TURUN YLIOPISTO
Kauppakorkeakoulu

Käyttäjiin kohdistuvien kyberturvariskien hallinta organisaatiossa

Tietojärjestelmätieteen
kanditutkielma

Laatija:
Kerttu Kettunen

Ohjaaja:
KTT Jonna Järveläinen

8.12.2023
Turku

Kanditutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Kerttu Kettunen
Otsikko: Käyttäjiin kohdistuvien kyberturvariskien hallinta organisaatiossa
Ohjaaja: KTT Jonna Järveläinen
Sivumäärä: 35 sivua
Päivämäärä: 8.12.2023

Ihmisiin kohdistuvat niin sanotut sosiaaliset manipulointihyökkäykset, kuten tietojenkalastelu, ovat kasvava uhka organisaatioille ja niiden toiminnalle. Hyökkäyksen tavoitteena on saada kohde antamaan luottamuksellista tietoa tietämättään hyökkääjälle. Tietojenkalastelu on skaalautuva huijaus, jossa käytetään joksikin muuksi tekeytymistä hyödyksi saadakseen tietoa kohteelta. Tietojenkalastelu voi olla yksilöimätöntä ja tiettyihin yksilöihin tai ryhmiin kohdennettua. Tietojenkalastelua voidaan toteuttaa muun muassa sähköpostin, tekstiviestin ja puhelun välityksellä. Hyökkäys kohdistetaan ihmiseen, koska he saattavat tehdä inhimillisiä virheitä riskien tunnistamisessa. On siis tärkeää, että organisaation työntekijät koulutetaan varautumaan uhkiin ja reagoimaan niihin oikein.

Kun tietojenkalasteluhyökkäykset yleistyvät, on syytä pohtia sitä, miten riskejä voidaan hallita. On tärkeää, että käyttäjät koulutetaan puolustautumaan tietojenkalastelua vastaan, jotta he ovat tietoisia uhista ja valppaita niiden varalta. Koulutus on hyödyllistä sekä turvallisuustaitojen opettamisen että turvallisuuden tarpeen motivoimisen kannalta. Käyttäjien tulisi päästä harjoittelemaan taitoja käytännössä oppijoille relevanttien tehtävien avulla ympäristössä ja kontekstissa, jossa oikeatkin tietojenkalasteluhyökkäykset organisaatiossa tapahtuvat.

Tutkielma käsittelee tietojenkalastelun eri muotoja ja keinoja niiltä puolustautumiseen organisaatiossa.

Avainsanat: tietojenkalastelu, kyberturvallisuuskoulutus, sosiaalinen manipulointi, riskien hallinta

SISÄLLYS

1 Johdanto 7

2 Käyttäjiin kohdistuvat hyökkäykset 8

2.1 Sosiaaliset manipulointihyökkäykset 8

2.2 Tietojenkalastelu 9

2.2.1 Tietojenkalastelu sähköpostitse 9

2.2.2 Kohdennettu tietojenkalastelu 12

2.2.3 Valaanpyynti 14

2.2.4 Tietojenkalastelu tekstiviestitse 15

2.2.5 Tietojenkalastelu puhelimitse 16

3 Käyttäjiin kohdistuvan tietojenkalastelun riskien hallinta 18

3.1 Käyttäjien koulutus 18

3.1.1 Koulutuksen periaatteet 18

3.1.2 Pelillistäminen 23

3.1.3 Koulutuksen pitkäkestoisuus 25

3.2 Käyttäjien tukemisen keinot 26

3.2.1 Tietojenkalasteluviestien suodattaminen 26

3.2.2 Ohjeistavat käyttöliittymät 26

4 Yhteenveto ja johtopäätökset 28

Lähteet 31

KUVIOT

Kuva 1 Tietojenkalastelun vaiheet (Aleroud & Zhou, 2017) 9

Kuva 2 Esimerkki tietojenkalastelusähköpostiviestistä (Wright ym., 2023) 11

Kuva 3 Esimerkki tietojenkalastelusähköpostiviestistä (Wright ym., 2023) 11

Kuva 4 Vahvistuskoodin edelleenlähetyshyökkäyksen tapahtumakulku (Jakobsson, 2018) 15

Kuva 5 Ehdotus lähestymistavasta tietojenkalastelukoulutukseen (Alnajim & Munro, 2009) 22

Kuva 6 Kuvakaappaus Anti-Phishing Phil -pelin tutoriaalista (Kumaraguru ym., 2010) 23

Kuva 7 Kuvakaappaus Anti-Phishing Phil -pelistä (Kumaraguru ym., 2010) 24

Kuva 8 Kuvakaappaus Anti-Phishing Phil -pelin yhteenvedosta (Kumaraguru ym., 2010) 24

TAULUKOT

Taulukko 1 Yhteenveto tietojenkalastelutavoista ja niiden peruspiirteistä 28

1 Johdanto

Erilaisten kyberhyökkäysten määrä on kasvanut merkittävästi viime vuosina. On tärkeää, että organisaatiossa pystytään reagoimaan muuttuneeseen globaaliin toimintaympäristöön riittävällä nopeudella. Erityisesti ihmisiin kohdistuvat niin sanotut sosiaaliset manipulointihyökkäykset (engl. social engineering), kuten tietojenkalastelu (engl. phishing), ovat nopeasti kasvava uhka yrityksille ja niiden toiminnalle (Shahbaznezhad ym., 2020).

Keinoja kyberhyökkäyksiä vastaan puolustautumiseen on sekä teknologisia että sosiaalisia. Tämä tutkielma keskittyy sosiaalisiin keinoihin yrityksen tai organisaation näkökulmasta. Esimerkiksi työntekijöiden, eli käyttäjien, kouluttaminen haitallisten viestien ja verkkosivujen tunnistamiseen on yksi mahdollinen keino (Nguyen ym., 2023).

Yritys, jossa otetaan kyberriskit huomioon ja pyritään luomaan hyvä turvallisuuskulttuuri (engl. security culture), on vastustuskykyisempi kyberuhkia vastaan. Tällaisessa yrityksessä jokainen toimija on tietoinen oleellisista turvallisuusriskeistä ja niitä ennaltaehkäisevistä toimenpiteistä. On myös tärkeää, että jokainen kantaa vastuuta toiminnastaan ja pyrkii ylläpitämään organisaation turvallisuutta. (Georgiadou ym., 2022.)

Tutkielman tutkimuskysymykset ovat seuraavat:

1. Mitä käyttäjiin kohdistuvia tietojenkalastelutapoja on?
2. Miten käyttäjiin kohdistuvan tietojenkalastelun riskejä pystytään hallitsemaan?

Tutkielma on rajattu käsittelemään organisaatiossa toimiviin käyttäjiin kohdistuvia riskejä ja niiden hallintaa. Käyttäjiin kohdistuvista sosiaalisista manipulointihyökkäyksistä keskitytään käsittelemään tietojenkalastelun eri muotoja. Kyberturvallisuus ja erityisesti sen sosiaalinen näkökulma ovat ajankohtainen aihe. Ihmiset voivat tehdä inhimillisiä virheitä ja toimia yllättävästi. Siksi kyberhyökkäykset kohdistetaan ihmisiin ja tietojenkalastelu on niin tehokasta. Miten uhkia pystytään hallitsemaan ja varmistamaan, että uhkiin osataan varautua? Hyökkäyksiin reagoiminen oikein on tärkeää organisaatiolle.

2 Käyttäjiin kohdistuvat hyökkäykset

2.1 Sosiaaliset manipulointihyökkäykset

Organisaatioiden toimintaympäristö on muuttunut. Organisaation toiminnan joustavuuteen, kuten sisäiseen kommunikointiin ja siihen, missä töitä voi tehdä, on panostettu. Monet tekevät etätöitä, käyttävät omia laitteita ja kommunikoivat vain vähän kasvokkain muiden organisaation jäsenten kanssa. Muihin työntekijöihin luotetaan, vaikka vuorovaikutus tapahtuisi vain esimerkiksi sähköpostin välityksellä. Muuttuneen toimintaympäristön takia myös muuttuneisiin uhkiin täytyy varautua. (Krombholz ym., 2015.)

Viestintäjärjestelmät ja niiden käyttäjät ovat alttiita erilaisille käyttäjään kohdistuville sosiaalisille manipulointihyökkäyksille. Hyökkäyksen tavoitteena on huijata ja manipuloida kohdetta antamaan luottamuksellista tietoa, kuten salasanoja tai henkilötietoja, tietämättään ulkopuoliselle taholle. Sosiaaliset manipulointihyökkäykset ovat yksi isoimmista kyberturvauhista, koska ne pyrkivät hyödyntämään käyttäjän heikkouksia. (Salahdine & Kaabouch, 2019.)

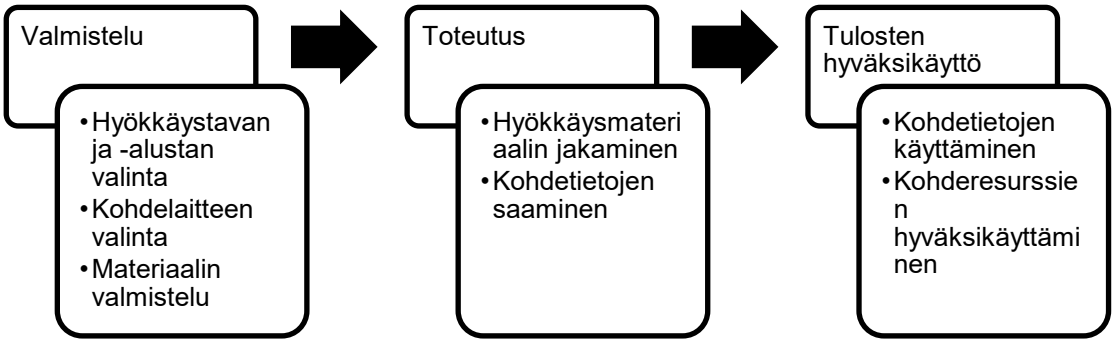
Sosiaaliset manipulointihyökkäykset pystyvät uhkaamaan kaikkia järjestelmiä, joihin ihmisillä on pääsy. Hyökkäyksessä käytetään sosiaalisia manipulointitaktiikoita, kun tietojärjestelmään ei ole mahdollista hakkeroitua muuten. On tärkeää, että käyttäjä on koulutettu tunnistamaan uhkia ja puolustautumaan niitä vastaan. (Salahdine & Kaabouch, 2019.)

Hyökkääjän tavoittelema tieto voi liittyä maksukortteihin, vakuutuksiin, henkilötietoihin tai muihin vastaaviin tietoihin, joita hyökkääjä voi käyttää hyväkseen. Organisaatioon kohdistuvassa hyökkäyksessä näitä tietoja ovat esimerkiksi käyttäjätunnukset ja salasanat, joilla pääsee organisaation tietojärjestelmiin käsiksi. (Salahdine & Kaabouch, 2019.)

Sosiaalisia manipulointihyökkäyksiä on erilaisia. Yksi esimerkki niistä on tietojenkalastelu (engl. phishing), johon tässä tutkielmassa keskitytään. Tietojenkalastelu yhdistää teknistä ja sosiaalista lähestymistapaa (Krombholz ym., 2015).

2.2 Tietojenkalastelu

Tietojenkalastelulle on erilaisia määritelmiä. Tässä tutkielmassa käytetään Lastdragerin (2014) määritelmää: ”Tietojenkalastelu on skaalautuva huijaus, jossa käytetään joksikin muuksi tekeytymistä hyödyksi saadakseen tietoa kohteelta”. Skaalautuvuudella tarkoitetaan sitä, että kanava, jolla huijaus toteutetaan, tukee massajakelua. Hyökkäys voi olla soitto, tekstiviesti tai sähköposti, jotka voivat viedä hyökkäyksen kohteen esimerkiksi väärennetylle nettisivulle (Salahdine & Kaabouch, 2019).



Kuva 1 Tietojenkalastelun vaiheet (Aleroud & Zhou, 2017)

Aleroudin ja Zhoun (2017) mukaan tietojenkalasteluhyökkäys koostuu kolmesta vaiheesta: valmistelusta, toteuttamisesta ja tulosten hyväksikäytöstä. Kuva 1 kuvaa näitä kolmea vaihetta. Valmisteluvaiheessa hyökkääjä valitsee hyökkäystavan ja -alustan sekä kohdelaitteen. Hän myös valmistelee hyökkäysmateriaalin. Toteutusvaiheessa hyökkääjä laittaa hyökkäysmateriaalin jakoon ja kerää huijatun uhrin tiedot. Hyökkääjä voi myös käyttää saatuja tietoja lisätiedon hankkimiseksi. Tulosten hyväksikäyttövaiheessa hyökkääjä käyttää saatuja tietoja hyväkseen päästäkseen käsiksi kohderesursseihin. (Aleroud & Zhou, 2017.)

Tietojenkalastelun tavoitteena on saada yksityistä tai luottamuksellista tietoa hyökkäyksen kohteelta vilpillisesti (Chiew ym., 2018). Tietojenkalastelu voidaan jakaa ryhmiin kohteen ja hyökkäyskanavan perusteella (Salahdine & Kaabouch, 2019).

2.2.1 Tietojenkalastelu sähköpostitse

Sähköpostin välityksellä tapahtuva tietojenkalastelu on yksi yleisimmistä tietojenkalastelutavoista. Se on laajalle levittäytynyt ongelma, joka voi aiheuttaa sekä henkilökohtaista kärsimystä että organisaatiollisia haasteita (Wright ym., 2023). Hyökkääjä lähettää väärennetyn sähköpostin huijatakseen kohdetta jakamaan

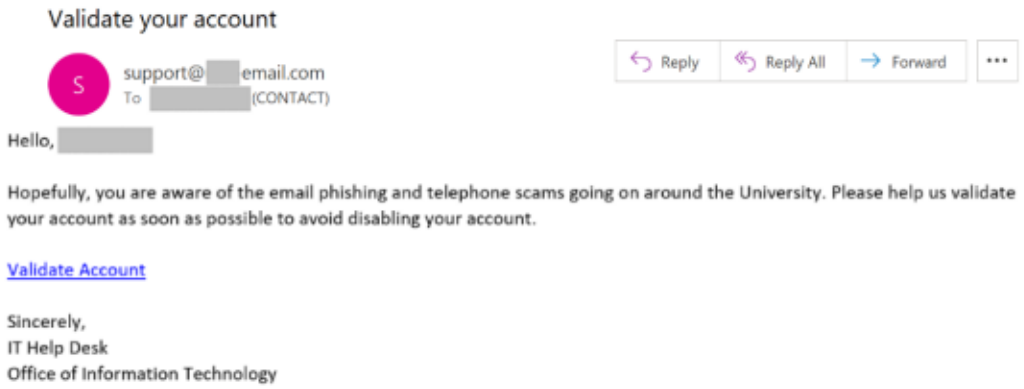
luottamuksellista tietoa tai asentamaan haittaohjelmia laitteelleen (Hong, 2012). Vaikka kyberturvallisuuteen panostetaan organisaatioissa ja siihen kiinnitetään yhä enemmän huomiota, tietojenkalasteluhyökkäyksille ollaan yhä haavoittuvaisia (Wright ym., 2023). Useimmat teknologiset keinot tietojenkalastelun estämiseksi ovat pitkälti tehottomia, joten käyttäjän vastuulle jää suuri osa vastuusta tunnistaa tietojenkalasteluhyökkäykset (Wright & Marett, 2010). Tietojenkalasteluhyökkäysten tunnistaminen on tärkeää niiltä puolustautuessa.

Usein ihmiset käyvät läpi heille tulleita sähköpostiviestejä nopeasti ja rutiininomaisesti eivätkä välttämättä tästä syystä havaitse niissä huijauksen merkkejä (Luo ym., 2013). Hyökkääjät käyttävät hyväksi käyttäjien rajallista tietoa tai tietoisuutta kyberturvallisuudesta saadakseen heiltä tietoa (Aleroud & Zhou, 2017). Usein tietojenkalastelusähköposti yrittää saada käyttäjän vierailemaan huijausverkkosivulla, joka vaikuttaa luotettavalta taholta (Hong, 2012).

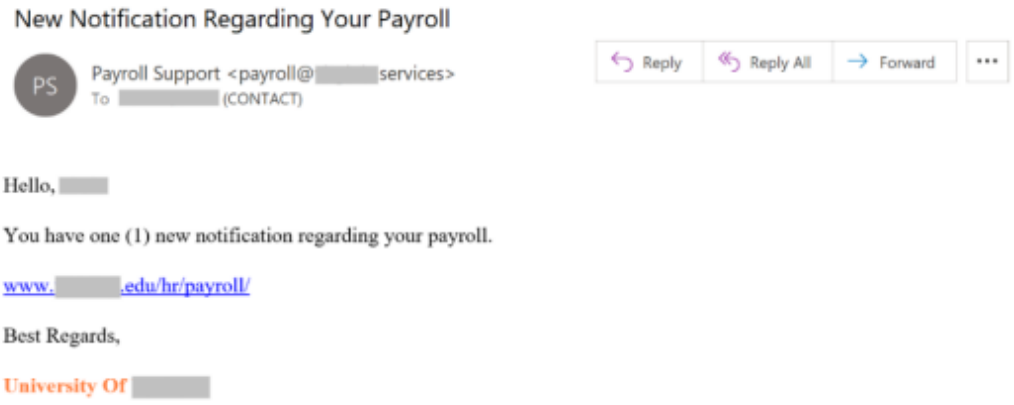
Sosiaalinen manipulointi keskittyy ihmisten väliseen vuorovaikutukseen ja käyttää usein hyväkseen psykologisia keinoja saadakseen uhrin toimimaan halutulla tavalla (Aleroud & Zhou, 2017). Suurin osa tietojenkalastelusähköposteista käyttää hyväksi sosiaalisia keinoja ennemmin kuin teknologisia keinoja huijatakseen käyttäjää. Hyökkääjä voi yrittää saada käyttäjälle kiireen tunteen tai tarjota jotain, mitä käyttäjä haluaa. (Hong, 2012.) Tietojenkalasteluhyökkäys onnistuu, kun sähköpostin luotettavuuden tunnistamisessa tehdään virhe (Wright ym., 2023). Huolellisesti rakennetun tietojenkalasteluviestin avulla hyökkääjä pyrkii herättämään vastaanottajassa tunteita, jotka saavat vastaanottajan toimimaan hyökkääjän ohjeiden mukaisesti (Goel ym., 2017). Tietojenkalasteluhyökkäykset on suunniteltu käyttämään hyväksi vastaanottajan kognitiivisia harhoja (Luo ym., 2013). Viestit, jotka kohdistuvat käyttäjän ongelmiin tai huoliin ja jotka ovat relevantteja käyttäjälle, onnistuvat parhaiten. Tällaiset viestit vaikuttavat vastaanottajan tunteisiin. (Goel ym., 2017.) Esimerkiksi jos tietojenkalastelija haluaisi opiskelijalta hänen yliopistotunnuksensa, hän voisi suunnitella kiireellisen viestin, joka liittyy kurssi-ilmoittautumisiin tai lukukausimaksuihin. Sähköpostiviestissä oleva linkki voisi johdattaa huijauksen kohteena olevan opiskelijan huijausverkkosivustolle, joka näyttää samalta kuin yliopiston sisäänkirjautumissivu.

Kuvat 2 ja 3 ovat simuloituja esimerkkejä tietojenkalastelusähköpostiviesteistä, joita käytettiin Wrightin ym. (2023) toteuttamassa tutkimuksessa. Kuvan 2 sähköpostiviesti

kehottaa vastaanottajaa vahvistamaan yliopiston käyttäjätilin alla olevasta linkistä mahdollisimman nopeasti, koska yliopistolla on havaittu tietojenkalasteluyrityksiä ja muita huijauksia. Vastaanottajalle syntyy helposti viestistä kiireen ja pelon tunteita, koska hän ei todennäköisesti halua, että hänen yliopiston käyttäjätilinsä poistetaan käytöstä. Sähköposti vaikuttaa tulevan luotettavasta lähteestä IT-tuesta, mutta linkki vie todennäköisesti väärennetylle verkkosivulle, jonka avulla hyökkääjä saa uhrin käyttäjätilin tiedot. Kuva 3 on yksinkertainen viesti näennäisesti yliopiston palkanlaskennan tuesta. Viesti koskee sitä, että vastaanottajalla on yksi uusi ilmoitus palkanlaskentajärjestelmässä. Useimmat ihmiset todennäköisesti kokevat palkkaansa liittyvät asiat tärkeiksi, jolloin he haluavat tietää, mitä heille tullut ilmoitus koskee. Käyttäjän tarve suojella arvokkaita asioita ja mahdollisuus saada arvokkaita asioita saavat hänet alttiiksi tietojenkalasteluyrityksille (Goel ym., 2017).



Kuva 2 Esimerkki tietojenkalastelusähköpostiviestistä (Wright ym., 2023)



Kuva 3 Esimerkki tietojenkalastelusähköpostiviestistä (Wright ym., 2023)

Syksyllä 2023 liikenne- ja viestintävirasto Traficom varoitti tietomurrosta, jossa tietojenkalasteluyritykset levisivät organisaatiosta toiseen, kun yritysten työntekijöiden käyttäjätunnuksia ja salasanoja kalasteltiin sähköpostitse ja huijaussivustojen kautta.

Hyökkäys kohdistui Microsoft 365 -tileihin kymmenissä organisaatioissa ja eteni ketjuittain. (HS 27.10.2023.) Hyökkäys eteni siis niin, että kaapattuja tilejä käytettiin uusien tietojenkalasteluviestien lähettämiseen käyttäjätilin aiemmille kontakteille sekä yrityksen sisäisesti että muihin organisaatioihin (Yle 20.10.2023).

Traficomin (20.10.2023) kertoi tietoturvaloukkauksesta seuraavasti. Murretuilta käyttäjätileiltä lähetettiin tietojenkalasteluviestejä sähköpostitse käyttäjätilin aikaisemmille kontakteille. Hyökkääjä oli lisännyt linkin kalastelusivuille näihin viesteihin ja vastannut esimerkiksi aikaisemmin lähetettyihin oikeisiin sähköpostiviesteihin. Viesti oli väärennetty muistuttamaan yleistä turvapostiratkaisua. (Traficom 20.10.2023.) Hyökkääjän tavoitteena oli ollut saada hyökkäys levitettyä mahdollisimman laajalle ja uusiin uhreihin oli luotu luottamus käyttämällä heidän tuntemiaan henkilöitä viestien lähettäjänä.

Tietojenkalastelu on kohtuullisen edullista ja riskitöntä hyökkääjälle. Tietojenkalastelussa lähetetään massasähköposti suurelle määrälle vastaanottajia. Tätä viestiä voidaan kutsua myös syötiksi (engl. bait). Viesti näyttää ja vaikuttaa tulevan luotettavasta lähteestä. (Wright & Marett, 2010.) Proofpoint (2023) teki vuoden kestävän tutkimuksen, johon vastasi 7500 työskentelevää ihmistä 15 eri maasta ja 1050 IT-asiantuntijaa, jossa selvitettiin globaalia tietojenkalastelutilannetta. Vuoden aikana 30 miljoonaa tietojenkalasteluviestiä lähetettiin liittyen Microsoftiin. Muita organisaatioita, joiden brändiä käytettiin viesteissä, olivat Amazon, DocuSign ja Google. (Proofpoint, 2023.) Tuttujen brändien avulla tietojenkalastelijat pyrkivät saamaan kohteen luottamaan viestiin.

Viestissä on usein kehotus toimintaan tai pyyntö avunantoon, jossa vastaanottajalta pyydetään henkilökohtaisia tietoja, kuten käyttäjätunnus tai salasana. Syötissä on usein linkki luotettavalta vaikuttavalle verkkosivulle, jolle vastaanottajan pyydetään laittamaan tietonsa. Tätä verkkosivua voidaan kutsua myös koukuksi (engl. hook). (Wright & Marett, 2010.) Koukkuun tarttuvat käyttäjät joutuvat tietojenkalastelun uhriksi.

2.2.2 Kohdennettu tietojenkalastelu

Tietojenkalastelijat eivät aina lähetä vain massasähköposteja yksilöimättömille henkilöille. Tietojenkalastelu voi olla myös kohdennettua. Kohdennetuksi tietojenkalasteluksi (engl. spear-phishing) kutsutaan sitä, kun hyökkääjä lähettää

tietojenkalasteluviestejä yksilöidysti tietyille ihmisille. (Alkhalil ym., 2021.) Kohde ja hyökkäyksen konteksti on suunniteltu etukäteen, jolloin viesti on kohdennettu vastaanottajalleen (Bullee ym., 2017). Kohdennettu tietojenkalastelu kohdistetaan tiettyyn yksilöön tai pienempään ryhmään yksilöitä, kuten tietyn organisaation jäseniin tai tietyn verkkosivun käyttäjiin. Kohdennetussa tietojenkalastelussa saatetaan myös esiintyä kohteen organisaation sisäisenä vaikutusvaltaisena tahona. (Hanus ym., 2022.)

Kohdennettu tietojenkalastelu vaatii enemmän suunnittelua ja resursseja, kuten tietoa kohteesta. Tämä johtuu siitä, että kohdennettu tietojenkalastelu käyttää hyväkseen ennakkoon hankittua tietoa vaikuttaakseen uskottavammalta. (Burns ym., 2019.) Kun kohdennetun tietojenkalastelun kohde saa viestin, joka vaikuttaa olevan hänen tuntemaltaan henkilöltä tai taholta, hän näkee viestin luotettavana. Lisäksi hyökkääjä saattaa muokata lähetettävää viestiä niin, että se sisältää jotain henkilökohtaista tietoa vastaanottajasta. (Goel ym., 2017.) Muokkaus voi olla esimerkiksi vastaanottajan nimen mainitseminen viestissä. Kohdennettu tietojenkalastelu käyttää kohteelle relevanttia tietoa saadakseen kohteen luottamaan viestiin ja antamaan tietoa (Hanus ym., 2022). Kohdennettu tietojenkalastelu hyödyntää ihmisen taipumusta luottaa tuntemiinsa ihmisiin (Parmar, 2012). Kohdennetusta tietojenkalasteluhyökkäyksestä tekee helpompaa se, jos kohteesta löytyy tietoa internetistä. Monilla on sosiaalisessa mediassa, kuten LinkedInissä, Facebookissa tai Instagramissa, paljonkin tietoa itsestään (Parmar, 2012). Kohteesta löytyvien tietojen avulla hyökkääjän on helppo kohdentaa ja muokata hyökkäysviesti uskottavammaksi.

Kohdennettu tietojenkalastelu on muutamasta syystä houkuttelevampaa kuin perinteinen tietojenkalastelu. Kohdennettu tietojenkalastelu on vaikeampaa havaita (Burns ym., 2019), joten siltä on vaikeampaa puolustautua. Koska tietojenkalasteluviestejä lähetetään vähemmän, on epätodennäköisempää, että hyökkääjälle aiheutuu viesteistä haittaa (Bullee ym., 2017). Vaikka kohdennettu tietojenkalasteluhyökkäys on monimutkaisempi ja hitaampi valmistella, onnistuessaan sen tuoma hyöty on suurempi kuin ei-kohdennetussa tietojenkalasteluhyökkäyksessä (Parmar, 2012). Lisäksi se, että kohdennettu tietojenkalasteluviesti on uskottavampi kohteen mielestä, lisää onnistumisen mahdollisuutta (Bullee ym., 2017). Kohdennetulla tietojenkalastelulla on pienempi mahdollisuus onnistua, mutta suuremmat hyödyt onnistuessaan (Burns ym., 2019).

2.2.3 Valaanpyynti

Jos kohdennettu tietojenkalastelu on vieläkin kohdennetumpaa, sitä kutsutaan valaanpyynniksi (engl. whale phishing, whaling) (Alkhalil ym., 2021). Valaanpyynti kohdistuu johtavassa asemassa oleviin henkilöihin organisaatiossa (Hanus ym., 2022). Tällaisia henkilöitä voivat olla esimerkiksi toimitus- tai talousjohtajat (Alkhalil ym., 2021).

Valaanpyynti on monimutkainen ja edistynyt huijaus, joka vaatii hyökkääjältä kärsivällisyyttä, tarkkuutta ja suunnittelua onnistuakseen. Onnistuneen hyökkäyksen vaikutukset ovat usein vakavia kohteelle ja hänen organisaatiolleen. Hyökkäys on monivaiheinen ja pitkä prosessi, joka on riippuvainen täsmällisestä ajoituksesta ja tarkasta koordinoinnista. Hyökkäykseen liittyy usein tiedustelua esimerkiksi sosiaalisen median kautta sekä kohteesta että hänen läheisistään. (Pienta ym., 2020.)

Valaanpyynti eroaa perinteisestä ja kohdennetusta tietojenkalastelusta muutamalla tavalla. Ensinnäkin valaanpyynti keskittyy tiettyyn kohteeseen useamman yksilön tai laajan populaation sijaan. Lisäksi hyökkääjät näkevät enemmän vaivaa valaanpyyntiin keräämällä ja analysoimalla tietoa useista lähteistä parantaakseen hyökkäyksen tehokkuutta. Valaanpyynnissä hyökkääjän tavoitteena on usein rahan ansaitseminen tai haitan aiheuttaminen kohteelle. Myös hyökkääjän ansaitsema hyöty on yleensä suurempi valaanpyynnissä. (Pienta ym., 2020.)

Yksi esimerkki valaanpyynnistä on Mattelilla vuonna 2015 tapahtunut tietojenkalasteluhyökkäys. Hyökkääjät olivat saaneet pääsyn Mattelin järjestelmiin jo aikaisemmin ja saaneet tietoa yrityksen sisäisistä asioista, kuten työntekijöiden tavoista, protokollista, sisäisestä hierarkiasta ja toimittajien tiedoista. He olivat keränneet tietoa ja tutustuneet kohteeseensa hyvin jo etukäteen. (Pienta ym., 2020.)

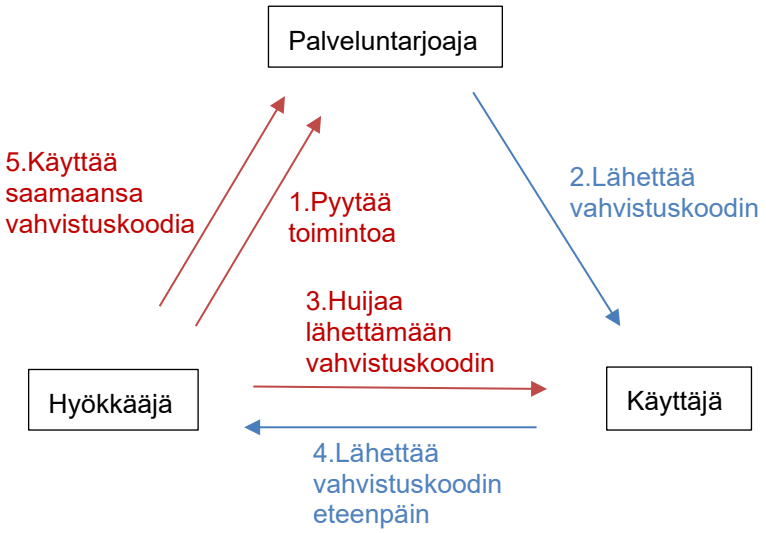
Kun Mattel nimesi tammikuussa 2015 uuden toimitusjohtajan, hyökkääjät päättivät käynnistää hyökkäyksen. Toimitusjohtajan vaihtumiseen liittyi Mattelilla epävarmuutta muutoksesta. Hyökkääjät lähettivät uuden toimitusjohtajan käyttäjältä korkean tason työntekijälle sähköpostin, jossa pyydettiin lähettämään 3 miljoonaa Yhdysvaltain dollaria pankkiin Wenzhouhun Kiinaan. Pyyntö oli nimetty maksuksi kiinalaiselle lelutoimittajalle. Lisäksi pyyntö oli merkitty myöhästyneeksi, eli kuin eräpäivä olisi jo mennyt. Mattel yleensä vaati isoihin maksuihin kahden ylemmän tason johtajan luvan ja

varmistuksen, mutta koska pyyntö vaikutti tulevan toimitusjohtajalta, työntekijä siirsi maksun. (Pienta ym., 2020.)

2.2.4 Tietojenkalastelu tekstiviestitse

Suurimmalla osalla ihmisistä on jonkinlainen puhelin, johon pystyy saada tekstiviestejä. Tekstiviestitse tapahtuvassa tietojenkalastelussa (engl. smishing, SMS phishing) hyökkääjä lähettää kohteelle tekstiviestin, joka sisältää esimerkiksi linkin haitalliselle verkkosivulle, jossa käyttäjää pyydetään antamaan tietoja kuten käyttäjätunnus, salasana tai maksukorttitietoja (Mishra & Soni, 2020). Hyökkääjä saattaa valita tehdä tietojenkalasteluhyökkäyksen tekstiviestitse esimerkiksi siitä syystä, että käyttäjä vastaa tekstiviestiin todennäköisemmin kuin sähköpostiin (Mishra & Soni, 2020). Tekstiviesti on myös kompaktin muotonsa ja muotoilun puutteen vuoksi helpompi väärentää (Jakobsson, 2018). Tekstiviestiä väärentäessä ei tarvitse esimerkiksi miettiä tekstin väriä tai fonttia.

Mobiililaitteiden käyttäjät ovat alttiimpia tekstiviestitse tapahtuville tietojenkalasteluhyökkäyksille muun muassa seuraavista syistä. URL-osoitteen oikeellisuus on vaikeampaa tarkistaa, koska mobiililaitteiden pienen näytön takia se ei näy kokonaan. (Mishra & Soni, 2020.) Lisäksi tekstiviestit toimivat sekä uusimmilla älypuhelimilla että vanhemmilla malleilla ja lähes kaikki käyttäjät osaavat käyttää niitä (Jakobsson, 2018). Kaikilla käyttäjillä ei ole kuitenkaan tietoa mobiililaitteisiin liittyvistä kyberturvariskeistä ja niiden hallinnasta (Mishra & Soni, 2020).



Kuva 4 Vahvistuskoodin edelleenlähetyshyökkäyksen tapahtumakulku (Jakobsson, 2018)

Yksi taktiikka, jota tietojenkalastelijat käyttävät tekstiviestitietojenkalastelussa, on vahvistuskoodin edelleenlähetyshyökkäys (engl. verification code forwarding attack), joka esitetään kuvassa 4. Siinä hyökkääjä pyytää ensin palveluntarjoajaa esimerkiksi resetoimaan käyttäjän salasanan. Pyynnön jälkeen hyökkääjä lähettää käyttäjälle tekstiviestin ja esiintyy palveluntarjoajana, joka pyytää käyttäjää lähettämään hänen juuri saamansa vahvistuskoodin vielä varmistuksena. Kun käyttäjä lähettää vahvistuskoodin, hyökkääjä lähettää sen palveluntarjoajalle ja pääsee käsiksi käyttäjän tietoihin. (Jakobsson, 2018.) Palveluntarjoaja ja käyttäjä luulevat siis keskustelevansa vain keskenään, eivätkä ole tietoisia kolmannesta osapuolesta, eli hyökkääjästä.

2.2.5 Tietojenkalastelu puhelimitse

Puhelinurkinta (engl. vishing, voice phishing) on puhelimitse tapahtuvaa systemaattista tietojenkalastelua. Hyökkäyksen tavoitteena on saada kohteelta luottamuksellista tietoa. (Maggi, 2010.) Puhelinurkinnassa hyökkääjän ja kohteen välillä on jatkuva suullinen vuorovaikutus (Jones ym., 2021), joten se eroaa hieman muista tekstin välityksellä tapahtuvista tietojenkalastelumuodoista.

Kun huijaus tapahtuu reaaliaikaisesti keskustelun muodossa, sosiaalisen manipuloinnin keinojen tehokkuus kasvaa merkittävästi (Maggi, 2010). Yksi esimerkki puhelinurkinnasta on puhelu hyökkääjältä, joka tekeytyy hyökkäyksen kohteena olevan henkilön pankin työntekijäksi. Hyökkääjä kertoo, että kohteen pankkitilillä on havaittu epäilyttävää toimintaa ja pyytää kohdetta vahvistamaan maksukorttitietonsa. Jos kohde toimii ohjeiden mukaisesti, hyökkääjä saa hänen tietonsa käyttöönsä. (Jones ym., 2021.)

Puhelinurkinnan onnistuminen vaatii siis sitä, että uhri toimii hyökkääjän ohjeiden mukaisesti. Koska ohjeet koostuvat usein useammasta eri vaiheesta, kohteella on enemmän mahdollisuuksia tajuta, että hän on tulossa huijatuksi. (Jones ym., 2021.) Myös IP-puheen (engl. voice over IP, VoIP) kehitys on tehnyt puhelintietojenkalastelusta suositumpaa. Puheluiden hinnat ovat laskeneet kehityksen myötä merkittävästi. Lisäksi IP-puheen kehitys on tehnyt hyökkäyksistä riskittömämpiä ja helpompia, koska hyökkääjiä on vaikeampi jäljittää ja he pystyvät tekeytymään muiksi tahoiksi helpommin. (Maggi, 2010.)

Jones ym. (2021) tutkivat puhelinurkinnassa käytettäviä sosiaalisen manipuloinnin suostuttelukeinoja. Tutkituista 86 hyökkäyksestä pyrittiin erottelemaan Ferreiran ym.

(2015) määrittelemiä suostuttelukeinoja, joita käytetään sosiaalisessa manipuloinnissa. Auktoriteettia (engl. authority) käytetään hyväksi, kun oletetaan ihmisen kunnioittavan auktoriteettia ja toimivan sen antamien ohjeiden mukaisesti. Sosiaalisen näytön (engl. social proof) avulla ihminen saadaan käyttäytymään lauman mukaisesti. Ihmisen tunne vastuusta alenee, kun samassa tilanteessa on muitakin, joihin kohdistuvat samat riskit. Häiriötekijöitä (engl. distraction) käytetään hyväksi, kun tiedostetaan, että ihminen kiinnittää huomiota itselleen tärkeisiin asioihin, eikä välttämättä huomaa, mitä muuta samaan aikaan tapahtuu. Miellyttävyys ja samankaltaisuus (engl. liking, similarity and deception) käyttää hyväksi sitä, että ihminen kuuntelee mieluiten henkilöä, josta hän pitää ja johon hän pystyy samaistua. (Ferreira ym., 2015.)

Jones ym. (2021) tutkimissa puhelinurkintahyökkäyksissä käytettiin näistä keinoista eniten auktoriteettia, sosiaalista näyttöä ja häiriötekijöitä. Näiden jälkeen suosituin keino oli miellyttävyys ja samankaltaisuus. (Jones ym., 2021.)

3 Käyttäjiin kohdistuvan tietojenkalastelun riskien hallinta

Tietojenkalasteluhyökkäysten yleistyessä on syytä arvioida, miten niitä vastaan pystytään puolustautumaan (Jansson & von Solms, 2013). Kun otetaan tietojenkalasteluhyökkäyksiin puolustautumiseen loppukäyttäjän näkökulma, vastatoimia on kolme (Hong, 2012). Nämä kolme tietojenkalastelun vastakeinoa ovat toisiaan täydentäviä (Kumaraguru ym., 2010). Ensimmäinen vaihtoehto on tehdä tietojenkalastelusta näkymätöntä loppukäyttäjälle, eli estää tietojenkalasteluviestien pääseminen hänelle kokonaan. Tämä voidaan toteuttaa esimerkiksi suodattamalla hyökkäysviestit tai estämällä tietojenkalasteluverkkosivujen käyttö. Toinen vaihtoehto on ottaa käyttöön käyttöliittymät, jotka varoittavat käyttäjää havaitessaan epäilyttävää toimintaa. Kolmas vaihtoehto on käyttäjien kouluttaminen. (Kumaraguru ym., 2010; Hong, 2012.) Tässä tutkielmassa keskitytään tutkimaan käyttäjien koulutusta.

Käyttäjien kouluttaminen voi olla vaikeaa toteuttaa, koska ihmisten motivointi on haastavaa, eikä onnistuessaankaan takaa kokonaista ratkaisua turvallisuusongelmaan (Hong, 2012). Se on kuitenkin tärkeä osa ratkaisua ja riskien hallintaa.

3.1 Käyttäjien koulutus

3.1.1 Koulutuksen periaatteet

Käyttäjät voidaan kouluttaa puolustautumaan itse aktiivisesti tietojenkalastelua vastaan (Kumaraguru ym., 2010). Vaikka käyttäjien kouluttaminen ei pelkästään ratkaise tietojenkalasteluun liittyvää turvallisuusriskiä, valppaat ja riskeistä tietoiset käyttäjät muodostavat tärkeän osan puolustuksesta (Alsharnouby ym., 2015). Koulutukset auttavat organisaatiota tekemään työntekijöistään tietoisempia parhaista kyberturvakäytännöistä (Abraham & Chengalur-Smith, 2019). Aiemmin mainitun Proofpointin (2023) tutkimuksen mukaan, johon osallistui 7500 työskentelevää ihmistä 15 eri maasta ja 1050 IT-asiantuntijaa, 98%:lla organisaatioista oli käytössä jonkinlainen koulutuskäytäntö. Kuitenkin vain 56% organisaatioista kouluttivat kaikki organisaation työntekijät. (Proofpoint, 2023.) Kouluttamisen tarkoitus on kasvattaa osallistujien tietämystä aiheesta, jotta he pystyvät käsittelemään aihetta koskevia tapahtumia vaaditulla tavalla (Sumner & Yuan, 2019). On tärkeää tehdä käyttäjät tietoiseksi mahdollisista uhista (Aleroud & Zhou, 2017).

Käyttäjien kouluttaminen voi kuitenkin olla haastavaa, koska monille turvallisuus on toisarvoinen tehtävä. Jos käyttäjät eivät ole motivoituneita oppimaan turvallisuudesta, he eivät halua käyttää aikaa tietojenkalasteluun tutustumiseen. (Kumaraguru ym., 2010.)

Käyttäjiä voidaan kouluttaa muun muassa pelien tai sulautetun koulutuksen (engl. embedded training) avulla. Sulautetun koulutuksen avulla käyttäjä oppii siinä ympäristössä ja kontekstissa, missä oikeatkin tietojenkalasteluhyökkäykset tapahtuvat. Jos käyttäjä epäonnistuu tietojenkalastelulta puolustautumisessa ja klikkaa simuloitua tietojenkalasteluviestiä, häntä muistutetaan tietojenkalastelusta ja sen uhista. (Hong, 2012.) Proofpointin (2023) tutkimuksessa yksi kymmenestä tietojenkalastelu-uhasta estettiin käyttäjän raportoinnin ansiosta. Silti 1/3 ihmisistä toimi riskialttiisti kohdatessaan hyökkäyksen, eli klikkasi linkkiä tai latasi haittaohjelman. (Proofpoint, 2023.) Turvallisuuskoulutukset ovat hyödyllisiä sekä turvallisuustaitojen opettamisen että turvallisuuden tarpeen motivoimisen kannalta (Kumaraguru ym., 2010). Ihmiset täytyy saada kiinnostuneeksi koulutuksesta, jotta he kiinnittävät huomiota ja ottavat tarjotun informaation vastaan (Zielinska ym., 2014).

Käyttäjät eivät välttämättä ole huolissaan kyberturvallisuudesta, jos he eivät tiedä uhriksi joutumisen seurauksista. He eivät ehkä usko olevansa alttiita uhriksi joutumiselle. Suurin osa ihmisistä uskoo, että he ovat tarpeeksi huolellisia eikä tietojenkalastelua voisi tapahtua heille. (Zielinska ym., 2014.)

Siihen, että käyttäjä tekee virheen viestin turvallisuuden tunnistamisessa, on muutamia: käyttäjä ei tiedä, mitä tietojenkalastelu on, käyttäjä ei osaa tunnistaa tietojenkalastelua tai käyttäjä ei epäile lähettäjää tietojenkalastelusta (Robila & Ragucci, 2006).

Kumaraguru ym. (2010) esittelivät opetuksen suunnittelussa huomioon otettavat periaatteet ja käyttivät niitä kehittäessään verkkopeliä tietojenkalastelulta puolustautumisen opetukseen. Periaatteiden mukaan koulutuksessa on tärkeää, että käyttäjät pääsevät harjoittelemaan taitoa käytännössä (engl. learning-by-doing), käyttäjille annetaan välitöntä palautetta (engl. immediate feedback), aiheita käsitellään sekä käsitteellisesti että proseduraalisesti (engl. conceptual-procedural), toisiaan lähellä olevat aiheet käsitellään yhdessä (engl. contiguity), asiat käsitellään käyttäjälle sopivalla kielellä (engl. personalization), koulutuksessa käytetään hyväksi tarinallisuutta (engl. story-based agent environment) ja käyttäjille annetaan mahdollisuus reflektoida oppimaansa (engl. reflection). (Kumaraguru ym., 2010.) Puhakaisen & Siposen (2010)

mukaan tietojärjestelmien turvallisuuskoulutusten tulisi käyttää tehtäviä, jotka ovat relevantteja oppijoille ja jotka mahdollistavat oppilaiden systemaattisen kognitiivisen tiedon prosessoinnin. Tämän lisäksi koulutuksen tulisi ottaa huomioon oppijan edellinen taitotaso. (Puhakainen & Siponen, 2010.)

Helpoiten estettävissä olevat kyberturvariskit ovat ne, jotka aiheutuvat käytäntöjen noudattamatta jättämisestä. Käytäntöjä asettamalla määritellään toimintatavat, joita organisaation sisäisten toimijoiden tulisi noudattaa, jotta turvallisuusriskit minimoitaisiin. Käytäntöjä voivat olla esimerkiksi se, mitä ohjelmia toimijat saavat käyttää, millaisia salasanakäytäntöjen tulisi olla, mitä oikeuksia erilaisilla käyttäjillä on ja miten organisaation kannettavia laitteita tulisi käyttää. (Piccoli ym., 2022.) Pelkkä käytäntöjen asettaminen ei kuitenkaan takaa, että käytäntöjä noudatetaan.

Organisaatiot ovat huolissaan siitä, että työntekijät jättävät kyberturvallisuuskäytäntöjä noudattamatta. Tällöin turvallisuusratkaisujen tehokkuus kärsii. Jotta käyttäjät saadaan motivoitua käyttäytymään tietojärjestelmien turvallisuuskäytäntöjen mukaan, koulutus täytyy integroida osaksi organisaation normaalia yritysviestintää. Myös ylimmän johdon tuki on tärkeää. (Puhakainen & Siponen, 2010.)

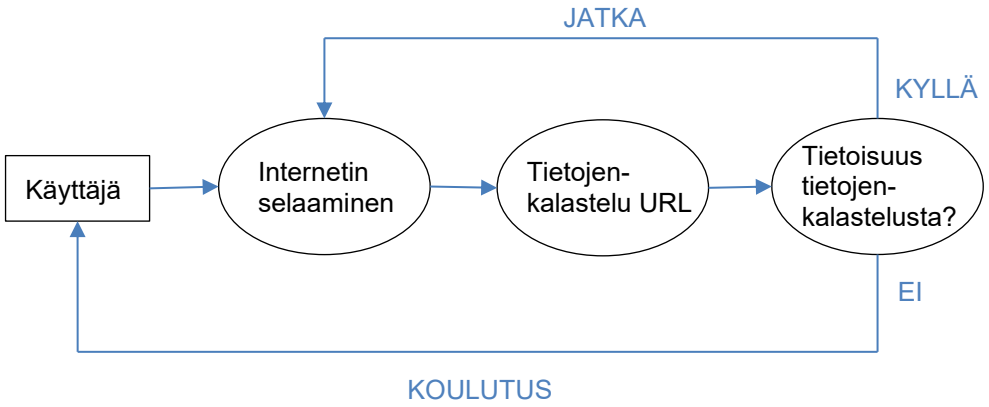
Käyttäjille täytyy opettaa, mitä tietojenkalastelu on, miten sen voi tunnistaa ja mitä täytyy tehdä, jos kohtaa tietojenkalastelua. Nguyen ym. (2023) esittelee kolme koulutuskeinoa, jotka ovat sääntöihin perustuva koulutus (engl. rule-based training), tietoisuustaitoihin perustuva koulutus (engl mindfulness training) ja ylioppiminen (engl. overlearning). (Nguyen ym., 2023.) Sääntöihin perustuva koulutus opettaa käyttäjän tunnistamaan tiettyjä tietojenkalastelun merkkejä tai asettaa käyttäjälle sääntöjä tietojenkalastelun välttämiseksi. Tietoisuustaitoihin perustuva koulutus opettaa käyttäjän kiinnittämään huomiota eri asioihin viestiä arvioidessa ja olemaan tietoisempi viestin kontekstista. (Jensen ym., 2017.) Ylioppimista käytetään avuksi tiedon muistamisessa, koska se vahvistaa opittuja käyttäytymistapoja ja siirtää taidon pitkäkestoiseen muistiin. Näin taito saadaan automatisoitua käyttäjän toimintatapoihin. (Nguyen ym., 2023.)

Sääntöihin perustuvan koulutuksen ongelma on muun muassa se, että tietojenkalasteluviestien oletetaan olevan suhteellisen samanlaisia pitkälläkin aikavälillä. Koulutus saattaa siis vanhentua, kun tietojenkalastelijat kehittävät viestejään. (Nguyen ym., 2023.) Myöskään koulutuksen toisto ei välttämättä kasvata organisaation vastustuskykyä (Jensen ym., 2017). Jensenin ym. (2017) tutkimuksessa ne, jotka saivat

tietoisuustaitoja hyödyntävän koulutuksen sääntöihin perustuvan koulutuksen lisäksi, onnistuivat puolustautumaan paremmin tietojenkalasteluhyökkäyksiltä. Ne, jotka ovat saaneet tietoisuustaitoihin perustuvan koulutuksen, erottavat paremmin tietojenkalasteluviestit turvallisista viesteistä ja ovat vähemmän alttiita hyökkäyksille (Nguyen ym., 2023).

Abraham & Chengalur-Smith (2019) tutkivat, miten oppijan hallinta (engl. learner control) vaikuttaa kyberturvakoulutusten tehokkuuteen. Oppijan hallinnoimassa opetuksessa oppijan täytyy tehdä itsenäisiä päätöksiä ja hän on vastuussa ohjeistettujen aktiviteettien läpi pääsemisestä (Williams, 1993). Abrahamin & Chengalur-Smithin mukaan oppijan hallinnalla koulutuksessa on positiivinen vaikutus tyytyväisyyteen, suoritukseen ja itseluottamukseen. Lisäksi oppijan hallintaa käytettäessä koulutuksen tiedot pysyivät paremmin oppijan muistissa. (Abraham & Chengalur-Smith, 2019.)

Yksi tapa varmistaa, onko käyttäjä tietoinen tietojenkalastelusta, on Alnajimin & Munron (2009) ehdottama lähestymistapa. Kuvassa 5 esitellään heidän ehdotuksensa. Käyttäjän koulutus on jatkuva prosessi, joka on upotettu käyttäjän normaaliin internetin käyttöön. Jos käyttäjä päätyy tietojenkalasteluverkkosivulle ja antaa sinne luottamuksellista tietoa, hänelle näytetään viesti, joka auttaa ymmärtämään, mitä tietojenkalasteluverkkosivut ovat ja miten ne voi tunnistaa. Jos käyttäjä ei anna luottamuksellista tietoa, hän saa jatkaa internetin selaamista, koska silloin oletetaan, että hän on tietoinen tietojenkalastelusta eikä siksi joutunut uhriksi. Järjestelmä tunnistaa tietojenkalasteluverkkosivut mustan listan avulla. Vaikka käyttäjä luovuttaisikin tietoja, ne eivät päädy hyökkääjien käsiin, koska järjestelmä on suunniteltu toimimaan välipalvelimen (engl. proxy) avulla, joka estää tietojen lähettämisen. (Alnajim & Munro, 2009.) Tapa kouluttaa käyttäjiä on siis turvallinen, mikäli musta lista on ajan tasalla, ja sen avulla käyttäjät pääsevät oppimaan kontekstissa, jossa he kohtaavat oikeitakin uhkia. Toisaalta tietojenkalastelu kehittyy nopeasti, jolloin musta lista myös vanhentuu nopeasti. Jos musta lista ei ole ajan tasalla, käyttäjän turvallisuus vaarantuu.



Kuva 5 Ehdotus lähestymistavasta tietojenkalastelukoulutukseen (Alnajim & Munro, 2009)

Jansson & von Solms (2013) tutkivat sitä, auttaako tietojenkalasteluhyökkäysten simuloiminen yhdistettynä koulutukseen vahvistamaan käyttäjien vastustuskykyä oikeita hyökkäyksiä vastaan. Työntekijöille lähetettiin simuloituja tietojenkalasteluviestejä. Jos työntekijä joutui viestin uhriksi, eli reagoi niihin, hänelle tuli varoitusikkuna, ilmoitus sähköpostiin ja mahdollisuus osallistua verkkokoulutukseen aiheesta. Simuloituja tietojenkalasteluviestejä oli muutamia erilaisia. Ne esimerkiksi pyysivät käyttäjää päivittämään tunnuksensa tietokannan kaatumisen vuoksi tai avaamaan viestiin liitetyn zip-tiedoston, joka auttaa poistamaan koneelle päässeen viruksen. Useimmat työntekijät, jotka reagoivat ensimmäisellä viikolla simuloituun viestiin, eivät reagoineet enää toisella viikolla. Ensimmäisellä viikolla 14,06% aktiivisista käyttäjistä reagoivat viestiin ja toisella viikolla 8,06%. Tietojenkalasteluhyökkäysten simulointi organisaatiossa johtaa Janssonin & von Solmsin (2013) mukaan käyttäjien parempaan valmiuteen tietojenkalasteluhyökkäysten varalta. Näin organisaation turvallisuus paranee, kun sen käyttäjät ovat valppaampia. Lisäksi koulutus saadaan simuloinnin avulla kohdistettua paremmin niihin käyttäjiin, jotka ovat alttiimpia tietojenkalastelulle. Koulutus kohdistetaan siis niihin, jotka reagoivat simuloituihin tietojenkalasteluviesteihin. Simuloidut tietojenkalasteluhyökkäykset voivat kuitenkin johtaa myös liialliseen varovaisuuteen. (Jansson & von Solms, 2013.)

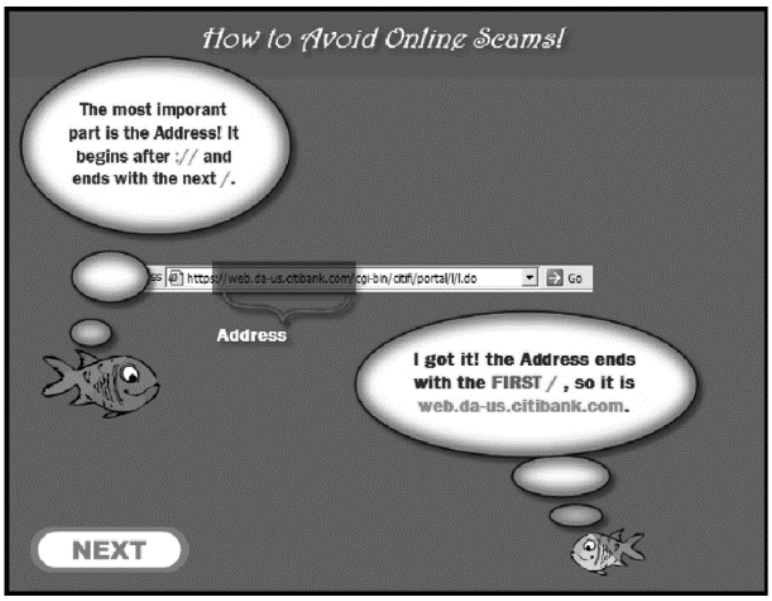
Vaikka hyökkäysten estämiseen käytetään usein myös teknisiä keinoja, loppukäyttäjän kouluttaminen on keskeistä tietojenkalasteluhyökkäysten vaikutuksen lieventämisessä (Robila & Ragucci, 2006).

3.1.2 Pelillistäminen

Kyberturvallisuuskoulutus, jossa hyödynnetään pelillistämisen periaatteita, voi olla ratkaisu koulutuksen tehokkuuden parantamiseen. Käyttäjät ovat motivoituneempia ja tunnollisempia, kun koulutus on immersiivinen ja miellyttävä kokemus. Sen avulla käyttäjää kannustetaan turvallisempaan käyttäytymiseen jotain tavoitetta tavoitellessa. (Silic & Lowry, 2020.)

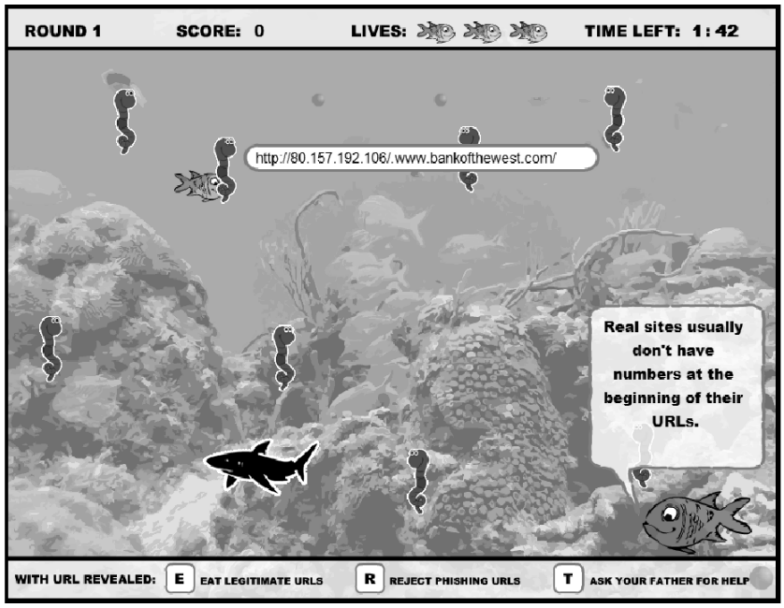
Kyberturvallisuutta voidaan opettaa pelien avulla, joista löytyy tietoa tietojenkalasteluhyökkäyksistä, niiden tekniikoista ja tavoista estää niitä. Pelit mahdollistavat päivittäiseen elämään upotetun tilanteen ja oppimiskokemuksen, jossa pelaaja ymmärtää säännöt, rajoitteet ja asiat, mitä kannattaa ja ei kannata tehdä. (Fatima ym., 2019.) Turvallisuuskoulutuksen pelillistämistä voidaan käyttää työntekijän motivaation vahvistamiseksi, jotta oppimista, tehokkuutta ja organisaation turvallisuusaloitteiden noudattamista saadaan kannustettua (Silic & Lowry, 2020).

Fatima ym. (2019) suunnittelivat pelipohjaisen ratkaisun opettaa käyttäjille tietojenkalasteluhyökkäyksistä. Pelissä pelaaja on hyökkääjän roolissa ja hän muun muassa pääsee valitsemaan kohteensa organisaatiossa, kerätä hänestä tietoa, kirjoittaa tietojenkalasteluviestin ja laittaa viestin pelissä jakeluun. Näin pelaaja oppii, miten tietojenkalastelu ja mitä heikkouksia kohteilla voi olla. (Fatima ym., 2019.)

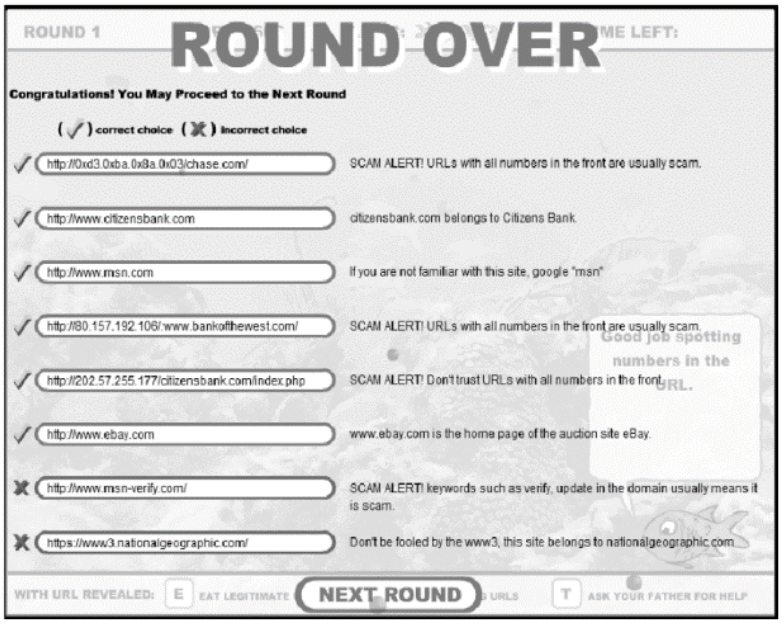


Kuva 6 Kuvakaappaus Anti-Phishing Phil -pelin tutoriaalista (Kumaraguru ym., 2010)

Kumaraguru ym. (2010) kehittivät verkkopelin, joka opettaa käyttäjille, miten URL-osoitteiden erilaisia vihjeitä voidaan käyttää avuksi tietojenkalasteluhyökkäysten tunnistamisessa. Kuvat 6, 7 ja 8 ovat kyseisestä pelistä otettuja kuvakaappauksia. Pelin nimi on Anti-Phishing Phil. Kuva 6 on kuva pelin tutoriaalista, joka näytetään ennen kierroksen alkua. Tutoriaalissa opetetaan käyttäjälle, miten verkkosivun turvallisuuden voi tunnistaa. Kuva 7 on kuva pelistä, jossa Phil ui matojen ohi. Alareunassa on vihjeitä antava toinen kala. Kuva 8 on yhteenveto, joka näytetään kierroksen jälkeen, josta käyttäjä näkee vielä vastauksensa ja pystyy oppimaan virheistään.



Kuva 7 Kuvakaappaus Anti-Phishing Phil -pelistä (Kumaraguru ym., 2010)



Kuva 8 Kuvakaappaus Anti-Phishing Phil -pelin yhteenvedosta (Kumaraguru ym., 2010)

Pelillistäminen voisi olla ratkaisu siihen, että työntekijät eivät näe koulutuksia tarpeeksi motivoivina ja mielenkiintoisina (Silic & Lowry, 2020).

3.1.3 Koulutuksen pitkäkestoisuus

Kun työntekijöitä koulutetaan, on tärkeää, että pyritään varmistamaan opittujen asioiden säilyminen muistissa (Sumner & Yuan, 2019). Sekä onnistuneiden tietojenkalasteluhyökkäysten vakavien seurausten että tietojenkalastelun vastaisen koulutuksen kulujen vuoksi on tärkeää, että koulutus sisältää myös tapaamisia, joissa ylläpidetään alkuperäisessä koulutuksessa opittuja tietoja ja taitoja (Nguyen ym., 2023).

Jatkuva harjoittelu ja välittömän palautteen antaminen heti alkuperäisen taidon oppimisen jälkeen vahvistaa taidon ja opitun käyttäytymismallin säilyvyyttä muistissa. Näin taidosta tulee rutiini ja se jää pitkäkestoiseen muistiin. (Nguyen ym., 2023.) Ylioppimiseksi kutsutaan tarkoituksellista tehtävän harjoittelemista, vaikka taito olisi jo opittu perustasolla. Ylioppimista harjoitellaan, kunnes tavoite saavutetaan. Tavoite voisi olla esimerkiksi se, ettei yhtään virhettä enää tapahdu tietojenkalastelun tunnistamisessa. (Driskell ym., 1992.) Oppimista ei siis lopeteta, kun taito on ensimmäisen kerran hallinnassa, vaan jatketaan toistojen ja harjoitusten tekemistä.

Työntekijöiden ylioppimista voidaan harjoittaa esimerkiksi lähettämällä heille simuloituja tietojenkalasteluviestejä. Kumaraguru ym. (2007) tutkivat upotetun koulutusjärjestelmän käyttöä, joka opettaa käyttäjää tietojenkalastelusta normaalin sähköpostin käyttämisen aikana. Käyttäjälle lähetetään ajoittain simuloituja tietojenkalasteluviestejä, joihin hänen täytyy reagoida oikein. Jos käyttäjä tulee huijatuksi, hän näkee välittömän palautteen siitä, mitä tapahtui ja mitä käyttäjä olisi voinut tehdä toisin. Kumaragurun ym. (2007) mukaan järjestelmä auttaa käyttäjiä oppimaan tehokkaammin. Järjestelmä keskittyy käyttäjän kouluttamiseen tietojenkalastelun riskeistä ja siihen, että käyttäjä opetetaan käytännönläheisesti tunnistamaan ja välttämään tietojenkalasteluviestejä. (Kumaraguru ym., 2007.)

Kuitenkin vastaavien järjestelmien käyttö on vielä harvinaista ja vain 35% Proofpointin (2023) aiemmin esiteltyyn tutkimukseen osallistuneista organisaatioista järjestivät työntekijöilleen tietojenkalastelusimulaatioita. Kumaragurun ym. (2007) mukaan heidän järjestelmänsä auttaa käyttäjiä oppimaan tehokkaammin ja siitä on hyötyä organisaation puolustautuessa tietojenkalastelulta.

3.2 Käyttäjien tukemisen keinot

Tietojenkalastelulta puolustautumisen voi jakaa erilaisiin lähestymistapoihin. Yksi niistä, eli käyttäjien kouluttamisen, on jo käsitelty tässä tutkielmassa. Muita tärkeitä lähestymistapoja on automatisoitu tietojenkalastelun tunnistus ja käyttäjää ohjeistavan käyttöliittymän käyttäminen, joka auttaa käyttäjää tunnistamaan uhkia (Alsharnouby ym., 2015). Nämä kaksi keinoa auttavat käyttäjää toimimaan turvallisesti.

Hyökkäysten havaitseminen on tapa vähentää sosiaalisia manipulointihyökkäyksiä. Se voi olla manuaalista tai automatisoitua. Käyttäjä saa työkaluja avuksi uhkien havaitsemiseen. Ne havaitsevat uhan tai hyökkäyksen ja joko estävät tapahtuman tai varoittavat käyttäjää siitä. (Sumner & Yuan, 2019.)

3.2.1 Tietojenkalasteluviestien suodattaminen

Automaattinen oikean ja väärennetyn verkkosivun vertailu on osoittautunut lupaavaksi tavaksi tunnistaa mahdolliset tietojenkalasteluyritykset, mutta se vaatii, että verkkosivuarkisto, johon verkkosivuja vertaillaan, on jatkuvasti ajan tasalla (Wenyin ym., 2006). On tärkeää, että käytössä on automatisoitu havaitsemisjärjestelmä, mutta järjestelmät toimivat harvoin täysin virheettömästi, joten on myös tärkeää, että käyttäjät koulutetaan havaitsemaan tietojenkalastelua ja että heillä on sitä tukevat käyttöjärjestelmät (Kumaraguru ym., 2010).

Tietojenkalasteluviestien suodattaminen ei vaadi käyttäjältä tietoisuutta riskeistä tai muita toimia. Jos kaikki tietojenkalasteluriskit pystyttäisiin estämään ennen käyttäjän tavoittamista, ei tarvitsisi olla olemassa muita riskien vähentämisen keinoja. (Kumaraguru ym., 2010.) Tämä ei kuitenkaan ole mahdollista, koska järjestelmäkin tekee virheitä, tästä syystä ratkaisun on hyvä olla monen tekijän summa.

3.2.2 Ohjeistavat käyttöliittymät

Yksi tapa auttaa käyttäjää uhkien tunnistamisessa on tarjota käyttöliittymä, joka auttaa tunnistamisessa ja varoittaa käyttäjää uhista. Käyttäjä ei kuitenkaan välttämättä toimi ohjeiden mukaisesti, jolloin varoituksista voi tulla tehottomia, jos ne eivät ole tarpeeksi yksinkertaisia ja helppoja ymmärtää. (Kumaraguru ym., 2010.)

Modernit verkkoselaimet antavat käyttäjälle työkaluja oikeiden turvallisuuspäätösten tekemiseen. Esimerkiksi osoitepalkissa olevat visuaaliset indikaattorit auttavat käyttäjää arvioimaan nettisivun turvallisuutta. (Alsharnouby ym., 2015.) Kolme visuaalista indikaattoria, joiden avulla käyttäjät voivat tunnistaa vierailemansa verkkosivuston turvallisuuden, ovat osoitepalkki, jossa on sivun URL-osoite, https-etuliite ja lukkokuvake, joka kertoo, onko yhteys suojattu (Herzberg & Margulies, 2011). Nämä indikaattorit ovat kuitenkin olleet vain osittain onnistuneita tietojenkalastelun estämisessä. Kun käyttäjä keskittyy siihen, mitä hän tekee nettisivulla, hän ei välttämättä huomaa turvallisuusindikaattoreita. (Alsharnouby ym., 2015.) Tutuissa tilanteissa ihminen toimii automaattisesti (Herzberg & Margulies, 2011).

Alnajim & Munro (2008) määrittivät epäilyttävällä sivustolla vierailevalle käyttäjälle ilmestyvän ohjeviestin (engl. tip) tehokkuutta. Viesti ilmestyy, kun havaitaan, että käyttäjä menee uhkaavalle sivustolle. Tutkimuksessa ohjeen kriteereinä olivat sen kyky estää tyypillisin tietojenkalastelun ominaisuus, eli vihje (engl. clue), sen luotettava toimiminen yksinään, sen väärentämättömyys ja se, ettei se tuota vääriä tuloksia. Tehokkain ohjeviesti oli ”väärennetyllä sivustolla voi olla tämä piirre: Verkkosivun osoite on erilainen, johon olet tottunut. Siinä voi olla ylimääräisiä merkkejä tai sanoja, tai sillä voi olla täysin eri nimi tai ei nimeä ollenkaan vain numeroita. Tarkista oikean sivun URL-osoite. Oikea URL-osoite näkyy sivun ominaisuuksissa.” Ohje täytti neljästä kriteeristä ensimmäiset kolme, mutta oli silti paras vertailluista ohjeista. (Alnajim & Munro, 2008.) Vaikka tietojenkalastelu on kehittynyt Alnajimin & Munron (2008) tutkimuksen jälkeen, se antaa yhä esimerkin hyvästä selaimen antamasta varoitusviestistä. Varoitusviestin tulisi olla kohdennettu vähiten taidokkaille käyttäjille ja viestistä tulisi tehdä mahdollisimman helposti ymmärrettävä poistamalla tarpeettoman monimutkaiset tekniset termit (Aneke ym., 2021). Ohjeistavat käyttöliittymät pyrkivät tukemaan käyttäjää tekemään turvallisia päätöksiä ja antamaan tietoa uhista käyttäjälle.

4 Yhteenveto ja johtopäätökset

Tietojenkalastelun tavoitteena on saada yksityistä tai luottamuksellista tietoa hyökkäyksen kohteelta vilpillisesti (Chiew ym., 2018). Hyökkäykset voivat kohdistua joko henkilöön tai organisaatioon, mutta tässä tutkielmassa keskityttiin etsimään ratkaisuja organisaatioon kohdistuviin hyökkäyksiin. Tutkielman tavoitteena oli käsittää, millaisia tietojenkalasteluun liittyviä uhkia organisaatioihin kohdistuu ja miten näitä riskejä pystytään hallitsemaan.

Ensimmäinen tutkimuskysymys oli: mitä käyttäjiin kohdistuvia tietojenkalastelutapoja on? Tutkitut tietojenkalastelutavat ja niiden peruspiirteet on listattu alla olevassa taulukossa 1. Kaikille tavoille yhteistä on se, että hyökkäys on skaalautuva huijaus, jossa pyritään saamaan tietoa kohteelta tekeytymällä joksikin muuksi henkilöksi tai tahoksi.

Taulukko 1 Yhteenveto tietojenkalastelutavoista ja niiden peruspiirteistä

Tietojenkalastelutapa	**Peruspiirteet**
Tietojenkalastelu sähköpostitse	Hyökkäys tapahtuu luotettavalta vaikuttavan sähköpostin välityksellä ja hyödyntää sosiaalisia keinoja, kuten kiireen tunteen luomista.
Kohdennettu tietojenkalastelu	Hyökkäys kohdistuu tiettyyn ihmiseen tai pienempään ryhmään, jotka ovat usein organisaatioissaan sellaisessa asemassa, että heillä on pääsy laajaan määrään tietoa. Tietojenkalasteluviesti on räätälöity vastaanottajalle.
Valaanpyynti	Hyökkäys on kohdennettua tietojenkalastelua, mutta kohdistuu korkeammassa asemassa oleviin henkilöihin organisaatiossa, kuten toimitus- tai talousjohtajiin.
Tietojenkalastelu tekstiviestitse	Hyökkäys kohdistuu mobiililaitteisiin ja tapahtuu tekstiviestin välityksellä. Tekstiviesti sisältää yleensä linkin, joka johtaa haitalliselle verkkosivulle.
Puhelinurkinta	Hyökkäys tapahtuu systemaattisesti puhelimitse, jossa kohde pyritään saamaan toimimaan usein monivaiheisten ohjeiden mukaisesti puhelun aikana.

Tietojenkalastelutapoihin tutustuessa kävi ilmi, että tiedon ja tietoisuuden puute altistaa käyttäjän tietojenkalastelulle. Tietojenkalasteluhyökkäys onnistuu, kun luotettavuuden tunnistamisessa tehdään virhe (Wright ym., 2023). Tietojenkalastelu on hyökkäyskeinona yleistynyt näiden lisäksi myös sosiaalisen median puolella, mutta sen uhat kohdistuvat

ennemmin yksilöön kuin organisaatioihin. Tästä syystä sosiaalisen median välityksellä tapahtuvaa tietojenkalastelua ei käsitelty tässä tutkielmassa. Tietojenkalastelu kuitenkin muuttuu ja kehittyy jatkuvasti, joten voi olla syytä kiinnittää huomiota myös sosiaalisen median kautta tapahtuvaan tietojenkalasteluun organisaation näkökulmasta.

Toinen tutkimuskysymys oli: miten käyttäjiin kohdistuvan tietojenkalastelun riskejä pystytään hallitsemaan? Vaihtoehdoista tutkittiin tarkemmin käyttäjien koulutusta. Valppaat ja tietoiset käyttäjät muodostavat tärkeän osan puolustuksesta (Alsharnouby ym., 2015) teknisten ratkaisujen lisäksi. Tekniset ratkaisut, kuten tulevien viestien estäminen ennen käyttäjälle pääsyä tai varoittavien käyttöliittymien, voivat toimia sekä sähköpostin että puhelimen, eli puheluiden tai tekstiviestin, välityksellä tulevia hyökkäyksiä vastaan, mikäli lähettäjä tunnistetaan epäilyttäväksi. On kuitenkin lisäksi tärkeää kouluttaa käyttäjät puolustautumaan itse aktiivisesti tietojenkalastelua vastaan (Kumaraguru ym., 2010), jos tekniset ratkaisut epäonnistuvat. Erityisesti ne käyttäjät, joihin voi kohdistua kohdennettua tietojenkalastelua tai valaanpyyntiä, on tärkeää kouluttaa perusteellisesti, koska näiden hyökkäysten vaikutukset ovat usein suuria. Koulutuksessa voidaan käyttää tiedon jakamisen lisäksi hyväksi esimerkiksi pelillistämistä tai sulautettua koulutusta. Koulutuksessa on myös tärkeää varmistaa, että käyttäjät säilyttävät opitut asiat muistissa (Sumner & Yuan, 2019). Taitoja on siis tärkeää harjoitella jatkuvasti ja käyttäjän on hyvä saada välitöntä palautetta toiminnastaan. Tämä vahvistaa asian säilyvyyttä muistissa. (Nguyen et al., 2023.)

Tutkielma antaa katsauksen tietojenkalasteluhyökkäysten eri muotoihin ja niiltä puolustautumisen keinoihin. Tietojenkalastelun eri muotojen käsittely antaa kattavan kuvauksen erilaisista tietojenkalasteluhyökkäysten muodoista, jotka voidaan toteuttaa eri alustoja käyttäen ja kohdentaa eri yksilöille tai ryhmille. Käyttäjien kouluttamisessa on tärkeää, että koulutus on jatkuvaa ja että sitä kehitetään uhkien kehittyessä. On myös tärkeää, että käyttäjä pääsee harjoittelemaan taitoja käytännössä, että asiat esitetään oppijalle helposti ymmärrettävällä tavalla ja että hän saa välitöntä palautetta toiminnastaan. Puolustautumisratkaisuissa tutkielma keskittyi käyttäjän kouluttamisen tarkasteluun, joten muita ratkaisuja voisi olla syytä tutkia tarkemmin. Myös erilaisiin koulutustapoihin voisi syventyä. Kuitenkin käyttäjien koulutus luo tärkeän pohjan kyberturvaratkaisuille, joten muut ratkaisut ovat sitä täydentäviä. Suurin osa käyttäjien koulutuksen keinoista keskittyy sähköpostitse ja verkkoselaimen kautta tapahtuvaan tietojenkalasteluun. Näitä keinoja, kuten sulautettua koulutusta ja hyökkäysten

simulointia, voisi pyrkiä hyödyntämään myös muita tietojenkalastelutapoja vastaan. Pystytäänkö näitä koulutuskeinoja käyttämään myös huijauspuheluilta tai -tekstiviesteiltä puolustautumisen opettamiseen? Esimerkiksi tekoälyn mahdollisuuksia huijauspuheluiden simuloimisessa organisaation sisällä voisi pohtia tarkemmin. Tämän tutkielman tietoja voidaan käyttää organisaatioissa kyberturvallisuusratkaisuvaihtoehtoja tarkastellessa ja pohtiessa.

Lähteet

Abraham, Sherly – Chengalur-Smith, Shobha (2019) Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, Vol. 87, 101586-. DOI: https://doi.org/10.1016/j.cose.2019.101586

Aleroud, Ahmed – Zhou, Lina (2017) Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, Vol. 68, 160–196. DOI: https://doi.org/10.1016/j.cose.2017.04.006

Alkhalil, Zainab – Hewage, Chaminda – Nawaf, Liqaa – Khan, Imtiaz (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, Vol. 3. DOI: https://doi.org/10.3389/fcomp.2021.563060

Alnajim, Abdullah – Munro, Malcolm (2008) An evaluation of users' tips effectiveness for Phishing websites detection. *2008 Third International Conference on Digital Information Management*, 63–68. IEEE. DOI: https://doi.org/10.1109/ICDIM.2008.4746717

Alnajim, Abdullah – Munro, Malcolm (2009) An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. *2009 Sixth International Conference on Information Technology: New Generations*, 405–410. IEEE. DOI: https://doi.org/10.1109/ITNG.2009.109

Alsharnouby, Mohamed – Alaca, Furkan – Chiasson, Sonia (2015) Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, Vol. 82, 69–82. DOI: https://doi.org/10.1016/j.ijhcs.2015.05.005

Aneke, Joseph – Ardito, Carmelo – Desolda, Giuseppe (2021) Help the User Recognize a Phishing Scam: Design of Explanation Messages in Warning Interfaces for Phishing Attacks. *HCI for Cybersecurity, Privacy and Trust*, 403–416. DOI: https://doi.org/10.1007/978-3-030-77392-2_26

Bullee, Jan-Willem – Montoya, Lorena – Junger, Marianne – Hartel, Pieter (2017) Spear phishing in organisations explained. *Information and Computer Security*, Vol. 25(5), 593–613. DOI: https://doi.org/10.1108/ICS-03-2017-0009

Burns, A. J. – Johnson, Eric – Caputo, Deanna (2019) Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, Vol. 29(1), 24–39. DOI: https://doi.org/10.1080/10919392.2019.1552745

Chiew, Kang Leng – Yong, Kelvin Sheng Chek – Tan, Choon Lin (2018) A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, Vol. 106, 1–20. DOI: https://doi.org/10.1016/j.eswa.2018.03.050

Driskell, James – Willis, Ruth – Copper, Carolyn (1992) Effect of overlearning on retention. *Journal of Applied Psychology*, Vol. 77(5), 615–622. DOI: https://doi.org/10.1037/0021-9010.77.5.615

Fatima, Rubia – Yasin, Affan – Liu, Lin – Wang, Jianmin (2019) How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, Vol. 27(6), 581–612. DOI: https://doi.org/10.3233/JCS-181253

Ferreira, Ana – Coventry, Lynne – Lenzini, Gabrilele (2015) Principles of Persuasion in Social Engineering and Their Use in Phishing. *Human Aspects of Information Security, Privacy, and Trust*, 36–47. DOI: https://doi.org/10.1007/978-3-319-20376-8_4

Georgiadou, Anna – Mouzakitis, Spiros – Bounas, Kanaris –Askounis, Dimitrios (2022) A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, Vol. 62(3), 452–462, DOI: https://doi.org/10.1080/08874417.2020.1845583

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

Hanus, Bartlomiej – Wu, Yu Andy – Parrish, James (2022) Phish Me, Phish Me Not. *The Journal of Computer Information Systems*, Vol. 62(3), 516–526. DOI: https://doi.org/10.1080/08874417.2020.1858730

Helsingin Sanomat 27.10.2023 Tietomurto jatkaa leviämistään yleisessä sähköpostiohjelmassa. <https://www.hs.fi/kotimaa/art-2000009952129.html>, haettu 8.11.2023

Herzberg, Amir – Margulies, Ronen (2011) Forcing Johnny to Login Safely: Long-Term User Study of Forcing and Training Login Mechanisms. *Computer Security – ESORICS 2011*, 452–471. DOI: https://doi.org/10.1007/978-3-642-23822-2_25

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

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

Jansson, K. – von Solms, R. (2013) Phishing for phishing awareness. *Behaviour & Information Technology*, Vol. 32(6), 584–593. DOI: https://doi.org/10.1080/0144929X.2011.632650

Jensen, Matthew – Dinger, Michael – Wright, Ryan – Thatcher, Jason Bennett (2017) Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, Vol. 34(2), 597–626. DOI: https://doi.org/10.1080/07421222.2017.1334499

Jones, Keith – Armstrong, Miriam – Tornblad, McKenna – Siami Namin, Akbar (2021) How social engineers use persuasion principles during vishing attacks. *Information and Computer Security*, Vol. 29(2), 314–331. DOI: https://doi.org/10.1108/ICS-07-2020-0113

Krombholz, Katharina – Hobel, Heidelinde – Huber, Markus – Weippl, Edgar (2015) Advanced social engineering attacks. *Journal of Information Security and Applications*, Vol 22, 113–122, DOI: https://doi.org/10.1016/j.jisa.2014.09.005

Kumaraguru, Ponnurangam – Rhee, Yong – Acquisti, Alessandro – Cranor, Lorrie – Hong, Jason – Nunge, Elizabeth (2007) Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 905–914. DOI: https://doi.org/10.1145/1240624.1240760

Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie – Hong, Jason (2010) Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, Vol. 10(2), 1–31. DOI : https://doi.org/10.1145/1754393.1754396

Lastdrager, Elmer (2014) Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature. *Crime Science*, Vol. 3(1), 1–. DOI: https://doi.org/10.1186/s40163-014-0009-y

Liu, Wenyin – Deng, Xiaotie – Huang, Guanglin – Fu, Anthony (2006) An antiphishing strategy based on visual similarity assessment. *IEEE Internet Computing*, Vol. 10(2), 58–65. DOI: https://doi.org/10.1109/MIC.2006.23

Luo, Xin Robert – Zhang, Wei – Burd, Stephen – Seazzu, Alessandro (2013) Investigating phishing victimization with the Heuristic–Systematic Model: A

theoretical framework and an exploration. *Computers & Security*, Vol. 38, 28–38. DOI: https://doi.org/10.1016/j.cose.2012.12.003

Maggi, Federio (2010) Are the Con Artists Back? A Preliminary Analysis of Modern Phone Frauds. *2010 10th IEEE International Conference on Computer and Information Technology*, 824–831. DOI: https://doi.org/10.1109/CIT.2010.156

Mishra, Sandhya – Soni, Devpriya (2020) Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, Vol. 108, 803–815. DOI: https://doi.org/10.1016/j.future.2020.03.021

Nguyen, Christopher – Jensen, Matthew – Day, Eric (2023) Learning not to take the bait: a longitudinal examination of digital training methods and overlearning on phishing susceptibility. *European Journal of Information Systems*, Vol. 32(2), 238–262, DOI: https://doi.org/10.1080/0960085X.2021.1931494

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

Piccoli, Gabriele – Pigni, Federico – Golup, Beth Lang (2022) Information systems for managers in the digital age : with cases (Edition 5.0.). Burlington, VT: Prospect Press.

Pienta, Daniel – Thatcher, Jason Bennett – Johnston, Allen (2020) Protecting a whale in a sea of phish. *Journal of Information Technology*, Vol. 35(3), 214–231. DOI: https://doi.org/10.1177/0268396220918594

Proofpoint (2023) State of the Phish <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2023.pdf>, haettu 10.11.2023

Puhakainen, Petri – Siponen, Mikko (2010) Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, Vol. 34(4), 757–778. DOI: https://doi.org/10.2307/25750704

Robila, Stefan – Ragucci, James (2006) Don't be a phish: steps in user education. *SIGCSE Bulletin*, Vol. 38(3), 237–241. DOI: https://doi.org/10.1145/1140123.1140187

Salahdine, Fatima – Kaabouch, Naima (2019) Social engineering attacks: A survey. *Future Internet*, Vol. 11(4), 89–, DOI: https://doi.org/10.3390/FI11040089

Shahbaznezhad, Hamidreza – Kolini, Farzan – Rashidirad, Mona (2021) Employees' Behavior in Phishing Attacks: What Individual, Organizational, and

Technological Factors Matter? *Journal of Computer Information Systems*, Vol. 61(6), 539–550, DOI: https://doi.org/10.1080/08874417.2020.1812134

Silic, Mario – Lowry, Paul Benjamin (2020) Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*, Vol. 37(1), 129–161. DOI: https://doi.org/10.1080/07421222.2019.1705512

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

Traficom 20.10.2023 Tietomurtoaalto leviää organisaatiosta toiseen – katkaise tietojenkalastelu. <https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoaalto-leviaa-organisaatiosta-toiseen-katkaise-tietojenkalastelu>, haettu 8.11.2023

Van der Merwe, Alta – Loock, Marianne – Dabrowski, Marek (2005) Characteristics and responsibilities involved in a phishing attack. *Proceedings of the 4th international symposium on Information and communication technologies*, 249-254.

Williams, Michael (1993) A Comprehensive Review of Learner-Control: The Role of Learner Characteristics.

Wright, Ryan – Johnson, Steven – Kitchens, Brent (2023) Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection. *MIS Quarterly*, Vol. 47(2), 803–832. DOI: https://doi.org/10.25300/MISQ/2022/16625

Wright, Ryan – Marett, Kent (2010) The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, Vol. 27(1), 273–303. DOI: https://doi.org/10.2753/MIS0742-1222270111

Yle 20.10.2023 Traficomilta vakava varoitus tietomurtoaalloista sähköpostitileillä – näin voit suojautua. <https://yle.fi/a/74-20056195>, haettu 8.11.2023

Zielinska, Olga – Tembe, Rucha – Hong, Kuyng Wha – Ge, Xi – Murphy-Hill, Emerson – Mayhorn, Christopher (2014) One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 58(1), 1466–1470. DOI: https://doi.org/10.1177/1541931214581306