Verkossa jaetun tiedon vaarat

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus
syksy, 2022

Teemu Oivanen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus — Tiivistelmä

Tekijä Teemu Oivanen

Vuosi 2022

Työn nimi Verkossa jaetun tiedon vaarat

Ohjaaja Pentti Ojaniemi

TIIVISTELMÄ

Opinnäytetyöni aihe on ajankohtainen, minkä vuoksi se on tärkeä kaikille verkonkäyttäjille. Verkkorikollisuudesta ja tietoturvaan liittyvistä asioista uutisoidaan lähes päivittäin valtamedioissa, mutta yksittäiselle ihmiselle aihe voi silti tuntua vieraalta ja kaukaiselta. Jokaisella on kuitenkin mahdollisuus parantaa omaa tietoturvaansa pienillä teoilla, sekä vähentää mahdollisia uhkia.

Opinnäytetyön tavoitteena oli luoda kattava ja monipuolinen selvitys siitä, millaisia tietoturvaan liittyviä riskejä verkkoon jaetut tiedot mahdollisesti tuottavat. Opinnäytetyön tarkoituksena oli tutkia tietoturvaan liittyviä asioita ja analysoida niitä yksilön näkökulmasta. Tarkoituksena oli myös ilmentää tietoturvaan vaikuttavia asioita ja luoda taustaa esimerkiksi aiheen jatkokäyttöä varten. Opinnäytetyö on tutkimuspainotteinen, eikä sillä ole toimeksiantajaa, mutta sitä voidaan helposti soveltaa monenlaisiin ympäristöihin, kuten työpaikkojen tietoturvakoulutukseen.

Opinnäytetyön tietopohja koostuu verkkoon jaetun tiedon vaarojen ja siihen liittyvien uhkien sekä ilmiöiden käsittelystä. Opinnäytetyö antaa luotettavaa tietoa ja antaa lukijalle ohjeita, miten välttää uhkia omalla käytöksellä.

Johtopäätöksenä voidaan todeta, että henkilökohtaiseen tietoturvaan pystytään vaikuttamaan pienillä muutoksilla omassa verkkokäyttäytymisessä. Henkilökohtaisen tietoturvan osaaminen vahvistaa myös esimerkiksi organisaatioiden tietoturvaa.

Avainsanat tietoturva, sosiaalinen manipulointi, verkkorikollinen

Sivut 27 sivua ja liitteitä 1 sivu

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Author Teemu Oivanen
Subject Dangers of information shared online
Supervisor Pentti Ojaniemi

Abstract
Year 2022

ABSTRACT

The topic of my thesis is current, which is why it is relevant for all internet users. Cybercrime and issues related to information security are reported in the mainstream media almost every day, but to an individual the subject may still seem foreign and distant. However, everyone can improve their own information security with small actions, as well as reduce possible threats.

The objective of the thesis was to create a comprehensive and versatile report on what kind of information security risk of the information shared online might produce. The purpose of the thesis was to investigate issues related to information security and analyze them from an individual's point of view. The purpose was also to express issues affecting information security and to create a background, for example, further use of the topic. The thesis is research-oriented and does not have a commissioner, but it can easily be applied to a wide variety of environments, such as workplace information security training.

Theoretical background of the thesis consists of discussing the dangers of information shared online, and threats and phenomena related to it. The thesis provides reliable information and gives the reader instructions on how to avoid threats with their own behavior.

In conclusion, it can be stated that personal information security can be influenced by small changes in person´s own online behavior. Moreover, knowledge of personal information security strengthens the information security of organizations.

Keywords information security, social engineering, cyber criminal
Pages 27 pages and appendices 1 page

Sanasto

Avoin lähde	Lähde, johon on avoin tai kaupallisesti saatavilla oleva pääsy.
Sosiaalinen media	Verkkosivuja ja sovelluksia, joissa on mahdollista tuottaa ja jakaa sisältöä.
Verkkorikollinen	Rikollinen, joka tekee rikoksia verkossa.
Tietoturva	Ylläpitää tiedon saatavuutta, luottamuksellisuutta ja eheyttä. Kokonaisvaltainen termi, jota käytetään tiedon ja järjestelmien suojaamiseen.
Viraali	Ilmiö joka saavuttaa suuren näkyvyyden nopeasti.

Sisällys

Kuvat

Liitteet

Liite 1 Aineistonhallintasuunnitelma

1 Johdanto

Mille vaaroille verkkoon jaettu tieto, kuten kuvat lomamatkoilta ja tiedot käytössä olevista ajoneuvoista ja niiden merkeistä voivat altistaa? Miksi vaarat tulisi huomioida esimerkiksi sosiaalisen median eri alustoille tehtävissä julkaisuissa? Huolettomasti ja liian avoimesti verkkoon jaettu tieto voi altistaa monille erilaisille uhille ja vaikuttaa negatiivisesti yksityisyyteen. Erilaiset tietoturvariskit muuttuvat ja kehittyvät jatkuvasti, josta johtuen verkonkäyttäjien pitäisi olla tietoisia yleisimmistä tiedon jakamiseen liittyvistä riskeistä ja niiden mahdollisista seurauksista. Tämän opinnäytetyön tavoitteena on luoda kattava ja monipuolinen käsitys siitä, millaisia mahdollisia riskejä tiedon jakamiseen avoimiin lähteisiin, kuten sosiaaliseen mediaan liittyy, sekä miten ja miksi niitä pitäisi huomioida omassa verkkokäyttäytymisessään.

Oppinnäytetyössä käydään esimerkkien avulla läpi, miten ja mihin verkon avoimista lähteistä kerättyjä tietoja voidaan käyttää. Lisäksi työn tarkoitus on havainnollistaa, kuinka pienistä tiedon palasista yhdistelemällä, on mahdollista rakentaa laaja kuva esimerkiksi yksittäisestä henkilöstä.

Tämä työ lisää verkonkäyttäjien tietoisuutta tietojen jakamiseen liittyvistä vaaroista, jonka johdosta käyttäjillä on paremmat mahdollisuudet tutkia ja muuttaa omaa verkkokäyttäytymistään. Tutkimuskysymykset joihin opinnäytetyö vastaa ovat:

- Mitä vaaroja omien tietojen jakaminen verkkoon voi aiheuttaa?
- Ketkä voivat hyötyä avoimista lähteistä kerätyistä materiaaleista?
- Miksi mahdollisia vaaroja tulisi ottaa huomioon?
- Miksi jokaisen pitäisi olla tietoinen materiaalista, jota verkosta voi itsestään löytää?

2 Tausta, tavoitteita ja tarkoitus

Tietoturvasta tai tietoturvallisuuteen liittyviin aiheisiin tutustuessa törmää väistämättä väittämään: ”ihminen on tietoturvan heikoin lenkki.” Tästä lähtökohdasta liikkeelle lähdettäessä, on ensimmäinen teko tietoturvallisuustiedon lisääminen. Tärkeintä on auttaa ihmisiä ymmärtämään mitä riskejä heidän jokapäiväiset ja arkiset toimet verkossa voivat aiheuttaa. Henkilökohtaisen tietoturvallisuus tietoisuuden parantuessa ja tietoturvaa paremmin ymmärtäessä, on samat periaatteet helpompi omaksua ja ottaa käyttöön myös työelämässä.

Työpaikkojen tietoturva on asia, jota tässä opinnäytetyössä sivutaan, mutta siihen ei syvennytä. Työpaikoilla on omat säädöksensä ja määräykset kuinka tietoturvaa toteutetaan. Kuitenkin jokaisen omalla toiminnalla on vaikutusta ja yksittäisen henkilön näkökulmasta pieneltä tuntuvat asiat voivat johtaa isoihin tietoturvauhkiin. Lisäksi yritysten tietoturvassa voi olla isoja haavoittuvuuksia ja puutteita. Kuten Vastaamon tilanteessa nähtiin, tietoturva aukot aiheuttivat useille yksityishenkilöille haittaa heidän henkilökohtaisten tietojensa vuodettua julkiseksi.

Opinnäytetyöni tavoitteena on luoda käsiteltävästä aihepiiristä laaja ja monipuolinen kuva, jonka avulla lukija pystyy pohtimaan ja mahdollisesti muuttamaan omaa käyttäytymistään esimerkiksi sosiaalisessa mediassa. Työn tavoitteena on auttaa ihmisiä ymmärtämään niitä tietoturvariskejä, joita jokainen omalla verkkokäyttäytymisellään mahdollisesti luo. Opinnäytetyöni tietopohjan avulla pyritään tuomaan esiin ja yhdistämään tietoturvauhat isompiin kokonaisuuksiin, jotka vaikuttavat uhkien takana.

Tavoitteeni on oppia ymmärtämään tietoturvaa syvällisemmin ja soveltaa hankkimiani tietoja opinnäytetyössä. Konkreettisten esimerkkien avulla yritän luoda selkeämpää kuvaa siitä, mitä teoria tarkoittaa käytännössä. Opinnäytetyön tekeminen kehittää analysointitaitojani ja kriittistä ajattelua. Tietoturvaan kuuluu paljon erilaisia aihealueita ja tämän työn avulla tutustun niihin perusteellisemmin.

Opinnäytetyön tarkoitus on tutkia tietoturvaan liittyviä asioita ja analysoida niitä yksilön näkökulmasta. Tarkoituksena on ilmentää tietoturvaan liittyviä ongelmia ja luoda pohjaa

esimerkiksi jatkokäyttöä varten. Opinnäytetyöni ei ole työelämälähtöinen, mutta sitä voidaan helposti soveltaa monenlaisiin ympäristöihin, kuten työpaikkojen tietoturvakoulutukseen. Toisaalta opinnäytetyöni on helposti ymmärrettävä ja kuka tahansa voi saada tästä lisätietoa omaan käyttöönsä.

3 Verkkoon jaetun tiedon vaaroja

Kaikki verkon käyttäjät ovat potentiaalisia verkkorikollisuuden kohteita. Verkkorikolliset voivat yrittää varastaa henkilöiltä erilaista tietoa, kuten identiteetin tai vaihtoehtoisesti tavoitteena voi myös olla esimerkiksi pelkkä kiusanteko. (Kyberturvallisuuskeskus, 2020) Ihmisten henkilökohtaiset- ja taloudelliset tiedot toimivat valuuttana verkkorikollisille. Ihmisten tulisi olla varovaisia siitä, kuinka paljon henkilökohtaista tietoa he jakavat itsestään verkossa. Omien osoitteiden, puhelinnumeroiden ja syntymäpäivien jakaminen lisää huomattavasti riskiä joutua verkkorikollisten ja esimerkiksi identiteettivarkauden uhriksi. Verkkorikolliset voivat koota verkon useasta eri lähteestä kohteistaan tietoja ja näitä tietoja yhdistelemällä koota isomman kokonaiskuvan. (Australian Cyber Security Centre, 2020)

Sosiaalinen media kuluu modernin ihmisen päivittäiseen elämään ja oman elämän tapahtumien jakaminen eri palveluiden kautta on iso osa nykypäivää. Jakamalla henkilökohtaisia tietoja voi tietämättään helpottaa rikollisten työtä. Kuvien jakaminen omasta kodista voi tarjota rikollisille tietoja esimerkiksi kodin arvoesineistä ja muista mahdollisista varkauden kohteista. Kuvat lomamatkalta tarjoavat rikollisille tiedon parhaalle ajankohdalle suorittaa mahdollinen murto asukkaiden ollessa poissa kotoa. (Microsoft, n.d. a)

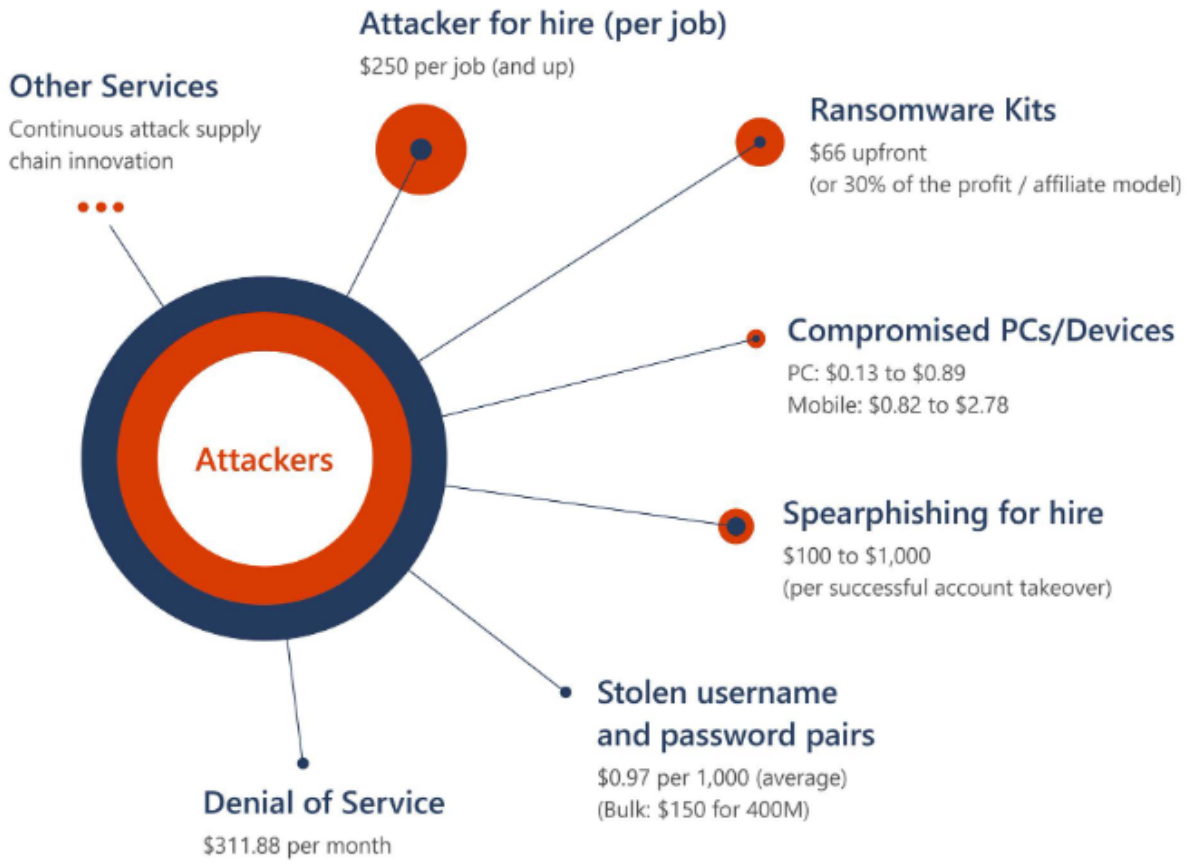
Sosiaalisessa mediassa kulkee erilaisia viraaleja haasteita, joissa jaetaan henkilökohtaisia tietoja, kuten vanhojen omistuksessa olleiden autojen merkkejä ja malleja. Viattoman oloiset haasteet eivät yleensä ole tarkoituksella pahantahtoisia, mutta henkilö voi niissä huomaamattaan paljastaa vastauksia yleisimpiin käytössä oleviin turvallisuuskysymyksiin, joita esimerkiksi pankit voivat palveluissaan käyttää. (Patel, 2020)

Useat työnantajat tekevät rekrytoinnin yhteydessä taustatarkistuksia, joihin kuuluu yhtenä osana hakijoiden sosiaalisten medioiden läpikäynti, sekä muun verkon avoimista lähteistä löytyvän tiedon tarkistaminen. Sosiaalisen mediaan ja verkkoon jakamistaan muista tiedoista tulisi olla tietoinen ja pitää huolta siitä, että löytyvät tiedot ovat oikein eivätkä vaikuta negatiivisesti esimerkiksi mahdollisuuksiin tulla palkatuksi. (Bridges, 2021)

Verkosta löytyvistä tiedon palasista verkkorikollisten on mahdollista luoda kuva henkilön kiinnostuksen kohteista, jonka avulla voidaan lähettää yhdelle henkilölle juuri hänelle kohdennettua huijausviestintää, kuten tietojenkalastelu sähköposteja. Viestien harkitsematon klikkaus altistaa laitteet ja henkilökohtaiset tiedot esimerkiksi haittaohjelmille. (Kyberturvallisuuskeskus, 2020)

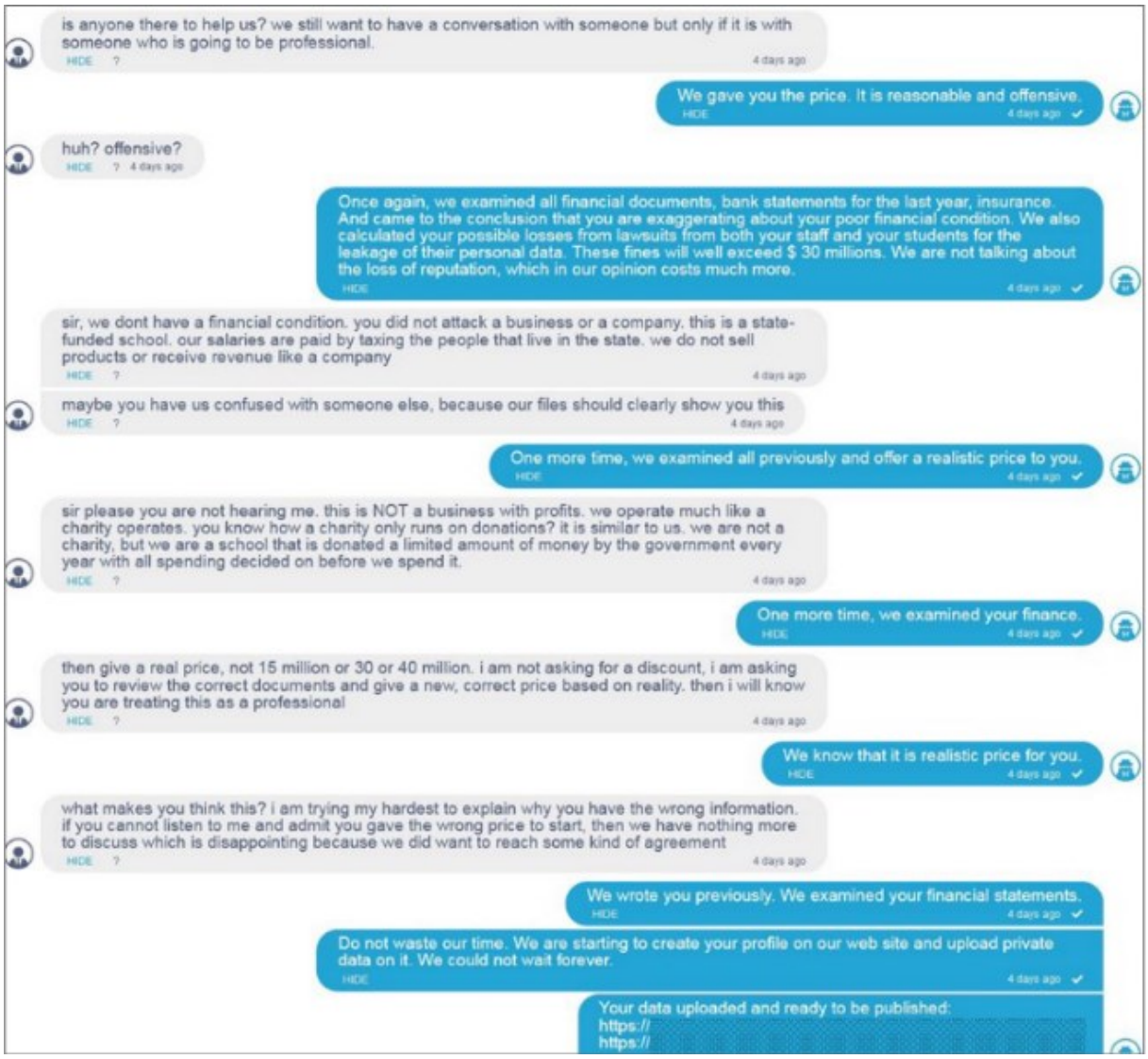
Verkkorikollisuus ja erityisesti kiristyshaittaohjelmilla tehtävät hyökkäykset ovat kehittymässä suuntaan, jossa itse tekniset hyökkäykset ovat ostettavissa pimeänverkon kauppapaikoilla palveluina. Varsinaisten hyökkääjien pääpaino on taas henkilötiedustelussa ja tietojen keräämisessä. Tämän ilmiön ansiosta verkkorikollisella ei tarvitse enää olla suuriakaan teknisiä taitoja hyökkäyksen suorittamiseen. Kuva 1 kertoo verkossa ostettavissa olevien verkkorikollisuuden palveluiden keskiarvohintoja. (Microsoft, 2021, ss. 8-14)

Kuva 1 Ostettavien palveluiden keskiarvohintoja (Microsoft, 2021, s. 9)



Verkkorikollisten ja erityisesti itse hyökkäyksiä suorittavien tahojen painopisteen siirron tiedustelu painotteisempaan suuntaan on myös muuttanut tapaa, jolla muodostetaan vaadittavia lunnassummia. Verkkorikollisten päästessä sisään kohteen järjestelmiin saavat he mahdollisesti käsiinsä erilaisia talous- ja vakuutustietoja, jonka perusteella he muodostavat mielestään sopivan lunnassumman. Kuva 2 on esimerkki hyökkääjän ja kohteen välillä käydystä keskustelusta, jossa keskustellaan lunnasvaatimuksen kohtuullisesta summasta.

Kuva 2 Lunnasvaatimus keskustelu (Microsoft, 2021, s. 13)



4 Sosiaalinen manipulointi

Social-engineer.org (n.d.) sivustolla määritellään sosiaalinen manipulointi (engl. social engineering) seuraavasti: ”Mikä tahansa teko, joka saa henkilön ryhtymään toimiin, jotka voivat olla tai eivät ole hänen etunsa mukaisia”. Verkkorikollisten käyttämät sosiaalisen manipuloinnin tekniikat luottavat ihmisten tekemiin virheisiin, joiden avulla he pääsevät tavoitteisiinsa. Useissa sosiaaliseen manipulointiin perustuvissa hyökkäyksissä pyritään vaikuttamaan ihmisten tunteisiin. Manipuloinnin kohteena olevat henkilöt tekevät todennäköisimmin riskialttiimpia toimia ollessaan tunteiden vallassa. Tunteita, joita pyritään saamaan aikaan ja hyödyntämään ovat esimerkiksi pelko, viha, uteliaisuus ja innostuneisuus. (Kaspersky, n.d. a)

Verkkorikollisten tavoitteena on yleensä joko varkaus tai sabotaasi. Varkauksissa suoran rahan varastamisen lisäksi uhreja yritetään saada paljastamaan itsestään henkilökohtaisia tietoja ja/tai yritetään uhrin avulla saada pääsy erilaisiin muuten rajattuihin järjestelmiin. Sosiaalinen manipulointi perustuu verkkorikollisen kykyyn ymmärtää valittuja uhreja ja siihen, miten he toimivat. Mitä paremmin verkkorikollinen on tietoinen uhristaan, sitä paremmin hän pystyy uhriaan manipuloimaan. Usein myös uhrin mahdollista tietämättömyyttä teknologiasta käytetään hyväksi sosiaaliseen manipulointiin perustuvissa hyökkäyksissä. (Kaspersky, n.d. a)

Useimmat sosiaalisen manipuloinnin hyökkäykset perustuvat hyökkääjän ja uhrin väliseen suoraan kommunikaatioon. Kommunikaatio voi olla jopa kasvotusten tapahtuvaa, mutta useimmiten kommunikaatio tapahtuu verkon välityksellä. Verkossa tapahtuva kommunikaatio voi prosessista riippuen käsittää yhden sähköpostiviestin tai usean kuukauden viestittelyn esimerkiksi eri sosiaalisen median alustoilla. (Kaspersky, n.d. a)

Sosiaalisen manipuloinnin hyökkäykset seuraavat usein samanlaista kaavaa, joka sisältää neljä erilaista vaihetta.

1. Vaiheessa verkkorikollinen valmistelee hyökkäystä keräämällä kohteestaan mahdollisimman paljon tietoa. Tietoa kerätään suoraan kohteesta ja usein

myös isommasta kokonaisuudesta, johon kohde kuuluu, esimerkiksi harrastustoiminnan kautta.

2. Vaiheessa verkkorikollinen luo suhteen uhriin ja kasvattaa tämän luottamusta itseensä.
3. Vaiheessa suoritetaan hyökkäyksen varsinainen toimenpide, jossa uhri saadaan suorittamaan haluttu toiminto.
4. Viimeisessä vaiheessa irtaudutaan hyökkäyksestä, kun kohteen avulla on suoritettu halutut toimenpiteet ja päästy tavoitteeseen. (Kaspersky, n.d. a)

Ihmiset eivät usein ymmärrä, kuinka pienellä määrällä juuri oikeaa tietoa verkkorikollisten on mahdollista saavuttaa haluttu lopputulos, joka voi olla esimerkiksi pääsy haluttuun järjestelmään. Sosiaalinen manipulointi on hyökkääjille usein helpompi tapa saavuttaa haluttu tulos, kuin yrittämällä murtaa esimerkiksi kohteen käyttäjätunnuksia ja salasanoja muilla keinoilla. (Kaspersky, n.d. a)

4.1 Sosiaalisen manipuloinnin menetelmiä

Useimmat kyberhyökkäykset sisältävät sosiaalista manipulointia osana hyökkäystä (Kaspersky, n.d. a). Sosiaalista manipulointia voidaankin hyödyntää kaikissa kyberhyökkäyksissä, joissa ihmisen toiminta on jollain tavalla mukana (Impreva, n.d.). Verozon Data Breach Investigations Reporin (DBIR) mukaan 82 % kaikista kyberhyökkäyksistä sisälsi ihmisen vaikutuksen osana hyökkäystä. Ihmisen vaikutuksiin lukeutuvat virheet ja väärinkäytöt, mutta isoimpana yksittäisenä tekijänä on sosiaalinen manipulointi. (Verizon, 2022)

4.1.1 Tietojenkalastelu

Tietojenkalastelu on erittäin nopeasti kasvava verkkorikollisuuden muoto, joka luo ison uhan esimerkiksi identiteettivarkauksille. Vuonna 2020 raportoitiin kaksi kertaa enemmän tietojenkalasteluyrityksiä, kuin vuotta aikaisemmin. (Microsoft, 2021, s. 20)

Verkkorikolliset ovat myös tietojenkalastelussa siirtyneet tietojenkalastelu palveluna malliin (engl. phishing as a service), joka tarkoittaa sitä, että verkkorikollisten on mahdollista ostaa

valmiita tietojenkalastelu paketteja, joiden avulla heidän on mahdollista suorittaa halutut toimenpiteet. (ENISA, 2022)

Tietojenkalastelussa (engl. phishing) hyökkääjä tekeytyy luotettavaksi toimijaksi, kuten henkilöksi tai instituutioksi ja yrittää tällä tavoin saada uhrin luottamuksen. Tietojenkalastelu hyökkäykset kohdennetaan kahdella eri tavalla.

1. Tapana on joukkotietojenkalastelu, jossa tietojenkalastelu kohdennetaan isolle joukolle.

2. Tapana on kohdennettu tietojenkastelu (engl. spear-phishing), jossa tietojenkalasteluun käytetään henkilökohtaisia tietoja ja se kohdennetaan yksittäiseen henkilöön. (Kaspersky, n.d. a)

Tietojenkalasteluun käytetään useita erilaisia metodeja, joilla yritetään saada kohde luovuttamaan hyökkääjälle haluttuja tietoja tai vaihtoehtoisesti saada kohde lataamaan esimerkiksi haittaohjelma omalle laitteelleen. Yleisesti tunnettuja metodeja kalastelusähköpostien ja huijausverkkosivujen (engl. phishing webpages) lisäksi ovat huijauspuhelut (engl. vishing) ja huijausviestit (engl. smishing). (F-Secure, n.d.)

4.1.2 Syöttihuijaukset

Syöttihuijaukset (engl. bating) perustuvat ihmisten luonteeseen ja erityisesti uteliaisuuteen, jonka avulla kohde yritetään altistaa huijaukselle. Tyypillisesti syöttihuijauksissa tartutetaan kohteen laitteeseen haittaohjelma. Haittaohjelman tartuttaminen kohteen laitteelle tapahtuu esimerkiksi jättämällä haittaohjelman sisältävä muistitikku julkiselle paikalle, kuten parkkipaikalle kohteen auton lähettyville. Kohteen löytäessä muistitikun parkkipaikalta ja liittäessä sen omaan laitteeseen, haittaohjelma pääsee tarttumaan laitteen. (Kaspersky, n.d. a)

4.1.3 Verukkeenluominen

Verukkeenluominen (engl. pretexting) sosiaalisen manipuloinnin metodina on lähellä tietojenkalastelua. Tässä metodissa hyökkääjä esiintyy jonakin luotettavana toimijana ja

yrittää saada verukkeen avulla kohdettaan luovuttamaan esimerkiksi henkilötietojaan varmennusta varten. Metodia voidaan käyttää myös osana tietojenkalastelua. (imperva, n.d.) Tämä tapa edellyttää määrätietoista ja ennakoivaa otetta hyökkääjältä. (Kaspersky, n.d.)

4.2 Avointen lähteiden tiedustelu

Oikarinen (2020) kuvaa avointen lähteiden tiedustelua (engl. Open-source intelligence, OSINT) seuraavasti: ”Avointen lähteiden tiedustelu tarkoittaa tiedon keräämistä erilaisista julkisista lähteistä, niiden analysointia ja käyttöä tiedustelutarkoitukseen.” Tiedonlähteet voivat olla mitä vain, kunhan lähteet ovat julkisia. Julkisia tiedonlähteitä ovat esimerkiksi sosiaalinen media, televisio ja verkkosivut. (Oikarinen, 2020)

Kaikki se tieto mitä julkisissa lähteissä on saatavilla, on myös verkkorikollisten käytettävissä. Avointen lähteiden tiedustelu tekniikoita voidaan käyttää myös sosiaalisen manipuloinnin yhteydessä. Jokainen verkonkäyttäjä, joka tekee verkossa ostoksia ja käyttää esimerkiksi instagramia, jättää jälkeensä digitaalisen jalanjäljen. (Oikarinen, 2020). Tietoista digitaalisen jäljen jättämista kutsutaan aktiiviseksi digitaaliseksi jalanjäljeksi. Digitaalinen jalanjälki kasvaa monissa tapauksissa myös käyttäjän huomaamatta. Sovellukset voivat jakaa tietoja käyttäjien tietämättä ja verkkosivut seuraavat kävijöitänsä esimerkiksi evästeiden avulla. Käyttäjän tietämättä jättämää jälkeä kutsutaan passiiviseksi digitaaliseksi jalanjäljeksi. (Kaspersky, n.d. b)

Katsoessa Kuva 3 olevaa ajatuskarttaa ymmärtää, kuinka paljon erilaisia työvälineita ja lähteitä tiedonkeruuseen avoimista lähteistä löytyy ja kuinka paljon niiden avulla on mahdollista kerätä tietoa. Kuva 3 ajatuskartta on luotu yrityksiin kohdistuvan tiedon keruun näkökulmasta. Samat tiedonkeruun työvälineet ja lähteet ovat kuitenkin täysin sovellettavissa tiedonkeruuseen yksittäisitä henkilöistä esimerkiksi sosiaalista manipulointia varten. (Oikarinen, 2020).

Kuva 3 Ajatuskartta lähteistä ja välineistä (Oikarinen, 2020)

5 Verkkoon jakamisen vaikutus tietoturvaan ja yksityisyyteen

Jakaessaan itsestään tietoa, kuten esimerkiksi kuvia sosiaaliseen mediaan, tulisi käyttäjien arvioida toimiensa mahdollisia vaikutuksia myös tietoturvan näkökulmasta. Sosiaalisen median pääasiallisena tarkoituksena on jakaa kuvia ja tietoja itsestään, sekä kertoa muille omasta elämästään. Tästä johtuen tietoturvan huomioon ottaminen normaalilta vaikuttavien asioiden jakamisen yhteydessä voi tuntua jopa vainoharhaiselta tai asialta, joka ei kosketa yksittäisiä käyttäjiä. Liiallinen avoimuus ja ajattelematon henkilökohtaisten tietojen jakaminen saattaa kuitenkin aiheuttaa huomattavia tietoturva- ja turvallisuus riskejä (Microsoft, n.d. a). Jaettu tieto, kuten kuva voi sisältää itse kuvan lisäksi paljon muutakin dataa, kuin mistä käyttäjä on tietoinen (Oikarinen, 2020).

5.1 Sijainti

Sijainnin, kuten kotiosoitteen selvittäminen verkkoon jaetun henkilökohtaisen datan avulla onnistuu monilla erilaisilla keinoilla ja välineillä. Verkkorikollisilla on useita erilaisia syitä selvittää kohteen sijainti. Kohteen kotiosoite voi olla tärkeä palanen koottaessa tietoja esimerkiksi sosiaalista manipulointia varten. Oman osoitteen näkeminen tietojenkalasteluviestissä luo myös osaltaan luottamuksen tunnetta ja voi vaikuttaa päätökseen jatkaa viestissä kehotetulla tavalla.

5.1.1 Julkaisut paikkatietojen kanssa

Useissa sosiaalisen median palveluissa julkaisuja ja päivityksiä on mahdollista jakaa automaattisesti tarkan sijainnin kanssa. Sijainti voi olla päivityksessä näkyvänä paikkana, kuten lentokentän nimenä, josta kuva on otettu ennen matkaan lähtemistä. Sijainti voi vaihtoehtoisesti olla näkyvissä myös tarkkoina koordinaatteina paikasta, jossa kuva on otettu. Yksittäisten sosiaaliseen mediaan tai muualle verkkoon tehtyjen julkaisujen, kuten ravintolassa ruokakuvan jakaminen paikkatietojen kanssa ei vielä aiheuta suurta tietoturvariskiä tai ole uhka yksityisyydelle.

Usean sijainnin kanssa julkaistun päivityksen avulla on kuitenkin mahdollista rakentaa esimerkiksi niin sanottu lämpökartta alueesta, jossa päivityksiä on tehty (engl. heatmap).

Lämpökartalla paikat, joista tehdään usein päivityksiä, kuten koti ja esimerkiksi kuntosali näkyvät lämpöjälkinä kartassa. Julkaisujen perusteella tehdyn lämpökartan avulla voidaan siis päätellä esimerkiksi käyttäjän kotiosoite tai kuntosali, jota hän käyttää. Paikkatietoja sisältävien julkaisujen avulla tehtävään lämpökartan tekoon pelkän sosiaalisen median käyttäjänimen avulla löytyy verkosta helposti käytettäviä apuvälineitä. (Shubber, 2013)

Julkaisujen tekemistä tarkkojen sijaintitietojen kanssa tulisi välttää. Usein sijainti voi paljastaa tietoja, joita ei julkaisuvaiheessa osaa ajatella, kuten lomalle lähdettäessä tulevan loman lisäksi kertoo päivityksellä tyhjilleen jäävästä asunnosta. Useassa sosiaalisen median palvelussa julkaisujen paikkatiedot ovat automaattisesti pois päältä. Yksityisyysasetukset tulisi kuitenkin aina palvelua käyttöön otettaessa tarkistaa ja säätää itselle sopivaksi.

5.1.2 Sovellusten jakama sijaintitieto

Älykellojen ja sykemittareiden yleistyessä on treeneistä ja liikkumisen datasta tullut arkipäiväisempää ja helposti kerättävissä olevaa tietoa. Monella palveluntarjoajalla on sovellus tietojen keräämistä ja visualisointia varten. Sovelluksia voi yhdistää eri laitteisiin tai käyttää kännykän eri liikeantureita hyödyntäen. Sovelluksen avulla esimerkiksi omasta harjoittelusta kertynyttä tietoa pystyy seuraamaan ja tietoa on myös mahdollista jakaa muille. Käyttäjän jakaessaan lenkistään kertynyttä tietoa sosiaaliseen mediaan voi hän ajattelemattaan paljastaa myös tietoa, jota ei ollut tarkoitusta jakaa, kuten oman kotiosoitteensa. Kotiosoitteen jakaminen vahingossa lenkkireitin yhteydessä käy helposti ja huomaamatta tapauksissa, joissa kotiosoite on toiminut lenkin lähtö- ja paluupaikkana.

Käytössä olevat sovellukset keräävät ja analysoivat käyttäjistä kerättyä tietoa. Sovelluksen takana olevat yritykset voivat myös jakaa käyttäjistä kerättyä yksilöimätöntä tietoa verkkoon osana palvelua. Tämä mahdollistaa esimerkiksi omien suorituksien vertailua muihin käyttäjiin. Myös yksilöimätön data voi aiheuttaa tietoturva- ja turvallisuusriskejä rajatulle osalle käyttäjistä. Tästä esimerkkinä verkossa toimiva urheiluseuranta sovellus Strava, joka julkaisee käyttäjien sovellukseen tallennettujen suorituksiin perustuvia lämpökarttoja. Lämpökartta muodostuu alueista, joista sovelluksen käyttäjät ovat ladanneet omia tietoja urheilusuorituksestaan tai muuten käyttäneet sovellusta. Isossa mittakaavassa yksittäisiä käyttäjiä tai heidän reittejään on mahdotonta tunnistaa tai yksilöidä yksittäiseen käyttäjään

asti. Sovelluksen käyttäjistä kootun tiedon avulla luodun lämpökartan näyttäessä aktiviteetteja paikassa, jossa ei yleisen kartan mukaan ole kuin aavikkoa, herättää tämä lämpökarttaa tutkivien mielenkiinnon. Strava julkaisi julkaisemissaan lämpökartoissa tietoa, joka oli kerätty sotilastukikohdista sotilaiden sovellukseen tuottamasta datasta. Stravan tuottaman lämpökartan avulla pystyttiin päättelemään jopa salaisten tai väliaikaisten tukikohtien tarkkoja sijainteja. Sotilastukikohdat ovat usein yleisesti tunnettuja paikkoja, kuten tässäkin tapauksessa useimmat olivat, mutta lämpökartan avulla pystyttiin päättelemään tukikohtien eniten käytettyjä rakennuksia ja sotilaiden käyttämiä kulkureittejä. Tämä voi aiheuttaa riskejä eri maiden operaatioturvallisuudelle ja saattaa yksittäisiä sotilaita vaaraan. Kuva 4 näyttää lämpökarttakuvan sotilaiden liikkeistä, jotka ovat tallennettu sovellukseen ja julkaistu myöhemmin verkossa lämpökarttana. (BBC, 2018)

Kuva 4 Sotilaiden liikkeet Bagramin tukikohdassa Afganistanissa (BBC, 2018).

5.1.3 Sijainnin selvittäminen kuvien analysoinnilla

Sijainti voidaan joissakin tapauksissa määritellä myös pelkän kuvan ja sen sisältämien yksityiskohtien perusteella. Kuvan avulla tehtävään paikantunnistukseen on useita erilaisia tapoja ja monia erilaisia työkaluja. Tässä työssä käyn läpi yhden helposti jokaisen saatavilla olevan tavan. Kyseessä on käänteinen kuvanhaku, jonka tekemiseen on mahdollista käyttää

useita eri hakukoneita, kuten esimerkiksi Googlea. Käänteinen kuvanhaku on hakukoneella tehtävä haku, joka tehdään normaalisti hakukonetta käyttäen, mutta tekstin sijaan haetaan haluttua tietoa kuvan avulla. Kuvat jotka sisältävät paljon tunnistettavia yksityiskohtia, kuten rakennuksia ja muuta infrastruktuuria ovat helpommin tunnistettavissa pelkän käänteisen kuvanhaun avulla. Myös kohteet, joista on hakukoneen tietokannoissa valmiiksi paljon kuvia vertailuun haun kohteena olevan kuvaan, kuten nähtävyydet, ovat helpommin tunnistettavissa. Vähemmän yksityiskohtia sisältävän kuvan avulla sijainnin selvittäminen on vaikeaa ja monissa tapauksissa mahdotonta.

5.2 Kuvan analysointi

Käänteisellä kuvanhaulla pystytään joissakin tapauksissa selvittämään kohteen henkilöllisyys pelkän kuvan avulla. Käänteisessä kuvanhaussa hakukone vertailee haettua kuvaa tietokannoista löytyviin vastaavaisuuksiin, jolloin kohteesta on mahdollista löytää mm. sosiaalisen median profiileja tai vaikka lehtikuvia, jotka ovat julkaistu verkossa.

Kuvien avulla verkkorikollisten on mahdollista tehdä esimerkiksi profilointeja valituista kohteista tai valita halutun kaltaisia kohteita sosiaaliseen manipulointiin tai murtokohteiksi. Kokenut verkkorikollinen voi erilaisia kuvia yhdistelemällä ja niitä analysoimalla selvittää kohteestaan paljon erilaista tietoa. Sosiaalisen median ollessa täynnä erilaisia kuvia harrastuksista, lemmikeistä tai työpaikasta on verkkorikollisen helppo löytää sopivia aiheita kalasteluviesteihin tai aiheita, joilla lähestyä kohdetta sosiaalisen manipuloinnin yrityksellä.

Kuva omasta ajoneuvosta rekisterikilven kanssa voi myös altistaa erilaisille riskeille. Rekisterikilpi on autoa käyttäessä kaikkien nähtävissä ja kuskiin yhdistettävissä. Verkkoon jaettuna se luo kuitenkin erilaisia riskejä. Suomessa rekisterikilven perusteella tehtävällä haulla on mahdollista saada selville ajoneuvon omistajasta huomattavan paljon tietoa. Tiedot voivat sisältää esimerkiksi nimen, osoitteen ja rahoitusyhtiön, jos auto on ostettu rahoitusta käyttäen. Rekisterikilvestä saatujen tietojen avulla pysytään taas saamaan aiheita kalasteluviesteihin tai sosiaaliseen manipulointiin.

5.3 Metatiedot

Jaetut tiedot, kuten kuvat ja eri formaattia olevat tiedostot voivat sisältää huomattavasti enemmän tietoa, kuin mistä niiden julkaisija on itse tietoinen (Oikarinen, 2020). Suurin osa sosiaalisen median alustoista, kuten Facebook ja Instagram poistavat alustoillaan julkaisuista kuvista metadatan. Kaikki sosiaalisen median alustat eivät kuitenkaan poista alustalla julkaisujen kuvien metadataa, jolloin julkaisusta kuvasta voidaan selvittää useita erilaisia tietoja. Kuvien metadata voi sisältää tietoja esimerkiksi siitä milloin, millä ja missä kuva on otettu. Kuvien metadatan lukemiseen on useita erilaisia ilmaisia verkossa käytettäviä työkaluja, jotka ovat helposti kenen tahansa käytettävissä. Mökiltä lähetetty kesälomatervehdys kuvan kera voi siis paljastaa mökin tarkan sijainnin. Myös eri tiedostoformaatit, kuten pdf ja docx tiedostot sisältävät metatietoja. Tiedostojen sisältämät metatiedot voivat paljastaa tiedoston tekijästä lisätietoja, sekä tietoja tiedoston tekoon käytetyistä ohjelmista ja tekijän käyttöjärjestelmästä. Näiden tietojen avulla verkkorikollisten on mahdollista selvittää esimerkiksi erilaisten käyttöjärjestelmien ja ohjelmien tietoturva haavoittuvaisuuksia. Ne mahdollistavat erilaisia hyökkäystapoja, joilla voidaan hyökätä uhrin laitteelle.

5.4 Henkilökohtaisten tietojen jakaminen

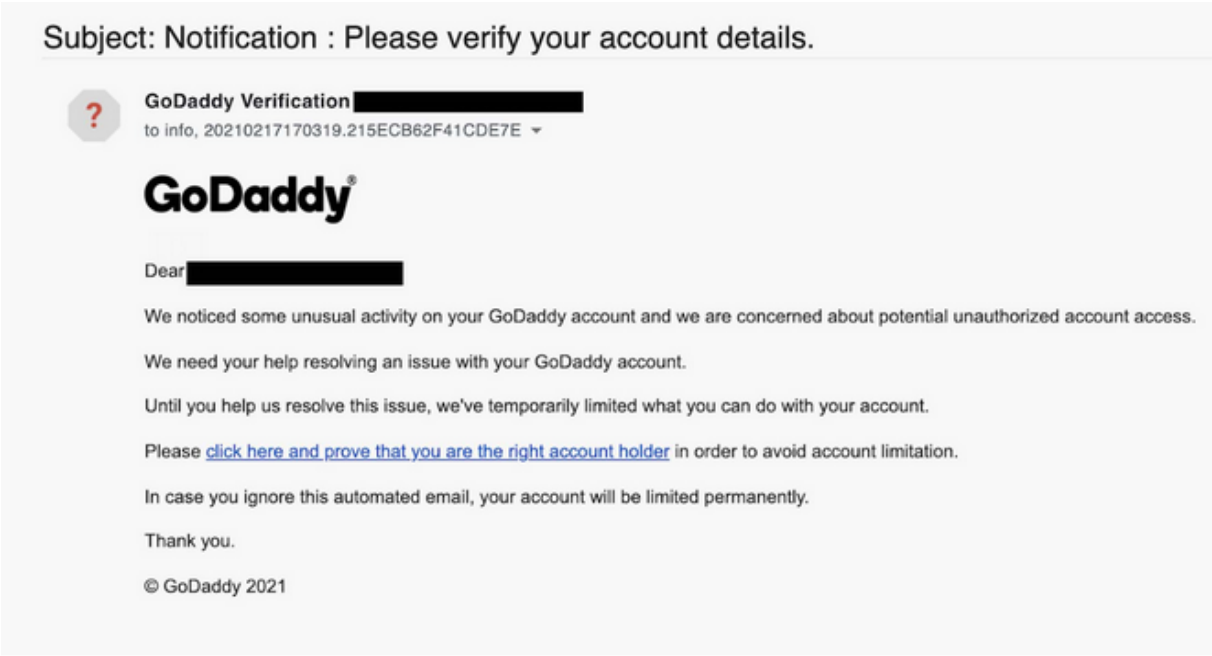
Mitä enemmän ja mitä henkilökohtaisempaa tietoa verkossa jakaa, sitä todennäköisempää on joutua identiteettivarkauden uhriksi. Tietoa voi jakaa tarkoituksella tietämättään sen joutuvan vääriin käsiin tai vääränlaiseen käyttöön. Kaikki jaettu tieto kasvattaa digitaalista jalanjälkeä, jonka avulla voidaan avoimen lähteiden tiedustelun metodeja käyttäen luoda laajoja profiileja yksittäisitä henkilöistä tai organisaatioista. Luotuja profiileja voidaan käyttää avuksi esimerkiksi sosiaaliseen manipulointiin. Kun kohteesta on käytettävissä paljon erilaista tietoa, on häntä helpompi lähestyä ja luoda onnistunut yhteys. Yleensä kohteen luottamus on helpompi saada, kun taustatietoa on riittävästi. Laaja tietämys kohteesta helpottaa myös sisällön luomista esimerkiksi kohdennettuun tietojenkalasteluun.

5.5 Viestit

Sähköpostiin tai muihin viesti palveluihin saapuvat kalasteluviestit voivat olla parhaimmillaan vaikeasti erotettavista asiallisista lähestymisistä. Viestin tullessa arveluttavalta tai vieraalta taholta on viestin luotettavuudesta varmennuttava ennen muita toimia, kuten painamista viestin mahdollisesti sisältämää linkkiä. Kohdennettu tietojenkalasteluyritys voi olla seurausta verkkorikollisen avoimista lähteistä kerätyistä tiedoista koottua kokonaisuutta, jonka avulla verkkorikollinen osaa kohdentaa tietynlaista sisältöä valitsemalleen kohteelleen.

Kuva 5 on aito esimerkki sähköpostilla tapahtuneesta kohdennetusta tietojenkalasteluyrityksestä. Tietojenkalasteluyritys on tehty GoDaddyn nimissä. GoDaddy on maailman suurin verkkotunnusrekisteriyritys. Kyseisessä tietojenkalasteluviestissä tavoitellaan uhrin GoDaddy palvelun käyttäjätunnuksia ja salasanaa. Klikkaamalla tietojenkalasteluviestissä olevaa linkkiä, johdattaa se uhrin väärennetylle GoDaddyn kirjautumissivulle. Kirjauduttaessa palveluun väärennetyn sivun kautta saa verkkorikollinen haltuunsa kirjautujan käyttäjätunnuksen ja salasanan. Saaduilla tiedoilla verkkorikollinen pystyy kirjautumaan kohteen nimissä GoDaddyn palveluun. (Rosenthal, 2021)

Kuva 5 Kohdennettu kalastelusähköposti (Rosenthal, 2021)



Sähköpostiviestin luotettavuutta arvioidessa tulee kiinnittää huomiota muutamiin eri asioihin. Ensimmäisenä huomio tulee kiinnittää saapuneen viestin sähköpostiosoitteeseen. Osoitetta arvioidessa tulee kiinnittää huomiota osoitteen loppuosan verkkotunnukseen, eli onko osoite muotoa esimerkki@yritys.fi vai huono.esimerkki@muuta.net. Ensimmäinen vaihtoehto on yksi indikaattori luotettavasta osoitteesta, yritykset käyttävät pääsääntöisesti @yrityksennimi verkkotunnusteisia sähköposteja. Toinen vaihtoehto antaa syytä epäilyille. Verkkorikolliset voivat myös lähestyä melko aidon näköisillä osoitteilla, jotka ovat todella lähellä yrityksien käyttämiä osoitteita, esimerkiksi esimerkki@yr1tys.fi. Luotettavat ja isot organisaatiot eivät myöskään lähesty asiakkaitaan @gmail.com tai muilla samankaltaisilla julkisilla sähköpostin verkkotunnuksilla. (Microsoft, n.d. b) Poikkeuksena voivat olla pienet paikalliset yritykset.

Sähköpostiviestin luotettavuutta arvioidessa tulee myös kiinnittää huomiota viestin sisältöön ja sen kielioppiin. Isoilla organisaatioilla on ammattilaisia tekemässä ja tuottamassa sisältöä, jolloin viestit ovat kieliopillisesti oikein. Kalasteluviestin sisältö taas voi olla esimerkiksi sovelluksella tehty käännös toisesta kielestä ja sisältää paljon kirjoitusvirheitä. (Microsoft, n.d. b)

Viestin sisältöä arvioidessa tulee huomiota kiinnittää myös siihen, mitä viestissä pyydetään tekemään. Tietojenkalasteluviestit voivat vedota myös toiminnan kiireellisyyteen, jos kohde ei toimi heti seuraa siitä rangaistus. Kiireen tai sen tunteen luomisella kohde yritetään saada suorittamaan haluttu toimenpide harkitsemattomasti. (Microsoft, n.d. b)

Tietojenkalasteluviestit sisältävät yleensä pyynnön suoritettavasta toimenpiteestä, useimmiten toimenpide pitäisi suorittaa viestissä olevan linkin kautta. Suomalaiset pankit tai viranomaiset eivät pyydä kirjautumaan palveluihinsa yllättäen sähköposti- tai muulla viestillä (Handelsbanken, n.d.). Varmin tapa on kirjautua palveluun muuta kautta kuin viestissä olevasta linkistä, jos epäilee linkin ohjaavan muualle, kuin viestissä sen sanotaan ohjaavan. Viestin luotettavuutta arvioidessa tulisi kiinnittää huomiota viestin sisältämään linkkiin ja siihen, mihin se johtaa. Hyperlinkki, jossa on oikean näköinen verkko-osoite voi tosiasiassa ohjata painalluksesta johonkin muuhun, kuin tekstin osoittamalle sivustolle. Hyperlinkin todellisen osoitteen saa tietokoneella selville esimerkiksi laittamalla hiirenkursorin hyperlinkin päälle ja odottamalla hetken. Android puhelimessa linkin osoitteen saa esiin

painamalla linkkiä pohjassa. Kuva 6 on esimerkki hyperlinkistä, joka johtaa eri sivustolle mitä teksti antaa ymmärtää. Oikeassa yläkulmassa oleva osoite näyttää verkkosivun, johon hyperlinkkiä painamalla päätyy.

Kuva 6 Esimerkki hyperlinkistä, jossa teksti on eri kuin sisältö

5.6 Keskustelut

Verkossa keskustelu tapahtuu, joko omalla nimellä tai nimimerkillä, jolloin keskustelua voidaan käydä anonyyminä. Verkon keskustelupalstoilla tai sosiaalisessa mediassa omalla nimellään keskusteltaessa voidaan keskustelut hakea ja yhdistää keskustelijoihin myös usean vuoden jälkeen. Keskusteluja on myös helppo irrottaa asiayhteyksistään, jolloin niiden avulla pystytään luomaan negatiivisia näkökulmia alkuperäisestä yhteydestä huolimatta. Ihmiset myös ymmärtävät asioita omista näkökulmistaan, jolloin hyvässäkin tahdossa käyty keskustelu voi aiheuttaa erilaisia reaktioita ja näyttäytyä ulkopuolisesta erilaiselta kuin keskustelussa on tarkoitus. Edellä mainittujen seikkojen vuoksi vanhat keskustelut voivat vaikuttaa tulevaisuudessa esimerkiksi työnhakuun.

Keskustelujen osapuolet eivät aina ole keitä he väittävät olevansa. Valeprofiilien avulla verkkorikolliset pystyvät keskustelualustoilla tai sosiaalisessa mediassa kalastelemaan tietoja esiintymällä luotettavana henkilönä. Sosiaalisen manipuloinnin apukeinona käytetään usein valeprofiileja, joita erilaisiin palveluihin on erittäin helppo luoda. Valeprofiileja voi myös olla

todella vaikea havaita tai erottaa aidosta. Verkossa tapahtuviin keskusteluihin valeprofiileilla osallistuvilla voi päätarkoituksena olla myös muiden käyttäjien häiriköinti.

Romanssihuijaus on esimerkki sosiaalista manipulaatiota hyväkseen käyttävästä verkon keskustelualustoilla tapahtuvasta huijauksesta. Tämä huijausmuoto perustuu luottamuksen luomiseen huijarin ja kohteen välillä. Luottamuksen luominen tapahtuu erilaisin sosiaalisen manipuloinnin apukeinoin ja nojautuu suuresti kohteen haluun löytää esimerkiksi elämänkumppani (Rikosuhripäivystys, n.d.). Romanssihuijauksissa huijarin tavoitteena on usein saada kohde siirtämään rahaa omille tileilleen, jonkin keksityn verukkeen avulla. Veruke voi olla mitä tahansa, mutta liittyy monissa tapauksissa jollakin tavoin yhteisen elämän aloittamiseen. Romanssihuijaukset voivat olla usein ainakin alkuun vaikeasti erotettavissa oikeista lähestymisistä esimerkiksi erilaisissa seuranhakupalveluissa. Rahan pyyntöä voi edeltää usean kuukauden mittainen viestittely, jossa on rakennettu luottamusta uhrin ja huijarin välillä. Romanssihuijauksen uhriksi voi joutua ketä tahansa ikään tai sukupuoleen katsomatta. Suurin osa uhreista on kuitenkin keski-ikäisiä naisia. Huijarit valitsevat ikääntyneimpiä uhreja, koska heillä on todennäköisemmin kertynyt enemmän varallisuutta (Kaspersky, n.d. c).

Verkossa tapahtuviin romanssihuijauksiin, sekä muihin samankaltaisiin huijauksiin ja niiden estämiseen liittyen tulisi muistaa muutamia asioita. Älä tee seuraavia asioita, jollet ole varma henkilön oikeasta henkilöllisyydestä:

1. Lähetä rahaa
2. Luovuta omia henkilötietoja
3. Jaa materiaalia, jota voidaan käyttää myöhemmin sinua vastaan, esimerkiksi kiristämiseen.

Romanssihuijauksen ja muiden samankaltaisten hujausten tunnistamisen helpottamiseksi tulisi kiinnittää huomioita erilaisiin tunnettuihin vaaran merkkeihin. Usein huijari asuu kohteestaan kaukana ja hänen tarinansa kuulostaa uskomattomalta ja on epäjohdonmukainen. Profiilissa tai viesteissä käytetyt kuvat voivat olla mallikuvan kaltaisia kuvia. Kuvan aitouden selvittämiseksi on mahdollista tehdä esimerkiksi käänteinen kuvan haku, jonka avulla selviää löytyykö verkosta samanlaista kuvaa käytettynä muissa

yhteyksissä. Myös viesteissä käytettyä tekstiä on voitu kopioida muualta. Viesteissä käytettyä tekstiä on myös mahdollista hakea hakukoneilla ja katsoa löytyykö vastaava tekstiä muista lähteistä. Huijauksissa keskustelu muuttuu myös usein nopeasti vakavaksi ja keskustelun yhteydessä huijari yrittää saada kohteeltaan mahdollisimman paljon tietoa. Keskustelussa aikaisemmin saatua tietoa voidaan myöhemmissä vaiheissa käyttää hyödyksi kohdetta manipuloidessa. (Kaspersky, n.d. c)

Huijausyritysten uhriksi jouduttaessa, on hyvä pitää mielessä vanha sääntö: asia, joka kuulostaa liian hyvältä ollakseen totta, ei yleensä ole totta.

6 Johtopäätökset ja pohdinta

Opinnäytetyötä tehdessä olen ymmärtänyt, kuinka ilmeisiä tietoturvariskit voivat olla, kun niitä ajattelee tarkemmin. Silti käyttäjät luovat niitä itse helposti ajattelemattomuuttaan ja huolimattomuuttaan. Nykypäivänä esimerkiksi puhelimen kamera ja verkkoyhteys mahdollistavat jokaisessa tilanteessa kaikkien tapahtumien jakamisen. Ihmisten olisi tärkeää hetkeksi pysähtyä miettimään miksi jaan tätä tietoa ja voiko sitä esimerkiksi myöhemmin käyttää minua vastaan. Tietoturvariskien lisäksi tulisi muistaa, että verkkoon julkaistaessa kantaa julkaisija vastuun myös mahdollisista rikosoikeudellisista seuraamuksista.

Opinnäytetyöprosessi eteni nopeaa vauhtia. Minulla oli hieman yllättäen kiireinen aikataulu, mutta kun pääsin aloittamaan työn, se valmistui yllättävän helposti. Valitsemani aihe oli itselleni kiinnostava ja sen vuoksi tein työtä mielelläni. Tutkimuskysymyksiä miettiessä, valitsin sellaiset aiheet, joista ajattelin isommankin yleisön olevan kiinnostunut. Mielestäni työ vastaa kaikkiin neljään esitettyyn kysymykseen hyvin. Teoriapohjan etsiminen vaati minulta eniten aikaa, sillä lähteiden luotettavuutta täytyi arvioida koko ajan. Tietoa oli kuitenkin suhteellisen helposti löydettävissä, mutta sen yhdistelyyn järkeväksi kokonaisuudeksi käytin eniten aikaa. Ajoittain joidenkin otsikoiden alle oli vaikea keksiä punaista lankaa, joka johdattaisi lukijan sujuvasti ja johdonmukaisesti asiasta toiseen. Toisaalta prosessin aikana olen oppinut arvioimaan omaa tekstiäni kriittisesti ja ymmärtänyt, että opinnäytetyötä tehdessä on tärkeää välillä pysähtyä miettimään mitä ja miksi tekee jotakin asiaa. Tärkeää oli myös pitää mielessä aiheen rajaus, jotta työ ei kasva liian isoksi tai jätä vastaamatta tutkimuskysymyksiin.

Mielestäni onnistunein osuus opinnäytetyössäni on kappale viisi: ”verkkoon jakamisen vaikutus tietoturvaan ja yksityisyyteen”. Siinä lukija pääsee tutustumaan melko syvällisesti aihepiiriin, mutta kuitenkin niin, että asia on helposti ymmärrettävää. Mielestäni löysin myös kappaleeseen hyviä esimerkkejä aiheesta. Vaikeinta työssä oli omalle tekstille sokeutuminen. Jos minulla olisi ollut aikaa rajattomasti tehdä työtä, olisin varmasti pystynyt tuottamaan laajempaa sisältöä ja toisaalta myös hienosäätämään työn joitakin osioita. Toisaalta koen, että olen tehnyt tässä ajassa laadullisesti ja laajuudeltaan hyvän opinnäytetyön ja pystyin tuottamaan luotettavaa tietoa.

Opinnäytetyöni on ajankohtainen aihe, joka koskettaa suurta osaa ihmisistä. Tietoturvan ajankohtaisuus tuskin tulee enää koskaan vähentymään, sillä esimerkiksi erilaiset älylaitteet ja ratkaisut lisääntyvät koko ajan. Niissä voi olla haavoittuvuuksia ja ne voivat helposti unohtua huomioimatta käyttäjiltä, sillä esimerkiksi kodin älylaitteita ajatellaan usein enemmän mahdollisuutena kuin uhkana.

Opinnäytetyön teoriaa kerätessä tallensin hyviä lähteitä itselleni ylös ja tiedonhaun jälkeen vertailin lähteiden tietoja ja luotettavuutta. Ajan puutteen vuoksi kirjalähteiden käyttö jäi vähäiseksi ja mikäli aikaa olisi ollut enemmän, olisin niistä saanut vielä lisäarvoa opinnäytetyölleni. Tiedon hakeminen itsessään oli helppoa ja hakukoneiden käyttäminen ongelmatonta.

Osa opinnäytetyön prosessia on arvioida työn luotettavuutta. Tässä opinnäytetyössä esitetty tieto on oikeaa ja yleistettävää. Työ on tehty johdonmukaisesti, niin että esimerkiksi tietoa on kerätty ja säilytetty oikein. Tietoperustan pohjalta on kuvattu omin sanoin tietoturvaan liittyviä asioita ja ilmiöitä. Lähteiden luotettavuutta lisää se, että mukana on kansainvälisiä lähteitä ja useasta eri lähteestä löytyi samankaltaista tietoa. Lisäksi työn lopussa esitettävät johtopäätökset ovat päteviä ja esittävät mahdollisia kehittämisideoita.

Tietoturva lähtee jokaisesta itsestään ja siihen voidaan vaikuttaa kouluttamalla ja valistamalla ihmisiä. Pelkkien riskien esille tuomien tai kiellettyjen ja sallittujen toimien kertominen ei riitä tietoturvatietoisuuden lisääntymiseen. Riskien toteutumisen muodot muuntautuvat ja kehittyvät koko ajan, mutta ilmiöt riskien takana pysyvät samoina. Kun ilmiöistä tehdään tunnettuja, pystytään niihin liittyviä riskejä tunnistamaan paremmin.

Jatkosuunnitelmat opinnäytetyön käyttöön liittyvät koulutusmateriaalin kehittämiseen. Opinnäytetyötä on mahdollista käyttää opetusmateriaalin pohjana. Aiheena tietoturva on laaja ja mahdollisuuksia laajentaa isompiin opetuskokonaisuuksiin on useita. Tietoturvaan liittyvät uhat voivat pahimmillaan vaikuttaa suuresti ihmisten elämään, esim. identiteetti varkauksien kautta ja tämän vuoksi asiaan pitäisi suhtautua sen tarvitsemalla vakavuudella. Mikäli halutaan tavoittaa laaja joukko ihmisiä, olisi tietoturvan opetus hyvä tapahtua jo varhaisessa vaiheessa perusopetusta. Näin kaikki saisivat saman sisältöistä ja oikeaa tietoa asiasta. Pitkässä juoksussa nuorten tietoisuus tietoturvasta kasvaa ja he pystyvät auttamaan

myös esimerkiksi omia vanhempiaan asiassa. Pienemmässä mittakaavassa ajatellen voisin kuvitella kehittäväni itseäni aiheen parissa vielä enemmän, kuten tietoturva asiantuntijaksi ja mahdollisesti toimia kouluttajana asian tiimoilta.

Johtopäätöksenä voidaan todeta, että tietoturvaan liittyvät asiat ovat usein ilmeisiä, mutta ne voivat jäädä helposti huomioimatta. Lisäksi voidaan ajatella, että nykyihmisen tulisi laitteen käyttöoppaan lisäksi tutustua yhtä lailla tietoturvan perusteisiin. Uusia ohjelmia ja sovelluksia käyttöön otettaessa tulisi aina tutustua myös niiden yksityisyysasetuksiin. Näin varmistetaan omien tietojen pysyminen omassa hallinnassa. Ihmisten tietoisuus tietoturvasta lisääntyy niin kouluttautumisen, mutta myös esimerkiksi juuri sosiaalisen median ja uutisten kautta.

7 Yhteenveto

Opinnäytetyössä pyrittiin tuomaan esille verkkoon jaettujen henkilökohtaisten tietojen luomia riskejä ja ilmiöitä niiden takana. Ilmiön taustan ymmärtäminen esimerkiksi sosiaalisessa manipuloinnissa tuo mielestäni kokonaisvaltaisemman ja helpommin ymmärrettävän, sekä hyväksyttävän kuvan riskeistä. Työssä esiintyvät esimerkit tekevät riskeistä helpommin tunnistettavia ja tuovat ne lähemmäs käyttäjiä.

Mielestäni opinnäytetyössä esitettyihin neljään tutkimuskysymykseen vastattiin. Vastaukset ovat työn sisällöstä helposti löydettävissä ja niihin on vastattu kattavasti. Kysymysten asettelu oli mielestäni sellainen, että opinnäytetyötä tehdessäni minun ei kertaakaan tarvinnut palata kysymysten pariin, vaan työ vastasi automaattisesti asetettuihin kysymyksiin.

Opinnäytetyön aihepiiri on minulle entuudestaan tuttu omien opintojeni, sekä oman kiinnostukseni kautta. Opinnäytetyön aiheen tunteminen entuudestaan antoi mielestäni hyvät lähtökohdat opinnäytetyön tekemiseen. Työn edetessä ja lähdemateriaalia etsiessä tietoni aiheesta lisääntyi ja opin paljon uutta.

Jatkossa valmistunutta opinnäytetyötä on mahdollista käyttää materiaalina tietoturvakoulutuksissa ja erilaisissa valistuksissa. Työn avulla on helppo käydä yleistajuisesti läpi käyttäjän itsensä luomia tietoturvariskejä.

Lähteet

Australian Cyber Security Centre. (2020). *Personal information and privacy*. https://www.cyber.gov.au/acsc/view-all-content/advice/personal-information-and-privacy

BBC. (29.1.2018). *Fitness app Strava lights up staff at military bases.* https://www.bbc.com/news/technology-42853072

BBC. (29.1.2018). *Fitness app Strava lights up staff at military bases.* [kuva] https://www.bbc.com/news/technology-42853072

Bridges, J. (22.11.2021). *TOP 10 reasons to keep your personal information private.* Reputation Defender. *https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private*

European Union Agency for Cybersecurity (ENISA). (2022). *Threat landscape 2022.* ENISA

F-Secure. (n.d.). *Mitä on tietojenkalastelu?* https://www.f-secure.com/fi/home/articles/what-is-phishing

Handelsbanken. (n.d.). *Huijareita liikkeella.* https://www.handelsbanken.fi/fi/henkiloasiakkaat/mobiili-ja-verkko/turvallisuus/huijaukset

Imperva. (n.d.). *Pretexting.* https://www.imperva.com/learn/application-security/pretexting/

Imperva. (n.d.). *Social Engineering.* https://www.imperva.com/learn/application-security/social-engineering-attack/

Kaspersky. (n.d. a). *What is Social Engineering?* https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kaspersky. (n.d. b) *What is digital footprint? And how to protect it from hackers.* *https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint*

Kaspersky. (n.d. c.). *Verkkodeittailuhuijaukset ja kuinka voit välttää ne.* https://www.kaspersky.fi/resource-center/threats/beware-online-dating-scams

Kyberturvallisuuskeskus. (2020). *Näin pidät huolta tietoturvasta kotona ja työpaikalla.* *https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla?toggle=Sosiaalinen%20vaikuttaminen*

Microsoft. (2021). *Digital Defence Report.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Microsoft. (2021). *Digital Defence Report.* [kuva] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Microsoft. (n.d. a). *The dangers of oversharing.* https://support.microsoft.com/en-us/topic/the-dangers-of-oversharing-79330a32-4ee1-433a-812e-fe4bb3d34511

Microsoft. (n.d. b). *Protect yourself from phishing.* https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Oikarinen, A. (8.4.2020) *Open-source intelligence – it's incredible what you can find from public sources.* Nixu cybersecurity. https://www.nixu.com/fi/node/1933

Oikarinen, A. (8.4.2020) *Open-source intelligence – it's incredible what you can find from public sources.* [kuva] Nixu cybersecurity. https://www.nixu.com/fi/node/1933

Patel, D. (19.5.2020). *The dangers of sharing personal information on social media.* Penn Today. https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media

Rikosuhripäivystys. (n.d.). *Rakkauspetokset ja romanssihuijaukset verkossa.* https://www.riku.fi/erilaisia-rikoksia/rakkauspetokset-verkossa/

Rosenthal, M. (4.3.2021). *Real Spear Phising Examples and Why They Worked.* Tessian. https://www.tessian.com/blog/5-real-world-examples-of-phishing-attacks/

Rosenthal, M. (4.3.2021). *Real Spear Phising Examples and Why They Worked.* [kuva] Tessian. https://www.tessian.com/blog/5-real-world-examples-of-phishing-attacks/

Social Engineer LLC. (n.d.). *What is Social Engineering?. https://www.social-engineer.org/about/*

Shubber, K. (4.9.2013). *Mapping websites reveal just how stupid it is to geotag your tweets.* Wired. https://www.wired.co.uk/article/twitter-geotagging

Verizon. (2022). *2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/*

Liite 1: Aineistonhallintasuunnitelma

Opinnäytetyön tietopohjassa käytetty aineisto merkitään lähdeluetteloon. Lähdeluettelossa lähteet on merkattu asianmukaisesti ja täsmällisesti niin, että ne ovat kaikille saatavilla.

Opinnäytetyössä käytetyt kuvat ovat ei-kaupallisessa käytössä ja tieteellisessä tekstissä niitä voidaan käyttää, mikäli lähdeviitteet ovat asianmukaiset. Työ sisältää myös itse tehtyjä kuvia.

Opinnäytetyötä ja varmuuskopioita säilytetään omalla koneella vuosi työn valmistumisesta. Opinnäytetyö ei sisällä salassa pidettäviä tietoja.

Opinnäytetyö julkaistaan Theseus-palvelussa.