Tampereen yliopisto

Oskari Päärni

TIETOJENKALASTELU OSANA KÄYTTÄJÄN MANIPULOINTIA

Tavat, tekniikat ja suojautuminen

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Toukokuu 2021

TIIVISTELMÄ

Oskari Päärni: Tietojenkalastelu osana käyttäjän manipulointia – Tavat, tekniikat ja suojautuminen
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Toukokuu 2021

Teknologian kehittyessä tietoteknisten tietoturvaratkaisujen kehittäjät käyvät kilpavarustelua hakkereita vastaan. Tietojärjestelmän tietoturvan heikoin lenkki on usein ihminen eli järjestelmän käyttäjä. Tämän vuoksi hyökkääjät hyödyntävät usein käyttäjän manipuloinnin menetelmiä kyberhyökkäystä toteuttaessaan. Yleisin näistä menetelmistä on *phishing* eli tietojenkalastelu, jota kohtaavat organisaatioiden lisäksi tavalliset kansalaiset. Tietojenkalastelu on yleistynyt jo pitkään, mutta koronaviruspandemia ja sen mukanaan tuoma etätyö ja -kommunikaatio on lisännyt sen riskiä entisestään. Tietojenkalastelun tunnistaminen, ennaltaehkäisy ja estäminen on siten tärkeämpää kuin koskaan.

Tämä tutkielma on aiempaan tutkimustyöhön pohjautuva kirjallisuuskatsaus, jonka tarkoituksena on selvittää, mitä käyttäjän manipulointi ja tietojenkalastelu ovat, mihin alaluokkiin tietojenkalastelu jakautuu, ja miten tietojenkalastelulta voi suojautua. Käyttäjän manipulointiin sisältyy tietojenkalastelun lisäksi monia muita tekniikoita, joita käytetään usein yhdessä tietojenkalastelun kanssa hyökkäyksen tavoitteiden saavuttamiseksi. Käyttäjän manipulointihyökkäys on monivaiheinen ja vaatii toteuttajaltaan kattavia esivalmisteluja onnistuakseen.

Kuten käyttäjän manipulointi, myös tietojenkalastelu jakautuu useisiin alaluokkiin, jotka määräytyvät muun muassa kohteen tai lähestymismedian perusteella. Tietojenkalastelun tunnistamiseen ja siltä suojautumiseen on olemassa sekä teknisiä että käyttäjälähtöisiä ratkaisuja. Yksi näistä on SEADMv2 (Social Engineering Attack Detection Model), jonka avulla pyritään tunnistamaan käyttäjän manipulointiyrityksiä.

Avainsanat: tietoturvallisuus, kyberturvallisuus, käyttäjän manipulointi, tietojenkalastelu

Sisällysluettelo

1 Johdanto

Jatkuvasti nopeutuva teknologinen kehitys on johtanut siihen, että tietotekniset laitteet ovat merkittävässä osassa monien ihmisten arkipäiväistä elämää. Tämä kehitys on johtanut uusien hyökkäysvektorien avautumiseen kyberhyökkäysten tekijöille. Proofpoint (2019) raportoi, että lähes kaikki kyberhyökkäykset tarvitsevat käyttäjän tekemän varmistuksen onnistuakseen. Vuonna 2020 tapahtuneista tietomurroista 23 % johtui käyttäjän virheestä ja 53 % haitallisista hyökkäyksistä (IBM 2020). Käyttäjän osa tietoturvallisuudessa on siis merkittävä. Vaikka organisaation tai henkilön tietoturva olisi siis teknisiltä toteutuksiltaan hyvällä tasolla, on hyökkääjien silti mahdollista hyökätä kaikista haavoittuvimpaan osaan järjestelmän tietoturvaa, eli käyttäjään.

Yksittäiselle ihmiselle onnistuneesta hyökkäyksestä aiheutuva rahallinen haitta ei mitä luultavimmin ole määrällisesti läheskään yhtä suuri kuin yritykselle, mutta vaikutus omaan taloudelliseen tilanteeseen voi kuitenkin olla merkittävä. Yle (2021) uutisoi, että Microsoft-yrityksen tukipalveluna esiintyvät tietojenkalastelijat veivät suomalaisilta 2,8 miljoonaa euroa vuoden 2020 aikana. Alkaneen vuoden 2021 aikana, eli alle kahdessa kuukaudessa, vastaavien huijausten kustannukset suomalaisille ovat nousseet yli miljoonaan euroon.

Hyökkääjillä on monia lähestymisvaihtoehtoja hyökkäystä suunnitellessaan. Näistä lähestymisvaihtoehdoista vaikein suojattava on ihmiselementti eli käyttäjät, koska heidän tarkka ja tehokas hallinnointi on käytännössä mahdotonta. Käyttäjän oikeuksien rajoittaminen on mahdollista, mutta liika rajoittaminen hankaloittaa käyttäjän toimintaa ja hidastaa laitteen käyttöä, joka johtaa työskentelytehokkuuden laskuun. Myös BYOD-kulttuuri (Bring Your Own Device) eli käyttäjien henkilökohtaisten laitteiden käyttäminen työtehtävissä vaikeuttaa turvallisen käyttöympäristön takaamista. Thompson (2013) kuvailee näitä työpaikan ulkopuolella käytettäviä laitteita osuvasti ikkunoiksi yrityksiin, viitaten niiden haavoittuvaisuuteen hallinnoimattomassa ympäristössä.

Käyttäjään kohdistuvissa hyökkäyksissä käytetään suurta kirjoa erilaisia tekniikoita, ja yksi yleisimmin tavattavista on *tietojenkalastelu* (phishing). Tästä syystä tutkielmassa käsitellään tarkemmin juuri tietojenkalastelua suuremman kokonaisuuden tai vaihtoehtoisen tekniikan sijaan. Aiemman tutkimuksen avulla pyritään selvittämään, mitä erilaisia tekniikoita ja menetelmiä tietojenkalastelussa käytetään, sekä mahdollisia puolustautumiskeinoja kyseisiä hyökkäyksiä vastaan. Tässä tutkielmassa tietojenkalastelua tarkastellaan pääasiassa yksittäisen käyttäjän näkökulmasta. Vaikka hyökkääjän tavoite olisikin päästä käsiksi yrityksen omaisuuteen, käyttäjän manipuloinnin uhreja ovat kuitenkin käyttäjät yksilöinä ja tällöin hyökkäysten torjunta on tehokkainta ja järkevintä toteuttaa yksilötasolla.

Tutkielman rakenne on seuraava: Luvussa kaksi käsitellään tutkimusmenetelmä, eli miten, miltä alustoilta ja millä kriteereillä lähdekirjallisuutta on haettu, luokiteltu ja sisällytetty tähän tutkielmaan. Kolmas luku käsittelee käyttäjän manipulointia yleisesti. Tämä johtuu siitä, että tietojenkalastelu on osa käyttäjän manipulointia ja termin määrittely ja avaaminen on tärkeää pohjustusta tietojenkalastelun käsittelylle. Luvussa neljä käydään läpi tietojenkalastelua yleisesti sekä avataan tietojenkalastelun alaluokkia, joille on omat vakiintuneet terminsä. Viides luku keskittyy erilaisiin keinoihin, joilla käyttäjä pystyy suojautumaan tietojenkalastelulta sekä teknisten toteutusten että käyttäjän oman toiminnan näkökulmasta. Luvussa kuusi tarkastellaan saatuja tuloksia ja luku seitsemän on yhteenveto koko tutkielmasta.

2 Tutkimusmenetelmä

Tämä kandidaatintutkielma on toteutettu kirjallisuuskatsauksena pohjautuen aiempaan tutkimukseen käyttäjän manipuloinnista ja tietojenkalastelusta. Kirjallisuuden etsintään käytettiin tietokantoina Tampereen yliopiston Andor-palvelua sekä Elsevier ScienceDirect-alustaa ja ACM (Association for Computing Machinery) Digital Library-alustaa. Mouton et al. (2014) artikkeli "Towards an ontological model defining the social engineering domain" haettiin SpringerLink-alustalta, koska sitä ei löytynyt muilta edeltä mainituilta alustoilta.

Alkuvaiheen hakuja tehdessä käytettiin avainsanoja "social engineering" ja "phishing" yhdessä "cyber security" -termin kanssa. Tämän jälkeen tarkasteltiin noin ensimmäistä 20 haun tuloksena saatua lähdettä tarkemmin, ja relevantit lähteet valittiin otsikon ja tiivistelmän perusteella.

Osa lähteistä löytyi ensimmäisten hakujen perusteella löydettyjen ja tarkemmin tarkasteltujen lähteiden omasta lähdekirjallisuudesta. Myös nämä lähteet haettiin yllä mainituista tietokannoista niiden otsikoita ja/tai kirjoittajien nimiä hyödyntäen. Etsinnän alkuvaiheessa tuloksia rajattiin julkaisuvuoden perusteella vuosiin 2010–2021, mutta edellä mainittuihin myöhemmin sisällytettyihin johdannaislähteisiin lukeutuu myös tälle aikavälille kuulumattomia teoksia.

Tutkielman lähteiksi valikoituneista artikkeleista merkittiin muistiin oleellisia löydöksiä ja huomioita tutkimusaiheeseen liittyen, jonka jälkeen ne luokiteltiin eri luokkiin aiheensa mukaan: Ensimmäiseen luokkaan laitettiin yleiseen käsitteenmäärittelyyn ja luokitteluun käytettävät lähteet. Toiseen luokkaan päätyivät artikkelit, jotka kuvasivat tietojenkalastelun eri osa-alueita ja tekniikoita. Kolmannessa luokassa ovat tietojenkalastelulta suojautumista käsittelevät lähteet. Lähteet asetettiin niille sopiviin kohtiin tutkielman rakenteessa tukemaan muuta sisältöä kyseisen luokittelun perusteella.

3 Käyttäjän manipulointi

Tämä luku käsittelee termiä *social engineering*. Kyseessä on laajempi, tietojärjestelmien ihmiselementtiä hyväksi käyttävät hyökkäykset kattava termi, jonka alle myös tietojenkalastelu lukeutuu. Kirjoitushetkellä social engineering -termistä käytettäviä suomennoksia ovat "käyttäjän manipulointi" tai "sosiaalinen manipulointi". Käytän tässä kandidaattitutkielmassa termeistä ensimmäistä eli "käyttäjän manipulointia".

Kuten Mouton et al. (2014) toteaa, käyttäjän manipuloinnille ei löydy yhtä tyhjentävää määritelmää, vaikka moni niistä muistuttaa toisiaan. Hadnagy (2018) määrittelee sen "minä tahansa tekona, joka saa toisen henkilön toimimaan tavalla, joka saattaa olla tai olla olematta hänen etujensa mukaista", kun taas Krombholz et al. (2014) määritelmä on tiiviimpi "henkilön manipulointia antamaan tietoa hyökkääjälle". Yksinkertaistettuna käyttäjän manipuloinnin voidaan todeta olevan kyberhyökkäystekniikka, jonka kohteena on nimenomaan tietojärjestelmän käyttäjä. Monissa reaalimaailman tilanteissa hyökkäykseen sisältyy sekä käyttäjän manipulointia että muita ratkaisuja. Esimerkkinä tästä voisi olla hyökkäys, jossa uhri vastaanottaa sähköpostiviestin, jolla onnistutaan manipuloimaan käyttäjä lataamaan laitteelleen haittaohjelma.

3.1 Kategorointi

Käyttäjän manipulointi voidaan jakaa osa-alueisiin useiden eri piirteiden perusteella. Näihin lukeutuvat muun muassa lähestymisväylä, tekniikka ja kommunikaatiotapa. Lähestymisväylällä tarkoitetaan mediaa tai formaattia, jota hyödyntämällä hyökkääjä on yhteydessä uhriinsa. Esimerkkejä tästä ovat puhelut, sähköposti- ja SMS-viestit sekä verkkosivut.

Tekniikka tarkoittaa tämän tutkielman kontekstissa käyttäjän manipuloinnin metodia, jolla hyökkääjä pyrkii tavoitteeseensa. Tässä tutkielmassa tarkemmin käsiteltävä tietojenkalastelu lukeutuu näihin tekniikoihin. Tietojenkalastelun lisäksi käyttäjän manipuloinnin tekniikoita ovat esimerkiksi *syötittäminen* (baiting), jossa hyökkääjä jättää haittaohjelmalla varustetun massamuistilaitteen odottamaan uhria, tai *juomapaikkahyökkäys* (waterholing), jossa hyökkääjät saastuttavat uhrille kiinnostavaksi oletetun verkkosivun haittaohjelmalla ja odottavat uhrin saapumista (Krombholz et al., 2014).

Kommunikaatiotavat jakautuvat *epäsuoraan kommunikaatioon* (indirect communication) ja *suoraan kommunikaatioon* (direct communication). Epäsuorassa kommunikaatiossa hyökkääjä ja uhri eivät käy suoraa keskustelua, vaan hyökkääjä esimerkiksi jättää massamuistilaitteen julkiselle paikalle uhrinsa löydettäväksi. Kuten epäsuora kommunikaatio, myös suora kommunikaatio toimii nimensä mukaisesti, eli hyökkääjä ja uhri ovat suorassa kommunikaatioyhteydessä keskenään. Suora kommunikaatio jakautuu edelleen *yksisuuntaiseen kommunikaatioon* (unidirectional communication) ja *kaksisuuntaiseen kommunikaatioon.* (bidirectional communication). Yksisuuntaisessa kommunikaatiossa

hyökkääjä on yhteydessä uhriin, mutta uhrilta ei joko odoteta vastausta tai hänelle ei anneta mahdollisuutta siihen. Yksisuuntaista kommunikaatiota käytetään esimerkiksi hyökkäyksessä, jossa uhrin auton tuulilasiin asetetaan "parkkisakko" pelkällä maksuohjeella ilman yhteystietoja. Kaksisuuntaisessa kommunikaatiossa puolestaan molemmat osapuolet ovat yhteydessä toisiinsa esimerkiksi sähköpostiviestien tai puhelimen välityksellä. (Mouton et al., 2014)

3.2 Hyökkäyksen kulku

Käyttäjän manipulointiin tähtäävä hyökkäys on monivaiheinen prosessi. Tämän prosessin kronologista etenemistä on pyrkinyt mallintamaan muun muassa Mitnick (2002), jonka malli on laajalti tunnettu. Mouton et al. (2014) on luonut oman mallinsa, joka pohjautuu Mitnickin malliin, mutta käsittelee hyökkäysprosessin eri vaiheita tarkemmin ja jakaa ne pienempiin osiin. Mallin suomenkielinen versio on nähtävissä kuvassa yksi.

Malli jakaa hyökkäyksen kuuteen eri vaiheeseen: *hyökkäyksen muotoilu*, *tiedonkeruu*, *valmistelu*, *suhteen luominen*, *suhteen hyväksikäyttö* ja *viimeistely*. Mikäli hyökkääjä onnistuu kaikissa kuudessa vaiheessa, päämäärä voidaan saavuttaa.

Hyökkäysprosessi alkaa hyökkäyksen muotoilusta. Tässä vaiheessa hyökkääjä tunnistaa ja päättää oman päämääränsä, joka voi olla esimerkiksi taloudellinen höyty tai arkaluontoisten tietojen hankkiminen uhrilta. Kun päämäärä on määritelty, hyökkääjä valitsee kohteekseen uhrin, jonka avulla kyseinen päämäärä on mahdollista saavuttaa.

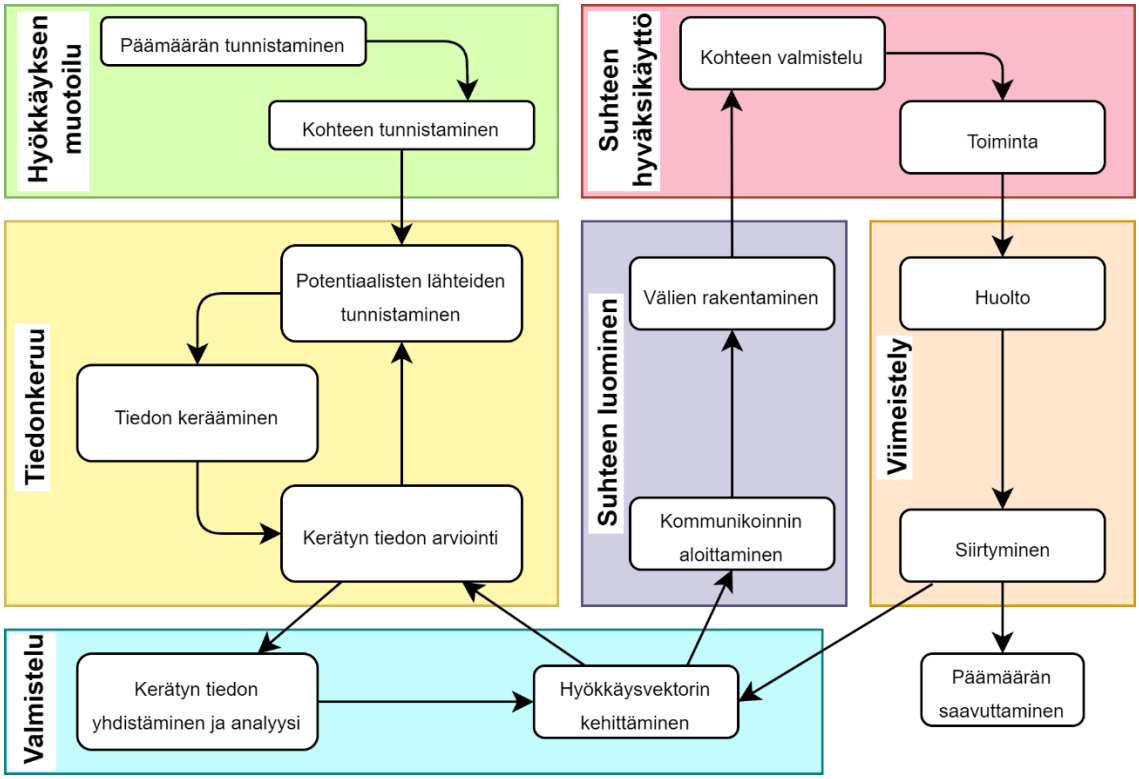
Hyökkäyksen muotoilun jälkeen hyökkääjä suorittaa tiedonkeruun. Hyökkääjä etsii siis tietoa uhristaan ja tämän lähipiiristä tai työtehtävistä, jotta hän pystyy vaikuttamaan uskottavalta uhrille, kun hyökkäys toteutetaan. Ensin hyökkääjä tunnistaa potentiaaliset tiedonlähteet, kuten sosiaalisen median alustat. Tämän jälkeen hän suorittaa varsinaisen tiedon keräämisen, jonka jälkeen kerätyn tiedon määrä ja laatu arvioidaan. Mikäli tietoa ei ole tarpeeksi, siirrytään takaisin lähteiden tunnistamiseen lisätiedon hankkimiseksi.

Tiedon määrän ja laadun ollessa riittävät hyökkääjä siirtyy valmisteluvaiheeseen. Valmisteluvaiheessa hyökkääjä yhdistää ja analysoi hankkimaansa tietoa, jonka jälkeen hän muodostaa itselleen hyökkäysvektorin tiedon perusteella. Jos hyökkäysvektorin muodostaminen ei analyysin perusteella onnistu, hyökkääjä palaa tiedonkeruuvaiheeseen arvioimaan hankittua tietoa uudelleen, ja tarvittaessa suorittaa tiedonkeruuvaiheen kokonaan uudelleen.

Kun hyökkääjä on luonut itselleen onnistuneesti hyökkäysvektorin, hän jatkaa suhteen luomiseen. Tässä vaiheessa hyökkääjä aloittaa uhrin kanssa kommunikoinnin ja alkaa luomaan välejä ja luottamusta uhrin kanssa. Kun hyökkääjä on saavuttanut mielestään riittävän luottamuksen uhrin kanssa, hän aloittaa suhteen hyväksikäytön. Tämän mallin kontekstissa kohteen valmistelu tarkoittaa, että hyökkääjä pyrkii saattamaan uhrinsa mie-

lentilaan, jossa hän on haavoittuvainen ja todennäköisemmin luovuttaa arkaluontoisia tietoja hyökkääjälle. Kun uhri on saatettu sopivaan mielentilaan alkaa varsinainen toiminta, eli hyökkääjä tekee aloitteen tietojen saamiseen uhrilta.

Viimeinen vaihe eli viimeistely puuttuu Mitnickin (2002) mallista ja jonka Mouton et al. (2014) kokee erityisen tärkeäksi onnistuneen hyökkäyksen takaamiseksi. Huolto (maintenance) on vaihe, jossa uhri pyritään saattamaan mielentilaan, jossa hän ei koe joutuneensa hyökkäyksen uhriksi tai ainakaan koe häpeää tai riittämättömyyttä uhriksi joutumisen takia. Viimeisessä kohdassa eli siirtymiskohdassa hyökkääjä arvioi, onko hän päässyt päämääräänsä vai vaaditaanko siihen lisää tietoa. Mikäli uhrilta saatu tieto ei riitä, palataan uuden hyökkäysvektorin kehittämiseen tai jos riittää, voidaan päämäärä todeta saavutetuksi.



Kuva 1. Suomennettu versio käyttäjän manipulointiin pyrkivän hyökkäyksen kulusta (Mouton et al., 2014).

4 Tietojenkalastelu

Tietojenkalastelu (phishing), toiselta suomennokseltaan *verkkourkinta,* on käyttäjän manipuloinnin tekniikka, jossa hyökkääjä pyrkii saamaan uhriltaan arkaluontoista tietoa esiintyen luotettavana tahona (Jagatic et al., 2007). Tällä hetkellä yleisin tapa lähestyä uhreja on sähköpostitse, mutta hyökkäysten tekemiseen käytetään myös muita medioita,

joista keskustellaan luvussa 4.3. Luvut 4.1 ja 4.2 käsittelevät kohdennettua tietojenkalastelua, valaanpyyntiä sekä sosiaalista tietojenkalastelua. Näiden alaluokkien määritelmät perustuvat tietojenkalastelun uhrin tyyppiin lähestymismedian sijaan.

4.1 Kohdennettu tietojenkalastelu ja valaanpyynti

Kohdennettu tietojenkalastelu (spear-phishing) toimii pohjimmiltaan samalla tavalla kuin "perinteinen" tietojenkalastelu, käyttäen samoja teknisiä toteutuksia kuten pankkien tai muiden palveluiden verkkosivujen imitaatioita tietojen keräämiseen. Merkittävä ero näiden välillä on kuitenkin se, että kohdennetussa tietojenkalastelussa ainakin alkuperäinen yhteydenotto räätälöidään kullekin uhrille henkilökohtaiseksi. Tämä tarkoittaa esimerkiksi nimellä puhuttelua sekä henkilökohtaisten tietojen esittämistä, jotta hyökkääjän onnistuisi saada uhrin luottamus. Tarkoituksena on luoda uhrille tunne, että hyökkääjä on kuka väittää olevansa, koska tämä tietää uhrista henkilökohtaisia tietoja. Yhteydenotoissa käytetty tieto hankitaan useimmiten verkosta, kuten sosiaalisen median sivuilta (Facebook, LinkedIn, tms.) tai uhrin työnantajan verkkosivuilta. Tällaisiin hyökkäyksiin saattaa sisältyä myös konkreettisempaa ennakkotietojen etsintää esimerkiksi etsimällä roskaastioista sinne epähuomiossa päätyneitä dokumentteja, jotka sisältävät luottamuksellista tietoa uhrista. Tästä käyttäjän manipuloinnin tekniikasta käytetään termiä *pengonta* (dumpster diving). Usein uhri valikoituu ennakkotietojen saatavuuden mukaan, koska kattavampi arsenaali ennakkotietoja parantaa hyökkäyksen onnistumismahdollisuuksia. Merkittävä esimerkki kohdennetusta tietojenkalastelusta on Kaspersky Labin (2014) paljastama laaja kybervakoilukampanja, lempinimeltään "Red October" eli "Punainen lokakuu". Kyseisen hyökkäyksen kohteena oli useita diplomaattisia ja hallinnollisia organisaatioita. Uhreja löytyi ympäri maailman, mutta iskujen painopiste oli Itä-Euroopassa ja Keski-Aasiassa.

Valaanpyynti (Whaling) tarkoittaa kohdennettua tietojenkalastelua, jossa uhriksi pyritään valikoimaan mahdollisimman korkea-arvoinen ja auktoriteettinen hahmo hyökkäyksen kohteena olevan organisaation hierarkiassa (Salahdine & Kaabouch, 2019). Tällä pyritään takaamaan, että onnistuneen hyökkäyksen seurauksena saatavat tiedot ovat organisaatiolle (ja siten myös hyökkääjälle) erityisen arvokkaita ja arkaluontoisia.

4.2 Sosiaalinen tietojenkalastelu

Tämän tyyppisessä tietojenkalastelussa hyökkääjä väärentää sähköpostiosoitteensa ja/tai muotoilee uhrille lähetettävän viestin siten, että yhteydenotto näyttää tulleen uhrin ystävältä. Tällä pyritään vahvistamaan uhrin luottamusta ja laskemaan ennakkoluuloja ja epäilyksiä mahdollisesti epätavallista yhteydenottoa kohtaan. Social phishing -termille ei tämän tutkielman kirjoitushetkellä löydy vakiintunutta suomennosta, mutta karkea suomennos voisi olla *sosiaalinen tietojenkalastelu*.

Jagatic et al. (2007) tutkivat tekniikan vaikutusta yhdysvaltalaisten opiskelijoiden keskuudessa. Vaikka tutkimuksen otanta ei ole kovin suuri, ero satunnaisesta osoitteesta viestin saaneen kontrolliryhmän (16 % jakoi henkilökohtaisia tietoja) ja ystävältä saapuneeksi naamioidun viestin saaneen vertailuryhmän (72 % jakoi henkilökohtaisia tietoja) välillä on merkittävä. Tämän tuloksen perusteella sosiaalisen kalastelun uhka on siis huomattava.

4.3 SMS- ja äänipuhelutietojenkalastelu

Osa tietojenkalastelun vakiintuneista alalajeista määrittyy tekniikan sijasta hyökkääjän valitseman lähestymismedian perusteella. Termi *SMiShing* muodostetaan yhdistämällä *tietojenkalastelu* (phishing) sekä SMS, eli tekstiviesti. Suomenkielinen termi voisi olla *SMS-tietojenkalastelu*. SMS-tietojenkalasteluhyökkäyksessä hyökkääjä lähestyy siis kohdettaan tekstiviestin välityksellä (Hadnagy & Wozniak, 2018). Näihin hyökkäyksiin lukeutuvat muun muassa Postin saapumisilmoituksia imitoivat viestit, jotka pyytävät useimmissa tapauksissa joko kirjautumaan sisään Apple ID -tunnuksilla tai maksamaan kuvitteellisen käsittelymaksun luottokortilla (Kyberturvallisuuskeskus, 2020).

Vishing puolestaan koostuu sanoista *tietojenkalastelu* (phishing) ja *ääni* (voice) viitaten siis tietojenkalasteluun, jossa hyökkääjä pyrkii manipuloimaan uhriaan puhutun keskustelun keinoin, yleensä puhelimen välityksellä (Hadnagy & Wozniak, 2018). Sujuvaa suomenkielistä termiä vishing-tietojenkalastelulle on kenties vaikeampi muodostaa kuin SMS-tietojenkalastelulle, mutta yhtenä suomennoksena voisi käyttää *äänipuhelutietojenkalastelua*. Tunnettu esimerkki tästä ovat puhelut, jossa hyökkääjä tekeytyy Microsoftin tukipalveluksi ja väittää havainneensa ongelman uhrin tietokoneessa. Tämän todellisuudessa olemattoman ongelmatilanteen korjaamiseksi hyökkääjä pyytää uhrin henkilötietoja ja/tai pyytää uhria asentamaan laitteelleen etäohjaussovelluksen (Microsoft, 2021).

5 Suojautuminen

Tietojenkalastelulta suojautumiseen on tarjolla useita ratkaisuja, joista nostetaan tässä tutkielmassa muutamia esimerkkejä. Osa niistä on tietoteknisiä toteutuksia, ja esimerkiksi sähköpostin roskapostisuodatin on oletuksena käytössä. Toiset puolestaan ovat käyttäjän omaan toimintaan ja tarkkaavaisuuteen nojaavia, usein epäkohtien tunnistamiseen liittyviä menetelmiä. Tietojenkalastelun tunnistamiseen on myös ammattilaisten kehittämiä malleja, joista yhtä käsitellään kappaleessa 5.3.

5.1 Tekniset ratkaisut

Käyttäjälle kaikista helpoin ja tehokkain työkalu kalasteluviestien estämiseen on sähköpostin roskapostisuodatin. Se on esimerkiksi Googlen Gmail-palvelussa automaattisesti päällä, ja suodattaa automaattisesti epäilyttävältä vaikuttavat viestit pois käyttäjän posti-

laatikosta (Google, 2021). Nämä suodattimet eivät ole täysin luotettavia ja saattavat joissakin tapauksissa joko suodattaa oikeellista sähköpostia roskapostikansioon tai jättää roskapostiviestejä käyttäjän postilaatikkoon, mutta ne toimivat silti tietojenkalastelun ehkäisemiseksi. Verkkoselaimiin on myös saatavilla useita tietojenkalastelusivuja tunnistavia lisäosia kuten Netcraft Extension, joka etsii tietojenkalastelun lisäksi verkkosivulta esimerkiksi poikkeuksellisesta JavaScript-koodia (Netcraft, 2021). Kyberhyökkäykset ovat harvoin puhtaasti käyttäjän manipulointia vaan hyökkääjä käyttää myös haittaohjelmia tai muita teknisiä ratkaisuja, joten myös laitteiden käyttöjärjestelmien ja virustorjunnan pitäminen ajan tasalla on tehokas tapa pitää omat päätelaitteet turvassa käyttäjän manipuloinnin ohessa vaikuttavilta haittaohjelmilta.

5.2 Käyttäjän toimet

Tietojenkalasteluyrityksiä on mahdollista tunnistaa ja tietojenkalastelua välttää käyttäjän omilla toimilla usein eri tavoin. Käytetään esimerkkinä tietojenkalasteluviestiä, joka pyrkii jäljittelemään Postin saapumisilmoitusta, jossa pyydetään maksamaan käsittelymaksu viestiin linkatulla verkkosivulla (Posti, 2021). Ensimmäisenä kannattaa huomioida viestin lähettäjän osoite ja tarkastaa, vaikuttaako se Postin palvelusähköpostilta. Mikäli omassa sähköpostin postilaatikossa on todistetusti aitoja Postin palveluviestejä, voi niiden lähettäjää ja ulkoasua verrata uuteen viestiin.

Yllä mainittujen seikkojen lisäksi viestin sisältöön kannattaa kiinnittää huomiota. Postia tai vastaavaa tahoa esittävät tietojenkalasteluviestit ovat harvoin kohdennettuja, joten niiden sisältö saattaa olla tarkoituksella epätarkka, eikä esimerkiksi saapuneen paketin lähetystunnuksesta tai lähettäjästä ole mainintoja. Tietojenkalasteluviesteille on myös ominaista pyrkiä minimoimaan potentiaalisen uhrin harkinta-aika, joten niissä vedotaan usein kiireellisyyteen, jotta käyttäjä luovuttaisi tietonsa miettimättä viestin oikeellisuutta ja pyynnon järkevyyttä.

Tyypillinen epäkohta nimenomaan suomenkielisissä kalasteluviesteissä on kielioppi- tai kirjoitusvirheet. Tämä saattaa olla merkki siitä, että lähettäjän suomen kielen taito on heikko ja hän on käyttänyt kääntöpalvelua viestin kirjoittamiseksi. Suomalaiselta taholta lähetetty englanninkielinen viesti saattaa myös olla poikkeava tapa kommunikoida asiakkaalle, ja sen pitäisi silloin herättää huolta viestin aitoudesta.

Oppiminen ja kouluttautuminen tietojenkalastelun tunnistamiseen ja torjumiseen liittyen ovat hyväksi. Monet yritykset tarjoavat verkkomateriaaleja ja -koulutuksia, jotka opettavat käyttäjiä tunnistamaan tietojenkalastelua ja välttämään sen uhriksi joutumista. Useimmat näistä ratkaisuista ovat suunnattu toisille yrityksille, jotka ostavat koulutuksen työntekijöilleen käytettäväksi. Tietoturvatietoisuuden parantamiseksi käyttäjiä innostavammalla tavalla on kehitetty myös pelillisiä ratkaisuja, kuten esimerkiksi Fatiman et al. (2019) kehittämä PhishI-pelikonsepti.

5.3 Malli tietojenkalastelun tunnistamiseen

Mouton et al. (2015) esittää käyttäjän manipulointiin tähtäävän hyökkäyksen tunnistamiseksi ja estämiseksi mallia, jonka rakenne ja toiminta käydään läpi heidän tutkimusartikkelissaan "Social Engineering Attack Detection Model: SEADMv2". Malli on paranneltu versio alkuperäisestä, vuonna 2010 esitetystä mallista (Bezuidenhout et al., 2010) ja esittää pyynnön vastaanottajalle kysymyksiä vastaanottajan omista valmiuksista pyynnön täyttämiseen, pyynnön tarpeellisuudesta ja järkevyydestä sekä pyynnön lähettäjän identiteetin vahvistamisesta ja oikeudesta esittää kyseinen pyyntö. Tavoitteena on päätyä tilanteeseen sopivaan lopputulokseen joko täyttämällä pyyntö sen ollessa oikeellinen, tai torjumalla tai siirtämällä pyyntö eteenpäin, mikäli asetetut ehdot eivät täyty. Mallista tehty kaavio on alkuperäisessä muodossaan englanninkielinen, mutta suomenkielinen versio on nähtävissä kuvassa kaksi. Vaikka malli on alun perin suunniteltu käyttäjän manipulointiin tähtäävien hyökkäysten torjumiseen yleisesti, se toimii luonnollisesti myös tietojenkalastelun tunnistamiseen ja ehkäisyyn, koska tietojenkalastelu on osa käyttäjän manipulointia. Seuraava kuvaus perustuu Mouton et al. (2015) teoksessaan esittämään kuvaukseen.

Kaaviossa edetään ylhäältä alas vastaten laatikoissa esitettyihin kysymyksiin ja seuraten nuolia vastausten perusteella. Kaaviossa keltainen väri tarkoittaa kysymystä, joka koskee itse esitettyä pyyntöä, sininen väri kysymystä koskien pyynnön vastaanottajaa, vihreä väri kysymystä pyynnön esittäjään liittyen, ja punainen väri kysymystä, joka on suunnattu kolmannelle osapuolelle.

Ensimmäinen oleellinen kysymys pyyntöä vastaanottaessa on, ymmärtääkö pyynnön vastaanottaja esitetyn pyynnön. Jos vastaanottaja ei ymmärrä pyyntöä, hänen täytyy pyrkiä kysymään pyynnön esittäjältä lisätietoja pyynnöstä. Tätä toistetaan, kunnes joko vastaanottaja ymmärtää pyynnön tai pyytäjä ei pysty tai halua antaa enempää lisätietoja. Jälkimmäisessä tilanteessa pyynnöstä joko kieltäydytään tai pyyntö siirretään edelleen toiselle henkilölle.

Vastaanottajan ymmärtäessä pyynnön siirrytään vastaanottajaa koskeviin kysymyksiin. Nämä ovat:

1. Ymmärtääkö vastaanottaja, miten pyyntö toteutetaan?
2. Kykeneekö vastaanottaja toteuttamaan pyynnön?
3. Onko vastaanottajalla oikeus toteuttaa pyyntö?

Mikäli vastaus yhteenkään näistä on "ei", pyynnöstä kieltäydytään tai se siirretään edelleen. Jos kaikkiin näihin kysymyksiin vastataan myönteisesti, siirrytään kysymään, onko pyydetty tieto julkista. Mikäli näin on, pyyntö toteutetaan. Jos näin ei kuitenkaan

ole, kysytään, onko kyseessä ennalta hyväksytty pyyntö, joka voidaan toteuttaa hengenvaarallisen tilanteen välttämiseksi. Tämä kysymys on hyvin laaja ja melko epätarkka, mutta koska malli on suunniteltu yleisenä ohjenuorana eikä kohdistettu tietylle alalle tai tiettyyn kontekstiin, mainittu "hengenvaarallinen tilanne" määrittyy siis kontekstin ja mallin käyttöympäristön mukaan.

Mikäli vastaus on myönteinen, eli pyyntö on ennalta hyväksytty ja se voidaan toteuttaa hengenvaarallisen tilanteen välttämiseksi, pyyntö toteutetaan, mutta mikäli näin ei ole, siirrytään tarkastelemaan mahdollisia perusteita pyynnön hylkäämiselle. Tässä vaiheessa pyynnön vastaanottaja arvioi, onko pyynnöstä kieltäytymiselle *hallinnollisia* (administrative), *toimenpiteellisiä* (procedural) tai muita syitä, tai onko kyseessä poikkeuksellinen tai vastaanottajalle uudenlainen pyyntö. Mikäli yksikään näistä ei toteudu, pyynnöstä kieltäytyminen on mallin mukaan tarpeetonta ja pyyntö toteutetaan, mutta muussa tapauksessa edetään arvioimaan pyynnön esittäjän uskottavuutta.

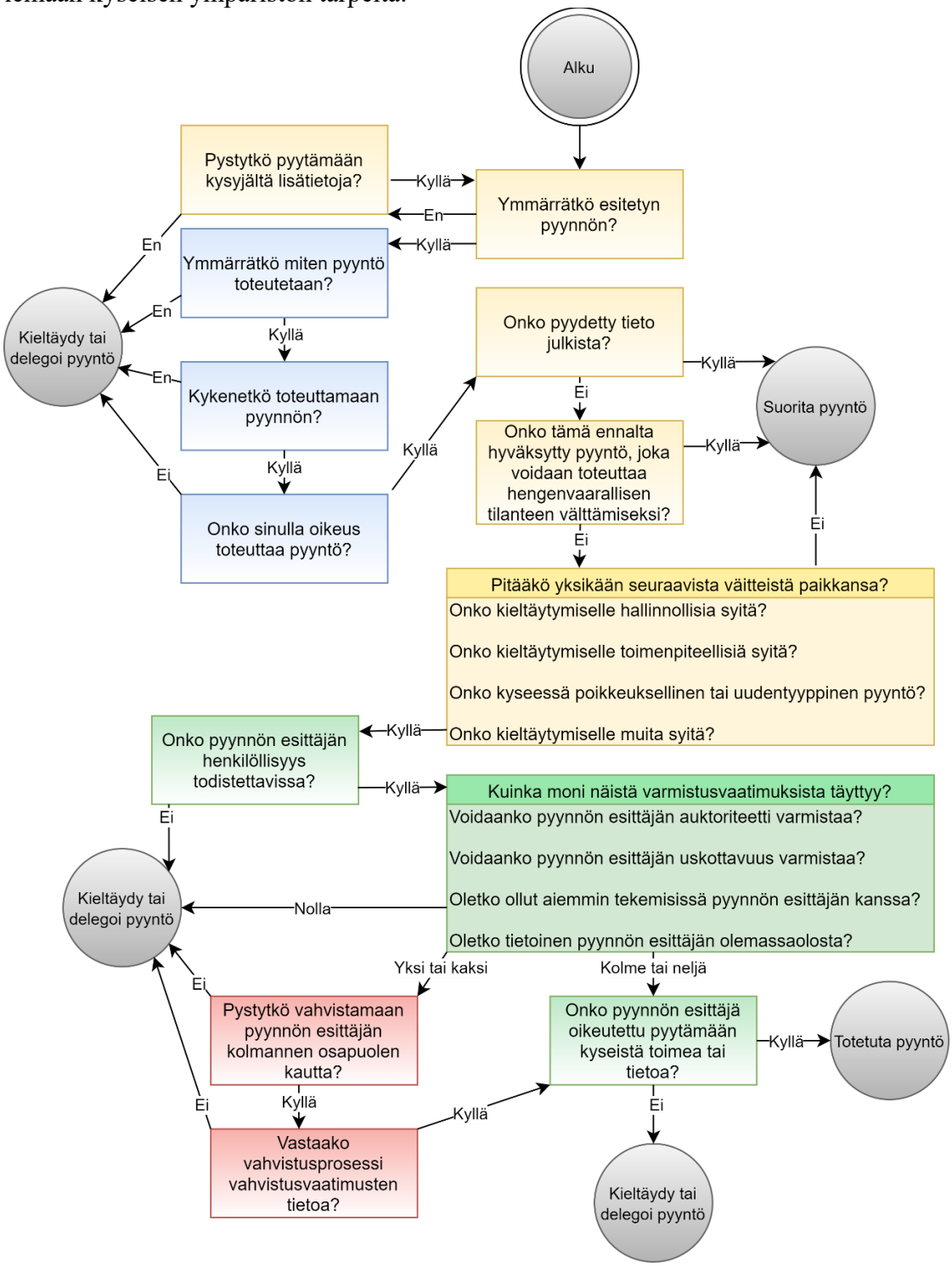
Ensimmäisenä tarkistetaan, onko pyynnön esittäjän henkilöllisyys todistettavissa. Mikäli näin ei ole, aiemman kohdan syitä kieltäytymiselle ei voida sivuuttaa, ja pyynnöstä kieltäydytään tai se siirretään edelleen. Jos pyynnön esittäjän henkilöllisyyden todistaminen kuitenkin on mahdollista, malli esittää neljä varmistusvaatimusta, joiden täyttymisen perusteella päätetään jatkotoimenpiteet. Nämä varmistusvaatimukset ovat:

1. Voidaanko pyynnön esittäjän auktoriteetti varmistaa?
2. Voidaanko pyynnön esittäjän *uskottavuus* (credibility) varmistaa?
3. Onko pyynnön vastaanottaja ollut pyynnön esittäjän kanssa aiemmin tekemisissä?
4. Onko pyynnön vastaanottaja tietoinen pyynnön esittäjän olemassaolosta?

Näiden varmistusvaatimusten perusteella voidaan päätyä kolmeen eri lopputulokseen: Mikäli yksikään kriteereistä ei täyty, pyynnöstä kieltäydytään tai se siirretään edelleen. Kolmen tai neljän kriteerin täyttyessä arvioidaan, onko pyynnön esittäjä oikeutettu pyytämään toimintoa tai tietoa, jota hän pyytää. Jos näin on, pyyntö toteutetaan ja jos ei, pyynnöstä kieltäydytään tai se siirretään edelleen.

Mikäli edellä mainituista neljästä varmistusvaatimuksesta täyttyy yksi tai kaksi, turvaudutaan pyynnön esittäjän henkilöllisyyden varmistamisessa kolmanteen osapuoleen. Mikäli pyynnön vastaanottaja ei pysty varmistamaan pyynnön esittäjää kolmannen osapuolen kautta, tai pyynnön esittäjä pystytään varmistamaan mutta saatu tieto ei vastaa edellisessä vaiheessa täyttyneitä varmistusvaatimuksia, pyynnöstä kieltäydytään tai se siirretään edelleen. Jos molemmat kohdat kuitenkin täyttyvät, kysytään tässäkin tilanteessa, onko pyynnön esittäjä oikeutettu pyynnön esittämiseen ja vastauksen perusteella pyynnöstä joko kieltäydytään tai se siirretään edelleen, tai sen toteutetaan. Mallia on tarkoitus käyttää työkaluna ehkäisemään käyttäjän manipulointiin pyrkiviä hyökkäyksiä, ja

se on suunniteltu muokattavaksi käyttökohteen ja -ympäristön mukaan tarkemmin palvelemaan kyseisen ympäristön tarpeita.



Kuva 2. Suomennettu versio käyttäjän manipuloinnin tunnistamisen mallista SEADMv2 (Mouton et al., 2015).

6 Keskustelu

Aiemman tutkimuksen perusteella löytyi useita käyttäjän manipuloinnin tekniikoita, ja sama päti myös tietojenkalasteluun. Tämän lisäksi tietojenkalastelun ennaltaehkäisemiseen ja estämiseen on kehitetty ja ehdotettu ratkaisuja sekä teoria- että käytäntöpainotteisesti, joista yhtä tämä tutkielma avasi ja käsitteli tarkemmin luvussa 5.3.

Tutkielman tekoprosessin alkuvaiheessa tehdyn tiedonhaun perusteella tietojenkalastelu on käyttäjän manipuloinnin alalajeista eniten tutkittu ja käsitelty. Tämä on loogista, koska kuten johdannossa esitetyistä raporteista (Proofpoint 2019, IBM 2020) ja uutisesta (Yle 2021) käy ilmi, tietojenkalastelu aiheuttaa suuria kuluja sekä yrityksille että yksityishenkilöille. Erityisesti kohdentamattoman tietojenkalastelun tapauksessa hyökkäys ei myöskään vaadi hyökkääjältä suurta työmäärää sen jälkeen, kun kalasteluviesti on muodostettu, joten sen helppous varmasti houkuttelee potentiaalisia kyberrikollisia. Tämän vuoksi aiheen tutkiminen sekä torjunta- ja ennaltaehkäisykeinojen kehittäminen on tärkeää.

Tietojenkalastelun todellisesta vaarallisuudesta ollaan myös erimielisiä. Muun muassa Herley & Florêncsio (2008) kyseenalaistavat tietojenkalastelun tuottavuuden ja kokevat, että tietojenkalastelun raportoidut kustannukset uhreille ovat liioiteltuja. Tästä huolimatta tietojenkalastelu on myös heidän mielestään vakavasti otettava ongelma, jonka ennaltaehkäisy ja torjuminen on tärkeää tietoturvan ylläpitämiseksi.

Tietojenkalastelun onnistumisprosenttiin vaikuttaa myös potentiaalisen uhrin ikä ja mahdolliset puutteelliset tietotekniikkataidot. Uskon kohdentamattomien ja/tai huolimattomasti väärennettyjen tietojenkalasteluyritysten onnistumisprosentin laskevan tulevaisuudessa. Tietotekniikka ja sen toiminta tulee yleisyytensä vuoksi myös osaamattomille tutuksi, ja samaan aikaan niin sanotut "diginatiivit" eli tietotekniikkaa lapsesta asti käyttäneet (Dingli & Seychell, 2015) ikääntyvät ja siten heidän osuutensa väestöstä kasvaa.

7 Yhteenveto

Tässä tutkielmassa perehdyttiin käyttäjän manipulointiin ja tarkemmin tietojenkalasteluun, sen eri muotoihin sekä keinoihin suojautua siltä kirjallisuuskatsauksen muodossa. Käyttäjän manipulointi on laaja käsite, jonka alle muodostuu arsenaali tekniikoita ja työkaluja hyökkääjälle uhreihin vaikuttamiseen ja heidän hyväksi käyttämiseen. Hyökkääjä voi hyödyntää tekniikoita, kuten tietojenkalastelua, syötittämistä tai juomapaikkahyökkäyksiä uhreja houkutellakseen. Lisäksi hän pystyy valitsemaan tilanteeseen sopivan kommunikaatiotavan, joka varmimmin tuottaa suotuisan lopputuloksen. Käyttäjän manipulointihyökkäys on monivaiheinen prosessi, jossa hyökkääjä tekee valmisteluja ja taustatyötä jo ennen yhteydenottoa kohteeseen, sekä viimeistelee tekemänsä työn epäilysten, ja siten kiinni jäämisen minimoimiseksi.

Tietojenkalastelu on käyttäjän manipuloinnin yleisin esiintymismuoto, minkä takia siihen tässä tutkielmassa perehdyttiinkin. Kuten käyttäjän manipulointi kokonaisuudessaan, myös tietojenkalastelu on monijakoinen ja -väyläinen tapa hyökätä tietojärjestelmän käyttäjään. Kohdetta valitessa hyökkääjän tekemä taustatyö ja tiedonhaku mahdollistavat tarkkaan kohdennetut, yksilöllistetyt hyökkäykset. Lähestymismedian muuttaminen taas tekee hyökkäyksistä vaikeammin tunnistettavia ja kasvattaa mahdollisten uhrien määrää. Nykyään arkipäiväiset sosiaalisen median alustat puolestaan altistavat käyttäjiä tietojenkalastelulle tarjoamalla hyökkääjälle sekä lähestymisväylän että alustan tietojen keräämiselle.

Tietojenkalastelu on merkittävä ja alati kasvava uhka sekä yksilöille että organisaatioille, ja sitä hyödyntävällä hyökkääjällä on monia tapoja lähestyä uhria ja anastaa tältä tietoja. Käyttäjän tarkkaavaisuudella ja käyttämällä oikeita työkaluja, kuten luvussa 5.3 käsiteltyä käyttäjän manipuloinnin tunnistamisen mallia, tietojenkalastelun ehkäiseminen on kuitenkin mahdollista.

Lähdeluettelo

Bezuidenhout, M., Mouton, F. & Venter, H. (2010). Social engineering attack detection model: SEADM. *2010 Information Security for South Africa*, 1–8. https://doi.org/10.1109/ISSA.2010.5588500

Dingli, A. & Seychell, D. (2015). Who are the digital natives? Teoksessa *The New Digital Natives* (ss. 9–22). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-46590-5_2

Fatima, R., Yasin, A., Liu, L. & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, *27*(6), 581–612. https://doi.org/10.3233/JCS-181253

Google. (2021). *Mark or unmark Spam in Gmail.* Google. https://support.google.com/mail/answer/1366858 (Haettu 21.4.2021)

Hadnagy, C. & Wozniak, S. (2018). *Social engineering: the science of human hacking*. Wiley.

Herley, C. & Florêncio, D. (2008) A profitless endeavor: phishing as tragedy of the commons. *NSPW '08: Proceedings of the 2008 New Security Paradigms Workshop,* 59–70. https://doi.org/10.1145/1595676.1595686

IBM Corporation. (2020). *Cost of a Data Breach Report 2020.* https://www.ibm.com/security/digital-assets/cost-data-breach-report (Haettu 23.2.2021)

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

Kaspersky. (2014) *Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide*. Kaspersky.com. https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-

espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide (Haettu 16.3.2021)

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*. *2015*(22), 113–122. http://doi.org/10.1016/j.jisa.2014.09.005

Kyberturvallisuuskeskus. (2020). *Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus*. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus (Haettu 15.3.2021)

Microsoft. (2021). *Tukipalveluhuijaukset.* https://www.microsoft.com/fi-fi/wdsi/threats/support-scams (Haettu 15.3.2021)

Mitnick, K. & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Mouton, F., Leenen, L. & Venter, H. (2015). Social engineering attack detection model: SEADMv2. *2015 International Conference on Cyberworlds (CW),* 216–223. https://doi.org/10.1109/CW.2015.52

Mouton, F., Leenen, L., Malan, M. & Venter, H. (2014). Towards an ontological model defining the social engineering domain. *IFIP Advances in Information and Communication Technology, 2014*(432), 266–279. https://doi.org/10.1007/978-3-662-44208-1_22

Mouton, F., Malan, M., Leenen, L. & Venter, H. (2014). Social engineering attack framework. *2014 Information Security for South Africa*, 1–9. https://doi.org/10.1109/ISSA.2014.6950510

Netcraft. *Cybercrime protection, in your favourite browser.* https://www.netcraft.com/apps/browser/ (Haettu 21.4.2021)

Näveri, A. (2021). *Microsoft-huijarit ovat vieneet tänä vuonna jo miljoona euroa suomalaisten rahoja – nettirikollisten uusi temppu on verottajana esiintyminen*. Yle Uutiset. https://yle.fi/uutiset/3-11802472 (Haettu 23.2.2021)

Posti. *Tietoa huijausviesteistä*. https://www.posti.fi/fi/asiakastuki/ehdot-ja-tietosuoja/tietoa-huijausviesteista (Haettu 27.4.2021)

Proofpoint. (2019). *Human Factor Report 2019.* https://www.proofpoint.com/us/resources/threat-reports/human-factor (Haettu 23.2.2021)

Salahdine, F. & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/FI11040089

Thompson, H. (2013). The human element of information security. *IEEE Security & Privacy*, *11*(1), 32–35. https://doi.org/10.1109/MSP.2012.161