyritysten määrää. On siis oletettavasti parempi, että ehkäisymenetelmiä kehitetään ja hyödynnetään sen sijaan, että tietojenkalastelun ehkäisemiseksi ei olisi olemassa mitään ratkaisuja.

4.2 Ehkäisykeinojen jaottelu palveluntarjoajalle ja käyttäjälle

Ehkäisykeinojen lähempää tarkastelua varten keinot jaotellaan niiden soveltuvuuden mukaan käyttäjälle sekä palveluntarjoajalle. Tämä jaottelu perustuu edellisessä luvussa esiteltyihin ehkäisykeinoihin sekä tutkielman kannalta olennaisiin tietojenkalastelun menetelmiin. Voidaan ajatella, että suurin osa esitellyistä ehkäisykeinoista soveltuu moneen kalastelumenetelmään esimerkiksi ehkäisykeinojen muokattavuuden takia. Lisäksi voidaan tulkita, että ehkäisykeinojen jakautuminen käyttäjälle ja palveluntarjoajalle riippuu näkökulmasta. Osaa

ehkäisykeinoista on mahdollista hyödyntää sekä palveluntarjoajan että käyttäjän toimesta soveltamalla ehkäisykeinon toimintatapaa. Ehkäisykeinojen jakautumista käyttäjälle ja palveluntarjoajalle sekä keinojen soveltuvuutta kalastelumenetelmiin kuvataan taulukossa 1.

TAULUKKO 1 Tietojenkalastelun ehkäisykeinojen jakautuminen

Ehkäisykeino	**Tietojenkalastelumenetelmä**	**Soveltuvuus**
Tietoisuuden lisääminen (kurssit, seminaarit)	Kalastelusähköposti, väärennetty nettisivu, kalastelu sosiaalisessa mediassa, puhelinkalastelu, haittaohjelmat, hakukonekalastelu, välityshyökkäys	Käyttäjä
Tekokalasteluhyökkäykset	Kalastelusähköposti	Käyttäjä, palveluntarjoaja
Opetuspelit	Väärennetty nettisivu, kalastelusähköposti	Käyttäjä
Sivustojen ja URL-osoitteiden skannaus	Väärennetty nettisivu, kalastelusähköposti, hakukonekalastelu, puhelinkalastelu (tekstiviestit)	Palveluntarjoaja
Työkalupalkit ja lisäosat	Kalastelusähköposti, puhelinkalastelu (tekstiviesti), väärennetty nettisivu	Käyttäjä
Hyökkäyksen estäminen ennen sen pääsyä käyttäjälle (esim. roskapostia tunnistavat työkalut)	Kalastelusähköposti, väärennetty nettisivu, kalastelu sosiaalisessa mediassa, puhelinkalastelu, haittaohjelmat, hakukonekalastelu, välityshyökkäys	Palveluntarjoaja
Korjaavat tekniikat (esim. sivuston sulkeminen)	Väärennetty nettisivu, kalastelusähköposti, puhelinkalastelu (tekstiviesti), hakukonekalastelu	Palveluntarjoaja
Turvallisuusilmoitukset ja varoitustyökalut	Kalastelusähköposti, väärennetty nettisivu, kalastelu sosiaalisessa mediassa, puhelinkalastelu, haittaohjelmat, hakukonekalastelu	Käyttäjä
Upotetut turvallisuusominaisuudet	Väärennetty nettisivu, hakukonekalastelu, kalastelusähköposti, puhelinkalastelu (tekstiviesti)	Käyttäjä
Todentaminen	Kalastelusähköposti, väärennetty nettisivu, kalastelu sosiaalisessa mediassa	Käyttäjä, palveluntarjoaja

4.3 Palveluntarjoajan ja käyttäjän näkökulmien vertailu kalastelun ehkäisyn kannalta

Palveluntarjoajan näkökulma tietojenkalastelussa on hyvin erilainen kuin käyttäjän näkökulma. Tämän vuoksi tässä alaluvussa vertaillaan sitä, miten palveluntarjoajan näkökulma eroaa käyttäjän näkökulmasta tietojenkalastelun ehkäisemisessä. Vertailussa esitellään myös, miten näkökulma vaikuttaa tietyn ehkäisykeinon hyödyntämiseen. Vertailun apuna käytetään edellisen alaluvun taulukkoa (taulukko 1) sekä tutkielman aikana esille nostettuja asioita esimerkiksi kalastelun, palveluntarjoajan ja käyttäjän välisistä suhteista. Edellä mainittujen asioiden kautta pyritään vastaamaan tutkimuskysymykseen.

Palveluntarjoajan näkökulma tietojenkalastelun ehkäisyssä eroaa käyttäjänäkökulmasta muun muassa soveltuvien ehkäisykeinojen kautta. Esimerkiksi keinot, joilla pyritään ehkäisemään käynnissä olevia kalasteluhyökkäyksiä tukevat palveluntarjoajan näkökulmaa. Käynnissä olevien hyökkäysten ehkäisemisen voidaan ajatella soveltuvan palveluntarjoajalle, koska käyttäjä ei voi esimerkiksi lopettaa palveluntarjoajan palvelussa tapahtuvaa kalastelua eikä näin ollen myöskään käynnissä olevaa kalasteluhyökkäystä. Palveluntarjoajan näkökulmaan soveltuvia ehkäisykeinoja käynnissä olevien hyökkäysten kannalta olivat sivustojen skannaus sekä URL-osoitteiden skannaus.

Ehkäisykeinot, jotka painottavat kalastelun ehkäisyä ennen sen päätymistä palveluun tukevat myös osaltaan palveluntarjoajan näkökulmaa kalastelun ehkäisyssä. Esimerkiksi roskapostia tunnistavat ja estävät työkalut mainittiin aiemmin kuuluvaksi tähän ehkäisykeinojen kategoriaan. Nämä keinot soveltuvat palveluntarjoajan näkökulmaan, koska ne pyrkivät estämään kalastelun päätymistä palvelun käyttäjille. Esimerkiksi Alkhalil ym. (2021) kertovat tämän kaltaisten ehkäisymenetelmien toimivan jo hyökkäyksen alkuvaiheessa estämällä uhkan pääsyä käyttäjän laitteelle. Kalastelun ehkäisyssä on tärkeää estää käyttäjää näkemästä palvelussa tapahtuvaa hyökkäystä (Alkhalil ym., 2021). Voidaan siis tulkita, että palveluntarjoajan näkökulmassa keskitytään esimerkiksi suojelemaan käyttäjää ja se onnistuu muun muassa hyödyntämällä ehkäisykeinoja, jotka estävät tietojenkalastelun pääsyä käyttäjän laitteisiin. Vastaavat ehkäisykeinot taas eivät tukisi käyttäjänäkökulmaa, sillä keinojen idea on estää kalastelun näkyminen käyttäjälle kokonaisuudessaan.

Lisäksi korjaavat tekniikat kalastelun ehkäisyssä voidaan nähdä osana palveluntarjoajan näkökulmaa. Niin kuin aiemmin tutkielmassa kerrottiin nämä tekniikat pyrkivät korjaamaan kalastelutilanteen esimerkiksi sulkemalla väärennetyn nettisivun. Tällaisissa tilanteissa palveluntarjoajan voidaan ajatella hoitavan väärennettyjen nettisivujen sulkemisen tai niistä tiedottamisen. Esimerkiksi Alkhalil ym. (2021) mainitsevat internet palveluntarjoajien olevan vastuussa väärennettyjen sivujen sulkemisesta. Korjaavien tekniikoiden voidaan siis ajatella tukevan palveluntarjoajan näkökulmaa, koska ne auttavat poistamaan ilmenneitä uhkia sekä turvaamaan palvelua sen käyttäjiä varten. Ehkäisykeino ei soveltuisi tukemaan käyttäjänäkökulmaa, koska käyttäjä käyttää palveluntarjoajan

palvelua eikä pysty käyttäjän roolissa poistamaan palvelussa mahdollisesti uhkaavia tekijöitä.

Käyttäjänäkökulman ja palveluntarjoajan näkökulmat eroavat toisistaan myös käyttäjälle soveltuvien ehkäisykeinojen takia. Keskeisin ero näkökulmiin soveltuvien ehkäisymenetelmien välillä on niiden teknisyys. Palveluntarjoajan näkökulmaa tukevat ehkäisykeinot perustuvat enemmän teknisiin ratkaisuihin ja pyrkivät näin ehkäisemään kalastelua. Käyttäjänäkökulmassa taas puolestaan ehkäisykeinot muodostuvat erilaisista kouluttamismenetelmistä teknisten ratkaisujen sijaan. Pelkkä teknologia ei myöskään pysty turvaamaan käyttäjää kalastelulta (Bailey, Ph.D. ym., 2008). Tämän takia voidaan ajatella kouluttamismenetelmien olevan käyttäjänäkökulmalle olennainen osa tietojenkalastelun ehkäisyä.

Käyttäjänäkökulmaa tukee esimerkiksi käyttäjän tietoisuuden lisääminen ehkäisykeinona. Tietoisuuden lisääminen on yksi tehokkaimpia tapoja ehkäistä kalastelua (Bailey, Ph.D. ym., 2008). Voidaan ajatella, että kalastelun tunnistaminen helpottuu lisäämällä käyttäjän tietoisuutta. Tämä kuitenkin osaltaan siirtää kalastelun ehkäisemisen aiheuttaman taakan käyttäjälle, koska palveluntarjoajat voivat tulkita käyttäjien olevan tietoisia kalastelun mahdollisuudesta palveluissa.

Kouluttamismenetelmistä opetuspelit soveltuvat myös käyttäjänäkökulmaan. Esimerkiksi opetuspeli Phishy oli onnistunut ratkaisu yrityskäyttäjien opettamisessa (CJ ym., 2018). Voidaan esimerkiksi havaita opetuspelien kouluttavan käyttäjää sekä näin myös ehkäisevän tietojenkalastelua. Menetelmä siis tukee käyttäjänäkökulmaa kalastelun ehkäisyssä.

Lisäksi käyttäjänäkökulmaa tukevia ehkäisykeinoja ovat työkalupalkit ja lisäosat sekä varoitustyökalut ja turvallisuusilmoitukset. Voidaan ajatella kyseisten ehkäisykeinojen soveltuvan käyttäjänäkökulmaan, koska niiden tehtävä on toimia käyttäjän hyödyksi. Työkalujen ja turvallisuusilmoitusten idea on ilmoittaa käyttäjälle huomattuaan kalasteluhyökkäyksen (Alkhalil ym., 2021). Verkkoselaimeen upotettujen turvallisuusominaisuuksien voidaan ajatella kuuluvan edellä mainittujen ehkäisykeinojen kanssa samaan kategoriaan. Esimerkiksi Gupta ym. (2017) mainitsevat upotettavien turvallisuusominaisuuksien ilmoittavan käyttäjälle turvallisuusriskistä haitallisen linkin tai sivuston kohdalla. Tämä voidaan tulkita käyttäjänäkökulmaa tukevaksi menetelmäksi käyttäjälle näkyvien ilmoitusten perusteella. Edellä mainitut ehkäisykeinot eivät soveltuisi puolestaan palveluntarjoajan näkökulmaan niiden perusidean takia. Kyseisten ehkäisymenetelmien ajatus on toimia esimerkiksi selaimessa kalastelua havaitsevana ja ehkäisevänä keinona sekä ilmoittaa tästä käyttäjälle. Palveluntarjoaja ei hyödy ilmoituksesta, jos sen tarkoituksena on varoittaa käyttäjää.

Osa tutkielmassa esitellyistä ehkäisykeinoista soveltuu sekä käyttäjänäkökulmaan että palveluntarjoajan näkökulmaan. Molempiin näkökulmiin soveltuvien ehkäisykeinojen kohdalla näkökulmat kuitenkin poikkeavat esimerkiksi ehkäisykeinon vaikutuksen sekä hyödyntämisen kautta. Tällaisena keinona voidaan ajatella esimerkiksi kouluttamisratkaisuihin kuuluvia tekokalasteluhyökkäyksiä. Tekokalasteluhyökkäysten voidaan ajatella auttavan käyttäjää tunnistamaan kalasteluhyökkäyksiä sekä näin myös tukevan käyttäjänäkökulmaa

kalastelun ehkäisyssä. Esimerkiksi Wash ja Cooper (2018) esittävät tekokalasteluhyökkäyksien hyödyntämisen koulutuksessa vaikuttavan positiivisesti käyttäjän taitoihin tunnistaa kalastelusähköposteja ja linkkejä. Tekokalasteluhyökkäysten voidaan kuitenkin tulkita myös osaksi palveluntarjoajan näkökulmaa. Päätarkoitus tekokalasteluhyökkäyksissä on antaa käyttäjälle mahdollisuus arvioida omaa tietämystään kalastelusta sekä testata käyttäjän haavoittuvuutta kalasteluhyökkäyksille (Alkhalil ym., 2021). Tätä ideaa muokkaamalla palveluntarjoajan näkökulmalle soveltuvaksi voidaan tulkita tekokalastelun hyödyttävän palveluntarjoajaa. Palveluntarjoajan palveluun kohdistettu tekokalasteluhyökkäys voi mahdollisesti auttaa palveluntarjoajaa huomaamaan palvelunsa haavoittuvuuksia sekä arvioimaan palvelun turvallisuutta. Palveluntarjoajan ja käyttäjän näkökulmiin soveltuvat tekokalasteluhyökkäykset olisivat luultavasti tyypiltään erilaisia, joten ehkäisykeinon vaikutus ja hyödyntäminen eroaa näkökulmien välillä.

Myös todentamisen hyödyntäminen ehkäisykeinona voidaan ajatella soveltuvaksi sekä palveluntarjoajan että käyttäjän näkökulmaan. Ehkäisykeinojen vaikutuksen voidaan taas kuitenkin ajatella eroavan näkökulmien välillä. Todentaminen varmistaa esimerkiksi lähetetyn viestin reitin aitoutta (Gupta ym., 2017). Lisäksi todentaminen estää kalastelijoita pääsemästä käsiksi suojattuihin tietoihin (Alkhalil ym., 2021). Voidaankin tulkita, että nämä ominaisuudet auttavat muun muassa käyttäjänäkökulmassa turvaamaan käyttäjän tietoja sekä viestintää palveluissa. Palveluntarjoajan näkökulmaa ominaisuudet tukevat taas puolestaan lisäämällä palvelun turvallisuutta, koska käyttäjien todentaminen pitää palvelun käyttäjien tiedot turvassa.

Ehkäisykeinojen lisäksi palveluntarjoajan ja käyttäjän näkökulmat eroavat niiden motiiveilta kalastelun ehkäisyssä. Kuten tutkielmassa aiemmin todettiin, käyttäjä on tietojenkalastelun kohde. Tietojenkalastelu kohdistuu käyttäjään sen järjestelmäturvallisuuteen aiheuttaman heikkouden takia (Khonji ym., 2013). Tästä voidaan tulkita käyttäjän motiivien tietojenkalastelun ehkäisyssä keskittyvän itsensä suojelemiseen sekä omien tietojensa turvaamiseen. Tutkielmassa aiemmin mainitun mukaan palveluntarjoaja taas puolestaan tarjoaa alustan kalastelulle, koska kalastelu tapahtuu palveluntarjoajan palvelussa. Tämän pohjalta voidaan ajatella palveluntarjoajan motiiviksi kalastelun ehkäisyssä suojella sekä palvelua että palvelun käyttäjiä kalastelulta. Näkökulmat siis eroavat toisistaan ehkäisyn motiivin kannalta.

Molempien näkökulmien päätavoitteeksi voidaan ajatella tietojenkalastelun havaitseminen sekä ehkäiseminen. Esimerkiksi Apandi ym. (2020) kertovat tietojenkalastelun torjumisen jakautuvan kahteen yläkategoriaan eli kalastelun havaitsemiseen ja ehkäisemiseen. Heidän mukaansa kalastelu täytyy havaita ennen sen ehkäisyä. Tietojenkalastelun havaitsemisen jälkeen soveltuvia ehkäisykeinoja voi hyödyntää kalastelun ehkäisemiseksi (Apandi ym., 2020). Voidaan tulkita, että kalastelun havaitseminen ja ehkäiseminen ovat siis tärkeitä vaiheita tietojenkalastelun torjunnassa. Kyseisten vaiheiden vaikutus palveluntarjoajan ja käyttäjän näkökulmiin kuitenkin poikkeaa toisistaan. Voidaan esimerkiksi ajatella, että palveluntarjoaja havaitsee kalastelun eri tavalla kuin käyttäjä. Lisäksi tiedetään, että näkökulmille olennaiset ehkäisykeinot eroavat toistaan

vähintäänkin niiden toimintatavaltaan. Voidaan kuitenkin päätellä havaitsemisen ja ehkäisemisen olevan olennaisia sekä palveluntarjoajan että käyttäjän näkökulmalle.

On olennaista ajatella, että edellä mainitut eroavaisuudet esimerkiksi tavoitteissa sekä ehkäisykeinoissa ja niiden hyödyntämisessä auttavat tarkastelemaan palveluntarjoajan ja käyttäjän näkökulmia. Ehkäisykeinojen soveltuvuus näkökulmiin auttaa osaltaan havaitsemaan näkökulmien eroavaisuuksia. Lisäksi eroavaisuuksista voidaan päätellä, mihin näkökulmissa keskitytään. Palveluntarjoajan näkökulman tarkastelun jälkeen voidaan esimerkiksi tulkita sen keskittyvän palvelun turvallisuudelle olennaisiin tekijöihin sekä käyttäjiin vaikuttaviin tekijöihin kalasteluhyökkäyksien ehkäisemisessä. Käyttäjänäkökulman voidaan taas ajatella keskittyvän käyttäjän omien tietojen suojelemiseen niiden tekijöiden avulla, joita käyttäjän on mahdollista hyödyntää kalastelun ehkäisemiseksi. Tutkielman tuloksista voidaan päätellä, että suurimmat eroavaisuudet näkökulmien välillä ovat esimerkiksi ehkäisykeinojen tyypissä ja hyödyntämisessä sekä kalastelun ehkäisyn takana olevassa motiivissa.

5 YHTEENVETO

Tutkielman tavoitteena oli selvittää, miten käyttäjän ja palveluntarjoajan näkökulmat tietojenkalastelun ehkäisemisessä poikkeavat toisistaan. Tietojenkalastelun ehkäiseminen riippuu kuitenkin useammasta tekijästä, joiden vaikutuksen takia näkökulmien eroavaisuuksien tarkastelu on haasteellista. Esimerkiksi kalasteluhyökkäyksessä käytettävä menetelmä vaikuttaa paljon siihen, miten hyökkäystä ehkäistään. Lisäksi olemassa olevat kalastelumenetelmät muuttuvat jatkuvasti, joten niihin soveltuvien ehkäisykeinojen on myös muututtava. Tämä osaltaan vaikuttaa näkökulmien tarkastelun tuloksena löytyneiden eroavaisuuksien oleellisuuteen pidemmällä aikavälillä. Tutkielmassa on kuitenkin pyritty tarkastelemaan yleisimpiä kalastelumenetelmiä sekä ehkäisykeinoja.

Näkökulmien eroavaisuuksien vertailua varten oli ensin oleellista käydä läpi tietojenkalastelun määritelmä sekä erilaisia kalastelumenetelmiä. Tietojenkalastelun todettiin olevan uhriin kohdistuva sosiaalista manipulointia ja teknologiaa hyödyntävä hyökkäys, jonka tavoitteena on päästä käsiksi luottamukselliseen tietoon sekä näin aiheuttaa myös vahinkoa. Tietojenkalastelulle ei kuitenkaan ole olemassa yhtä tarkkaa määritelmää. Tutkielmassa käsiteltiin myös erilaisia kalastelumenetelmiä. Näitä menetelmiä olivat sähköpostin kautta tapahtuva tietojenkalastelu, väärennetyt nettisivut, sosiaalisen median, hakukoneen tai puhelimen kautta tapahtuva tietojenkalastelu, haittaohjelmapohjainen kalastelu sekä välityshyökkäys. Mainittujen menetelmien lisäksi on olemassa vielä useita erilaisia kalastelumenetelmiä, joten olemassa olevien menetelmien moninaisuuden tarkastelu jäi tutkielmassa vähäiseksi.

Lisäksi käyttäjän, palveluntarjoajan ja tietojenkalastelun välisten suhteiden käsittely oli oleellista suorittaa ennen näkökulmien eroavaisuuksien tarkastelua. Suhteiden tarkastelusta selvisi esimerkiksi se, että käyttäjä on kalastelun kohde sekä uhri. Palveluntarjoaja taas puolestaan tarjoaa alustan tietojenkalastelulle, sillä kalastelu tapahtuu palveluntarjoajan palvelussa. Käyttäjän ja palveluntarjoajan suhde taas vastaa asiakassuhdetta, sillä käyttäjä käyttää palveluntarjoajan tarjoamaa palvelua. Roolien osalta on kuitenkin tärkeää tunnistaa, että on mahdollista ajatella myös palveluntarjoajan olevan kalastelun uhri. Kyseistä suhdetta ei kuitenkaan tutkielman puitteissa tarkasteltu.

Tutkielman tarkoitusta pohjustettiin käsittelemällä ehkäisykeinoja tietojenkalastelulle sekä keinojen soveltuvuutta tutkielmassa esiteltyihin kalastelumenetelmiin. Ehkäisykeinoista käsiteltiin oleellisimmat tekniset ratkaisut sekä kouluttamisratkaisut. Teknisistä ratkaisuista havaittiin seitsemän oleellista keinoa kalastelun ehkäisyä varten. Näitä keinoja olivat sivustojen ja URL-osoitteiden skannaus, työkalupalkit ja lisäosat sekä hyökkäyksen estäminen ennen sen pääsyä käyttäjälle. Lisäksi korjaavat tekniikat, turvallisuusilmoitukset ja varoitustyökalut, upotetut turvallisuusominaisuudet sekä todentaminen havaittiin osaksi teknisiä ratkaisuja kalastelun ehkäisyssä. Kouluttamisratkaisuista taas tunnistettiin kolme oleellista keinoa. Näitä ehkäisykeinoja olivat tietoisuuden lisääminen, tekokalasteluhyökkäykset ja opetuspelit.

Ehkäisykeinoja tarkasteltiin taulukon avulla (taulukko 1) niiden soveltuvuuden osalta sekä esiteltyihin kalastelumenetelmiin että palveluntarjoajan ja käyttäjän näkökulmiin. Ehkäisykeinojen jaottelua kalastelumenetelmiin sekä palveluntarjoajan ja käyttäjän näkökulmiin käsiteltiin hyödyntämällä lähteitä. Jaottelu tuotti kuitenkin haasteita, sillä kaikkiin kalastelumenetelmiin soveltuvia ehkäisykeinoja ei suoraan ilmaistu lähteissä. Ehkäisymenetelmien jaottelussa palveluntarjoajan ja käyttäjän näkökulmiin hyödynnettiin johtopäätöksiä lähteiden pohjalta, koska tähänkään ei ollut suoraa vastausta lähteissä.

Tutkielman keskeiset tulokset palveluntarjoajan ja käyttäjän näkökulmien eroavaisuuksista sisälsivät kolme olennaista eroa näkökulmien välillä. Vertailusta saatujen tutkielman tuloksien mukaan näkökulmat erosivat esimerkiksi kalastelun ehkäisyn takana olevan motiivin, näkökulmiin soveltuvien ehkäisykeinojen tyypin sekä ehkäisykeinojen hyödyntämisen perusteella. Johtopäätösten muodostaminen lähteiden pohjalta oli tärkeässä roolissa eroavaisuuksien tunnistamisen kannalta.

Tutkielmaan liittyy myös rajoitteita. Esimerkiksi tutkielman tulokset ovat rajalliset, sillä ne nojaavat vain tutkielmassa käsiteltyihin lähteisiin sekä niiden pohjalta tehtyihin johtopäätöksiin. Tuloksia tarkastellessa on siis esimerkiksi muistettava niiden keskittyvän näkökulmien eroavaisuuksien tarkasteluun muun muassa tutkielmassa esiteltyjen ehkäisykeinojen sekä kalastelumenetelmien kautta. Tutkielmassa esitellyistä kalastelumenetelmistä poikkeavat kalastelumenetelmät eivät välttämättä sovellu tutkielmassa käsiteltyihin ehkäisykeinoihin. Myöskään tutkielman kannalta oleellisista ehkäisykeinoista poikkeavat ehkäisykeinot eivät mahdollisesti sovellu tutkielmassa esiteltyyn jaotteluun palveluntarjoajan ja käyttäjän näkökulmien osalta.

Tutkielmaan liittyvien rajoitteiden takia on oleellista käsitellä mahdollisia jatkotutkimusaiheita. Palveluntarjoajan ja käyttäjän näkökulmien eroavaisuuksia voisi tutkia tarkemmin esimerkiksi tekemällä tutkimuksen, jossa kerätään uutta tietoa käyttäjien sekä palveluntarjoajien näkemyksistä kalastelun ehkäisyn kannalta. Kerättyä tietoa voisi vertailla ja vertailun tuloksena olisi mahdollista löytää uusia eroja näkökulmien välillä. Tutkielman pohjalta olisi myös esimerkiksi mielenkiintoista tutkia, miten kalastelun ehkäiseminen yhdistää palveluntarjoajan ja käyttäjän näkökulmia. Lisäksi olisi kiinnostavaa tutkia onnistuneisiin kalasteluhyökkäyksiin liittyvää vastuuta. Vastuusta voisi tutkia esimerkiksi, miten vastuu

jakautuu palveluntarjoajan ja käyttäjän välillä tietojenkalastelun onnistuessa. Jatkotutkimuksissa voisi ylipäätään tarkastella, millainen vastuu palveluntarjoajalla tai käyttäjällä on kalasteluhyökkäyksissä.

LÄHTEET

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060

Altmann, J. (2000). A reference model of internet service provider businesses. *ICTEC*. https://sspace.snu.ac.kr/bitstream/10371/6836/1/A%20Reference%20Model%20of%20Internet%20Service%20Provider%20Businesses.pdf

Apandi, S. H., Sallim, J., & Sidek, R. M. (2020). Types of anti-phishing solutions for phishing attack. *IOP Conference Series: Materials Science and Engineering*, *769*(1), 012072. https://doi.org/10.1088/1757-899X/769/1/012072

Bailey, Ph.D., J., Robert Mitchell, D. B. A., & Bradley Jensen, P. D. (2008). Analysis of Student Vulnerabilities to Phishing. *AMCIS 2008 Proceedings*. https://aisel.aisnet.org/amcis2008/271

Banday, M. T., & Qadri, J. A. (2011). *Phishing – A Growing Threat to E-Commerce* (arXiv:1112.5732). arXiv. https://doi.org/10.48550/arXiv.1112.5732

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. https://doi.org/10.1016/j.eswa.2018.03.050

CJ, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 169–181. https://doi.org/10.1145/3270316.3273042

Coulter, K. S., & Coulter, R. A. (2002). Determinants of trust in a service provider: The moderating role of length of relationship. *Journal of Services Marketing*, *16*(1), 35–50. https://doi.org/10.1108/08876040210419406

Darwish, A., Zarka, A. E., & Aloul, F. (2012). Towards understanding phishing victims' profile. *2012 International Conference on Computer Systems and Industrial Informatics*, 1–5. https://doi.org/10.1109/ICCSII.2012.6454454

Fajar, A. (2020). The initial socio-technical solution for phishing attack. *Journal of Physics. Conference Series*, *1502*(1), 12034-. https://doi.org/10.1088/1742-6596/1502/1/012034

Garcia, K. R. (2023). Phishing in Social Media: Investigating Training Techniques on Instagram Shop. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *67*(1), 1850–1855. https://doi.org/10.1177/21695067231192588

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

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

Ivanov, M. A., Kliuchnikova, B. V., Chugunkov, I. V., & Plaksina, A. M. (2021). Phishing Attacks and Protection Against Them. *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, 425–428. https://doi.org/10.1109/ElConRus51938.2021.9396693

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

Jaswal, P., Sharma, S., Bindra, N., & Krishna, C. R. (2022). Detection and Prevention of Phishing Attacks on Banking Website. *2022 International Conference on Futuristic Technologies (INCOFT)*, 1–8. https://doi.org/10.1109/INCOFT55651.2022.10094345

Jeeva, S. C., & Rajsingh, E. B. (2016). Intelligent phishing url detection using association rule mining. *Human-Centric Computing and Information Sciences*, *6*(1), 10. https://doi.org/10.1186/s13673-016-0064-3

Kamruzzaman, A., Thakur, K., Ismat, S., Ali, M. L., Huang, K., & Thakur, H. N. (2023). Social Engineering Incidents and Preventions. *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 0494–0498. https://doi.org/10.1109/CCWC57344.2023.10099202

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Lu, L., Perdisci, R., & Lee, W. (2011). SURF: Detecting and measuring search poisoning. *Proceedings of the 18th ACM conference on Computer and communications security*, 467–476. https://doi.org/10.1145/2046707.2046762

Mohammad, R. M. (2014). Intelligent rule-based phishing websites classification. *IET Information Security*, *8*(3), 153. https://doi.org/10.1049/iet-ifs.2013.0202

Moore, T., & Clayton, R. (2007). Examining the impact of website take-down on phishing. *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, 1–13. https://doi.org/10.1145/1299015.1299016

Riah, A., Daniel, S., Frank, E., & Seriffdeen, K. (2024). *The role of technology in shaping user behavior and preventing phishing attacks*.

Sumner, A., & Yuan, X. (2019). Mitigating Phishing Attacks: An Overview. *Proceedings of the 2019 ACM Southeast Conference*, 72–77. https://doi.org/10.1145/3299815.3314437

Wash, R., & Cooper, M. M. (2018). Who Provides Phishing Training?: Facts, Stories, and People Like Me. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3173574.3174066

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 601–610. https://doi.org/10.1145/1124772.1124863

Yang, Z., Wu, B., Yu, N., Yu, G., & Chen, J. (2011). A Three-Step Service Experience Approach with Feedback for Service Provider. *2011 IEEE Asia-Pacific Services Computing Conference*, 188–194. https://doi.org/10.1109/APSCC.2011.47