Tuija Huusko

IDENTITEETIN VARASTAMINEN SOSIAALISEN MEDIAN PALVELUISSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Huusko, Tuija
Identiteetin varastaminen sosiaalisen median palveluissa
Jyväskylä: Jyväskylän yliopisto, 2015, 81 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Veijalainen, Jari

Identiteettivarkaus ja tietojen kalastelu ovat tätä päivää ja ne kasvavat jatkuvasti. Kohteena voi olla yksilö tai yhteisö, tuttu tai tuntematon, mutta yhteistä tapauksissa on se, että rikoksella voi olla kauaskantoiset seuraukset uhrin elämässä puhumattakaan taloudellisista menetyksistä. Sosiaalisen median palvelut tuovat tähän oman lisänsä, onhan rekisteröityneitä käyttäjä miljardeja. Tämän tutkielman tarkoituksena on selvittää identiteettivarkauden ja sosiaalisen median välistä yhteyttä ja miten sosiaalisen median palveluita hyödynnetään rikoksissa. Identiteettivarkaus ei vielä ole Suomessa rikos, mutta väärällä identiteetillä voi tehdä myös rikosoikeudellisesti rangaistavia tekoja. Tutkimus on toteutettu teoriaa testaavalla menetelmällä, jossa tutkitaan, miten kirjallisuuden antama kuva vastaa käytännön tilanteisiin. Tutkimus osoitti muun muassa, että Facebookia ja Twitteriä käytetään rikoksissa, mutta joukkoon mahtuu myös muita palveluja. Palveluissa huijausprofiilien luominen on helppoa eikä vaadi teknistä osaamista. Käytännön tapauksia tutkiessa havaittiin, että tekijät hyödyntävät juuri näitä helppoa keinoja, kuten väärällä nimellä tehtyjä profiileita. Luottamus uhrin ja tekijän välillä on myös tärkeässä osassa, joskin sen rooli vaihteli tapauksesta riippuen. Sosiaalinen media rikosympäristönä antaa omanlaisensa haasteen myös tutkintaan, sillä palveluntarjoajien palvelimet sijaitsevat tyypillisesti ulkomailla. Tutkimus tarjoaa katsauksen nykyisiin yleisiin ja tunnettuihin tietojen kalastelumenetelmiin ja identiteettivarkauteen. Tutkimuksessa myös kuvataan, millaisia rikoksia Suomessa on toisen henkilön identiteetin turvin tehty.

Asiasanat: digitaalinen identiteetti, Facebook, identiteettivarkaus, kunnianloukkaus, maksuvälinepetos, petos, sosiaalinen media, Twitter

ABSTRACT

Huusko, Tuija
Identity theft on social media services
Jyväskylä: University of Jyväskylä, 2015, 81 p.
Information Systems, Master's Thesis
Supervisor: Veijalainen, Jari

The purpose of this thesis is to examine the connection between identity theft and social media and how the social media services are exploited by the criminals. There are billions of users on social media services so the threat really exists. Identity theft is not criminalised yet in Finland, but by using another person's name a person can commit other acts that are punishable like fraud and defamation. Methodically, the research applies theory-testing. The writer examines how the theory meets the real life cases. The research points that crimes can be committed on Facebook and Twitter but there are also other social media services that are exploited. Creating a fake profile is easy and does not require technical skills. Criminals exploit easy methods to phish and steal a victim's identity. The social media as a crime scene is a challenge for criminal investigation, because the servers running the services are often located in countries other than where the victim and perpetrator reside. This research gives a review to common and well-known phishing methods. The research also describes what kinds of acts have been committed under another person's name in Finland.

Keywords: defamation, digital identity, Facebook, fraud, identity theft, means of payment fraud, social media, Twitter

KIITOKSET

Tutkielman kirjoittaminen on ollut monivaiheinen prosessi. Olin onnekkaassa asemassa, sillä tutkielman kirjoittamisen alkamisen aikoihin pääsin tekemään tutkimustyötä saman aiheen parissa Victim Support for Identity Theft -projektissa (VISIT-projekti), jossa tutkitaan identiteettivarkauksia ja niiden ehkäisemistä. Työskentely toi rutiinia myös tutkielman kirjoittamiseen ja tarjosi monipuolisia näkökulmia, joita en ehkä itse olisi välttämättä huomannut. Haluankin lämpimästi kiittää VISIT-projektia ja ohjaajaani Jari Veijalaista mahdollisuudesta työskennellä projektissa.

Tietoturvallisuus ja kyberrikollisuus ovat kiinnostaneet minua jo pitkään. Tein myös kandidaatintutkielmani aiheesta ja halusin jatkaa sitä myös pro gradu -tutkielmassanikin. Äskeiseen viitaten, olin iloinen mahdollisuudesta saada tehdä työtä itseä kiinnostavan aiheen parissa. Kirjoittaminen ei tuntunut niin työläältä, sillä projektin ansiosta sain tehtyä kaksi asiaa samaan aikaan.

Haasteita kohtasin siinä vaiheessa, kun aloin etsiä materiaalia empiirisen osan tueksi. Yhtäkkiä perinteinen Internet ja Google eivät tarjonneetkaan vastauksia, sillä suurin osa oikeustapauksista ei ole siellä saatavilla. Useat käräjäoikeudet joutuivat kysymysteni alle, kun yritin etsiä materiaalia. Tiesin jo ennalta, että tapauksia ei helposti löytyisi, sillä identiteettivarkaus ei vielä ole rikos, eikä siten sillä nimellä voisi tietokannoista hakea. Lopulta kuitenkin tapauksia löytyi ja pääsin etenemään.

Lisäksi haluan kiittää perhettäni ja ystäviäni henkisestä tuesta ja neuvoista tutkielmaani koskien. Kannustus ja motivointi olivat tervetulleita siinä vaiheessa, kun itsellä välillä usko onnistumiseen hiipui. Kaikkien tässä mainittujen henkilöiden ja tahojen avustuksella tutkielma kuitenkin valmistui, ja taas on yksi etappi elämässä saavutettuna. Nyt voin hyvillä mielin jatkaa kohti tulevia haasteita ja toivottavasti itselle tärkeän aiheen parissa.

ACKNOWLEDGEMENTS

This research was partly supported by the European Union under the grant number DG3. I would like to thank my supervisor Jari Veijalainen for a chance to work in a project called Victim Support for Identity Theft (Project number HOME/2013/ISEC/AG/FINEC/4000005189). It helped me write my thesis and also understand the subject more extensively. Thank you!

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Sosiaalinen media on käsite, joka synnyttää lähes jokaisessa kehittyneen maailman kansalaisessa jonkinlaisen mielikuvan. Toiselle tulee mieleen Facebook tilapäivityksineen ja kuvineen, toinen liittää sen LinkedIniin, joka kokoaa yhteen työelämän ammattilaiset ja asiantuntijat. Kolmas kirjoittaa blogia ja jakaa kuvia elämästään Instagramissa. Osa palveluista on siten suunnattu selkeästi tietylle käyttäjäryhmälle tai tarkoitukseen. Palveluiden kirjo on valtava, mutta keskeistä edellä mainituissa ja monissa muissa sosiaalisen median palveluissa on käyttäjien välinen kommunikointi ja yhteistyö. Kaplanin ja Haenleinin (2010) mukaan käyttäjät eivät ole pelkästään tiedon vastaanottajia, vaan he tuottavat itse sisällön. Tämä on olennainen piirre sosiaalisessa mediassa. Kansalaisyhteiskunnan tutkimusportaalin (2014) mukaan palveluiden käyttäjä voi kommentoida, jakaa materiaalia, verkostoitua ja olla vuorovaikutuksessa muiden käyttäjien kanssa. Tämä erottaa sosiaalisen median perinteisestä mediasta, jossa käyttäjät yleensä vain vastaanottavat sisällön sellaisenaan.

Tänä päivänä suuri osa ihmisistä on rekisteröitynyt vähintään yhden sosiaalisen median palvelun käyttäjäksi. Palveluiden kautta pidetään yhteyttä ystäviin, tutustutaan uusiin ihmisiin, etsitään töitä ja tuodaan omaa ammatillista osaamista esille. Lista voisi jatkua loputtomiin. Sosiaalisen median palveluita voidaan pitää eräänlaisena jatkumona fyysiselle elämälle ja sen suhteille (de Paula, 2010). Sen lisäksi että palveluiden kautta on kätevä pitää yhteyttä tuttaviin, käyttäjä usein jakaa käyttäjätilinsä kautta tietoa ja kuvia esimerkiksi itsestään, taustastaan, suhteistaan, koulutuksestaan ja mielenkiinnonkohteistaan (Devmane & Rana, 2014).

Kuitenkin siellä missä on ihmisiä, on myös rikollisuutta. Ihmisten siirtyessä Internetiin siirtyvät sinne myös tietojen kalastelijat, hakkerit ja muut kriminaalit. Normaalisti ihminen pitää hyvää huolta passistaan, luottokorttinumeroistaan ja muista henkilökohtaisista tiedoistaan, mutta sosiaalisen median palveluissa yksityisyyttä ei pidetä niin tärkeänä. Vain pieni osa käyttäjistä pitää profiilinsa näkyvyyden täysin rajoitettuna (Devmane & Rana, 2014). Toisaalta Lawler ja Molluzzo (2010) havaitsivat tutkimuksessaan koskien opiskelijoiden tietoutta yksityisyydestä sosiaalisessa mediassa, että yli puolet opiskelijoista

rajoittaa tietojensa näkymistä. Okunon, Ichinon, Kuboyaman ja Yoshiuran (2011) mukaan japanilaisessa Mixi-palvelussa 60 % nuorista aikuisista ei käytä profiilissaan oikeaa nimeään. Artikkeli ei kuitenkaan kerro, käyttävätkö nuoret aikuiset oman nimensä tilalla täysin keksittyä nimeä, jonkun toisen henkilön nimeä, lempinimeä vai oikeasta nimestä muokattua nimeä.

Tietojen kalastelu (engl. phishing) tarkoittaa arkaluontoisen ja henkilökohtaisen tiedon urkkimista rikollisin keinoin (Aggarwal, Rajadesingan & Kumaraguru, 2012). Yleensä tietojen saamiseksi hyödynnetään jotain menetelmää. Hyökkääjä voi käyttää perinteistä sähköpostia ja lähettää esimerkiksi haitallisia linkkejä tai kysyä suoraan sähköpostissa henkilökohtaisia tietoja. Myös teknisesti vaativampia ja monimutkaisempia hyökkäysmenetelmiä voidaan käyttää. Osa hyökkäyksistä perustuu ihmisen luontaisen käyttäytymisen ja luottamuksen hyödyntämiseen. Luomalla yhteyden käyttäjään hyökkääjällä on vapaa pääsy uhrin profiiliin. Tiedon keräämisen lisäksi hyökkääjä voi lähettää linkkejä saastuneille sivuille, joista käyttäjän koneelle voi lataantua virus. (Kontaxis, Polakis, Ioannidis & Markatos, 2011.) Henkilökohtaista tietoa on tarjolla valtavasti, eikä käyttäjä välttämättä itse huomaa tarjoavansa tietoa mahdolliselle rikolliselle tai pidä tiedon julkista jakamista riskinä, sillä muutkin tekevät niin.

Sosiaalisen median palveluissa profiilin luomiseen tarvitaan useimmiten ainoastaan toimiva sähköpostiosoite tai puhelinnumero. Rekisteröitymisen yhteydessä lähetetään vahvistusviesti joko sähköpostiin tai puhelimeen. Huijari voi kuitenkin tehtailla tarpeen mukaan useita sähköpostiosoitteita eri nimillä ja siten luoda monta profiilia sosiaalisen median palveluun. Toisaalta puhelinnumero on hyvä tunnistamiskeino, sillä uuden puhelinnumeron hankkiminen on usein työläämpää kuin uusien sähköpostiosoitteiden luominen. Poikkeuksena tästä on kuitenkin prepaid-liittymät, joita voi Suomessa ostaa haluamansa määrän tunnistautumatta.

On olemassa erilaisia palveluita, joissa henkilöllisyys varmennetaan passin tai luottokortin avulla. Suomessa pankit tarjoavat verkkoasiakkaan vahvaan tunnistamiseen Tupas-varmennepalvelun, joka perustuu verkkopankkitunnusten käyttöön. Sosiaalisessa mediassa sen sijaan mikään ei takaa käyttäjän henkilöllisyyden aitoutta (Bhumiratana, 2011).

Identiteetti tarkoittaa eri yhteyksissä hieman eri asioita. Psykologian näkökulmasta identiteetti on ihmisen käsitys itsestään eli minäkuva. Tätä identiteettiä ei voi varmentaa dokumentista. Sisäasiainministeriön identiteettiohjelman raportissa (2010) määritellään identiteetin muodostuvan niistä tiedoista, joiden avulla henkilöt voidaan erotella toisistaan ja tunnistaa. Näitä tietoja ovat esimerkiksi sosiaaliturvatunnus, nimi, pankki- ja luottokortinnumero, verkkopankkitunnukset. Tietoverkossa identiteetti on virtuaalinen. Virtuaalista identiteettiä käytetään erottelemaan tietyn palvelun käyttäjät toisistaan (Sisäasiainministeriö, 2010). Virtuaalisen identiteetin tietoja ovat esimerkiksi käyttäjätunnus ja IP-osoite.

Muun muassa Sisäasiainministeriö (2010) ja Euroopan komissio (2012) määrittelevät identiteettivarkauden tarkoittavan toisen henkilön tietojen keräämistä ja käyttämistä oikeudettomasti. Tavoitteena on saavuttaa taloudellista

ja muuta hyötyä tai aiheuttaa uhrille vastaavaa haittaa. Identiteettivarkaudessa on aina kyse informaation kopioimisesta, sillä identiteetti jää uhrin haltuun myös kopioinnin (varastamisen) jälkeen.

Toistaiseksi Suomessa identiteettivarkaus ei ole rikos, sillä käsityksen mukaan varkaus voi kohdistua vain irtaimeen omaisuuteen. Näillä näkymin identiteettivarkaus tulee rangaistavaksi itsenäisenä rikoksena vuoden 2015 syksyllä, jolloin Euroopan unionin tietoverkkorikosdirektiivi on pantava jäsenvaltioissa täytäntöön. Enimmäisrangaistukseksi identiteettivarkaudesta on kaavailtu sakkoa. (Oikeusministeriö, 2014.).

Koska identiteettivarkaus ei vielä ole rikos, periaatteessa tällä hetkellä Suomessa saa esiintyä toisena henkilönä niin kauan, kun siitä ei aiheudu toiselle osapuolelle haittaa tai taloudellista vahinkoa eikä toisen identiteetillä esiintyvä saa itse etua esiintyessään toisena. Varastettua identiteettiä voidaan käyttää myös niin, että jonkun muun rikoksen tai rikosten tunnusmerkistöt täyttyvät. Tyypillisiä rikoksia ovat petos, maksuvälinepetos ja kunnianloukkaus. Myös tekijänoikeusrikos voi tulla kyseeseen, jos esiintyy esimerkiksi sosiaalisen median palvelussa toisen ottamalla kuvalla ilman lupaa. Väärää identiteettiä voidaan käyttää esimerkiksi pikavippien ottamiseen, tavaran ostamiseen tai puhelinliittymän avaamiseen. (Helsingin poliisilaitos, 2014.) On olemassa paljonkin tapauksia, joissa puhelinliittymä on onnistuttu avaamaan väärillä henkilötiedoilla. Huijaus on saattanut käydä ilmi vasta siinä vaiheessa, kun ensimmäinen lasku tai maksumuistutus tulee uhrille.

Tämän tutkielman tarkoituksena on tarkastella identiteetin varastamista ja väärän identiteetin hyödyntämistä sosiaalisen median näkökulmasta sekä teoreettisesti että käytännön kautta. Tutkimusongelma on:

Miten sosiaalisen median palveluita on hyödynnetty identiteetin varastamisessa?

Tutkimusongelma jakautuu seuraaviin tutkimuskysymyksiin:

- Millaisia tietojen kalastelu- ja identiteetinvarastamiskeinoja kirjallisuudessa esitetään?
- Miten toisen henkilön identiteettiä on hyödynnetty sosiaalisen median palveluihin liittyvissä rikoksissa käytännössä ja miksi se on ollut mahdollista?

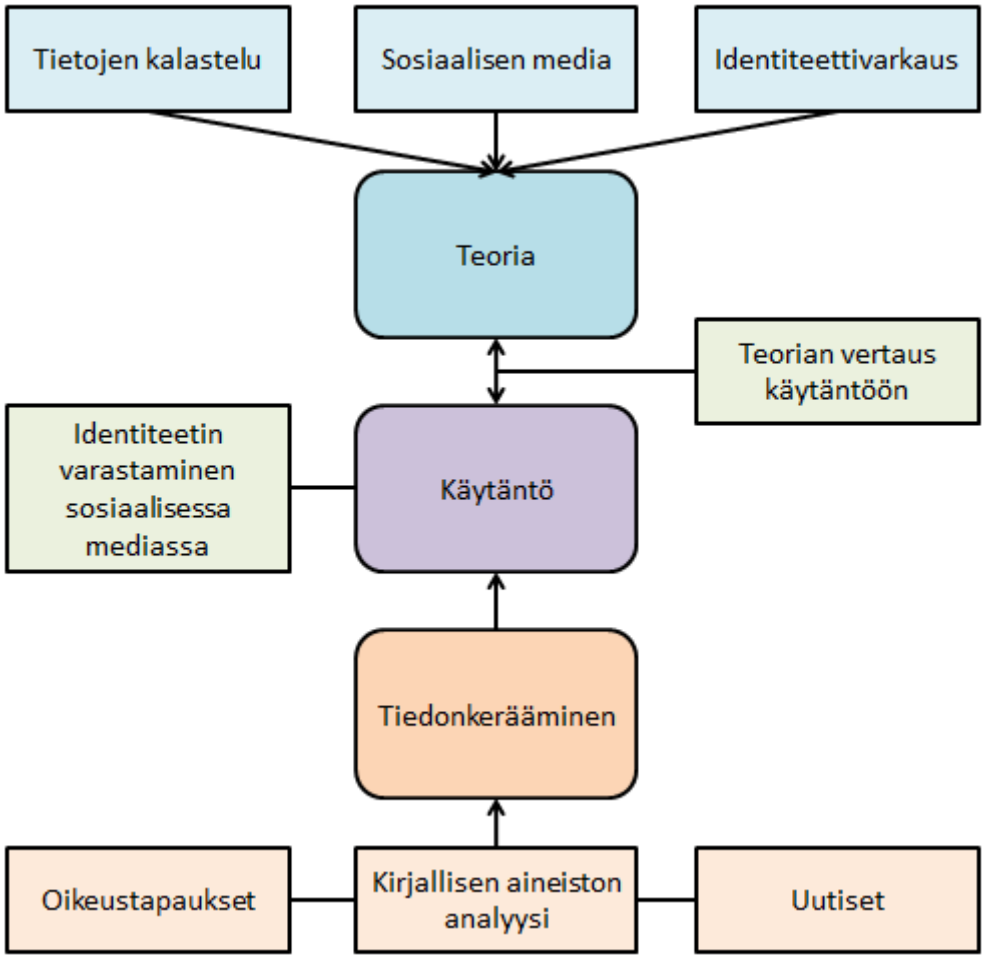
Tutkimuksen näkökulma on teoriaa testaava eli empiirisessä osuudessa tarkastellaan, miten kirjallisuuskatsaus vastaa käytännön tapauksiin ja toisin päin. Käytännön tapauksia havainnoidaan kirjallisuuden perusteella tehtyjen kysymysten kautta. Kirjallisuuskatsauksen perusteella siis oletetaan tiettyjä asioita ja tapauksissa tarkastellaan näiden oletusten toteutumista. Tapaukset koostuvat oikeustapauksista ja uutisista.

Tutkielma jakautuu kahdeksaan lukuun. Teoreettinen osuus käsittää luvut 2-4, joissa vastataan ensimmäiseen tutkimuskysymykseen. Tutkimuksen ensimmäinen vaihe on tutustua tietojen kalastelua, sosiaalista mediaa ja identiteettivarkautta käsittelevään kirjallisuuteen. Tällä tavalla saadaan käsitys siitä,

miten kirjallisuus esittää identiteettivarkauden ja sosiaalisen median välisen yhteyden ja mitä tietojen kalastelukeinoja on olemassa. Luvussa 2 käydään lyhyesti läpi identiteettivarkauden kriminalisoinnin taustalla vaikuttava Euroopan unionin direktiivi, Suomen hallituksen esitys, jossa käsitellään direktiivin täytäntöönpanoa ja uutta identiteettivarkautta. Lisäksi määritellään näiden perusteella identiteetti ja identiteettivarkaus. Luvussa 3 käsitellään käyttäjän manipulointia, joka on eräs tietojen kalastelukeino, mutta joka myös vaikuttaa usein muiden hyökkäysten taustalla. Lisäksi pohditaan käyttäjän luotettavuuteen vaikuttavia tekijöitä ja syitä hyväuskoisuudelle sekä kuvataan sosiaalisen median haavoittuvuutta. Luvussa 4 esitellään tarkemmin, miten sosiaalisen median palveluissa voidaan varastaa käyttäjien identiteetti, ja kerätä heistä henkilökohtaista ja arkaluontoista tietoa, jota voidaan myöhemmin hyödyntää myös muualla. Osa keinoista on teknisiä, kun taas osa perustuu aikaisemmin mainittuun käyttäjän manipulointiin.

Toisessa vaiheessa tarkoituksena on etsiä aineistoa empiiriseen osuuteen. Koska identiteettivarkaus ei tutkielman kirjoittamisen aikaan ole rikos, tulee etsiä muita vastaavia rikosnimikkeitä, joissa väärää identiteettiä on voitu hyödyntää. Tällaisia rikoksia ovat esimerkiksi petos, kunnianloukkaus, yksityiselämää loukkaavan tiedon levittäminen ja kiristys. Koska Suomen käräjäoikeuksista ei voi hakea vielä identiteettivarkaus-rikosnimikkeellä, ja muiden tapausten lukumäärä on valtava, on sopivien tapausten löytäminen hankalaa. Tapausten etsinnässä on hyödynnetty sekä poliisia että eri käräjäoikeuksia. Lopulta eri lähteitä hyödyntäen aineistoksi saatiin kahdesta tapauksesta käräjäoikeuden materiaali ja kahden tapauksen kohdalla hyödynnetään uutismateriaalia.

Empiirisen osuuden ensimmäisessä luvussa (luku 5) kuvataan käytetty tutkimusmenetelmä, tutkimuskohteet, sekä tiedonkerääminen ja analysointi. Kolmannessa vaiheessa tutkielman empiiristä aineistoa analysoidaan kirjallisuuden kautta. Luvussa 6 esitetään tutkimuksen tulokset. Kuviossa 1 havainnollistetaan tutkimusprosessia.



KUVIO 1 Tutkimusprosessi

Tapausten tutkimisessa tulee huomioida tietojärjestelmätieteen näkökulma, joten suurimmaksi osaksi tarkastellaan, miksi identiteettivarkaus tai siihen liittyvä rikos on ollut mahdollinen sosiaalisen median palveluissa ja mikä edesauttaa rikoksen tekemistä kyseisissä palveluissa. Tutkielmassa ei keskitytä psykologisiin syihin tai oteta suoranaisesti kantaa rangaistuksiin tai muuhun lopputulokseen, ellei se ole olennaista tutkielman kannalta. Luvussa 7 esitetään tutkimuksen tulokset tiivistettynä ja tehdään johtopäätökset sekä pohditaan tutkimuksen hyödyntämismahdollisuuksia. Viimeisenä on yhteenveto (luku 8).

2 IDENTITEETTIVARKAUDEN KRIMINALISOINTI JA MÄÄRITELMÄ

Tässä luvussa käydään läpi identiteettivarkauden kriminalisointi ja Euroopan unionin direktiivi, joka vaikuttaa kriminalisoinnin taustalla. Direktiivi 2013/40/EU, jota kutsutaan myös tietoverkkorikosdirektiiviksi, tulee saattaa osaksi jokaisen jäsenmaan kansallista lainsäädäntöä. Lakien, asetusten ja hallinnollisten määräysten on määrä astua kaikissa jäsenvaltioissa voimaan 4. syyskuuta 2015, jolloin myös identiteettivarkaudesta tulee rangaistava teko Suomessa.

2.1 Direktiivi 2013/40/EU

Euroopan parlamentin ja Euroopan unionin neuvoston direktiivin tietojärjestelmiin kohdistuvista hyökkäyksistä (2013/40/EU) tavoitteena on muun muassa yhdenmukaistaa jäsenvaltioiden rikoslakia tietojärjestelmiin kohdistuviin hyökkäyksiin liittyen ja parantaa yhteistyötä viranomaisten välillä. Direktiivin tarkoituksena on määrittää vähimmäissäännöt rikosten määrittelylle ja seuraamuksille. (Direktiivi 2013/40/EU, 2013.)

Direktiivin (2013) mukaan tietojärjestelmiä vastaan suunnatut hyökkäykset ovat lisääntyvä uhka sekä Euroopan unionissa että myös muualla maailmassa. Tietojärjestelmiin kohdistetaan terrorihyökkäyksiä samalla tavalla kuin fyysisesti olemassa oleviin kohteisiin.

Kasvava huoli tietojärjestelmiin kohdistetuista hyökkäyksistä on todellinen, sillä hyökkäys voi vahingoittaa jäsenvaltioiden ja unionin infrastruktuuria. Direktiivin (2013) mukaan elintärkeä infrastruktuuri käsittää kaikki ne hyödykkeet ja järjestelmät, jotka ovat keskeisessä roolissa yhteiskunnan välttämättömien toimintojen ylläpitämiseksi, ja joiden vahingoittumisella olisi kriittinen vaikutus jäsenvaltioon, koska toimintoja ei voitaisi ylläpitää. Välttämättömiä toimintoja ovat muun muassa terveydenhuolto, turvallisuus, voimalat, liikenneverkosto ja julkinen verkko.

Direktiivin (2013) mukaan tietojärjestelmään kohdistettu hyökkäys on rangaistavampi silloin, kun tekijänä on rikollisjärjestö tai kun käytetään niin kutsuttua bottiverkkoa, eli otetaan suuri määrä koneita etähallintaan saastuttamalla ne haittaohjelmilla, tai kun isku suunnataan elintärkeää infrastruktuuria vastaan. Perusteita ankarammalle rangaistukselle on myös vakava vahinko ja elintärkeään infrastruktuuriin kohdistettu hyökkäys.

Direktiivissä identiteettivarkaudesta käytetään sanaa ”henkilöllisyysvarkaus”. Direktiivi painottaa henkilöllisyysvarkauden ja muiden henkilöllisyyteen liittyvien rikosten ehkäisemistä yhdenmukaistettaessa jäsenvaltioiden tietoverkkorikollisuuden torjumista. Direktiivi velvoittaa myös huomioimaan rikosta edesauttaneet tekijät, esimerkiksi jos hyökkääjällä on työnsä puolesta ollut pääsy hyökkäyksen kohteena olleen tietojärjestelmän turvajärjestelmään. (Direktiivi 2013/40/EU, 2013.)

Direktiivi velvoittaa jäsenvaltioita varmistamaan, että kunkin maan lainsäädännössä rikosoikeudellisesti rangaistavia tekoja ovat laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä, laiton datan vahingoittaminen ja viestintäsalaisuuden loukkaus eli tietojen laiton hankkiminen. Myös näihin rikoksiin yllyttäminen, avunanto ja yritys on säädettävä rangaistaviksi. Lisäksi direktiivi velvoittaa säätämään rangaistuksen sellaisten välineiden myymisestä, tuottamisesta, tuonnista, levittämisestä ja hankkimisesta tahallisesti ja oikeudettomasti, joita voidaan käyttää edellä mainittujen rikosten tekemiseen. Tällaisia välineitä ovat muun muassa laittomaan tarkoitukseen suunniteltu tietokoneohjelma, salasana, pääsykoodi tai muu tieto, jonka avulla on mahdollista päästä sisälle tietojärjestelmään. (Direktiivi 2013/40/EU, 2013.)

2.2 Hallituksen esitys 232/2014 ja nykyinen laki

Hallituksen esityksen tarkoituksena on saattaa Suomen lainsäädäntö vastaamaan edellä käsiteltyä tietoverkkorikosdirektiivin sanelemia ehtoja. Muutoksia on tulossa rikoslakiin, pakkokeinolakiin, poliisilakiin ja sotilasoikeudenkäyntilakiin. Lisäksi esityksessä ehdotetaan identiteettivarkauden kriminalisointia. Identiteettivarkaus olisi esityksen (2014) mukaan asianomistajarikos, eli asianomistajalla on aloiteoikeus syytteen nostamisen suhteen. Hallituksen esitys määrittelee identiteettivarkauden seuraavalla tavalla:

> ”Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.”

Lain tarkoituksena on suojella identiteetin loukkaamattomuutta eli suojelun kohteena on se henkilö, jonka henkilötietoja on käytetty. Identiteettivarkauden kriminalisointi pyrkii huomioimaan henkilön, kun taas direktiivin mukaan rangaistavia tekoja ovat muun muassa laiton tunkeutuminen tietojärjestelmään ja laiton datan hankkiminen, eli suojelun kohteena on tietojärjestelmä. Näin ollen

yhteen hyökkäykseen syyllistynyt rikollinen voidaan tuomita sekä identiteettivarkaudesta (suojelukohde henkilö) että esimerkiksi laittomasta datan hankkimisesta (suojelukohde tietojärjestelmä). Itsenäisenä rikoksena identiteettivarkauden maksimirangaistus on esityksen mukaan sakko. (Hallituksen esitys, 2014.)

Esityksen (2014) mukaan identiteettivarkauden tunnusmerkistön täyttyminen edellyttää, että väärää identiteettiä käyttäneen henkilön tarkoituksena on ollut erehdyttää kolmatta osapuolta. Keskeistä on myös se, että kolmatta osapuolta on erehdytetty nimenomaan henkilöllisyyden tai identiteetin osalta. Esityksen (2014) mukaan tuomittavuuden edellytyksenä on tekijän oikeudeton toiminta. Olennaista identiteettivarkaudessa on, että kolmas osapuoli erehtyy tietojen perusteella luulemaan tekijää siksi, jonka tiedoilla tämä esiintyy. Rikos ei täyty, mikäli tietojen käyttö on vähäistä tai erehtymisvaaraa ei ole (Hallituksen esitys, 2014). Näin ollen on edelleen mahdollista esimerkiksi luoda pilailutarkoituksessa profiili sosiaalisen median palveluun, mikäli profiilista käy selkeästi ilmi, että se on tarkoitettu satiiriksi eikä kuvasta oikeasti kyseistä henkilöä, eikä siten mahdollisuutta erehtymiseen ole. Varsinkin julkisuuden henkilöistä luodaan usein satiirisia profiileja, eikä niiden tarkoituksena ole esiintyä oikeasti kyseisenä henkilönä. Tulee kuitenkin muistaa, ettei esimerkiksi kenenkään kunniaa saa loukata, vaikka pilailuprofiilien luominen onkin tietyissä asiayhteyksissä luvallista. Keskeistä on siis se, miten huijausprofiilia käyttää.

Myöskään pseudonyymillä esiintyminen ei tule olemaan rangaistavaa (Hallituksen esitys, 2014). Esimerkiksi Matti Meikäläinen -nimellä esiintyminen on edelleen sallittua, sillä sen tyyppistä nimeä käytetään usein halutessa esittää asia anonyymisti vaikkapa Internetin keskustelupalstoilla. Nimi ei viittaa tiettyyn henkilöön ja jokainen huomaa, ettei sillä nimellä esiintyvä henkilö ole todennäköisesti senniminen.

Vaikka aikaisemmin toisen identiteetin varastaminen ei ole ollut rikosoikeudellisesti rangaistavaa, on sen käyttö saattanut mahdollistaa jonkin rikoksen tunnusmerkistön täyttymisen. Toisen henkilön identiteettiä on voitu käyttää esimerkiksi petoksessa, rahanpesussa tai kavalluksessa. Myös väärän henkilötiedon antaminen viranomaiselle on rangaistava teko. Muita mahdollisia rikosnimikkeitä identiteettivarkauteen liittyen ovat ainakin kunnianloukkaus, yksityiselämää loukkaavan tiedon levittäminen ja luvaton käyttö.

2.3 Identiteetti ja identiteettivarkaus

Hallituksen esitykseen sisältyvä identiteettivarkauslaki ei määrittele tiettyä tietoa identiteettitiedoksi, vaan identiteettivarkaus edellyttää toisen henkilötietojen, tunnistamistietojen tai muun vastaavan tiedon käyttöä. Näin ollen myös Sisäasiainministeriön (2010) määrittelemä identiteettitieto nimestä IP-osoitteeseen sisältyy laissa määriteltyyn henkilötietoihin, tunnistamistietoihin tai muuhun vastaavaan tietoon. Koska tämän tutkielman tarkoituksena on selvittää oikeustapausten kautta, miten väärää identiteettiä on käytetty sosiaalisen

median palveluissa, on identiteetin määrittelyssä syytä nojata hallituksen esitykseen. Siten identiteetti-käsite ei rajaudu pelkästään niin sanottuihin dokumenttitietoihin (passi, luottokortti, sosiaaliturvatunnus), vaan käsite kattaa myös virtuaalisen identiteetin ja mitä tietoja henkilöstä on saatavilla Internetissä.

Kuten aikaisemmin mainittiin, identiteettivarkaus ei ole rangaistava teko itsenäisesti, mutta väärän identiteetin käyttämisellä voi syyllistyä muihin rikoksiin, kuten petokseen (myös maksuvälinepetos) tai kunnianloukkaukseen. Tällä hetkellä esimerkiksi Euroopan unionin jäsenvaltioilla ei ole yhtenäistä määritelmää identiteettivarkaudelle. Hallituksen esitys kattaa yksinkertaisuudessaan laajasti identiteettivarkauden, mutta koska laki ei vielä ole voimassa, on syytä tarkastella myös muita määritelmiä.

Euroopan komissio (2012) määrittelee identiteettivarkauden tapahtuvan silloin, kun tekijä hankkii toisten identiteettitietoja esimerkiksi murtautumalla tietojärjestelmään tai kun hän esiintyy tai käyttää toisen henkilön tietoja luvattomasti. Toimimalla näin tekijä voi hyötyä taloudellisesti, vahingoittaa uhria henkisesti (kunnianloukkaus) tai saavuttaa muuta etua.

Sisäasiainministeriön identiteettiohjelman raportin (2010) mukaan identiteettivarkaus käsittää ne teot, joissa identiteettitietoa kerätään ja käytetään luvattomasti ja oikeudetta rikoshyödyn hankkimiseksi tai vahingon aiheuttamiseksi. Terminä identiteettivarkaus on raportin (2010) mukaan harhaanjohtava, sillä käsityksen mukaan varkaus koskee vain irtainta omaisuutta eli uhrilta otetaan jotakin konkreettisesti pois. Käsite ”varkaus” sopii esimerkiksi luottokortin tai passin varastamiseen. Identiteetti sen sijaan säilyy uhrilla varkauden jälkeenkin, tekijä vain ”lainaa” ja kopioi sen itselleen. Digitaalisen identiteetin varastamisessa onkin aina kyse datan kopioimisesta.

Yleisesti identiteetti voidaan varastaa lähes missä vain. Uhrin käydessä pankkiautomaatilla rikollinen voi vilkuilla tunnusluvun ja varastaa myöhemmin kortin. On myös olemassa laitteita, joiden avulla voi lukea pankkiautomaattiin työnnetyn kortin magneettinauhan ja tyhjentää tilin saatujen tietojen avulla. Langattomuuden ansiosta rikollinen saa tiedot nopeasti ja helposti ilman, että hänen tarvitsee olla edes samassa maassa. Myös verkkokaupasta voi tilata toisen henkilön tiedoilla tavaroita. Uusi asia ei ole myöskään toisen henkilön kiusaaminen ja tämän kunnian loukkaaminen väärällä nimellä sosiaalisen median palvelussa. Näissä kaikissa yhdistyy taloudellinen haitta tai muu vahinko ja jonkun muun kuin tekijän oma identiteetti aivan kuten edellä esitetyissä määritelmissä.

Tässä tutkielmassa tutkitaan tapauksia, joissa on käytetty toisen henkilön identiteettiä. Edellä esitettyihin määritelmiin pohjautuen tässä tutkielmassa identiteettivarkaudella tarkoitetaan tekoa, jossa tekijä hankkii ja käyttää oikeudettomasti toisen henkilön identiteettitietoja erehdyttääkseen kolmatta osapuolta ja tehdäkseen rikosoikeudellisesti rangaistavan teon aiheuttaen siten identiteetin oikealle omistajalle tai muulle osapuolelle taloudellista tai muuta vahinkoa. Tällä määritelmällä pyritään kattamaan identiteettivarkaus laajasti, jotta sitä voitaisiin soveltaa tässä tutkielmassa tutkittaviin erilaisiin tapauksiin.

Esimerkiksi Euroopan komissio (2012) määrittelee raportissaan vielä tarkemmin muita elementtejä identiteettivarkauden käsitteeseen liittyen. Euroopan komissio (2012) huomio ensisijaisen (primääri) ja toissijaisen (sekundääri) uhrin lisäksi myös primääri- ja sekundääririkokset. Primääri- ja sekundääriuhri on huomioitu myös tämän tutkielman määritelmässä. Primääriuhri on se henkilö, jonka identiteettiä käytetään. Sekundääriuhrilla tarkoitetaan sitä, johon väärää identiteettiä käytetään, esimerkiksi pankki, toinen henkilö tai muu kolmas osapuoli. Tämän tutkielman määritelmä on haluttu pitää yksinkertaisena, joskin se pohjautuu hyvin vahvasti jo esitettyihin lakeihin ja säädöksiin.

2.4 Yhteenveto

Tässä luvussa käytiin ensin lyhyesti läpi Euroopan parlamentin ja Euroopan unionin neuvoston direktiivi tietoverkkorikoksista. Direktiivi velvoittaa unionin jäsenvaltiot saattamaan kansallisen lainsäädäntönsä vastaamaan direktiivissä sanottua. Jäsenvaltioiden tulee varmistaa, että muun muassa datan laiton hankkiminen, laiton tietojärjestelmän häirintä sekä näihin tekoihin yllyttäminen, avunato ja yritys ovat rikosoikeudellisesti rangaistavia tekoja. Direktiivin on määrä astua voimaan kaikissa jäsenvaltioissa 4. syyskuuta 2015.

Suomen hallituksen esityksessä ehdotetaan identiteettivarkauden kriminalisointia uutena rikoksena. Itsenäisenä rikoksena maksimirangaistukseksi on suunniteltu sakkoa, ja teko olisi asianomistajarikos. Nykyisen rikoslain puitteissa toisen henkilön nimellä voi tehdä rikollisia tekoja, mutta rikollista ei nykyisellään voi tuomita identiteettivarkaudesta. Toisen henkilön nimeä voi käyttää ainakin petoksessa, kunnianloukkauksessa ja maksuvälinepetoksessa. Myös väärän tiedon antaminen viranomaiselle on rangaistavaa. Vaikka nykyinen rikoslaki kattaakin laajasti tilanteet, joissa toisen nimeä hyödynnetään, on myös itse nimen käytön kriminalisoiminen tervetullut muutos. Nyt myös nimen oikea omistaja saa oikeutta, vaikka nimen avulla tehty rikos ei kohdistuisikaan häneen.

Luvussa pohdittiin myös identiteetin ja identiteettivarkauden määritelmää. Luvussa kuvattiin eri tahojen, kuten Euroopan komission ja Sisäasianministeriön, laatimia määritelmiä, ja lopulta muodostettiin näiden perusteella tutkielman tarkoitukseen sopivat määritelmät avainsanoista. Identiteettivarkauden ja tietojen kalastelun tarkoituksena on taloudellinen tai muu haitta. Hyökkääjä pyrkii käytännössä aina saavuttamaan itse jotain etua tai vastaavasti aiheuttamaan uhrille vahinkoa. Koska hyödyn saavuttaminen ja vahingon aiheuttaminen ovat keskeistä identiteettivarkaudessa, sitä on syytä tutkita myös käytännössä. Tämän perusteella empiirisessä osuudessa selvitetään, onko tutkittavissa tapauksissa saavutettu taloudellista tai muuta etua, tai aiheutettu uhrille vastaavaa haittaa.

3 KÄYTTÄJÄN MANIPULOINTI

Tässä luvussa käydään läpi ihmisen luontaista käyttäytymistä hyödyntävä käyttäjän manipulointi, joka vaikuttaa myös usean muun hyökkäyskeinon taustalla. Lisäksi luvussa pohditaan tekijöitä, jotka vaikuttavat luotettavuuteen ja ihmisen hyväuskoisuuteen

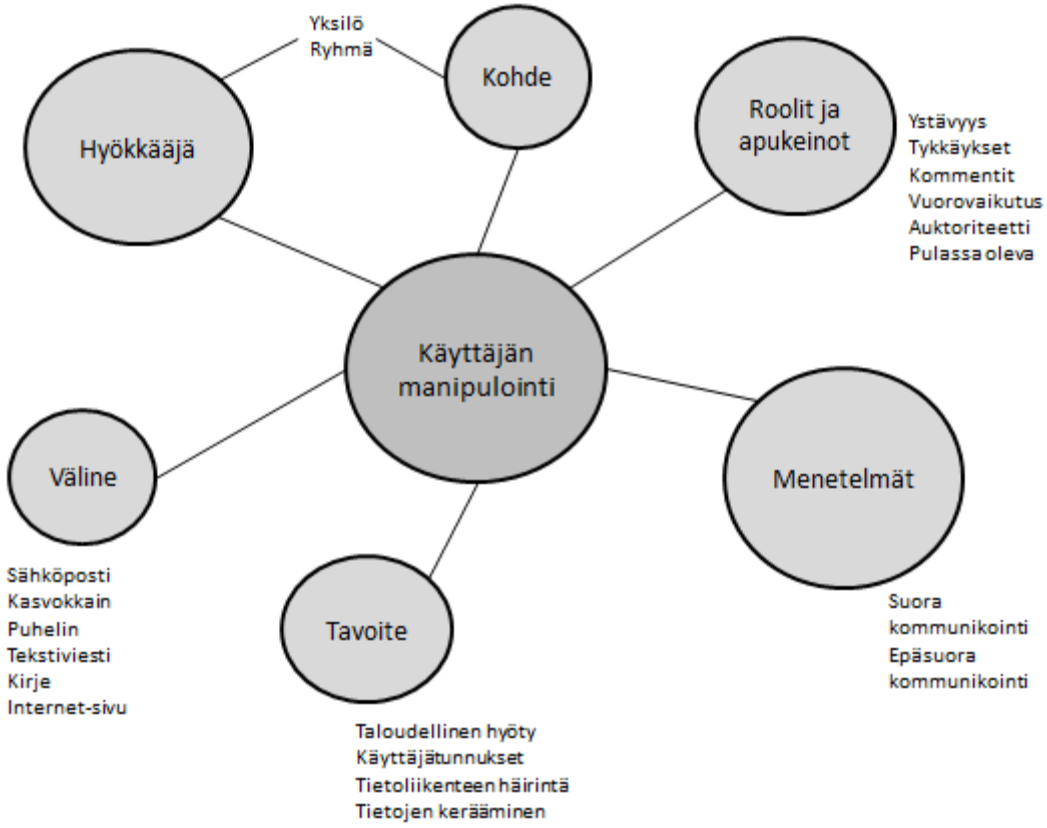
3.1 Määritelmä

Käyttäjän manipulointi (engl. social engineering) tarkoittaa ihmisten huijaamista niin, että hyökkääjä saa kerättyä tietoa, saavuttaa tavoitteensa tai saa houkuteltua käyttäjän tekemään jotain, josta on hyökkääjälle hyötyä (Algarni, Xu & Chan, 2014; Mouton, Malan, Leenen & Venter, 2014). Käyttäjän manipulointi on uhka turvallisuudelle ja yksityisyydelle sen monimutkaisen luonteen vuoksi. Se ei niinkään perustu tekniselle osaamiselle vaan ihmisen luontaisen käyttäytymisen hyödyntämiseen, mitä vastaan on vaikea suojautua teknisin keinoin.

Kuviossa 2 Mouton ym. (2014) esittelevät ontologisen mallin käyttäjän manipuloinnista. Mallin mukaan käyttäjän manipulointihyökkäyksessä hyödynnetään joko suoraa tai epäsuoraa kommunikointia. Suora kommunikointi voidaan jakaa kaksisuuntaiseen ja yksisuuntaiseen kommunikointiin. Kaksisuuntainen kommunikointi tarkoittaa sitä, että sekä uhri että hyökkääjä osallistuvat kommunikointiin. Hyökkääjä lähettää esimerkiksi Facebookissa viestin, johon uhri vastaa. Yksisuuntainen kommunikointi tarkoittaa kommunikointia, jossa vain hyökkääjä kommunikoi. Epäsuora kommunikointi kuvaa tilannetta, jossa hyökkääjä ja uhri eivät ole suoraan vuorovaikutuksessa, vaan välissä toimii kolmas osapuoli. (Mouton ym., 2014.)

Hyökkäyksellä on myös kohde, väline ja päämäärä sekä siinä käytetään yhtä tai useampaa menetelmää. Kohde voi olla joko yksilö tai isompi ryhmä, samoin kuin hyökkääjäkin. Kirves (2002) esittää esimerkin organisaatioon kohdistuvasta käyttäjän manipulointihyökkäyksestä, jossa huijari esiintyy tietokonekorjaajana, ja pyytää korjausta varten käyttäjätunnukset organisaation sihtee-

riltä. Isossa yrityksessä tällainen menetelmä on tehokkaampi kuin pienessä yrityksessä, sillä työntekijöiden lukumäärä on suurempi, eivätkä kaikki tunne toisiaan. Hyökkääjä voi etukäteen ottaa selville yrityksen tärkeiden henkilöiden nimiä, jotta kuulostaisi virallisemmalta ja tietävämmältä. Hän voi myös ensin ujuttautua tietokoneen luokse asentamaan jonkin haittaohjelman ja jättää yhteystietonsa ”sattumalta” löydettäviksi. Näin hyökkääjä varmistaa, että kun työntekijä huomaa vian, hän ottaa yhteyttä hyökkääjään. Mennessään korjaamaan vikaa hyökkääjä esittää tarvitsevansa tunnuksia järjestelmään, jolloin hän voi saada salaisia ja arkaluontoisia tietoja yrityksestä. Pienessä yrityksessä yleensä kaikki tuntevat toisensa, ja jatkuvan ja kaikki tavoittavan kommunikoinnin ansiosta huijaus on vaikeammin toteutettavissa. Tämä on vain yksi esimerkki hyökkäyksestä, jossa hyödynnetään käyttäjän manipulointia. Keinot vaihtelevat ympäristöstä ja tilanteesta riippuen.



KUVIO 2 Käyttäjän manipulointi (Mouton ym., 2014)

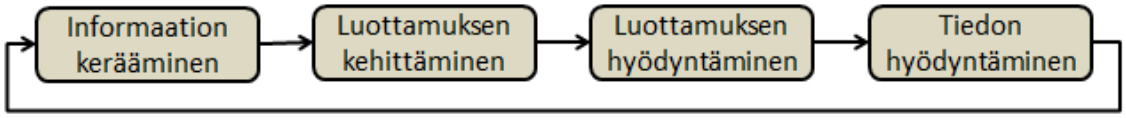
Käyttäjän manipulointihyökkäyksessä huijari voi hyödyntää melkein mitä tahansa välinettä. Edellä mainittu esimerkki organisaatioon kohdistuvasta hyökkäyksestä hyödyntää kasvokkain kommunikointia. Kasvokkain kommunikointi vaatii hyökkääjältä näyttelijän lahjoja, mutta Internetissä tietoja voidaan kalastella ilman, että käyttäjä edes tajuaa tulleensa huijatuksi. Hyökkääjä voi hyödyntää sähköpostia tai www-sivustoa. Tavoitteena on saada uhri luottamaan hyökkääjään niin paljon, että tämä toimii halutulla tavalla. Moutonin ym. (2014) mallin mukaan hyökkäyksen päämääränä on saavuttaa taloudellista hyötyä,

saada käyttäjätunnukset tai saada aikaan palvelun tai tietoliikenteen häiriö. Hyökkääjä voi myös pyrkiä saavuttamaan salaisia tietoja vaikkapa jostain yrityksestä tai valtiosta.

Hyökkääjä manipuloi käyttäjää esimerkiksi vetoamalla ystävyyteen tai tehtyyn lupaukseen. Hyökkääjä voi esiintyä köyhyydestä kärsivänä henkilönä ja vedota lähimmäisenrakkauteen. Usein myös hyödynnetään auktoriteetin asemaa, jolloin voidaan esiintyä esimerkiksi poliisina, verovirastona tai järjestelmän hallitsijana. (Mouton ym., 2014.)

3.2 Käyttäjän manipulointihyökkäyksen malleja

Mouton ym. (2014 mukaan tunnetuin malli käyttäjän manipuloinnista on entisen tietoturvarikollisen Kevin Mitnickin (2002) kehittämä malli. Mallissa on neljä vaihetta, jotka ovat informaation kerääminen, hyvän suhteen ja luottamuksen kehittäminen, luottamuksen hyödyntäminen ja tiedon hyödyntäminen. Informaation kerääminen tarkoittaa tiedonkeruuprosessia kohteesta. Ennen hyökkäystä hyökkääjän on tärkeää tietää uhristaan niin paljon kuin mahdollista. Hyökkääjän tulee luoda luottamus käyttäjän kanssa, sillä uhri paljastaa todennäköisemmin tietoa, jos hän luottaa hyökkääjään. Mouton ym. (2014) mukaan Mitnick (2002) esittää, että luottamus voidaan luoda muun muassa hyödyntämällä sisäpiirin tietoa ja esittämällä avuntarvitsijan tai auktoriteetin roolia. Kun hyökkääjä on saavuttanut uhrin luottamuksen, hän hyödyntää sitä saadakseen tietoja uhrilta. Saatua tietoa voidaan hyödyntää edelleen rikollisissa tarkoituksissa. Kuviossa 3 kuvataan edellä esitetty Mitnickin malli.



KUVIO 3 Mitnickin (2002) malli käyttäjän manipulointihyökkäyksen prosessista (Mouton ym., 2014)

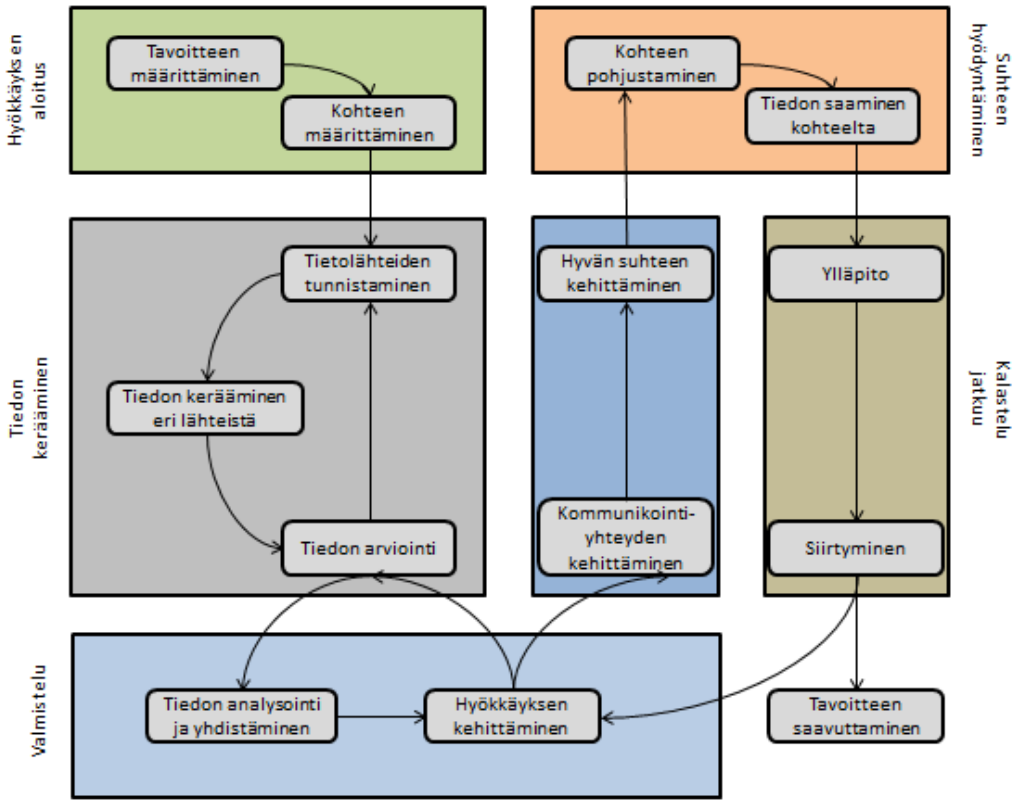
Mitnickin mallia on kuitenkin kritisoitu siitä, että malli olettaa ensimmäisessä vaiheessa, että kohde on jo tunnettu ja hyökkääjä on jo asettanut haluamansa tavoitteen. Moutonin ym. (2014) näkemyksen mukaan hyökkääjän asettaa hyökkäyksen päämäärä jo ennen kuin hän alkaa kerätä tietoa, sillä uhri valikoituu päämäärän mukaan. Vasta tämän jälkeen hyökkääjä aloittaa tiedon hankinnan. Hyökkääjän tulee myös määrittää, mistä lähteistä tietoa kerätään, ja kerätyn tiedon laatu on hyvä arvioida, jotta tieto on mielekästä hyökkäyksen onnistumisen kannalta.

Moutonin ym. (2014) mukaan myöskään toisen vaiheen luottamusta ei saavuteta noin vain. Heidän mukaansa ensimmäisessä vaiheessa kerättyä tietoa käytetään avaamaan keskusteluyhteys kohteeseen. Vasta tämän jälkeen voidaan alkaa rakentaa sidettä uhrin kanssa. Myös luottamuksen hyödyntäminen vaatii

enemmän kuvailua. Luottamus toista kohtaan vaihtelee ihmisestä riippuen. Toinen luottaa helpommin, kun taas toinen tarvitsee enemmän vakuuttelua. Eri keinot manipuloida käyttäjää toimivat eri ihmisiin eri tavoin. Tämän takia on tärkeää päästä uhrin kanssa tunnetasolle, jotta luottamusta voidaan hyödyntää (Mouton ym., 2014).

Mitnickin malli ei Moutonin ym. (2014) mukaan myöskään huomioi valmisteluvaihetta ennen varsinaista toteutusta. Valmisteluvaiheessa olennaista on kerätyn tiedon ja valittavan hyökkäysmenetelmän analysointi. Myös käsitys viimeisen vaiheen tiedon hyödyntämisestä on eroava, sillä Moutonin ym. (2014) mukaan käyttäjän manipulointi päättyy tähän. Esimerkiksi salasanan kalastelleminen uhrilta hyödyntäen uhrin luottamusta kuuluu Moutonin ym. (2014) käsityksen mukaan käyttäjän manipulointihyökkäyksen alle, vaan salasanan käyttö on jo erillinen rikos. Kuitenkin Mitnickillä oli alun perinkin lopullisena tavoitteenaan hyödyntää kerättyä tietoa rikoksessa ja siihen hän tähtäsi. Mitnickin (2002) mallissa siten kolme ensimmäistä vaihetta ovat valmistelua ja neljäs vaihe on koko hyökkäyksen päämäärä. Mallissa rikos (esimerkiksi salasanan hyödyntäminen) kuuluu siis käyttäjän manipulointihyökkäykseen.

Moutonin ym. (2014) mukaan Mitnickin malli on yksinkertaistettu, vaikkakin todenmukainen versio käyttäjän manipulaatioon perustuvasta hyökkäyksestä. Kuviossa 4 on kuvattu Moutonin ym. (2014) tekemien huomioiden perusteella päivitetty malli käyttäjän manipuloinnista, joka esittää prosessin laajemmin. He sisällyttävät malliin muun muassa valmisteluvaiheen, jota Mitnick (2002) ei heidän mukaansa huomioi.



KUVIO 4 Päivitetty malli käyttäjän manipulointihyökkäyksestä (Mouton ym., 2014)

Useassa seuraavassa luvussa esiteltävässä identiteetinvarastamiskeinossa on havaittavissa käyttäjän manipuloinnin hyödyntämistä. Luottamuksen saavuttaminen hyökkääjän ja käyttäjän välillä onkin useiden tietojen kalastelumenetelmien onnistumisen kannalta tärkeää. Siihen perustuvat muun muassa monien tuntema nigerialaiskirjeiden lähetys, joka on yksi vanhimmista keinoista saada käyttäjä paljastamaan henkilökohtaista ja arkaluontoista tietoa.

3.3 Lähteen luotettavuus

Lähteen luotettavuus (engl. source credibility) on moniulotteinen käsite, joka liittyy käyttäjän arvioon lähteestä suhteessa informaatioon. Arvio riippuu käyttäjän kyvystä luokitella todellisuus, totuus ja informaatio ja tehdä kokonaisarvio tietolähteen luotettavuudesta ja uskottavuudesta. Tutkimusten mukaan ihminen luottaa viestiin ja tekee pyydetyt toiminnot todennäköisemmin, jos viestin lähettäjä on luotettava. (Algarni, 2014.)

Tietojen kalastelussa hyödynnetään usein luotettavaa ja uskottavaa lähdettä. Tällaisia ovat esimerkiksi viranomainen, ystävä, julkisuuden henkilö, sukulainen ja esimies. Sosiaalisen median palvelut eivät rajoita luotujen profiilien määrää ja tiedot on helppo keksiä ja muokata profiiliin. Kohdekäyttäjän voi olla jopa mahdotonta tunnistaa huijaus sosiaalisen median palvelussa toisin kuin ollessaan tekemisissä kasvokkain. (Algarni ym., 2014.) Kasvokkain kohde on paljon vaikeampi vakuuttaa kuin toimiessa kasvottomasti verkon välityksellä.

Lähteen luotettavuusteoria kuvaa luotettavuuden tasapainotilana, jossa lähde kohtaa vastaanottajan tarpeet. Teoriaa on tutkittu erityisesti markkinoinnin ja mainonnan alalla, jossa on selvitetty, mihin ihmiset perustavat olettamuksensa ja arvionsa myyjän luotettavuudesta (Algarni ym., 2014). Myyjän ja tietojen kalastelijan vaikuttimet ovat tosin erilaisia, sillä toinen keskittyy myymään tuotetta toisen kerätessä henkilökohtaista tietoa ja taivutellessa kohdekäyttäjää tekemään jotain. Taivuttelu koostuu kolmesta osasta, jotka ovat lähettäjä eli lähde, viesti ja vastaanottaja. Kun käyttäjän manipulointi toteutetaan sosiaalisen median palvelussa, hyökkääjä on lähde, tietojen kalastelutekniikka toimii viestinä ja kohdekäyttäjä on vastaanottaja. (Algarni ym., 2014.)

3.4 Luotettavuus sosiaalisessa mediassa

Algarni ym. (2014) ovat tutkineet ihmisten arviota lähteen luotettavuudesta Facebookissa. He havaitsivat yhteensä 13 piirrettä, jotka liittyvät tutkimuksen perusteella luotettavuuden arviointiin. Piirteet jakautuvat neljään osa-alueeseen, jotka ovat havaittu vilpittömyys, havaittu kyvykkyys, havaittu vetovoima ja havaittu arvo. Kolme ensimmäistä osa-aluetta on aikaisemmin löydetty myös viestintä- ja markkinointitutkimuksessa (Algarni ym., 2014).

Vilpittömyyttä kuvaavat avainsanat ovat lähteen rehellisyys, luotettavuus ja uskottavuus. Sosiaalisessa mediassa vilpittömyyttä voidaan Algarnin ym., 2014) tutkimuksen mukaan arvioida havainnoilla kavereiden lukumäärästä, yhteisistä kavereista, profiilin sisällön määrästä, yleisistä käsityksistä ja todellisesta nimestä. Tutkimuksessa paljastui, ettei esimerkiksi lempinimeen luoteta niin paljon kuin todellisen nimen käyttämiseen profiilissa.

Kyvykkyyteen liittyviä piirteitä ovat pätevyys, kuuluisuus ja varallisuus. Nämä vaikuttavat vastapuolen luotettavuuteen, sillä päteviä ja asiantuntevia henkilöitä pidetään luotettavina. Algarnin ym. (2014) mukaan rikkailta vaikuttavia henkilöitä pidetään luotettavampina kuin köyhiä. Varallisuuteen liittyen ilmeni kuitenkin huijauskeino, jossa huijari esiintyi varakkaana henkilönä, mutta pyrki kuitenkin saamaan uhrilta rahaa vedoten sairauteen, liiketoiminnan heikentymiseen tai muuhun riskiin. Kun uhri oli lähettänyt rahaa, huijari poisti hänet kaverilistaltaan. (Algarni ym., 2014.). On yllättävää, ettei uhri kuitenkaan osaa epäillä, kun rikas henkilö pyytää taloudellista avustusta.

Vetovoimaan liitettäviä piirteitä ovat ulkonäkö ja kirjoitustaito. Hyvännäköisiin henkilöihin, jotka osaavat vieläpä kirjoittaa oikein ja mielenkiintoisesti, luotetaan tutkimuksen mukaan enemmän. Arvoon taas liittyvät auktoriteetti, seksuaalinen yhteensopivuus ja vastavuoroisuus. Käyttäjät, jotka kommentoivat toistensa kuvia ja muita julkaisuja, luottavat toisiinsa enemmän. (Algarni ym., 2014.)

Piirteiden perusteella Algarni ym. (2014) laativat hyökkääjää kuvaavia hypoteeseja. Niiden mukaan hyökkääjä muun muassa teeskentelee, että hänellä on paljon ystäviä ja yhteisiä ystäviä käyttäjän kanssa ja täysin samat käsitykset. Hyökkääjät myös huijaavat käyttävänsä oikeaa nimeään ja esittävät olevansa julkisuuden henkilöitä, viranomaisia tai muita korkean auktoriteetin henkilöitä. Kuitenkin viranomaiset usein muistuttavat, etteivät he koskaan kysy asiakkaittensa arkaluontoisia tietoja sähköpostitse tai varsinkaan sosiaalisen median palveluissa. Siksi on yllättävää, että huolimatta muistuttelusta ja tiedonlevityksestä osa käyttäjistä saattaa luottaa vaikkapa Facebookissa saapuneeseen viestiin, jossa poliisina esiintyvä pyytää maksamaan sakon.

On myös mielenkiintoista, että ulkonäkö vaikuttaa luotettavuuteen. Hyvännäköiseen ihmiseen luotetaan virtuaalisessa maailmassa enemmän kuin vähemmän omaa silmää miellyttävään henkilöön. Sen sijaan fyysisessä elämässä luotettavuudesta kertovat ulkonäköä enemmän persoonallisuus ja asenne (Algarni ym., 2014).

3.5 Huijausprofiilin piirteitä

Huijausprofiili tarkoittaa nimensä mukaisesti sellaista profiilia, jonka tiedot eivät vastaa oikean käyttäjänsä identiteettiä ja jota yleensä käytetään kyseenalaisiin tarkoituksiin. Henkilöllä on yleensä jonkin viranomaisen takaama oikea identiteetti. Esimerkiksi passista, syntymätodistuksesta ja henkilökortista käy ilmi henkilön koko nimi ja henkilötunnus, joissakin dokumenteissa on kuvakin.

Huijausprofiilissa tiedot eivät vastaa oikean identiteetin tietoja, vaan huijari käyttää keksittyä tai toisen henkilön nimeä ja kuvaa. Profiilista saatava identiteetti ei siten ole sama kuin tekijän identiteetti todellisuudessa. Toisinaan rajan vetäminen huijausprofiilin ja todellisen profiilin välillä voi olla hankalaa. Joku voi käyttää lempinimeään profiilissa ja rajoittaa tai muuttaa oikeita tietojaan muutenkin säilyttääkseen yksityisyytensä. Keskeistä lienee se, mihin tarkoitukseen profiilia käytetään. Pelkän syntymäpäivän valehteleminen ja nimen muuttaminen ei välttämättä tee profiilista huijausta, jos henkilö muuten on oma itsensä, eikä yritä esittää jotain toista henkilöä. Jos henkilö kuitenkin syystä tai toisesta esiintyy toisella identiteetillä tarkoituksenaan saada muut käyttäjät uskomaan esittämäänsä identiteettiin ja siten aiheuttaa vahinkoa, on kyseessä huijausprofiili.

Haddadin ja Huin (2010) mukaan useimmat käyttäjät eivät hyväksy kaveripyyntöä julkisuuden henkilöltä, mutta sen sijaan kaveripyyntö täysin tuntemattomalta henkilöltä todennäköisesti hyväksytään. Toisaalta muutamat käyttäjät etsivät aktiivisesti ”julkkisten” profiileita ja pyytävät heitä kaverikseen ajattelematta profiilin luojan henkilöllisyyden aitoutta ja oikeellisuutta. Profiili voi siis olla luotu tiedonkeruuta tai muuta vastaavaa tarkoitusta varten. (Haddadi & Hui, 2010.) Huijausprofiilit ovat niin sanottuja sosiaalisia hunajakennoja, joiden tarkoitus on houkuttaa hyväuskoisia käyttäjiä arkaluontoisen tiedon hankintaa varten.

Haddadi ja Hui (2010) ovat testanneet hunajaprofiilin toimintaa ja tehokkuutta käytännössä. Testiä varten he loivat yhteensä 40 huijausprofiilia, 20 kappaletta kumpaakin sukupuolta. Molemmissa ryhmissä oli kymmenen tunnetun elokuva-alan henkilön profiilia ja kymmenen täysin tavallisen ihmisen profiilia, joiden profiilitiedoissa ei ollut muuta kuin nimi. Sen sijaan tutkimuksessa ei kerrota, mitä tietoja kuuluisista henkilöistä oli. Tutkimuksessa Haddadi ja Hui lähettivät joka viikko yhden huijausprofiilin kautta kymmenelle samassa maassa asuvalle, mutta muuten sattumalta valitulle käyttäjälle kaveripyynnön, ja hyväksyivät mahdollisesti tulleet pyynnöt. Muuten he käyttäytyvät täysin passiivisesti eli eivät julkaisseet päivityksiä tai vastanneet saapuneisiin viesteihin. Testin seurauksena huijausprofiileilla oli satoja kavereita. Testiin joutuneiden käyttäjien profiileista paljastui suuri määrä henkilökohtaista tietoa aina osoitteesta ja syntymäpäivästä puhelinnumeroon. Haddadi ja Hui (2010) eivät kuitenkaan mainitse, missä palvelussa testi tehtiin ja olivatko luodut huijausprofiilit kopioita oikeasta profiilista vai oliko oikeaa profiilia edes olemassa. Huijaus onnistuu helpommin, jos oikeaa profiilia ei ole. Jos käyttäjä päättääkin etsiä kyseisen kuuluisan henkilön nimellä profiilia ja löytää sellaisen, jolla jo on huomattavan paljon kavereita tai seuraajia ja joka vaikuttaa aidolta, voi huijausprofiili herättää epäilyksiä.

Ahmedin ja Abulaishin (2012) mukaan huijausprofiilin tyypillinen piirre on se, että sen kaverilistalla on huomattavan paljon kavereita. Usein useamman huijausprofiilin takana on yksi ja sama henkilö tai ryhmä. Saman luojan profiilit ovat usein vuorovaikutuksessa myös keskenään joko suorasti siten, että huijausprofiilit ovat toistensa kavereita palvelussa tai epäsuorasti niin, että joku

muu käyttäjä on huijausprofiileiden kaveri, mutta huijausprofiilit eivät keskenään ole kavereita. (Ahmed & Abulaish, 2012.) Huolimatta suuresta kaverimäärästä, huijausprofiili on suorassa vuorovaikutuksessa vain harvojen käyttäjien kanssa. Sen sijaan huijausprofiili tekee muulla tavoin itseään näkyväksi. Sen kautta jaetaan valtava määrä linkkejä ja linkit johtavat samantyyppisille tai samalle sivustolle. Huijausprofiilit jakavat yleensä samaa linkkiä toistuvasti. Tavallisen käyttäjän jakamiskäyttäytyminen on monipuolisempaa, eivätkä jaetut linkit keskity vain yhteen sivustoon. (Ahmed & Abulaish, 2012.)

Nykyisin sosiaalisen median palveluissa on tavallista, että myös tavallisilla käyttäjillä on jopa yli tuhat kaveria, ja kavereita kerätään osittain suosion takia. Ajattelumalli on, että jokainen saapuva kaveripyyntö täytyy hyväksyä. Käyttäjiä myös pyydetään kaveriksi sillä perusteella, että profiililla on yhteinen kaveri pyynnön lähettäneen käyttäjän kanssa. Sinisilmäinen suhtautuminen kaveripyyntöihin edesauttaa osaltaan huijausprofiileiden käyttöä. De Paulan (2010) mukaan moni myös pitää julkaisujensa näkyvyyttä julkisena, mikä hyödyttää tietojen kalastelijoita.

Huijausprofiilin sisältö kertoo myös paljon. Yleensä normaalin käyttäjän profiilin sisältö on julkaistu tasaisesti pitkin profiilin olemassaoloa, kun taas huijausprofiilissa päivityksiä on huomattavan paljon, vaikka profiili olisi perustettu vasta äskettäin. (Forss, 2014). Sen sijaan profiilikuvien vähäisyys on tunnusomaista huijausprofiileille. Profiilista saattaa löytyä vain yksi kuva, joka todennäköisesti on otettu Internetistä. Kuva voi myös olla ”ristiriidassa” profiilin omistajan kanssa. Voi olla epäilyttävää, jos korkeassa asemassa esiintyvällä henkilöllä on profiilikuvanaan lapsuuskuva. Myös kirjoitustapa voi kieliä huijauksesta. Jos nuorena esiintyvä henkilö käyttää aikuiselle sopivampaa sanastoa tai tietää paljon tapahtumista, joista useimmat nuoret henkilöt eivät tiedä, todellinen käyttäjä on voinut väärentää profiilin.

Monet tietojen kalastelukeinot ja käyttäjän manipulaatiota hyödyntävät hyökkäykset perustuvat ainakin osittain huijausprofiilin käyttämiselle. Seuraavassa luvussa kerrotaan esimerkiksi profiilin kloonaushyökkäyksestä, jossa huijari luo kopion oikeasti olemassa olevan henkilön profiilista. Tässä luvussa sen sijaan kuvattiin yleisesti huijausprofiilin piirteitä ja profiileiden henkilöt voivat olla joko kuvitteellisia tai oikeita ihmisiä. Profiilin kloonaushyökkäys on eräs keino hyödyntää huijausprofiilia, mutta keskeistä siinä on se, että kloonatun profiilin henkilö on oikeasti olemassa ja hänellä on jo profiili. Ihmisen luontaista käyttäytymistä on helppo hyödyntää, eikä sitä voi estää teknisin keinoin. Tämä on heikko lenkki tietojen kalastelulta suojautumisessa, sillä palomuurit ja virustorjuntaohjelmistot eivät yllä suojaamaan tietokoneen ulkopuolella olevilta uhkilta.

3.6 Käyttäjien hyväuskoisuuden syyt

Kuten aikaisemmin mainittiin, käyttäjän manipulaatio perustuu ihmisen luontaisen käyttäytymisen hyödyntämiseen. Huijaus- ja roskapostiviestit on yleensä

helppo erottaa luotettavista viesteistä, mutta silti käyttäjät lankeavat niihin viesti toisensa jälkeen.

Luottamus yleensä kasvaa sitä vahvemmaksi, mitä kauemmin uhri on tekemisissä huijarin kanssa. Myös Mitnickin (2002) malli korostaa luottamuksen kehittämisen tärkeyttä, mutta on selvää, ettei luottamus synny sekunneissa. Wattersin (2009) mukaan positiivisiksi koetut ja onnistuneet tilanteet vastapuolen kanssa vähentävät epäluottamusta.

Käyttäjän suhde tiettyyn verkkokauppaan, sosiaalisen median palveluun ynnä muihin sellaisiin vaikuttaa siihen, miten paljon hän luottaa vastapuolelta tulleeseen viestiin. Mikäli käyttäjä esimerkiksi saa viestin verkkokaupassa tehdystä ostoksesta, johon hänellä ei ole yhteyttä, todennäköisesti käyttäjä epäilee viestin aitoutta. Vastaavasti jos käyttäjä on tilannut aikaisemmin tuotteita ja ollut tyytyväinen tekemiinsä kauppoihin, riski joutua tietojen kalastelun kohteeksi kasvaa, sillä käyttäjä todennäköisesti luottaa viestin oikeellisuuteen ja luotettavuuteen. (Watters, 2009.) Tiettyjen yritysten ja organisaatioiden nimissä tehdyt tietojen kalasteluyritykset nojaavat olettamukseen, että käyttäjä on juuri sen tahon asiakas. Aikaisempi luottamuksellinen suhde saa käyttäjän toimimaan halutulla tavalla ja jo olemassa oleva yhteys kasvattaa kynnystä kyseenalaistaa. Jos käyttäjä käyttää usein tiettyä verkkokauppaa tai palvelua ja on tottunut sieltä tulleisiin viesteihin ja ilmoituksiin, hän voi rutiininomaisesti avata huijarin viestissä olevan haitallisen linkin tai liitteen, koska epähuomiossa katsoo viestin tulevan käyttämästään palvelusta.

Benenson, Girard, Hintz ja Luder (2014) ovat vertailleet Facebookin ja perinteisen sähköpostin kautta tulleen haitallisen linkin avaamisen todennäköisyyttä. Tutkimuksessa huomattiin, että sähköpostin kautta linkki avattiin useammin kuin tilanteessa, jossa viesti vastaanotettiin Facebookin kautta. Sosiaalisen median palveluissa käyttäjällä on edes pieni mahdollisuus selvittää tietoja viestin lähettäjästä, ja tutkimuksen mukaan Facebookissa käyttäjät ottivatkin yhteyttä viestin lähettäjään lähes kolme kertaa niin useasti kuin sähköpostin lähettäjään. Toisaalta Benenson ym. (2014) havaitsivat, etteivät Facebook-viestin lähettäjän yksityisyysasetukset vaikuttaneet siihen, avasivatko käyttäjät viestin sisältämän linkin, mikä voi indikoida siitä, että linkki avattiin ennen kuin käyttäjä vieraili lähettäjän profiilissa.

Ihmisen luonteeseen kuuluu uteliaisuus, joka osaltaan on syynä tietojen kalasteluhyökkäysten onnistumiselle. Sosiaalisen median palveluissa kiertää jatkuvasti videoita ja linkkejä huomiota herättävillä otsikoilla, jotka houkuttelevat avaamaan linkin. Usein otsikot lupaavat videon paljastavan jotain uskomatonta, ennennäkemätöntä tai noloa. Uteliaisuus saa käyttäjän avaamaan linkin, joka todellisuudessa saattaakin olla tietojen kalasteluyritys tai sen kautta voi latautua virus- tai muu haittaohjelma.

On olemassa useita tapauksia nettirakkaasta, joka onkin lopulta paljastunut vain rahat vieväksi huijariksi. Tällaiset tapaukset vetoavat ihmistä vahvasti tunteisiin, ja tunne-elämältään haavoittuvaiset henkilöt ovat erityisen hyviä kohteita. Nettirakkaushuijauksessa huijari esiintyy väärän identiteetin turvin uhriin rakastuneena henkilönä. Kun uhri alkaa luottaa ja rakastua huijariin, hui-

jari vaatii häneltä eri syihin vedoten rahaa. Huijaus jatkuu, kunnes uhri tajuaa tulleensa huijatuksi. (Buchanan & Whitty, 2013.)

Buchananin ja Whittyn (2013) mukaan nettirakkaushuijauksiin lankeavat uhrit ovat yksinäisiä ja helposti johdateltavissa olevia henkilöitä. Ihmisen tarve kokea hyväksyntää, tulla rakastetuksi ja rakastaa ovat perustarpeita elämässä, ja näitä käyttäjä uskoo saavansa huijarilta.

3.7 Sosiaalisen median haavoittuvuus

Sosiaalisen median palvelut ovat haavoittuvaisia monesta syystä. Ensinnäkin niihin rekisteröityminen on helppoa, sillä profiilin tekemiseen tarvitaan yleensä vain nimi ja toimiva sähköpostiosoite. Nimen käyttäjä voi keksiä itse, eikä sähköpostinosoitteenkaan tarvitse perustua oikeille tiedoille. Pääasia on, että käyttäjällä on pääsy sähköpostiin kyseisellä osoitteella, sillä profiilin luomisen yhteydessä sähköpostiin yleensä lähetetään vahvistamisviesti. Koska profiilin luominen on näin yksinkertaista, on yhtä helppoa tehdä sekä oikea että huijaustili. Vaikka useat palvelut ovatkin kieltäneet huijausprofiileiden luomisen, käytännössä kiellon noudattamista on todella hankala valvoa. Useimmiten huijausprofiileiden kiinnisaaminen on muiden käyttäjien aktiivisuuden ansiota. Mutta vaikka huijausprofiilit poistetaankin, huijari voi edelleen yhtä helposti luoda uuden profiilin poistetun tilalle.

Palveluissa identiteettiä ei vahvisteta esimerkiksi verkkopankkitunnusten tai luottokortin avulla. On kuitenkin ymmärrettävää, että useassa maanosassa ja maassa toimivan palvelun on hankala järjestää universaalia ja luotettavaa tunnistautumista. Lisäksi myös alaikäiset käyttävät palveluita, eikä heillä välttämättä ole verkkopankkitunnuksia saati luottokorttia.

Eräs syy sosiaalisen median kyseenalaisesti hyödyntämisen helppouteen on käyttäjien huono tietoisuus yksityisyysasetuksista ja laiskuus muuttaa niitä. Useat palvelut määrittelevät oletusasetuksena profiilin olevan ainakin osittain julkinen, jolloin käyttäjä joutuu näkemään vaivaa ja hänen tulee itse haluta muuttaa asetuksia. De Paulan (2010) mukaan suuri osa käyttäjistä pitää profiilinsa ainakin osittain julkisena. Profiili voidaan jättää julkiseksi, sillä kavereiden ajatellaan löytävän tietty käyttäjä sitä helpommin, mitä enemmän tietoa on saatavilla. Myös suosiota voidaan tavoitella keräämällä paljon kavereita, mikä altistaa myös tietojen kalastelulle. Horjuvat perusteet pyytää kenet tahansa kaveriksi ja toisaalta hyväksyä tuntemattomienkin ihmisten kaveripyynnöt kasvattavat riskiä, että joku kaverilistalla olevista käyttäjistä on huijari.

Koska ihmiselle on luontaista luottaa tuttuihin henkilöihin, myös sosiaalisen median palveluissa uskotaan kavereiden julkaisemien linkkien viattomuuteen. Linkit on myös yleensä tehty houkuttelevan näköisiksi, mikä lisää alttiutta avata linkki.

Sosiaalisen median palveluiden ongelmana on myös se, että huijari ovat jo siellä. Heitä ei koskaan saada kitkettyä täysin pois jo olemassa olevista palveluista. Ratkaisuna voisi olla kokonaan uusi palvelu, joka perustuisi luotettavaan

tunnistautumiseen ja johon pääsisi vain muiden käyttäjien kutsusta. Toisaalta tämäkään ei poista ongelmaa lopullisesti, sillä yksikin palveluun pääsevä huijari romuttaa palvelun puhtauden. Näin ollen yksityisyyden ja tietoturvan parantaminen sekä tiedon levittäminen vaikuttavat toistaiseksi parhaalta mahdolliselta ratkaisulta ehkäistä tietojen kalastelua ja identiteetin varastamista.

3.8 Yhteenveto

Tässä luvussa käsiteltiin ensimmäisenä käyttäjän manipulointihyökkäystä, joka toimii paitsi omana tietojen kalastelukeinona, sitä hyödynnetään myös muiden hyökkäysten pohjana tai taustana. Käyttäjän manipulointi perustuu ihmisen luontaisen käyttäytymisen hyödyntämiseen. Tyypillisiä hyödynnettäviä luonteenpiirteitä ovat uteliaisuus, luottavaisuus ja auttamisen halu. Hyökkääjä saattaa myös esiintyä esimerkiksi työpaikan esimiehenä, poliisina tai verovirastona, jolloin käyttäjä tuntee velvollisuudekseen toimia pyydetyllä tavalla.

Vaikka käyttäjän manipulointi toimii myös itsenäisenä hyökkäyksenä, sitä hyödynnetään muun muassa huijausprofiileihin perustuvissa hyökkäyksissä. Käyttäjän manipuloinnin tarkoituksena on saada joku toimimaan hyökkääjän haluamalla tavalla ja uskomaan ja luottamaan hyökkääjään. Empiirisessä osuudessa tutkintaan, onko käyttäjän manipulointihyökkäyksen piirteitä havaittavissa tutkittavissa tapauksissa.

Käyttäjän manipuloinnista on olemassa erilaisia malleja, joilla kuvataan hyökkäyksen kaavaa. Käyttäjän manipuloinnin punainen lanka alkaa informaation keräämisestä kohteesta, ja siitä edetään luottamuksen kehittämiseen ja hyödyntämiseen, jolloin uhri paljastaa tietonsa. Eri tahot ovat eri mieltä siitä, päättyykö hyökkäys siihen, kun tarvittava tieto on saatu, vai katsotaanko vielä kerätyn tiedon jatkohyödyntäminen myös osaksi käyttäjän manipulointihyökkäystä. Kaikki mallit kuitenkin esittävät, että tavoitteena on muun muassa taloudellinen hyöty tai tietojen saaminen. Jos esimerkiksi uhrin salasanan käyttäminen on edellytys tavoitteen toteutumiselle, silloin salasanan hyödyntäminen tulee sisällyttää osaksi käyttäjän manipulointihyökkäystä.

Internetissä luottamuksen syntyminen eroaa fyysisen elämän vastaavasta. Fyysisessä elämässä toisen henkilön eleet, ilmeet ja sanattomat viestit kertovat paljon, kun taas Internetissä luotettavuus perustuu muihin tekijöihin. Vaikka hyökkääjä hyödyntääkin tyypillisiä, lähes jokaisessa ihmisessä esiintyviä piirteitä, tulee kuitenkin huomioida, etteivät ihmiset siltikään ole samanlaisia. Toinen luottaa herkästi tuntemattomaan henkilöön ja on helposti johdateltavissa, kun taas toinen tarvitsee enemmän vakuuttelua. Sosiaalisessa mediassa ihmistä pidetään luotettavana, mikäli hän on muun muassa hyvä kirjoittamaan, hyvännäköinen, kyvykäs, kuuluisa ja rehellinen. Luotettavana pidetään sellaista käyttäjää, joka on vuorovaikutuksessa muiden käyttäjien kanssa ja käyttää oikeaa nimeään. Tutkielman empiirisessä osuudessa selvitetäänkin, millaisia sosiaalisessa mediassa esiintyviä luotettavuuden piirteitä tutkittavissa tapauksissa on havaittavissa.

Eri sosiaalisen median palveluissa on helppo tehdä profiili. Toisen henkilön tietoja on helppo käyttää, sillä rekisteröitymiseen riittää puhelinnumero tai sähköpostiosoite. Puhelinnumero ja sähköpostiosoite tulee tietysti olla huijarin omia, mutta muut tiedot voi valehdella. Palvelut eivät tarkista esimerkiksi puhelinoperaattorilta numeron omistajan henkilöllisyyttä. Myös sähköpostiosoitteita voi luoda tarpeen mukaan. Huijausprofiilin avulla houkutellaan muut uskomaan, että käyttäjä on todellisuudessa se kuka väittääkin olevansa. Kirjallisuuden mukaan profiilin luominen sosiaalisen median palveluissa toisen henkilön nimellä on helppoa, eikä vaadi teknistä osaamista. Tutkielman empiirisessä osuudessa selvitetään, onko toisen henkilön nimellä tehtyjä huijausprofiileita hyödynnetty tutkittavissa tapauksissa ja millaisiin tarkoituksiin.

Seitsemännessä alaluvussa kuvattiin sosiaalisen median haavoittuvuutta. Sosiaalisen median palvelut ovat haavoittuvaisia ja alttiita käyttäjän manipuloinnille. Rekisteröityminen ei vaadi henkilöllisyyden vahvistamista. Vaikka huijausprofiileiden tekeminen onkin kielletty, säännön noudattamisen valvonta on hankalaa. Huijaustileistä voi ilmoittaa ylläpidolle, jolloin ne ajan myötä poistetaan, mutta uusia epäilyttäviä tilejä ilmestyy tilalle heti. Aikaa myöten rehellisistäkin ihmisistä voi tulla huijareita. Huijareita on siten mahdoton poistaa kokonaan yhdestäkään palvelusta nykyisillä keinoilla.

4 IDENTITEETIN VARASTAMINEN JA TIETOJEN KALASTELU

Tässä luvussa käsitellään erilaisia keinoja, joilla voidaan varastaa henkilön identiteetti tai muuta arkaluontoista tietoa sosiaalisen median palveluissa. Tietojen kalastelu voidaan toteuttaa joko käyttäen teknisiä menetelmiä (esimerkiksi välistävetohyökkäys) tai ihmisen luontaista käyttäytymistä hyödyntäviä menetelmiä.

4.1 Profiilin kloonaus

Profiilin tai identiteetin kloonaus (engl. profile cloning, identity clone attack, ICA) on hyökkäyskeino, jossa rikollinen kopioi ja väärentää olemassa olevan käyttäjän tiedoilla profiilin joko samassa tai toisessa sosiaalisen median palvelussa. Tarkoituksena on hankkia henkilökohtaista tietoa uhrista ja uhrin ystävistä ja kasvattaa luottamusta ystäväpiirissä, jotta yhä useampi käyttäjä olisi helpommin huijattavissa. (Rizi ym., 2014.) Usein käyttäjä ilmoittaa profiilissaan ainakin nimensä, sukupuolensa, koulutuksensa ja asuinpaikkansa (Khayyambashi & Rizi, 2013).

4.1.1 Kloonaus saman palvelun sisällä

Ensimmäinen keino toteuttaa profiilin kloonaushyökkäys on hyödyntää identiteettiä saman sosiaalisen median palvelun sisällä (engl. same-site profile cloning), jolloin sekä uhrin profiili sekä väärennetty profiili ovat samassa palvelussa (Rizi ym., 2014; Devmane & Rana, 2014). Hyökkääjä voi lähettää väärennetyn profiilin kautta kaveripyyntöjä uhrin ystäville. Ystävät olettavat, että pyyntö tulee oikealta henkilöltä ja näin ollen hyväksyvät sen. Tämän jälkeen hyökkääjän on mahdollista nähdä uhrin ystävien profiilien tiedot ja julkaisut. (Rizi ym., 2014; Khayyambashi & Rizi, 2013.) Hyökkääjän oletus on, etteivät uhrin ystävät

epäile kaveripyynnön aitoutta, vaikka kaveripyyntö tuleekin sellaiselta henkilöltä, jolla on jo tili kyseisessä palvelussa, ja joka on jo heidän kaverilistallaan (engl. friend list). Kaveripyynnön hyväksymisen todennäköisyyteen vaikuttaa myös se, kuinka paljon uhri ja hänen ystävänsä ovat toistensa kanssa yhteyksissä. Jos uhri ja ystävä ovat vain vähän yhteyksissä ja oikea kaveripyyntö on lähetetty ja hyväksytty vuosia aikaisemmin, ei ystävä välttämättä muista, että uhri on jo hänen kaverilistallaan. Näin ollen väärennetyn profiilin kaveripyyntö hyväksytään todennäköisemmin. (Devmane & Rana, 2014.) Vastaavasti jos uhri ja hänen ystävänsä ovat usein tekemisissä toistensa kanssa ja tapaavat myös fyysisessä elämässä, on oletettavaa, että uusi kaveripyyntö tulee jossain vaiheessa esille. Ainakaan Facebook ei toistaiseksi ilmoita uuden kaveripyynnön saapuessa, jos käyttäjä on jo samannimisen henkilön kaveri, joten on tärkeää olla itse aktiivinen ja valvoa omaa kaverilistaansa.

4.1.2 Kloonaus käyttäen eri palveluita

Toinen keino tehdä profiilin kloonaushyökkäys on hyödyntää kahta eri sosiaalisen median palvelua (engl. cross-site profile cloning). Tällöin uhrin profiili ja hyökkääjän luoma väärennetty profiili sijaitsevat eri sosiaalisen median palveluissa. Hyökkääjän on helpompi toteuttaa hyökkäys, jos palvelut ovat luonteeltaan samanlaisia. Esimerkiksi ammatillisten suhteiden luomiseen keskittyvät palvelut Linkedin ja XIAN ovat samankaltaisia ja käyttäjien julkaisema informaation luonne on yhtenevä molemmissa palveluissa. (Khayyambashi & Rizi, 2013.) Käytettäessä samankaltaisia palveluita hyökkääjä voi hyödyntää tehokkaammin uhrin profiilia.

Useampaa palvelua hyödyntävän kloonaushyökkäyksen tarkoituksena on kerätä ensin uhrista tietoa palvelussa, jossa hänellä on profiili, ja sitten luoda kerätyn tiedon avulla profiili johonkin sellaiseen toiseen palveluun, jossa uhrilla ei ole profiilia. (Rizi ym., 2014; Devmane & Rana, 2014.) Hyökkäyksen ensimmäinen vaihe on se, että hyökkääjä luo uhrista profiilin, jolla on sama nimi ja joka mahdollisesti sisältää muita väärennettyjä tietoja uhrista. Hyökkääjän tulee kerätä uhrista niin paljon tietoa, että väärennetty profiili näyttää oikealta. Useimmissa sosiaalisen median palveluissa käyttäjän nimi näkyy julkisesti ja se on myös avainattribuutti. Muita tietoja voi löytyä uhrin oikeasta profiilista toisessa sosiaalisen median palvelussa tai hänen kotisivultaan, jos hänellä sellainen on. (Rizi ym., 2014.) Toisaalta on myös mahdollista, että uhri on rajoittanut profiilinsa julkisuutta niin paljon, ettei se juurikaan tarjoa tietoa hyökkääjälle. Tämä ei kuitenkaan estä identiteetin ja tietojen varastamista, vaikka se vaatiikin hyökkäyksen tarkempaa suunnittelua. Mikäli attribuutit eivät ole hyökkääjän tiedossa, hän voi tehdä niistä yksityisiä, jolloin uhrin ystävät näkevät vain varmat julkiset tiedot. Hyökkääjä voi osittain arvata uhrin yksityisyysasetukset tutkimalla tämän julkisesti näkyvää profiilia. Se, mikä ei näy hyökkääjälle, on todennäköisesti yksityisyydeltään rajoitettu. Vaikka uhri olisikin asettanut osan henkilökohtaisesta tiedosta julkiseksi, voi hyökkääjä asettaa tiedon väärennetyssä profiilissa yksityiseksi, jotta väärennetty profiili vaikuttaisi aidommalta. (Rizi ym., 2014; Jin 2011.)

Useampaa sosiaalisen median palvelua hyödyntävää hyökkäystä vastaan sekä palvelun tarjoajien että uhrin on vaikeampaa suojautua ja väärennettyä profiilia on vaikeampi havaita (Devmane & Rana, 2014). Palvelun tarjoajan näkökulmasta näyttää vain siltä, että palveluun on rekisteröitynyt uusi käyttäjä (Khayyambashi & Rizi, 2013). On myös oletettavaa, ettei uhrilla ole syytä etsiä hänestä luotua profiilia muualta. Lisäksi ne uhrin ystävät, jotka käyttävät toista palvelua, ja joita hyökkääjä pyytää ystäväkseen, ajattelevat että kaveripyyntö tulee oikealta henkilöltä. Tulee kuitenkin ottaa huomioon, että myös tässä hyökkäyksessä todennäköisyys hyväksyä kaveripyyntö tai muu vastaava riippuu uhrin ja tämän ystävien välisestä muusta kommunikoinnista.

4.1.3 Väärennetyn profiilin hyödyntäminen

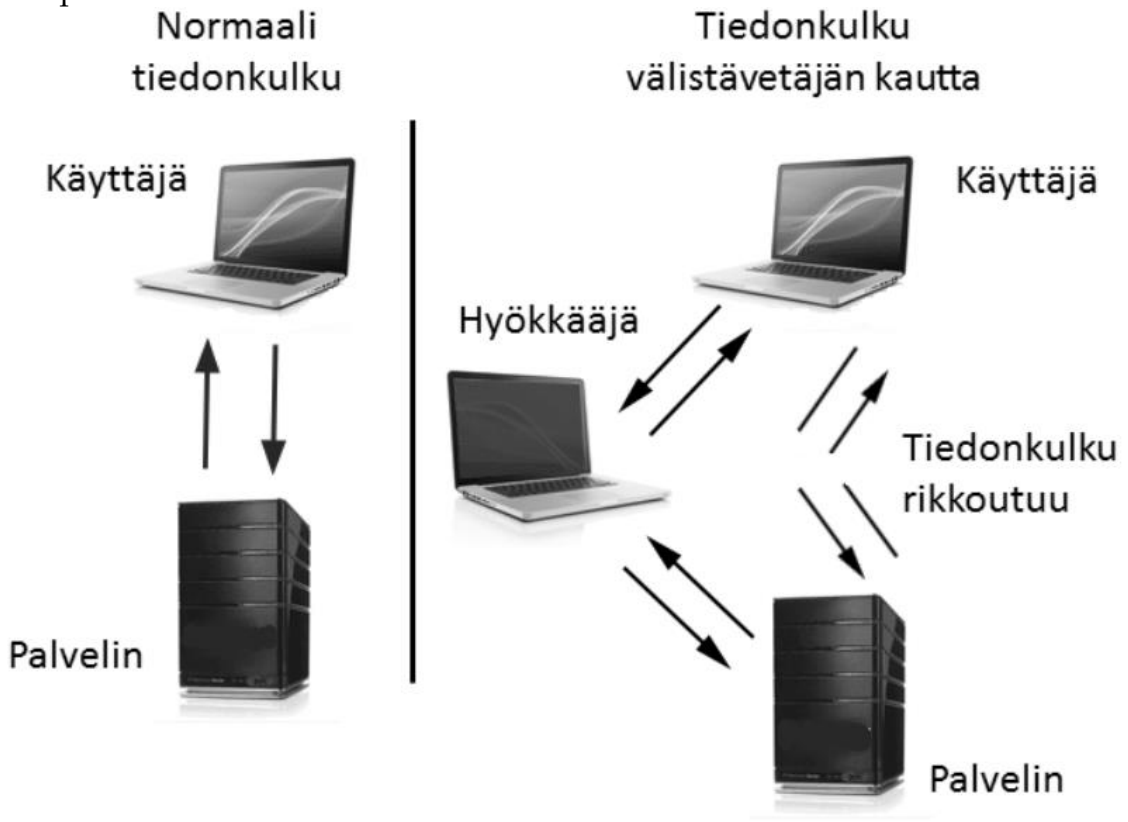
Kun hyökkääjä on saanut muodostettua siteen uhrin ystävien kanssa, väärennettyä profiilia voidaan hyödyntää ”drive-by download” -hyökkäykseen, tietojen kalasteluun ja muihin hyökkäyksiin (Kontaxis ym., 2011). Väärennetyn profiilin kautta on helppo lähettää linkkejä ja viestejä, jotka uhrin ystävät todennäköisesti avaavat, ovathan ne heidän luotetun ”ystävänsä” lähettämiä (Devmane & Rana, 2014.) Täten hyökkääjä myös hyödyntää uhrin mainetta tämän ystävien keskuudessa (Rizi ym. 2014). Lisäksi hyökkääjä voi lähettää uhrin nimissä väärennettyjä viestejä ja kommentteja, joiden tarkoituksena on aiheuttaa harmia uhrille (Kontaxis ym., 2011).

On myös mahdollista, ettei uhrilla ole lainkaan tiliä missään sosiaalisen median palvelussa. Hyökkääjä voi silti luoda profiilin uhrin nimissä, ja hyödyntää sitä saadakseen uhrin ystäviltä tietoa uhrista itsestään. (Rizi ym., 2014.) Hyökkääjän on tärkeä saada luottamusta uhrin ystävien keskuudessa. Mitä useampi käyttäjä hyväksyy hyökkääjän kaveripyynnön, sitä tarkemmin hyökkääjä pystyy väärentämään uhrin profiilin ja esiintymään uhrina. (Rizi ym., 2014.)

4.2 Välistävetohyökkäys

Sosiaalisen median palveluissa välistävetohyökkäystä (engl. man-in-the-middle attack, friend-in-the-middle attack) käytetään kerätessä tietoa. Kerättyä tietoa voidaan hyödyntää myöhemmin muissa tietojen kalastelu- ja hyökkäysmenetelmissä. Välistävetohyökkäys tarkoittaa aktiivista istunnon salakuunteluhyökkäystä sosiaalisen median palveluita vastaan. Hyökkäys perustuu suojaamattoman kommunikaatiolinkin hyödyntämiseen käyttäjän ja palveluntarjoajan välillä. Kaappaamalla istunnon evästeet hyökkääjä voi esiintyä uhrina ilman riittävää todentamista ja soluttautua uhrin sosiaaliseen verkostoon. (Huber, Mulazzani, Kitzler, Goluch & Weippl, 2011; Cashion & Bassiouni, 2011.) Joshin ym. (2009) mukaan hyökkääjä voi asettua välistävetäjäksi riippumatta siitä, onko sivusto suojattu vai ei. Kuviossa 5 kuvataan, miten tieto kulkee normaalisti

verrattuna tilanteeseen, jossa hyökkääjä on kaapannut istunnon käyttäjän ja alkuperäisen sivuston välillä.



KUVIO 5 Kaappauksen jälkeen tieto kulkee hyökkääjän kautta (DuPaul, 2014)

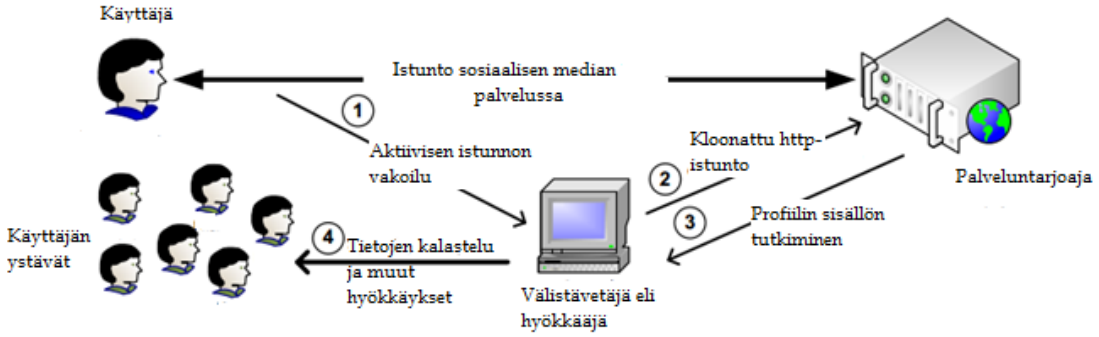
Aikaisemmin sosiaalisen median palveluissa oli ongelmana se, että suurin osa palveluista tarjosi tietojen lähetyksen salaamattoman http-yhteyden kautta. Yhteys saattoi olla salatussa https-muodossa vain kirjautumisen ajan, jonka jälkeen se muuttui salaamattomaksi. Aikaisemmin esimerkiksi Facebookin asetuksista pystyi valitsemaan salatun https-yhteyden käytön, mutta tämä suosi vain niitä käyttäjiä, jotka olivat riittävän tietoisia mahdollisuudesta salattuun yhteyteen, ja jotka näkivät vaivaa muuttaakseen oletusasetuksia. Oletuksena palvelu siis jätti käyttäjät suojaamattomiksi (Huber ym., 2011). Myöhemmin Facebook muutti käytäntöä, ja nykyisin sivusto käyttää https-yhteyttä koko istunnon ajan automaattisesti.

Toteutus

Hyökkääjä voi kaapata istunnon kommunikaatiolinkin palveluntarjoajan ja käyttäjän välillä joko passiivisesti tai aktiivisesti. Passiivinen hyökkäys tarkoittaa, että hyökkääjä hyödyntää salaamattomia langattomia verkkoja. Aktiivisessa hyökkäyksessä hyödynnetään käyttäjän koneelle asennettua haittaohjelmaa. (Huber ym., 2011.)

Kuviossa 6 havainnollistetaan välistävetohyökkäyksen toteuttamista. Hyökkäys vaatii onnistuakseen sen, että kohdekäyttäjä on juuri sillä hetkellä

kirjautuneena palveluun ja että hän käyttää suojaamatonta http-yhteyttä. Aluksi hyökkääjä valvoo erillisellä sovelluksella uhrin verkkoyhteyttä. Kun sovellus havaitsee aktiivisen istunnon sosiaalisen median palvelussa, se kloonaa täydellisen http-vastauksen, joka sisältää istuntoon liittyvät evästeet. Kloonattu http-vastaus toimii validina todentamisena palveluntarjoajan näkökulmasta, joten se kaappaa väliaikaisesti käyttäjän istunnon palvelussa. Hyökkääjä on tämän jälkeen yhteydessä palveluntarjoajaan ikään kuin käyttäjän näkökulmasta ilman, että palveluntarjoaja tai käyttäjä sitä huomaa. (Huber ym., 2011.)



KUVIO 6 Välistävetohyökkäys sosiaalisessa mediassa (Huber ym., 2011)

Kun hyökkääjä on kaapannut istunnon, hän voi lähettää kaapatun käyttäjän profiililla kaveripyyntöjä muille käyttäjille. Kaveripyyntö näyttää tulevan uhrilta, eikä mikään varoita siitä, että joku muu kuin uhri käyttää profiilia. Kaapatun istunnon ansiosta hyökkääjä pystyy toimimaan palvelussa kuten oikea käyttäjä, ikään kuin hän omistaisi profiilin. (Huber ym., 2011.) Näin hyökkääjä soluttautuu käyttäjän sosiaaliseen verkostoon ja pystyy hyödyntämään muiden käyttäjien profiileista saatavaa henkilökohtaista tietoa ja levittämään verkoston sisällä vahingollisia viestejä ja linkkejä. (Huber ym., 2011.) Vahingollisten viestien ja linkkien tarkoituksena on houkutella käyttäjää paljastamaan lisää henkilökohtaista tietoa, kuten salasanoja ja luottokorttinumeroita, joita myöhemmin voidaan käyttää identiteettivarkauksissa.

Hyökkääjä voi tehostaa lähettämiensä viestien luotettavuudentuntua tutkimalla käyttäjän aikaisempia kommentteja, viestejä ja muita julkaisuja (Huber ym., 2011). Näin hän pystyy selvittämään esimerkiksi uhrin kielen tai erikoiset sanat ja ilmaisut, joita tämä saattaa käyttää julkaisuissaan.

Hyökkääjä voi myös asentaa räätälöidyn kolmannen osapuolen sovelluksen uhrin profiiliin. Sovelluksen päämääränä on louhia käyttäjästä ja tämän ystävistä mahdollisimman paljon tietoa, muun muassa sähköpostiosoitteita. Sovelluksen kerättyä tarpeeksi tietoa hyökkääjä poistaa kyseisen sovelluksen profiilista. Louhittua arkaluontoista tietoa hyökkääjä käyttää esimerkiksi luodakseen roskaposti- ja tietojenkalasteluviestejä. (Huber ym., 2011.)

4.3 Profiilin deaktivoiminen

Facebookissa käyttäjällä on mahdollisuus tilapäisesti poistaa tili käytöstä eli deaktivoida se. Profiili ei siis poistu palvelusta, vaan se ikään kuin muuttuu näkymättömäksi. Deaktivoitu profiili ei löydy hakutoiminnolla eikä sitä pääse katsomaan. Kaikki profiilin aktiivisuus, julkaisut, kommentit ynnä muut sellaiset häviävät näkyvistä. Deaktivoitu profiili näkyy ainoastaan kaverilistalla, mutta sitäkään kautta ei voi siirtyä profiiliin, koska se on poistettu käytöstä. Kun käyttäjä palauttaa eli aktivoi profiilin uudestaan, näkyvät taas julkaisut ja itse profiili.

Mahmood ja Desmedt (2012) esittelevät hyökkäyksen, jossa hyödynnetään siirtymistä deaktivointi- ja aktivointi-tilan välillä. Hyökkäys oli ennen erityisen hankala estää, sillä deaktivoitua profiilia ei voinut poistaa kaverilistalta tai siirtää listalta toiselle. Sittemmin Facebook on muuttanut käytäntöään, mutta deaktivointihyökkäys on edelleen helppo ja tehokas keino kerätä henkilökohtaista tietoa käyttäjistä, sillä ollessaan deaktiivisena profiili näkyy vain kaverilistalla ja kohdekäyttäjä voi unohtaa, että hyökkääjä ylipäätään on hänen kaverilistallaan.

Hyökkäys on nimenomaan suunniteltu toteutettavaksi Facebookissa, sillä muut palvelut eivät tarjoa mahdollisuutta asettaa profiili käytöstä poistetuksi pelkän poistamisen sijasta. Hyökkäyksen ensimmäinen vaihe on se, että hyökkääjä yrittää tavalla tai toisella päästä kohdekäyttäjän kaveriksi. Tässä voidaan hyödyntää eri menetelmiä aina huijausprofiileista välistävetohyökkäykseen. Kun käyttäjä on hyväksynyt tai pakotettu hyväksymään hyökkääjän kaveripyyntö, muuttaa hyökkääjä profiilinsa deaktiiviseksi. Tämän jälkeen hyökkääjä palaa aktiiviseksi yleensä sellaiseen aikaan vuorokaudesta, kun on todennäköistä, ettei kohdekäyttäjä ole online-tilassa palvelussa eikä siten voi nähdä hyökkääjän esimerkiksi ilmestyvän keskustelulistalle (Mahmood & Desmedt, 2012). Näin hyökkääjä voi rauhassa etsiä tietoa käyttäjistä. Kun hyökkääjä on saanut kerättyä riittävän määrän tietoa, hän muuttaa profiilinsa takaisin deaktiiviseksi. Yleensä hyökkääjä on aktiivisena vain hetken aikaa minimoidakseen kiinnijäämisen riskin, joten hän joutuu toistamaan tilojen vaihtelua useamman kerran kerätäkseen suuren määrän tietoa. Toisaalta hyökkääjä voisi kirjoittaa jonkin ohjelman tai luoda sovelluksen, joka kerää automaattisesti tietoa uhrin ja tämän kavereiden profiileista.

Aikaisemmin profiilia ei voinut poistaa kaverilistalta profiilin ollessa deaktivoitu. Siten mahdollisuus poistaa profiili oli erittäin pieni, sillä poistaminen vaati sen, että kohdekäyttäjä ja aktiivinen hyökkääjä olivat online-tilassa samaan aikaan. Koska hyökkääjän tiedonkeruuhetket olivat lyhyitä, todennäköisyys olla samaan aikaan kirjautuneena Facebookiin oli minimaalinen. (Mahmood, & Desmedt, 2012.)

Facebookissa on mahdollista jaotella kavereita erilaisiin listoihin ja asettaa näille erilainen julkaisujen näkyvyys. Deaktivoitua profiilia ei voinut aikaisemmin siirtää edes listalta toiselle, mikä takasi hyökkääjälle sen, etteivät mitkään käyttäjän sille ryhmälle julkaisemat päivitykset olleet turvassa hyökkääjäl-

tä. Ainoa vaihtoehto oli olla julkaisematta päivityksiä kyseiselle ryhmälle tai siirtää muut ryhmään kuuluvat toiseen ryhmään, mikä toi käyttäjälle paljon lisätyötä. Tietysti käyttäjä olisi voinut itsekin deaktivoida tilinsä, jolloin tietojen kalastelija ei olisi nähnyt hänen profiiliaan. Kuitenkin on todennäköistä, että siinä vaiheessa, kun käyttäjä huomaa epäilyttävän deaktivoidun profiilin, on sen omistaja jo ehtinyt kerätä tietoa.

4.4 Twitterin hyödyntäminen

Twitter nojaa vahvasti avoimuuteen ja yksinkertaisuuteen. Käyttäjät ovat toistensa kanssa vuorovaikutuksessa tviittien kautta. Yhden tviitin pituus voi olla korkeintaan 140 merkkiä pitkä, mikä pakottaa käyttäjät tiivistämään sanottavansa. Tviitin voi luokitella koskemaan tiettyä aihetta laittamalla #-merkin ennen aihesanaa, esimerkiksi ”Jääkiekon #MM-kisat 2015”. Käyttäjä voi myös merkitä toisen käyttäjän tviittiinsä käyttämällä @-merkkiä halutun käyttäjänimen edessä, esimerkiksi @käyttäjä. (Sivanesh, Kavin & Hassan, 2013.) Tällöin tviitti on ikään kuin julkinen viesti kyseiselle käyttäjälle ja hän saa ilmoituksen siitä, että hänet on merkitty toisen käyttäjän tviittiin. Myös yksityisten viestien lähettäminen on mahdollista. Tämä edellyttää, että viestin osapuolet ovat toistensa seurannassa. Yksityisviestit näkevät ainoastaan lähettäjä ja vastaanottaja.

Twitterissä ei ole erillistä kaveripyyntöä, vaan kahden käyttäjän välinen linkki perustuu seuraamiseen (engl. following). Käyttäjä voi seurata muita käyttäjiä saadakseen näiden päivitykset eli tviitit ja häntä voidaan seurata. Tviittejä voi myös tviitata uudelleen (engl. retweet). Käyttäjä voi rajoittaa julkaisujensa näkyvyyttä suojaamalla tviittinsä, jolloin vain hänen hyväksymänsä käyttäjät näkevät ne. Tällöin käyttäjä tulee vahvistaa erikseen jokainen seurauspyyntö. Oletuksena tviitit kuitenkin näkyvät julkisesti.

Seuraamisen ei ole pakko perustua vastavuoroisuuteen: käyttäjä voi seurata henkilöä, joka ei seuraa häntä ja toisinpäin. Nykyisin myös Facebook on mahdollistanut toisen käyttäjän seuraamisen, jolloin seuraaja näkee seurattavan julkiset julkaisut.

4.4.1 Haitalliset tviitit

Koska yhden tviitin pituus on rajoitettu 140 merkkiin, erilaiset url-osoitteiden lyhennyspalvelut ovat tulleet suosituiksi. Lyhennyspalvelun ansiosta www-osoitteet eivät vie turhaan tilaa rajoitetussa tviittien merkkimäärässä, sillä palvelu lyhentää halutun osoitteen lyhytosoitteeksi. Lyhytosoitteet ovat normaaleja osoitteita, jotka on muutettu merkkimäärältään lyhyemmiksi. Esimerkkejä tunnetuista lyhennyspalveluista ovat TinyURL ja Bitly.

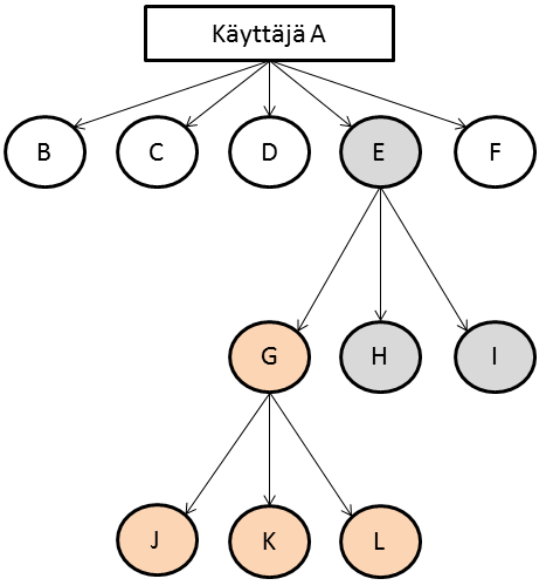
Lyhennyspalveluiden käyttöön liittyy kuitenkin muutamia riskejä. Sanzgirin, Hughesin ja Upadhyayan (2013) mukaan jotkut palvelut luovat samalle alkuperäiselle osoitteelle joka kerta uuden lyhytosoitteen. Tämä mahdollistaa sen, että esimerkiksi samalle tietojen kalastelusivustolle johtavalle osoitteelle

voi olla olemassa kymmeniä erilaisia lyhytosoitteita. Kun yksi lyhytosoite paljastuu haitalliseksi, tietojen kalastelijat luovat uuden. Toisaalta kalastelusivutkin ovat olemassa vain lyhyen aikaa, sillä paljastuttuaan huijauksiksi ne poistetaan.

Normaalisti käyttäjä voi varmistaa linkin todellisen osoitteen viemällä hiiren kursorin linkin päälle avaamatta sitä. Tällöin ilmestyy pieni valkoinen laatikko, joka ilmoittaa kohdeosoitteen. Lyhennyspalveluiden lyhentämät osoitteet eivät kuitenkaan paljasta alkuperäistä osoitetta, jolloin käyttäjä ei voi varmistaa, minne lyhytosoite todella johtaa. (Sanzgiri ym., 2013.)

Lyhennettyihin osoitteisiin liittyvät riskit ovat todellisia, sillä niiden kautta käyttäjä voi vahingossa ladata viruksia ja vakoiluohjelmia tai paljastaa henkilökohtaista tietoa. Hyökkääjät voivat levittää haitallisia linkkejä joko suoraan käyttäjille käyttämällä @-merkkiä päivityksissään tai julkaista haitallisen osoitteen sisältävän tviitin sellaisenaan ilman muiden käyttäjien merkitsemistä. Ensimmäisen keinon kautta linkki avataan Sanzgirin ym. (2013) mukaan epätodennäköisemmin, sillä monen käyttäjän merkitseminen herättää epäilyksiä ja Twitter luokitteleekin tällaista usein tekevät käyttäjät spämmääjiksi eli roskapostinlähettäjiksi. Lisäksi todennäköisyys, että merkitty käyttäjä avaa tuntemattoman tviitissä olevan lyhytosoitteen, on erittäin pieni. Jälkimmäinen keino vaatii sekin vaivannäköä, mutta onnistumisen todennäköisyys on korkeampi kuin ensimmäisessä tapauksessa. Tviitin tulee saavuttaa mahdollisimman suuri yleisö. Jos kukaan ei seuraa hyökkääjän tiliä eikä hän seuraa ketään, on tviitin näkyminen todella pientä. Hyökkääjä joutuu keräämään seurattavia ja seuraajia paitsi tviitin näkymisen takia, myös kasvattaakseen uskottavuutta, sillä pienikin interaktio lisää luottamusta käyttäjien välillä ja edesauttaa hyökkäyksen onnistumista. Syntyneen luottamuksen ansiosta linkki avataan todennäköisemmin. (Sanzgiri ym., 2013.)

Laajentamalla haitallisen tviitin näkyvyyttä hyökkääjä voi parantaa mahdollisuuksiaan saada käyttäjät avaamaan linkki. Twitterissä tviittien näkyvyydellä on puumainen rakenne. Kuvio 7 kuvaa tilannetta, jossa käyttäjän A tviitit näkyvät oletuksena kaikille hänen seuraajilleen. Kuvio havainnollistaa, miten tviitin näkyvyys laajentuu, kun käyttäjän A seuraajat uudelleentviittaavat sen. Kun A tviittaa, käyttäjät B-F näkevät A:n tviitin, koska he seuraavat tätä. Kun käyttäjä E uudelleentviittaa A:n tviitin, myös E:n seuraajat (G-I) näkevät A:n tviitin, vaikka he eivät seuraa A:ta. Tviitin näkyvyys laajenee edelleen, kun E:n seuraaja G tviittaa eteenpäin E:n uudelleentviittaaman tviitin omille seuraajilleen.



KUVIO 7 Tviitin näkyvyyden leviäminen (Sanzgiri ym., 2013)

Puumainen rakenne on eduksi haitallisen tviitin levittämisessä, mutta edelleenkin kohdekäyttäjien oma toiminta vaikuttaa tehokkuuteen ja todennäköisyyteen avata linkki. Mikäli hyökkääjä luottaa vain siihen, että käyttäjät uudelleentviittaavat vapaaehtoisesti tuntemattoman käyttäjän tviitin, hyökkäys voi epäonnistua eikä haitallinen tviitti leviä.

4.4.2 Twitter-botit

Twitterin käytön yleisyys ja palvelun avoin rakenne antavat mahdollisuuden käyttää botteja, jotka voivat uhata käyttäjien turvallisuutta. Botti (engl. bot, lyhenne sanasta robot) tarkoittaa skriptiä tai tietokoneohjelmaa, joka suorittaa määriteltyjä toimintoja toistuvasti ja automaattisesti. Botit voivat olla hyödyllisiä, sillä niitä voidaan käyttää suorittamaan toistuvia ja aikaakuluttavia toimintoja automaattisesti, mutta nykyään botteja hyödynnetään myös haitallisessa tarkoituksessa. Botteja voidaan käyttää esimerkiksi roskapostin lähettämisessä, tietojen kalastelussa ja palvelunestohyökkäyksissä. (Sivanesh ym., 2013.) Bottiverkko (engl. botnet, lyhenne sanoista robot network) koostuu nimensä mukaisesti boteista. Botit ovat kytkeytyneet toisiinsa tietoverkon välityksellä muodostaen oman verkon.

Bottien avulla Twitterissä voidaan suorittaa samoja toimintoja kuin normaalilla käyttäjätilillä. Twitterissä botit ovat luonteeltaan kuin kaksiteräinen miekka. Toisaalta botit vastaavat käyttäjiä hyödyttävistä toiminnoista, kuten RSS:stä, ja botteja voidaan käyttää myös julkaisemaan automaattisesti uutisia. (Sivanesh ym., 2013; Chu, Gianvechhio, Wang & Jajodia, 2012.) Vastakohtana hyvälle tarkoitukselle on bottien käyttäminen roskapostin ja haitallista materiaalia sisältävien tviittien julkaisemiseen. Botti voidaan ohjelmoida esimerkiksi seuraamaan mahdollisimman montaa käyttäjää siinä toivossa, että joku hyvä-

uskoinen käyttäjä seuraa takaisin. Näin haitalliset tviitit näkyvät käyttäjän uutisvirrassa. (Chu ym., 2012.)

4.4.3 Haitallisten tviittien ja bottien tunnistaminen

Haitalliset tviitit ovat usein houkuttelevia, jotta todennäköisyys avata niiden sisältämä linkki kasvaisi. Beckin (2011) mukaan jopa 98 % haitallisista tviiteistä sisältää linkin. Käyttäjän tuleekin suhtautua tuntemattomien käyttäjien tviittaamiin linkkeihin varauksella, ja tutkia mahdollisuuksien mukaan linkin todellinen alkuperä hiiren kursorin avulla. Lyhytosoitteista alkuperäistä linkkiä ei näe, joten tällaisia linkkejä ei kannata avata, ellei ole ehdottoman varma linkin luotettavuudesta. On aina parempi kirjoittaa haluttu osoite itse selaimen osoiteriville, kuin avata se valmiin linkin kautta.

Haitallisissa tviiteissä esiintyy myös tiettyjä sanoja useammin kuin tavallisissa tviiteissä. Haitalliset tviitit sisältävät usein muun muassa englanninkieliset sanat ”chat with” ja ”naughty”. Pornografisen materiaalin avulla houkuttelu on tavallista. (Beck, 2011.)

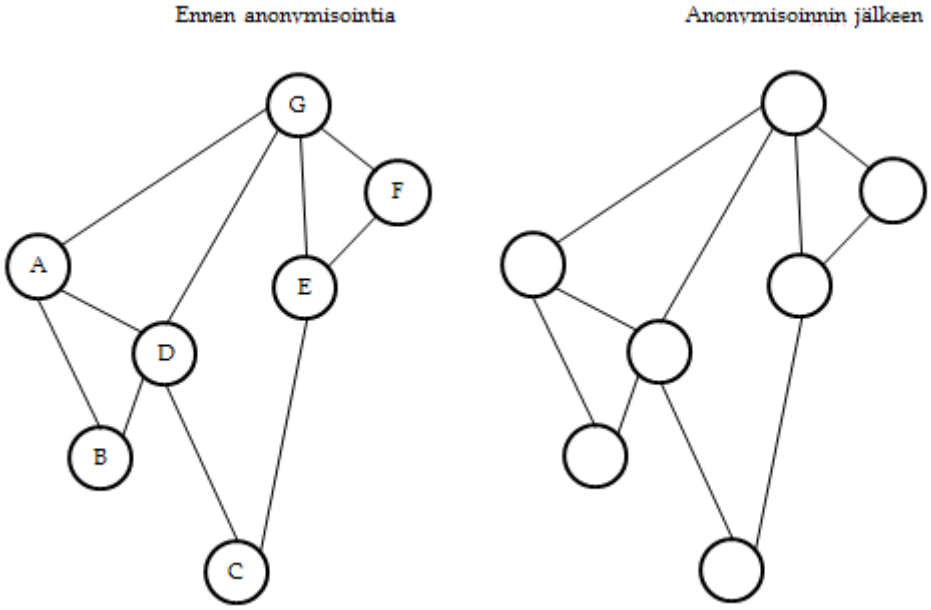
Haitalliset tviitit ovat myös yleensä pidempiä kuin normaalit tviitit, sillä niihin yritetään mahduttaa mahdollisimman paljon linkkejä sekä mainostavia ja houkuttelevia sanoja, jotta käyttää avaisi linkin. Myös käyttäjän seuraajien ja seurattavien määrä voi kertoa jotain tviitin vahingollisuudesta. Yleensä haitallisia tviittejä julkaiseva käyttäjä seuraa useampaa käyttäjää ja häntä seuraa useampi käyttäjä kuin normaalin käyttäjän kohdalla. (Lin & Huang, 2013.) Myös julkaisukanavasta voi tehdä päätelmiä, vaikka tämä ei luotettavasti kerrokaan, onko tviitti haitallinen. Linin ja Huangin (2013) mukaan normaalit käyttäjät tviittaavat tavallisimmin suoraan Twitterin kotisivun kautta Internetissä ja puhelimen avulla, kun taas roskapostinlähettäjät käyttävät Twitter-sovellusta ja muita varta vasten kehitettyjä työkaluja.

Myös interaktioiden määrä kertoo luotettavuudesta. Normaali käyttäjä on vuorovaikutuksessa sekä seurattavien että seuraajiensa kanssa (Lin & Huang, 2013). Hän kommentoi ja uudelleentviittaa muiden päivityksiä. Useimmat roskapostikäyttäjät eivät sen sijaan tee vastaavaa, vaan vuorovaikutus on yksisuuntaista, vaikka heillä olisikin paljon seuraajia tai seurattavia (Ahmed & Abulaish, 2012). Huijarit esimerkiksi merkitsevät muita käyttäjiä tviitteihinsä, mutta eivät kommentoi tai uudelleentviittaa näiden tviittejä.

Haitallisilla boteilla on samoja piirteitä kuin roskapostitviiteillä. Sivaneshin ym. (2013) mukaan bottien avulla generoidut käyttäjätilit ja julkaistut tviitit sisältävät usein url-osoitteita, jotka voivat johtaa vahingollisille sivustoille. Useimmat ”bottikäyttäjät” eivät ole myöskään suojanneet tai vahvistaneet käyttäjätiliään. Tviittien julkisuus on olennaista haitallisten tviittien levittämisessä. Lisäksi botit julkaisevat saman tviitin monta kertaa, kun taas tavalliset käyttäjät eivät toista itseään. Hieman ehkä yllättävä ominaisuus on myös se, että bottien avulla generoiduissa tviiteissä kiinnitetään huomiota myös välimerkkeihin, kun taas tavallinen käyttäjä ei ole niin tarkka kielioppisäännöistä. (Sivanesh ym., 2013.)

4.5 Käyttäjän deanonymisointi

Anonymisointi (engl. anonymisation) tarkoittaa henkilön arkaluontoisten tietojen korvaamista turvallisella tiedolla niin, ettei alkuperäistä henkilöä voida tunnistaa. Anonymisointi on eräs tapa suojata käyttäjän yksityisyys sosiaalisen median palveluissa. Sosiaalisen median palveluissa usein poistetaan tunnistetiedot, kuten nimi, osoite ja syntymäaika, mutta verkostosuhteet ovat edelleen nähtävissä (Peng, Li, Zou & Wu, 2014). Kuviossa 8 havainnollistetaan tätä prosessia. Vasemmanpuoleisessa kuvassa on anonymisoimaton tilanne, jossa voi nähdä kuka on kenenkin kanssa vuorovaikutuksessa. Oikeanpuoleinen tilanne on anonymisoinnin jälkeen. Kuvassa voi edelleen nähdä verkostosuhteet, mutta vuorovaikutuksessa olevien käyttäjien identiteettitiedot eivät näy.



KUVIO 8 Yksinkertainen havainnollistus anonymisoinnista (Peng ym., 2014)

Kuitenkin huolimatta käyttäjän identiteetin anonymisoinnista, on olemassa menetelmiä oikean identiteetin paljastamiseksi. Toteuttaakseen deanonymisointihyökkäyksen hyökkääjä hyödyntää olemassa olevaa taustatietoa käyttäjästä. Jos hyökkääjällä on uhrista tunnistettavaa tietoa, hän voi tunnistaa tämän anonymisoitujen käyttäjien tietojen joukosta. (Sharma, Mishra & Sharma, 2013.)

4.5.1 Ryhmän jäsenyyden hyödyntäminen deanonymisoinnissa

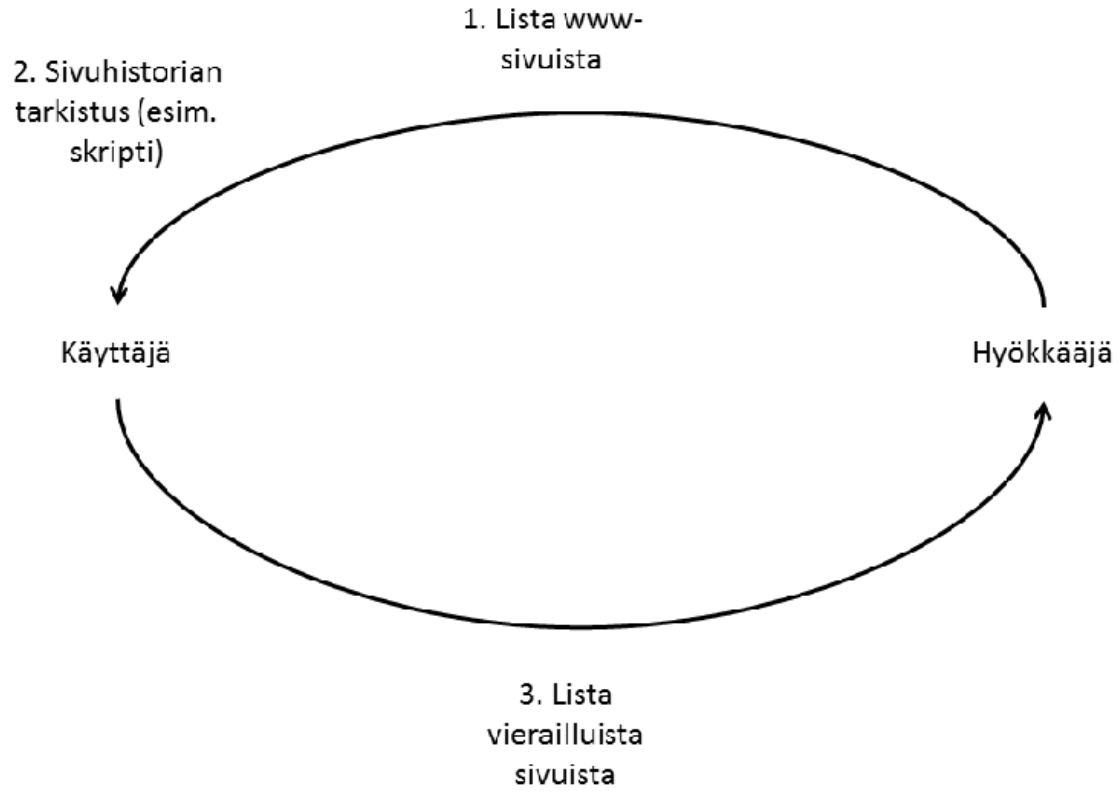
Useimmissa sosiaalisen median palveluissa käyttäjä voi luoda ryhmiä tai liittyä itse sellaiseen. Yleensä ryhmä keskittyy tiettyyn asiaan ja sen tarkoituksena on kerätä yhteen muita samasta asiasta kiinnostuneita käyttäjiä. Esimerkiksi Facebookissa ryhmien monipuolisuus on valtava. Palvelussa on ryhmiä aina puutarhanhoidosta, kimppakyytien etsintään ja kirpputoritoimintaan. Ryhmille on

ominaista hierarkkisesti järjestäytyminen. Yksi tai useampi käyttäjä voi toimia ryhmän ylläpitäjänä, jolla on oikeus poistaa muita käyttäjiä ja julkaisuja ja antaa ylläpito-oikeuksia. (Wondracek, Holz, Kirda & Kruegel, 2010.) Yleisesti ryhmät voivat olla joko julkisia tai yksityisiä. Julkinen ryhmä näkyy kaikille ja siihen voi kuka tahansa liittyä ilman erillistä pyyntöä tai vahvistusta. Yksityiseen ryhmään normaalisti täytyy lähettää liittymispyyntö, jonka ylläpitäjä hyväksyy tai hylkää. (Wondracek ym., 2010.) Yksityisten ryhmien päivitykset eivät yleensä näy ennen kuin ylläpitäjä on vahvistanut henkilön liittymisen ryhmään. Jäsenlista sen sijaan saattaa näkyä. Lisäksi esimerkiksi Facebookissa ryhmä voi olla myös salainen, jolloin se ei löydy edes hakutoiminnolla. Tällöin käyttäjä saa ylläpitäjältä erillisen kutsun liittyä ryhmään.

Wondracek ym. (2010) ovat tutkineet sellaista deanonymisointihyökkäystä, jossa hyödynnetään käyttäjän ryhmän jäsenyydestä saatavaa informaatiota sosiaalisen median palvelussa. Tietty käyttäjä on siis mahdollista identifioida tai ainakin voidaan merkittävästi vähentää mahdollisia vaihtoehtoja, mikäli käyttäjä kuuluu johonkin ryhmään palvelussa. Hyökkäys perustuu identiteettitietoa sisältävien dynaamisten hyperlinkkien analysointiin ja sivuhistorian vertaamiseen. Hyökkäyksen avulla ei voi sinänsä voi varastaa identiteettiä, mutta se voi mahdollistaa muun tiedon keräämisen käyttäjästä.

Kolmansien osapuolten evästeillä ja selainten laajennuksilla on mahdollista jäljittää käyttäjän Internetin käyttöä ja sivulatauksia, mutta ne eivät keskity käyttäjän identiteetin selvittämiseen. Näin käyttäjä voi vierailla sivustoilla anonyymisti tai ainakin pseudonyymin, joka on eräänlainen salanimi, suojassa. (Wondracek ym., 2010.)

Wondracekin ym. (2010) tutkimassa hyökkäyksessä hyökkääjä etsii tietoa sellaisen käyttäjän ryhmäjäsenyydestä, joka on juuri sillä hetkellä selailemassa Internetiä. Tässä hyökkääjä voi hyödyntää erilaisia keinoja varastaa käyttäjän sivuhistoria. Internet-selaimet käsittelevät hyperlinkkejä sen perusteella, onko käyttäjä aikaisemmin avannut linkin. Selain tarkistaa onko avattava linkki avattu aikaisemmin, ja jos on, se näkyy sivuhistoriassa. Hyökkääjä voi luoda html-sivun, jossa on linkkejä haluttuihin sivuihin ja taustakuvatagi. Kuviin voi viitata käyttämällä url-osoitetta, joten käyttäjän selain hakee nämä url-osoitteet, jos kohdesivu on sivuhistoriassa. Toinen vaihtoehto on käyttää käyttäjäpuolen skriptikieltä, esimerkiksi JavaScriptiä, jolla luodaan lista halutuista url-osoitteista ja sitten ohjelmallisesti tarkistetaan, onko osoite sivuhistoriassa. Hyökkääjän täytyy käydä läpi jokainen url-osoite erikseen saadakseen tietää, onko linkki sivuhistoriassa. (Wondracek ym., 2010.) Kuviossa 9 kuvataan, miten sivuhistorian varastaminen toimii semanttisesta näkökulmasta. Ensin uhri tulee saada sivulle, jossa hyökkääjän lista on. Selain saadaan lataamaan lista ja koodi, joka käy läpi uhrin sivuhistorian. Tämän jälkeen hyökkääjä saa tiedon sivuhistoriassa olevista osoitteista.



KUVIO 9 Käyttäjän sivuhistorian varastaminen (Wondracek ym., 2010)

Sivuhistorian avulla hyökkääjä voi etsiä tiettyjä web-osoitteita, jotka paljastavat käyttäjän kuuluvan johonkin ryhmään tietyssä sosiaalisen median palvelussa. Yhdistelemällä näitä tietoja aikaisemmin kerättyyn tietoon käyttäjän identiteetti on mahdollista selvittää. (Wondracek ym., 2010.) Sivuhistoria voi myös paljastaa esimerkiksi minkä pankin sivulla käyttäjä käy usein eli missä hänellä todennäköisesti on tili. Tietoa voidaan hyödyntää suunnitellessa muita hyökkäyksiä. Deanonymisointihyökkäys siis hyödyntää tietoa käyttäjän sosiaalisen median verkostoista ja hänen sivuhistoriaansa.

Hyökkääjän tulee saada mahdollisimman paljon tietoa ryhmistä ja niiden jäsenistä. Monissa sosiaalisen median palveluissa ryhmiä voi etsiä hakutoiminnolla ja palvelut voivat jopa tarjota listan olemassa olevista ryhmistä. Hyökkääjä on ennen kaikkea kiinnostunut ryhmän tunnisteista, jotta hän voi luoda hyperlinkkejä sivuhistorian varastamista varten. Hyökkääjä voi käyttää erilaisia valmiita tekniikoita, joilla voi ladata ryhmähakemiston ja louhia ryhmien tunnisteet sivuston lähdekoodista. (Wondracek, 2010.)

Saadakseen tietoa tietyn ryhmän jäsenistä hyökkääjä tutkii ryhmän jäsenlistaa, mikäli ryhmä on julkinen. Ongelmana kuitenkin on, että useat palvelut näyttävät vain tietyn määrän ryhmien jäsenistä, esimerkiksi Facebook on rajoittanut näkymistä niin, että palvelu listaa korkeintaan 6000 jäsentä, vaikka jäseniä olisikin enemmän. Kuitenkin julkisissa ryhmissä jäseniä voi hakea hakutoimin-

non kautta, joten hyökkääjä voi etsiä lisää jäseniä hakemalla esimerkiksi yleisimpien nimien perusteella. Yksityisten ryhmien tutkimista varten hyökkääjän tulee itse päästä ryhmän jäseneksi. Tiedonlouhinnan jälkeen hän poistuu ryhmästä. (Wondracek, 2010.)

4.5.2 Deanonymisointi tviittien ja ansioluettelon avulla

Okuno ym. (2011) esittelevät matemaattisen mallin, jonka avulla Twitterin käyttäjä voidaan identifioida lähettämiensä tviittien ja ansioluettelonsa kautta. Ansioluettelot sisältävät usein henkilökohtaista tietoa hakijasta. Niissä mainitaan muun muassa nimi, osoite, muut yhteystiedot, jopa kokonainen henkilötunnus ja koulutus. Ongelmana Okunon ym. (2011) mukaan on se, että näennäisesti anonyymi käyttäjä muuttuu tunnistettavaksi, jos profiilin tiedot saadaan yhdistettyä muualta kerätyn tiedon kanssa. Hyökkääjä ei välttämättä tarvitse muuta tietoa kuin käyttäjän ansioluettelon ja tämän lähettämät tviitit. Koska hyökkääjä yrittää yhdistää ansioluettelon ja Twitter-käyttäjän, on oletettavaa että Twitterissä käyttäjä ei käytä oikeaa nimeään, sillä muuten ansioluettelon voisi yhdistää tiettyyn käyttäjään nimen avulla. Poikkeuksena saattaa tosin olla tilanne, jossa käyttäjällä on useita kaimoja ja he kaikki esiintyvät omalla nimellään Twitterissä. Silloin mallin avulla voisi poimia juuri oikean käyttäjän.

Okunon ym. (2011) malli suhtautuu tviitteihin ja ansioluetteloon dokumentteina. Mallin avulla lasketaan dokumenttien samankaltaisuus, ja mikäli dokumentit ovat riittävän samanlaisia, on todennäköistä, että niiden tekijä on sama henkilö. Samanlaisuuden laskeminen perustuu vektoriavaruusmalliin, jota käytetään usein tiedon hakemiseen. Samanlaisuutta arvioidaan esiintyvien sanojen frekvensseillä eli kuinka usein tietty sana esiintyy tekstissä. (Okuno ym., 2011). Mallissa dokumentit esitetään vektoreina.

Vektoriavaruusmallin käyttäminen vaatii hyökkääjältä matemaattista lahjakkuutta. Sen avulla ei näennäisesti varasteta kenenkään identiteettiä, se vain antaa tietoa siitä, onko kahden dokumentin kirjoittaja sama henkilö. Toki tätä tietoa voi hyödyntää edelleen muualla. Vektoriavaruusmalliin ei voi myöskään luottaa täydellisesti, sillä Okunon ym. (2011) mukaan malli ei välttämättä aina anna korkeinta riippuvuussuhdetta ansioluettelon ja tviittien välillä, eli malli ei aina tulkitse niitä saman henkilön lähettämiksi, vaikka ne olisivatkin. Syynä tähän on erilainen kielenkäyttö eri dokumenteissa. Malli ei löydä samankaltaisuutta sanasta, johon on viitattu eri tavalla dokumenteissa. Esimerkiksi Twitterissä käyttäjä voi puhua Jyväskylän yliopistosta lyhenteellä ”JYU”. Ansioluettelossa hän todennäköisesti käyttää pitempää virallista muotoa. Malli ei osaa yhdistää näitä sanoja samaksi. Samalla tavalla ulkopuolinen henkilö ei välttämättä ymmärrä, että edellä mainitut sanat tarkoittavat samaa yliopistoa, ellei hänellä ole tietoa, mistä lyhenne tulee. (Okuno ym., 2011.)

4.5.3 Kaksitasoinen anonymisointihyökkäys

Kaksitasoinen anonymisointihyökkäys (engl. Seed-and-Grow). Englanninkielinen termi kuvaa hyökkäyksen rakennetta. Ensin hyökkääjä niin sanotusti istuttaa siemenen haluamaansa sosiaalisen median palveluun odottamaan anonymisoidun datan julkaisua. Kun data on julkaistu, hyökkääjä hakee siemenen ja kasvattaa sitä isommaksi uhaten näin yksityisyyttä. (Peng ym., 2014.)

Hyökkäys perustuu oletukseen, että yksittäisen käyttäjän toiminta ja suhteet ovat samantyyppisiä erilaisten palveluiden välillä. Ensin hyökkääjän tulee saada anonymisoitu graafi kohteesta eli yhdestä sosiaalisen median palvelusta (Peng, Li, Zou & Wu, 2012). Koska hyökkäyksessä tutkitaan kahden eri palvelun suhteiden samankaltaisuutta, toisen palvelun graafin tulee olla anonymisoimaton, jotta siihen voidaan verrata. Hyökkääjän tulee hankkia mahdollisimman paljon taustatietoa vertailukohteesta, jotta deanonymisointi onnistuu. Koska tutkittava ryhmä on molemmissa samankaltainen (muttei välttämättä identtinen), myös ryhmän väliset suhteet ovat samantyyppisiä ja siten graafeissa on yhtäläisyyksiä. (Peng ym., 2012.) Kaksitasoinen anonymisointihyökkäys perustuu siis sosiaalisia interaktioita kuvaavien graafien vertailuun. Hyökkääjä yrittää löytää verkon solmuille identiteetit.

Algoritmin avulla graafista on mahdollista identifioida käyttäjiä. Mittaamalla molempien graafien samankaltaisuutta, vastaavuutta ja erilaisuutta taustatiedon avulla voidaan ratkaista anonymisoitujen käyttäjien suhteet toisessa palvelussa, ja siten yhdistää kahden eri palvelun käyttäjän toiminta saman henkilön suorittamaksi.

4.6 Muu tietojen kerääminen

Myös palveluntarjoajat ja palveluiden rakenne mahdollistavat tietojen keräämisen. Aina käyttäjä ei itse pysty vaikuttamaan omilla asetuksillaan siihen, miten paljon hänestä on tietoa saatavilla, vaan yksityisyys riippuu myös muiden käyttäjien toiminnasta.

4.6.1 Kolmannet osapuolet

Sosiaalisen median palveluissa voi usein käyttää erilaisia sovelluksia ja pelata pelejä, jotka eivät ole palvelun omia, vaan niiden tarjoaja on ulkopuolinen taho. Näistä ulkopuolisista tahoista käytetään nimitystä kolmannet osapuolet. Usein kolmannet osapuolet tarjoavat varsin viattomilta kuulostavia ajanvietepelejä tai muita viihdyttäviä sovelluksia. Niiden käyttöön liittyy kuitenkin yksityisyyteen liittyvä riski, sillä useat kolmannet osapuolet vaativat sovellustensa käytön vastineeksi luvan käyttää käyttäjän tietoja.

Facebookissa toimivat kolmannen osapuolen sovellukset käyttävät omia palvelimiaan. Kun käyttäjä haluaa käyttää kolmannen osapuolen tarjoamaa sovellusta, Facebook vastaanottaa käyttäjäpyynnön, jonka se lähettää eteenpäin

palveluntarjoajalle. Sovellus lähettää takaisin pyynnön nähdä käyttäjän tietoja. (Ahmadinejad, Anwar & Fong, 2011.)

Kolmansien osapuolten sovellukset toimivat omina itsenäisinä osina, eikä esimerkiksi Facebook ja Twitter vastaa palveluissaan niiden ylläpidosta. (Ahmadinejad ym., 2011.) Turvallisuutta ja yksityisyyttä uhkaavat sovellukset voivat kerätä käyttäjistä henkilökohtaista ja arkaluontoista tietoa, jota voidaan hyödyntää rikollisissa tarkoituksissa.

Osaltaan sosiaalisen median palvelut itse ovat syyllisiä tietojen keräämisen helppouteen. Käytännössä kaikki palvelut keräävät käyttäjistään jotain tietoa. Vaikka käyttäjä poistaisikin profiilistaan henkilökohtaista tietoa, voi palveluntarjoaja silti säilyttää kaiken tiedon. Ainakin Facebook ilmoittaa käyttöehdoissaan säilyttävänsä tiedot niin kauan kuin se on tarpeen palvelujen ja tuotteiden tarjoamiseksi. Käyttöehdoissa sanotaan, että käyttäjätiliin liittyvät tiedot poistetaan silloin, kun itse tili poistetaan, ellei Facebook tarvitse kyseisiä tietoja. (Facebook, 2015b.) Kerätyn tiedon avulla Facebook muun muassa kohdentaa mainoksia käyttäjilleen. Myös kolmannet osapuolet hyödyntävät käyttäjistä kerättyä tietoa.

Nykyisin monilla ulkopuolisilla sivustoilla käyttäjällä on myös mahdollisuus kommentoida ja tykätä esimerkiksi uutisesta. Kolmannet osapuolet voivat kerätä myös näitä tietoja, sillä ne ovat täysin julkisesti näkyvissä. Käyttäjän profiilin yksityisyysasetukset eivät vaikuta siihen, näkyvätkö hänen tunnuksellaan tehdyt kommentit ulkopuolisilla sivustoilla. Profiilitietojen ja muualta löytyneiden tietojen avulla voidaan luoda graafi sosiaalisista interaktioista, mikä paljastaa tarkastikin käyttäjän toiminnan verkossa. (Erlandsson, Boldt & Johnson, 2012.) Näin ollen tietojen kalastelija voi saada todella tarkan kuvan käyttäjän henkilöllisyydestä ja persoonallisuudesta.

4.6.2 Sähköpostiosoitteen kartoittaminen

Sähköpostit olivat ja ovat edelleenkin haluttua materiaalia. Alkuperäiset tietojen kalasteluviestit lähetettiin sähköpostilla. Roskapostin määrä varsinkaan ilmaisohjelmissa ei ole vähentynyt, ja huijarit edelleen keräävät käyttäjien sähköpostiosoitteita. Mahmoodin (2012) mukaan tietojen kalastelu on sitä tehokkaampaa, mitä henkilökohtaisempaa tietoa kalastelija uhristaan tietää. Siksi nimellä kohdennetut viestit toimivat paremmin kuin massapostina lähetettävät kopiot ilman personointia. Sähköpostiosoitteen ja nimen yhteensovittamista kutsutaan kartoittamiseksi (engl. mapping). Facebookissa tietojen kalastelijat voivat yrittää etsiä sähköpostilla käyttäjiä, jolloin hakutuloksena tulee käyttäjän nimi. Tämän onnistuminen kuitenkin riippuu uhrin yksityisyysasetuksista, sillä Facebookissa on mahdollista valita, haluaako sähköpostiosoitteella etsimisen olemisen olevan mahdollista kaikille, kavereiden kavereille vai pelkästään kavereille.

On olemassa myös toinen keino kartoittaa sähköpostiosoitteeseen kuuluvaa nimeä. Tämä keino toimii aina, sillä käyttäjän yksityisyysasetukset eivät vaikuta keinon onnistumiseen. Tässä menetelmässä hyökkääjän ei tarvitse edes kirjautua palveluun sisälle, sillä kartoitus tapahtuu kirjautumissivulla. Hyök-

kääjän tulee kirjoittaa haluttu sähköpostiosoite sille varattuun paikkaan ja jättää salasanan kohta tyhjäksi. Kun hyökkääjä painaa Kirjaudu sisään -painiketta, luonnollisestikaan palvelu ei päästä hyökkääjää tilille, sillä hän ei ole antanut salasanaa. Sen sijaan palvelu siirtyy sivulle, jossa näkyy sähköpostinosoitteen omistavan käyttäjän profiilikuva ja koko nimi. (Mahmood, 2012). Sivu listaa myös mahdollisen aiemman nimen, mikäli käyttäjä on äskettäin muuttanut nimeään. Nyt tietojen kalastelijalla on tiedossa jo uhrin sähköpostiosoite ja koko nimi. Nimen avulla voi etsiä tietoa muualta Internetistä ja sosiaalisen median palveluista ja hyödyntää tietoa edelleen muissa hyökkäyksissä.

Usein käyttäjä käyttää samaa, yleensä helposti arvattavaa salasanaa monella sivustolla. Kartoittamisen yhteydessä tietojen kalastelija saa tietää, onko kyseisen sähköpostin omistaja Facebookissa. Salasana voidaan yrittää ohjelmallisesti murtaa, ja mitä helpompi salasana, sitä nopeammin se on murrettu. Näin huijari voi saada käyttäjän tunnukset palveluun, mikä aiheuttaa valtavan tietoturva- ja yksityisyysuhan.

4.6.3 Kaverilistan uudelleen rakentaminen

Vaikka käyttäjällä on yleensä mahdollisuus rajoittaa kontakti- ja kaverilistansa näkyvyyttä, tämä ei tarkoita, etteikö hyökkääjä voisi rekonstruoida yksityiseksi määritellyn listan (Mahmood, 2012). Muista asetuksista riippuen uudelleenrakentaminen voi olla työlästä, mutta olennaista on se, että yksityisyys riippuu myös käyttäjän kavereiden ja kontaktien asetuksista. Kaverilistan uudelleenrakentamisessa voidaan hyödyntää uhrin tilapäivitysten, kuvien, ilmoitusten ja muiden julkaisujen kommentteja ja tykkäyksiä, ja muiden käyttäjien julkaisuja uhrin profiilissa. Tällä tavoin hyökkääjä saa jo osan käyttäjän kavereiden nimistä, ja selaamalla julkaisuja pitkällä aikavälillä hän todennäköisesti saa tietää suurimman osan uhrin kavereista. (Mahmood, 2012.)

Facebookissa toinen käyttäjä on myös mahdollista merkitä (engl. tag) kuvaan. Merkityt kuvat näkyvät laajemmalle yleisölle, sillä asetuksista riippuen sekä merkityn että merkkaajan ystävät näkevät kuvan. Käyttäjällä on kuitenkin myös mahdollisuus valita asetuksista, ettei häntä voi merkata kuviin. Merkatut kuvat helpottavat kaverilistan rakentamista. (Mahmood, 2012.)

Facebook ei ole toistaiseksi mahdollistanut yhteisten kavereiden täydellistä piilottamista. Jos henkilö A on piilottanut kaverilistansa, henkilö B näkee kuitenkin ne yhteiset kaverit, jotka eivät ole piilottaneet omaa listaansa. Tämä pätee riippumatta siitä, onko henkilö B henkilön A:n kaveri vai ei. Näin ollen käyttäjän kavereiden yksityisyysasetukset vaikuttavat siihen, miten helppo toisen käyttäjän kaverilista on rakentaa uudelleen. Jos henkilön A:n ja B:n kaikki yhteiset kaverit olisivat piilottaneet oman kaverilistansa, A ja B eivät näkisi myöskään toistensa yhteisiä kavereita. Hyökkääjän on kuitenkin helppo päätellä, kuinka iso osa yhteisistä kavereista jää kaverilistan perusteella selvittämättä, sillä Facebook silti ilmoittaa kaikkien yhteisten kavereiden määrän. Jos henkilön A profiilissa lukee, että 32 yhteistä kaveria, mutta tarkemmin tutkiessa hyökkääjä näkee vain 29 yhteistä kaveria, on helppo laskea, että uhrilla ja hyökkääjällä on vielä kolme yhteistä tuntematonta kaveria. Siten hyökkääjä tietää lähes

kaikki yhteiset kaverit, koska vain kolme kaveria on tuntemattomia. Tässäkään tapauksessa hyökkääjän ei tarvitse olla henkilön A kaveri nähdäkseen kaikkien yhteisten kavereiden lukumäärän.

Facebookissa ei ole myöskään mahdollista rajoittaa omaa näkyvyyttään muiden vähintään kavereille näkyväksi asetetulla listalla. Jos käyttäjä B on asettanut listansa näkymään kavereille, kavereiden kavereille tai julkisesti, myös käyttäjä A näkyy listalla, vaikka hän olisikin piilottanut oman listansa.

4.7 Yhteenveto

Tässä luvussa käytiin läpi yleisimpiä menetelmiä, joilla voidaan varastaa käyttäjän identiteetti- ja muuta tietoa sosiaalisen median palveluissa. Osa keinoista vaatii teknistä osaamista, kun taas toisten hyökkäysmenetelmien perusidea pohjautuu käyttäjän manipulointiin, jota käsiteltiin luvussa kaksi. Jotkut keinoista voivat myös yhdistää sekä teknisen että käyttäjän manipuloinnin näkökulman. Osa hyökkäyksistä on helppoja toteuttaa, eivätkä ne vaadi teknistä osaamista. Tämä tarkoittaa sitä, että jopa tavalliset käyttäjät ovat kykeneväisiä toteuttamaan tietojen kalasteluhyökkäyksen. Esimerkki helposti toteutettavasta tietojen kalastelukeinosta on profiilin kloonaus, jossa hyödynnetään uhrista kerättyä tietoa ja luodaan tiedon perusteella profiili uhrin nimissä. Tarkoituksena on huijata muita käyttäjiä luulemaan huijarin profiilia aidoksi ja näin paljastamaan henkilökohtaista tietoa.

Sen sijaan välistävetohyökkäys on esimerkki teknisestä hyökkäyksestä. Se on suurimmaksi osaksi haitta- ja muiden ohjelmien hyödyntämiseen perustuva, mutta hyökkäyksestä seuraa mahdollisuus kerätä tietoa käyttäjästä ja tämän kavereista. Hyökkäyksen nimen mukaisesti hyökkääjä asettuu uhrin ja palveluntarjoajan väliin keräämään tietoa.

Osa luvussa esitellyistä hyökkäyksistä on palvelurajoitteisia, eli ne on suunniteltu toimimaan ainoastaan tietyntyyppisessä palvelussa. Tällaisia ovat esimerkiksi kolmannessa alaluvussa kuvattu deaktivointihyökkäys Facebookissa, joka perustuu hyökkääjän profiilin jatkuvaan poistoon ja palauttamiseen sekä tviittien hyödyntäminen haitalliseen tarkoitukseen Twitter-palvelussa. Tviittien kautta hyökkääjä voi levittää muun muassa haitallista materiaalia sisältäviä linkkejä

Internetissä käyttäjät voivat useimmiten liikkua anonyymisti nimimerkkien suojissa. Kaikki tieto, mistä heidät voidaan tunnistaa, anonymisoidaan eli muutetaan tunnistamattomaksi palveluntarjoajan toimesta. Viidennessä alaluvussa havainnollistettiin deanonymisointihyökkäystä, jossa anonymisoitu tietoa muutetaan taas tunnistettavaksi, ja näin voidaan yhdistää yksi käyttäjä kahdesta eri palvelusta samaksi henkilöksi.

On myös olemassa muita tiedon keräämistapoja, jotka perustuvat suurimmaksi osaksi palvelun ominaisuuksiin. Tällaisissa tapauksissa käyttäjä ei itse voi vaikuttaa tiedon vuotamiseen, vaan vika on palvelussa itsessään tai

muiden käyttäjien toiminnassa. Esimerkiksi kartoittamista on menetelmä, jonka avulla on mahdollista kerätä tietoa jo ennen kuin on edes kirjautunut palveluun.

Tähän tutkielmaan on valittu ne hyökkäyskeinot, joista löytyy eniten tieteellistä materiaalia. Koska käsitellyistä hyökkäyksistä on saatavissa paljon tietoa, ovat ne todennäköisesti tunnettuja ja yleisiä keinoja. Empiirisessä osuudessa selvitetään, pyrkivätkö huijarit, hyökkääjät ja rikoksen tekijät hyödyntämään kirjallisuuskatsauksessa esitettyjä keinoja tutkittavissa tapauksissa.

Kirjallisuuskatsauksessa suurin osa tieteellisistä lähteistä käsittelee identiteettivarkautta ja tietojen kastelua Facebookissa ja Twitterissä. Nämä ovat tunnetuimpia ja suosituimpia sosiaalisen median palveluita, ja siksi on ymmärrettävää, että näistä palveluista löytyy eniten aiheeseen liittyvää materiaalia. Koska kirjallisuus painottuu Facebookissa ja Twitterissä käytetyille tietojen kalastelu- ja identiteetin varastamiskeinoille, halutaan myös empiirisessä osuudessa selvittää, nousevatko kyseiset palvelut esille tutkittavissa tapauksissa.

5 TUTKIMUKSEN TOTEUTTAMINEN

Tässä luvussa kuvataan tutkielman empiirinen osuus. Tarkoituksena on selvittää suomalaisten oikeustapausten ja niitä vastaavan muun materiaalin kautta, miten väärää identiteettiä on käytetty muiden rikosten tekemisessä. Luku käsittelee tutkimusmenetelmää, tutkimuskohdetta, tutkimusprosessia ja -mallia sekä tiedonkeräämistä.

5.1 Tutkimusmenetelmä

Tässä tutkimuksessa tutkimusmenetelmäksi on valittu teoriaa testaava näkökulma. Järvisen ja Järvisen (2004) mukaan teoriaa testaava tutkimusote pyrkii ratkaisemaan kysymyksen reaalimaailman osan ja teorian, mallin tai viitekehyksen vastaavuudesta. Teoriaa testaavan menetelmä on luonteeltaan deduktiivinen.

Teoriaa testaavia tutkimuksia ovat muun muassa kontrolloitu koe, kenttämenetelmät, teoriaa testaava case-tutkimus ja teoriaa testaava pitkittäistutkimus. Järvisen ja Järvisen (2004) mukaan Lee (1989) määrittelee neljä vaatimusta tieteelliselle metodille. Teorian pitää olla empiirisesti testattavissa ja teorian perusteella johdettujen ennusteiden tulee olla loogisesti johdonmukaisia. Lisäksi teorian tulee selittää tutkittava ilmiö vähintään yhtä hyvin kuin joku muukin teoria ja sen tulee selviytyä falsifiointiyrityksistä.

Tässä tutkimuksessa teoriaa testataan suomalaisten oikeustapausten ja niihin liittyvien uutisten kautta. Tarkoituksena on tutkia, miten käytännössä tapahtuneet identiteetin varastamiskeinot peilautuvat teoriassa esitettyihin malleihin, ja vertaillaan käytännön ja teorian antamaa kuvaa sosiaalisen median palveluissa tapahtuvasta identiteetin väärinkäytöstä.

Teorian testaamiseen tutkimusmenetelmänä kuuluu olennaisena osana teorian kilpailuttaminen eli valitaan teorioiden joukosta se, jota testataan. Silloin kun kilpailuttamalla ei löydetä sopivaa teoriaa, joka selittää ja kuvaa ilmiötä, koostetaan testattava teoria tai viitekehys itse. (Järvinen & Järvinen, 2011.)

Tässä tutkielmassa viitekehys perustuu kirjallisuuskatsaukseen, jonka perusteella on laadittu selvitettäviä kysymyksiä identiteettivarkauden ilmiöstä sosiaalisen median palveluissa. Selvitettävät asiat on esitetty taulukossa 1. Tavoitteena on löytää vastaus esitettyihin kysymyksiin ja muodostaa sitä kautta käsitys tutkittavasta aiheesta.

TAULUKKO 1 Empiirisessä osuudessa selvitettävät kysymykset

1. Onko tutkittavissa tapauksissa saavutettu taloudellista tai muuta etua, tai aiheutettu uhrille vastaavaa haittaa?
2. Onko käyttäjän manipulointihyökkäyksen piirteitä havaittavissa tutkittavissa tapauksissa?
3. Millaisia sosiaalisessa mediassa esiintyviä luotettavuuden piirteitä tutkittavissa tapauksissa on havaittavissa?
4. Onko toisen henkilön nimellä tehtyjä huijausprofiileita hyödynnetty tutkittavissa tapauksissa ja millaisiin tarkoituksiin niitä on käytetty?
5. Pyrkivätkö huijarit, hyökkääjät ja rikoksen tekijät hyödyntämään kirjallisuuskatsauksessa esitettyjä tietojen kalastelu- ja identiteetin varastamiskeinoja tutkittavissa tapauksissa?
6. Hyödynnetäänkö tutkittavissa tapauksissa Facebookia ja Twitteriä?

Kysymykset ovat ikään kuin empiirisen osuuden tutkimuskysymyksiä, joihin haetaan vastauksia tutkittavasta aineistoista. Empiirisen osuuden avulla selvitetään, mitä samaa tai erilaista käytännön identiteettivarkaustapauksissa on verrattuna tieteellisen kirjallisuuden esittämään näkökulmaan aiheesta ja pätevätkö kirjallisuuskatsauksessa mainitut asiat myös käytännössä. Empiirisessä osuudessa testataan siis olemassa olevaa kirjallisuutta käytännön tapausten kautta.

5.2 Tutkimuskohteet

Tutkimuskohteena on kaksi oikeustapausta ja kaksi täysin uutisten varassa tutkittavaa tapausta. Oikeustapausten osalta on mainittu tapauksen diaarinumero ja uutisiin perustuvien tapausten lähdemateriaalit ovat liitteinä.

Tapaus 1, Helsingin käräjäoikeus, diaarinumero R 09/5097
Tapauksessa asianomistaja on vaatinut vastaajalle rangaistusta yksityiselämää loukkaavan tiedon levittämisestä Facebook-palvelussa. Haastehakemuksen (2.6.2009) mukaan vastaaja on oikeudettomasti toimittanut lukuisten ihmisten saataville alastonkuvia asianomistajasta. Vastaaja on luonut Facebook-palveluun profiilin asianomistajan nimellä ilman tämän suostumusta ja lisännyt profiiliin kaksi alastonkuvaa asianomistajasta. Tämän jälkeen vastaaja on kutsunut tällä profiililla asianomistajan tuntemia henkilöitä Facebook-kaveriksi, jolloin nämä ovat päässeet näkemään profiiliin lisätyt alastonkuvat.

Pöytäkirjan (6.6.2011) mukaan vastaaja on ollut asianomistajan kanssa parisuhteessa. Asianomistaja oli lainannut vastaajalta rahaa, ja vastaaja oli pyytänyt asianomistajaa maksamaan takaisin lainaamansa summan. Kun vastaaja ei ollut saanut rahojaan takaisin, hän oli lähettänyt asianomistajalle painostusmielessä tekstiviestejä, jotta saisi rahansa takaisin. Vastaajalla oli ollut joitakin alastonkuvia asianomistajasta, mutta hän oli hävittänyt ne myöhemmin.

Pöytäkirjan mukaan syyttäjä on pyytänyt huomioimaan Facebookin merkityksen nyky-yhteiskunnassa. Facebookia ei voi pitää enää pelkästään huvittelusivustona, vaan valtaosa yksityishenkilöistä ja myös yrityksistä käyttää sitä.

Tapaus 2, liite 1

Tapaus koskee kansanedustaja Jörn Donnerin nimellä tehtyä huijaustiliä Twitter-palvelussa. Donner teki asianajajansa välityksellä tutkintapyynnön asiasta 22.–25.3.2013 välisenä aikana, mutta tutkinta lopetettiin lopulta muun muassa kustannussyihin vedoten. Lisäksi tapauksesta olisi pitänyt tehdä oikeusapupyyntö Yhdysvaltoihin, sillä palveluntarjoaja sijaitsee siellä. Poliisin mukaan edes perusteellinen tutkinta ei takaa sitä, että tekijä saataisiin rikosoikeudelliseen vastuuseen tapahtuneesta. Tapauksesta on kuitenkin saatavilla tietoa muun muassa uutisten kautta, joten tapausta voidaan hyödyntää tutkimuksessa.

Tuntemattomaksi jäänyt henkilö tai ryhmä loi Jörn Donnerin nimellä tilin Twitteriin ja julkaisi tviittejä siellä. Muut poliitikot (muun muassa Alexander Stubb), kuuluisat henkilöt, tavalliset henkilöt ja virastot kommentoivat ja uudelleentviittasivat ”Donnerin” julkaisemia päivityksiä. Lisäksi myös useat lehdet siteerasivat huijaustilin tviittejä.

Tili on nimeltään jorndonner, ja aikaisin näkyvä maininta tilistä on käyttäjän Dream Bakeryn tviitissä 21.7.2012. Useat käyttäjät muun muassa onnittelivat huijaus-Donneria tämän syntymäpäivänä. Tiliä ei ole varmennettu eli ei ole vahvistettu, että käyttäjä on juuri se, kuka väittääkin olevansa.

Muiden käyttäjien tviiteissä alkoi näkyä 12.3.2013 tieto siitä, ettei jorndonner olekaan oikean Jörn Donnerin tili. Ennen paljastumistaan jorndonner-tilillä oli tuhansia seuraajia ja tili oli merkitty satoihin muiden käyttäjien tviitteihin. Kaiken kaikkiaan tekijä onnistui huijaamaan lehdistöä ja tuhansia ihmisiä noin vuoden ajan. Kesällä 2013 tili poistettiin. Vaikka profiilia ja sen lähettämiä tviittejä ei enää näy, tviittejä voi kuitenkin lukea, jos joku huijaustilin seuraajista on uudelleentviitannut tviitin ja alkuperäinen tviitti on ollut julkinen.

Tapaus 3, Tampereen käräjäoikeus, diaarinumero R 07/3284

Tapauksessa vastaajia syytetään törkeästi kunnianloukkauksesta. Vastaajat ovat laatineet Internetissä julkisia sivustoja, joissa he ovat esittäneet asianomistajista valheellisia ja halventavia väitteitä. Vastaajat ovat myös nimitelleet asianomistajia loukkaavin nimityksin. Osa väitteistä on kirjoitettu asianomistajien itsensä esittämiksi. Vastaajat ovat myös kehottaneet lukijoita lähettämään asianomistajien sähköpostiosoitteisiin loukkaavia viestejä.

Tapauksessa vastaajat ovat hyödyntäneet Blogspot-sivustoa, jossa voi perustaa ja kirjoittaa blogia ja esimerkiksi kommentoida muiden kirjoituksia. Vastaajat ovat luoneet tuntemiensa henkilöiden ja julkisuuden henkilöiden, pääasi-

assa poliitikkojen nimissä blogeja. Joistakin blogien nimistä käy selvästi ilmi, keneen blogi viittaa, ikään kuin kyseinen henkilö olisi tehnyt itse blogin. Vastaajat ovat käyttäneet muun muassa Matti Vanhasen, Timo Soinin, Tanja Karpelan ja Heidi Hautalan nimiä. Ainakin toinen vastaajista on aikaisemmin tuomittu muusta rikoksesta, ja tässä tapauksessa hän on myös luonut aikaisemman rikoksen oikeudenkäyntiin liittyvien henkilöiden nimissä blogeja.

Yhteensä luotuja blogeja tapauksessa on 41. Osassa blogeista solvataan toisen henkilön identiteetin takaa eri uskonnon ja rodun edustajia, ja kehotetaan myös tekemään rikoksia.

Tapaus 4, liite 2
Tapauksessa uhri on tutustunut tekijään Internetissä ja ollut tähän yhteydessä web-kameran välityksellä. Molemmat ovat olleet vähäpukeisia kameran edessä, ja tekijä on uhrin tietämättä tallentanut videon. Luottamuksen herättyä tekijä on suostutellut uhrin hyväksymään kaveripyynnön Facebookissa, ja tämän jälkeen kertonut uhrille julkaisseensa videon Youtube-palvelussa. Tekijä on myös lähettänyt uhrille linkin kyseiseen jo julkaistuun videoon. Tekijä on uhannut jakaa videon uhrin Facebook-kavereille, ellei uhri maksa tiettyyn päivään mennessä monta sataa euroa.

Alun perin uhrin ja tekijän välinen kontakti on syntynyt anonyymissa chat-palvelussa. Jonkun ajan kuluttua keskustelu on siirtynyt tekijän aloitteesta ensin Skype-nettipuhelinpalveluun ja sieltä Facebookiin. Facebookiin siirtymistä tekijä on perustellut esimerkiksi huonolla ja pätkivällä Skype-yhteydellä. Facebookissa tekijä on saanut tietoonsa uhrin lähipiiriin kuuluvat henkilöt, kaverit, työpaikat ja muuta henkilökohtaista tietoa.

Uutisten mukaan tapauksia on useita, mutta jokaisessa niistä kaava on samanlainen. Tapausten rikosnimikkeitä ovat aikuisen kohdalla kiristys ja kunnianloukkaus ja 16–17 vuotiaan kohdalla kyseeseen tulee lisäksi sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen.

5.3 Tiedonkerääminen ja analysointi

Tässä tutkimuksessa tietolähteenä käytetään lähinnä dokumentteja eli kirjallisia lähteitä. Järvisen ja Järvisen (2004) mukaan dokumentteihin luetaan muun muassa kirjeet, muistiot, tiedotteet, tutkimukset ja lehtileikkeet. Dokumentit ovat niin sanotusti sekundäärilähteitä, eikä niitä ole tehty alun perin tutkimusta varten.

Kirjallinen aineisto takaa sen, että tutkija voi tutustua siihen omassa tahdissaan haluamanaan ajankohtana, sillä aineistoon perehtymistä varten ei tarvitse sopia esimerkiksi haastatteluja (Järvinen & Järvinen, 2004). Dokumentteihin aineisto liittyy kuitenkin muutama hankaluus. Tutkijan tulee muistaa, että dokumenttien laatimistarkoitus ei ole ensisijaisesti tutkimus, vaan niiden tarkoituksena on välittää tietoa dokumentin laatijan ja käyttäjän kesken tai tukemaan dokumentin käyttäjän muistia. Dokumentin laatimisen tarkoituksen sel-

vittäminen helpottaa dokumentissa olevien tietojen käyttökelpoisuuden arviointia. (Järvinen & Järvinen, 2004.)

Tässä tutkimuksessa käytetään aineistona suomalaisia oikeustapauksia ja niihin liittyviä uutisia. Koska toistaiseksi identiteettivarkaus ei ole Suomessa rikos, ei esimerkiksi käräjäoikeuksien tietokannoista voi hakea oikeudenkäynnin dokumentteja identiteettivarkaus-hakusanalla. Läheisiä rikosnimikkeitä, joissa identiteettivarkaus voi tulla kyseeseen, ovat esimerkiksi kunnianloukkaus, petos, tietomurto ja yksityiselämää loukkaavan tiedon levittäminen. Kuitenkin näiden tapausten lukumäärä on jo yhdessä käräjäoikeudessa valtava, ja niiden kaikkien läpikäyminen sopivan tapauksen löytämiseksi on paitsi haastavaa myös aikaa vievää. Kirjoittaja on kuitenkin onnistunut muuta kautta löytämään muutaman tapauksen tutkimuksen aineistoksi. Käsiteltävät tapaukset ovat joko löytyneet osittain Internetistä tai niihin liittyvää tunnistetietoa on ollut tarpeeksi, jotta haku käräjäoikeudesta on ollut mahdollista.

Vaikka eri lehtien www-sivuilla on uutisia sosiaalisen median palveluissa tapahtuneista rikoksista, tulisi kyseisistä tapauksista tietää ainakin syyllisen nimi tai mielellään asiakirjanumero (diaarinumero), jotta tapaus olisi helposti haettavissa käräjäoikeudesta. Tämän takia tässä tutkielmassa käsiteltävien tapausten lukumäärä on pieni, ja lisänä kirjoittaja käyttää aiheesta löytyviä uutisia. Koska tarkoitus on tutkia, miten sosiaalisen median palvelut mahdollistavat väärän identiteetin hyödyntämisen, eikä ensisijaisena tavoitteena ole arvostella, pohtia tai tutkia identiteettivarkauteen liittyvää lainsäädäntöä, tapausten rangaistuksia tai psykologisia syitä, ovat uutiset käyttökelpoista materiaalia.

Tutkittavia tapauksia analysoidaan alaluvun 5.1 taulukossa esitettyjen kysymysten kautta. Tavoitteena on muun muassa selvittää missä palvelussa rikos tapahtui ja miten toisen henkilön tietoja käytettiin. Tarkoituksena on myös tutkia, millaisia kirjallisuudessa esitettyjä tietojen kalastelu- ja identiteetin varastamiskeinoja rikollinen käytti.

Tapauksista pyritään löytämään selkeät vastaukset esitettyihin kysymyksiin, jotta voidaan perustellusti kuvata identiteettivarkauden ilmiötä sosiaalisessa mediassa. Toisaalta koska kaksi tapausta perustuu uutisiin, on oletettavaa, ettei niistä tapauksista ole mahdollista saada täysin aukottomia vastauksia verrattuna oikeuden asiakirjoihin, joissa tapahtumat kuvataan tarkemmin.

Tapauksista kerätyn tiedon analysoinnin avulla pyritään selvittämään, eroavatko kirjallisuuden näkemykset identiteettivarkaudesta ja sosiaalisesta mediasta käytännön tapausten antamasta kuvasta. Koska kyseessä on laadullinen tutkimus, ei samankaltaisuutta voida mitata matemaattisesti. Tehdyt havainnot ja johtopäätökset perustellaan tapauksiin viitaten. Analysoinnissa hyödynnetään myös kirjallisuuden antamaa tietoa aiheesta.

6 TULOKSET

Empiirisessä osuudessa kirjallisuuskatsauksessa esiintuotuja asioita verrattiin käytännön tapauksiin ja tarkasteltiin sitä kautta identiteettivarkautta ja tietojen kalastelua sosiaalisen median palveluissa. Tässä luvussa esitetään tutkittavista tapauksista tehdyt havainnot ja tulokset.

6.1 Käytetyt keinot

Tapauksissa oli havaittavissa useita eri keinoja, joiden avulla toisen henkilön identiteettiä oli hyödynnetty. Tapauksessa 1 (alastonkuvat) oli käytetty osittain profiilin kloonaushyökkäystä ja sitä kautta tapauksessa oli huijausprofiilin piirteitä. Kloonaushyökkäyksille on tyypillistä, että nimensä mukaisesti profiili kopioidaan joko samasta tai eri sosiaalisen median palvelusta. Epäilty on tuntenut uhrin tosielämässä ja siten hän on todennäköisesti saanut tietonsa sitä kautta, mutta toisaalta on myös mahdollista, että hän on saattanut kerätä tietoa myös uhrin oikeasta Facebook-profiilista.

> Vastaaja myönsi, että hänellä oli ollut [asianomistajan] kanssa seurustelusuhde (Helsingin käräjäoikeus, R 09/5097).

Oikea profiili on edelleen käytössä ja se oli olemassa jo ennen huijausprofiilin luomista, sillä asianomistajan Facebook-kaveri oli ihmetellyt uutta kaveripyyntöä, vaikka hän oli jo asianomistajan kaveri.

> Todistaja on oikeudessa puhelimen välityksellä kuultuna kertonut, että hän oli saanut kaveripyynnön [asianomistajan] Facebook-profiiliin, vaikka hän oli jo [asianomistajan] ystävä Facebookissa. Todistaja oli ihmetellyt uutta kaveripyyntöä. (Helsingin käräjäoikeus, R 09/5097.)

Tapauksessa 1 ja 2 (Donnerin nimellä luotu huijaustili) on myös hyödynnetty käyttäjän manipulointia. Tekijöiden tarkoituksena on ollut saada muut usko-

maan, että huijari on profiilin esittämä henkilö. Esimerkiksi Donnerin huijaustiliä siteerasivat ja kommentoivat lehdet ja tunnetut henkilöt.

> Helsingin Sanomat julkaisi sunnuntaisivullaan viikon twiittinä yhden kyseisen tilin julkaisuista (Helsingin Sanomat, 13.3.2013).

> Sillä [Donnerin huijaustilillä] on ollut yli 2000 seuraajaa, ja ”Donnerin” twiittejä on kommentoinut muun muassa ministeri Alexander Stubb (kok) (Helsingin Sanomat, 13.3.2013).

Kuuluisista ja julkisuuden henkilöistä on saatavilla paljon tietoa Internetissä aina syntymäajasta ja koulutuksesta lähtien, joten sellaisen henkilön nimellä on helppo luoda huijausprofiili. Tapauksessa 2 tekijä on luottanut siihen, että kuuluisaan henkilöön luotetaan. Huijaustili on saanut tuhansia seuraajia ja useat sadat käyttäjät ovat kommentoineet tai uudelleentviitanneet ”Donnerin” päivityksiä. Jos huijaustilin julkaisut eivät silminnähden eroa siitä, mitä oikea henkilö sanoisi, voi olla todella hankalaa erottaa huijaustili oikeasta tilistä.

Tapauksessa 3 (blogi-kirjoitukset) tekijä on myös hyödyntänyt väärää identiteettiä, mutta hieman erilaisessa yhteydessä. Blogi-kirjoittaminen eroaa Facebookin ja Twitterin kaltaisista palveluista. Vaikka Twitterin tviitit ovatkin eräänlaisia miniblogeja, on siellä vuorovaikutus paljon suuremmassa osassa kuin blogeissa. Tapauksessa 3 hyökkääjä loi blogeja sekä tuttujen että tuntemattomien henkilöiden nimissä. Blogeja oli luotu useiden tunnettujen poliitikkojen nimissä, ja koska tietoa heistä on saatavilla helposti, on myös ollut helppoa luoda heidän nimissään blogeja.

Neljäs tapaus (videokiristys) sen sijaan eroaa kolmesta muusta tapauksesta. Koska tekijä ja uhri ovat olleet webkamera-yhteydessä toisiinsa, ei ainakaan väärällä kuvalla esiintyminen tule kysymykseen. Uhri olisi saattanut epäillä, mikäli kameran takana ollut henkilö ei olisikaan ollut sama kuin Facebook-kaveripyynnön lähettäneen henkilön profiilikuva. Tässäkin tapauksessa käyttäjän manipulointi vaikuttaa vahvasti. Sille on tyypillistä, että hyökkääjä on vuorovaikutuksessa uhrin kanssa ja syventää keskustelua pikkuhiljaa saavuttaakseen luottamuksen. Lopulta luottamus on ollut niin syvää että uhri on hyväksynyt kaveripyynnön Facebookissa, jossa hänestä on ollut saatavilla henkilökohtaista tietoa, jota myös tekijä on hyödyntänyt.

> Ensin uhrin kanssa avataan keskustelu chatissa, jonka jälkeen siirrytään Skypeen eroottiseen videokeskusteluun. Kun paljasta pintaa on näkynyt tarpeeksi, siirretään viestintä Facebookin puolelle. Teko syynä käytetään Skype-yhteyden pätkimistä tai muuta vastaavaa veruketta. (Ilta-Sanomat, 17.12.2013.)

Edellä esitettyjen havaintojen perusteella voidaan sanoa, tapauksissa on nähtävissä käyttäjän manipulointihyökkäyksen piirteitä. Luottamuksen synnyttäminen on keskeisessä osassa jokaisessa tapauksessa, joskin sen rooli vaihtelee. Luottamuksen avulla hyökkääjä pyrkii erilaisiin tavoitteisiin.

Ainakin kolmessa tapauksessa on käytetty huijausprofiileita, jotka on luotu toisen henkilön nimellä. Tavoitteena on ollut saada muut uskomaan siihen, että profiilin esittämä henkilö käyttää profiilia oikeasti. Lisäksi on mahdollista,

että tapauksessa 1 (alastonkuvat) tekijä on voinut hyödyntää lisäksi profiilin kloonaushyökkäystä, sillä asianomistajalla on ollut hyökkäyksen tekemisen aikaan oikea profiili samassa palvelussa, jossa huijausprofiili luotiin.

Näiden keinojen toteuttaminen on helppoa verrattuna teknisempiin keinoihin, sillä kuka tahansa pystyy luomaan huijausprofiilin ja etsimään toisesta tietoa muualta Internetistä.

6.2 Tiedonkeräys ja uhrin asema

Tietojen kalastelu ja uhrin suhde tekijään vaihtelee tapauksissa valtavasti. Tapauksessa 1 epäilty tekijä ja uhri ovat olleet tosielämässä parisuhteessa, joten he ovat tunteneet toisensa hyvin. Tätä ja mahdollisesti Internetistä uhrista löytyviä tietoja hyödyntämällä epäilty on onnistunut luomaan profiilin uhrin nimellä. Oikeuden asiakirjojen mukaan huijausprofiililta kaveripyynnön saanut henkilö on epäillyt profiilin aitoutta, sillä uhri on jo ollut tämän Facebook-kaveri. Hän on kuitenkin hyväksynyt myös uuden kaveripyynnön. Viimeistään kuitenkin sisällön laatu eli alastonkuvat ovat paljastaneet väärennetyn profiilin, sillä kukaan tuskin vapaaehtoisesti laittaa itsestään alastonkuvia kaveriensa nähtäville Facebookissa.

Kuten aikaisemmin mainittiin, kahdessa tapauksessa on käytetty tunnettujen henkilöiden identiteettejä. Julkisuuden henkilöitä on helppoa matkia, sillä heistä on saatavilla niin paljon tietoa. Jos oikean henkilön puheet ja huijausprofiilin julkaisut ovat toisiinsa nähden linjassa, niin huijausprofiilia voi olla vaikea havaita väärennetyksi. Toisaalta Twitter ja Facebook tarjoavat mahdollisuuden vahvistaa profiili, jolloin profiiliin tulee tunnus siitä, että henkilö on juuri se kuka väittääkin olevansa. Tapauksessa 2 ”Donnerin” tiliä ei kylläkään ollut vahvistettu. Siltikin jos profiili saa paljon seuraajia, se julkaisee uskottavia päivityksiä ja laajalevikkiset lehdetkin niitä siteeraavat, huijausprofiilin uskottavuus kasvaa väistämättä. On silti yllättävää, että Donnerin nimellä tehty huijausprofiili eli jopa noin kahdeksan kuukautta ennen paljastumistaan.

Myös tapauksessa 3 (blogi-kirjoitukset) tekijä on todennäköisesti kerännyt tietoa uhreistaan Internetistä. Tekijä oli myös tavannut osan asianomistajista aiemmissa oikeudenkäynneissä, joissa hänet oli tuomittu muista rikoksista.

> B:llä on ollut erityinen motiivi loukata asianomistajaa, koska tämä oli toiminut aiemmassa B:tä koskevassa rikosprosessia virkansa puolesta syyttäjänä (Tampereen käräjäoikeus, R 07/3284).

Vaikka oikeudenkäyntien asiakirjat olisikin määrätty salaisiksi, saavat asianosaiset ne täydellisinä. Oikeuden asiakirjoissa on usein täydelliset nimet, syntymäpäivät tai jopa henkilötunnukset, joten tekijä on voinut hyödyntää myös näitä asiakirjoja. Tuomiosta ei käy ilmi tarkemmin, mitä tekijä on kirjoittanut uhriensa nimissä, mutta ainakin osa blogeista oli tehty tunnettujen poliitikkojen nimillä ja luultavasti tekijä on etsinyt heistä julkista tietoa tehdäkseen blogeista vakuuttavampia. Tuomion mukaan kaikki blogit määrättiin poistettaviksi.

Tapaus 4 (kiristys) poikkeaa edellisistä tapauksista. Tekijä ei ole alun perin tuntenut uhriaan, vaan on tutustunut tähän Internetin anonyymissa chat-palvelussa ja siitä edelleen Skypessä. Tutustumalla hän on saavuttanut luottamuksen uhrin kanssa. Tapaus on tutkituista ainoa, jossa huijarin on ollut tarkoitus luoda todella henkilökohtainen yhteys toiseen käyttäjään. Huijari on päässyt niin lähelle uhria, että jopa estottoman webkamera-esiintymisen jälkeen uhri on ollut halukas paljastamaan yhä henkilökohtaisempaa tietoa ja hyväksymään Facebookissa tekijän kaveripyynnön. Facebookissa huijari on kerännyt tietoa pääasiassa uhrin ystävistä ja läheisistä, ja kerättyä tietoa hyökkääjä on voinut hyödyntää videon levittämisessä.

> Facebookista kerätään tietoa uhrin perheestä, ystävistä ja työnantajasta (Ilta-Sanomat, 17.12.2013).

> Samalla uhataan, että jos uhri ei maksa pikaisella aikataululla kiristäjän vaatimaa summaa, materiaali leviää (Ilta-Sanomat, 17.12.2013).

Tässä tapauksessa tekijä on nähnyt paljon vaivaa tavoitteensa onnistumiseksi. Uutiset eivät kerro, ovatko uhrit maksaneet vaaditun summan tekijälle/tekijöille ja ovatko uhrin Facebook-kaverit saaneet linkin kiristysvideoon. Ainakin uhrit ovat ottaneet yhteyttä poliisiin ja tehneet rikosilmoituksen. Kuten käsitteellisessä osuudessa mainittiin, luottamuksen syntymiseen vaikuttavat monet tekijät, jotka vaihtelevat eri ihmisten kesken. Toinen luottaa helpommin, kun taas toinen tarvitsee enemmän vakuuttelua.

Tapauksissa voidaan havaita kirjallisuudessa esitettyjä luotettavuuden tekijöitä. Kahdessa tapauksessa kohteena on ollut julkisuuden henkilö. Donnerin nimellä luotu huijaustili eli kohtuullisen kauan aikaa, ennen kuin se paljastui huijaukseksi. Mikäli huijaustilin kirjoitukset eivät silminnähden poikenneet totutusta Donnerin tyylistä, ei kukaan ole myöskään epäillyt tilin aitoutta. Hyvä kirjoitustaito on yksi uskottavuutta ja luotettavuutta herättävistä tekijöistä.

Lehtitietojen mukaan Donner ei itse edes tiennyt nimellään luodusta tilistä, eikä hänellä ole edes oikeaa tiliä Twitterissä. Donner on myös vaikutusvaltainen henkilö. Kirjallisuuden mukaan pätevyys ja kyvykkyys ovat luotettavuutta herättäviä tekijöitä. Oikean tilin puuttuminen oli keskeinen edellytys huijauksen onnistumiselle. Käyttäjien on tällöin ollut helppo uskoa, että ainoa tietyllä nimellä oleva tili kuuluu oikeasti kyseiselle henkilölle, jos mikään ei anna syytä epäillä tilin aitoutta.

Tapauksissa luottamuksen saavuttamisella on ollut hieman eri rooli tapauksesta riippuen. Tilanteesta riippuen luottamuksen ei ole tarvinnut olla niin lujaa, kun taas joissakin tapauksissa luottamuksen syntymisellä on ollut ratkaiseva merkitys, ja tekijä on käyttänyt aikaa ja vaivaa luottamuksen saavuttamiseen. Myös tämän perusteella voidaan sanoa, että käyttäjän manipuloinnilla on vahva rooli tutkittavissa tapauksissa. Keskeistä siinä on se, että hyökkääjä luottamuksen avulla yrittää saada uhrinsa tekemään jotain tai toimimaan hyökkääjää hyödyttävällä tavalla. Varsinkin tapauksessa 4 (kiristys) tämä käy ilmi selkeästi, sillä vaatii suurta luottamusta esiintyä vähäpukeisena web-kamerassa tuntemattoman ihmisen edessä ja olla itsekin tuntematon, ja tämän jälkeen hy-

väksyä tekijä Facebook-kaveriksi, jossa tekijä näkee paljon syvemmälle uhrin lähipiiriin ja elämään. Toisinaan tuntemattomia henkilöitä hyväksytään helposti kavereiksi, mutta koska taustalla on tuntemattomana ja alastomana esiintyminen web-kamerassa, voi Facebook-kaveruus tuntua liian henkilökohtaiselta.

6.3 Palvelut

Tapauksissa oli käytetty useita eri sosiaalisen median palveluita. Käsitteellinen osuus perustui suurimmaksi osaksi Facebook- ja Twitter-hyökkäyksiä käsitteleviin lähteisiin. Myös tutkituissa tapauksissa oli hyödynnetty kyseisiä palveluita, mutta näiden lisäksi hyödynnettiin myös Blogspot-palvelua ja Skypeä ja anonyymia chat-palvelua.

Tapauksessa 1 (alastonkuvat) rikos tapahtui Facebookissa, jossa tekijä julkaisi uhrista alastonkuvia.

> [Vastaaja] on oikeudettomasti toimittanut lukuisten ihmist4en saataville alastonkuvia [asianomistajasta]. [Vastaaja] on luonut Facebook.com:iin [asianomistajalle] profiilin ilman [asianomistajan] suostumusta, laittanut profiilin alle tästä kaksi alastonkuvaa ja kutsunut profiilin kautta [asianomistajan] tuntemia henkilöitä ns. Facebook-ystäviksi. (Helsingin käräjäoikeus, R 09/5097.)

Sen sijaan tapauksessa 2 (Donnerin nimellä luotu huijaustili) tekijä toimi Twitter-palvelussa.

> Tuntematon ihminen perusti Jörn Donnerin nimissä Twitter-tilin ja kirjoitti sinne noin 170 viestiä (Salokorpi, 16.5.2013).

Tapaus 3 (blogi-kirjoitukset) erosi edellisistä, sillä rikos toteutettiin täysin erilaisessa Blogspot-palvelussa.

> Tekijät ovat laatineet internetissä yleisölle avoimia sivustoja, joilla he ovat esittäneet [asianomistajat] lukuisia erilaisia valheellisia ja häntä halventavia väitteitä (Tampereen käräjäoikeus, R 07/3284).

> Tekijät ovat julkaisseet sanottuja lausuntoja [asianomistajista] ainakin seuraavilla sivustoilla: anja-aulomaa.blogspot.com, […] mattivanhanen.blogspot.com, [blogeja on noin 40] (Tampereen käräjäoikeus, R 07/3284).

Tapaus 4 (kiristys) oli myös hyvin erilainen verrattuna kolmeen muuhun, sillä se yhdisti kolme eri palvelua. Nämä olivat anonyymi chat-palvelu, Skype ja lopuksi Facebook. Lisäksi tähän liittyi myös videopalvelu Youtube, jossa tekijä julkaisi Skypessä kuvatun videon.

> Toiminnassa käytetään hyväksi verkon keskustelupalstoja, Skypeä ja Facebookia (Ilta-Sanomat, 17.12.2013).

> Tämän jälkeen [kun Facebookista on kerätty tietoa] lähetetään linkki Youtube-videoon, joka sisältää kaiken aiemmin kuvatun materiaalin (Ilta-Sanomat, 17.12.2013).

Tapauksissa palveluiden rooli erosi hieman toisistaan. Tapauksessa 1 tarkoituksena oli saavuttaa vain pieni yleisö kun taas tapauksessa 2 kohteena oli tuhansia käyttäjiä ja näiden lisäksi muut henkilöt ja media. Koska huijaustilin tviittejä siteerattiin muun muassa suomalaisissa päivälehdissä, on yleisö lopulta voinut olla kymmeniä tuhansia henkilöitä käsittävä.

> Jörn Donnerin nimissä tehtyä väärää Twitter-tiliä seurasi noin 2 000 ihmistä (Salokorpi, 16.5.2013).

> Valetilin viestejä ehdittiin siteerata melko laajasti (Salokorpi, 16.5.2013).

Tapauksen 4 osalta oli yllättävää, että hyökkäyksissä voi hyödyntää myös useampaa eri palvelua. Tapauksessa käytettiin chat-palvelua, Skypeä ja Facebookia. Näistä jokaisella oli hyökkäyksen ja rikoksen onnistumisen kannalta oma merkityksensä. Tekijän tuli saavuttaa luottamus uhriinsa ensin chat-palvelussa ja tämän jälkeen Skypessä, jossa kiristyksessä käytettävä video kuvattiin ja tallennettiin. Kun luottamus on rakennettu, on yhteydenpito siirretty Facebookiin, jossa on saatavilla Skypeä enemmän henkilökohtaista tietoa. Tekijä on hyödyntänyt tätä ja kerännyt uhrin profiilista tietoa muun muassa tämän kaverilistasta ja lähipiiristä. Uhrilla on voinut olla jopa satoja kavereita ja omista yksityisyysasetuksista on riippunut, miten laaja näkyvyys tekijällä on ollut uhrin henkilökohtaisiin tietoihin. Tutkimusten mukaan suuri osa käyttäjistä ei rajoita tietojen ja julkaisujen näkyvyyttä sosiaalisen median palveluissa, vaan luottavat oletusasetuksiin. Valitettavaa on, että oletusasetuksiin turvautuminen ei käytännössä koskaan ole paras, turvallisin ja yksityisin vaihtoehto. Kaverimäärästä riippuen lopulta videon olisi voinut nähdä sadat tai tuhannet käyttäjät. Julkaisuja voi myös jakaa, jolloin video olisi voinut lähteä leviämään nopeastikin. Osaltaan palveluiden toiminnot kääntyvät toisinaan rehellisiä käyttäjiä vastaan, sillä materiaalin edelleen levittäminen on tehty helposti. Toisaalta tulee huomioida se, että sinänsä täysin ulkopuolinen henkilö, joka jakaa videon eteenpäin, voi myös itse syyllistyä rikokseen.

Kirjallisuuden perusteella oli oletettavaa, että Facebookin ja Twitterin käyttö hyökkäyksissä nousisi esille. Vaikka tapausten määrä on pieni (4), palveluiden kirjo oli paljon laajempi kuin nämä kaksi. Tekijät olivat hyödyntäneet Facebookin ja Twitterin lisäksi Blogspotia, Skypeä, chat-palvelua ja Youtubea. Vaikka tutkituista tapauksista kolmessa oli käytetty Facebookia tai Twitteriä joko niin, että koko rikos tapahtui palvelussa tai osa rikoksesta toteutettiin siellä, ei voi sanoa, että vain näissä kahdessa sosiaalisen median palveluissa tehtäisiin rikoksia ja hyökkäyksiä. Aivan yhtä hyvin pienempiä ja erilaisempia palveluita käyttävät henkilöt voivat joutua identiteettivarkauden uhriksi, eikä rikollisuus todellakaan riipu palvelusta.

6.4 Rikokset

Tässä käsitellään lyhyesti tapausten perusteella rikoksia, joihin sosiaalisessa mediassa voi syyllistyä. Lisäksi kerrotaan aiheutuneesta haitasta ja tutkinnasta, joka vaikeutuu, kun kyseessä on ulkomaalainen sosiaalisen median palvelu.

6.4.1 Rikosnimikkeet

Kuten tutkielmassa on aikaisemmin useasti mainittu, identiteettivarkaus ei tutkielman kirjoittamisen aikaan ole vielä rikos. Mikäli väärää identiteettiä on käytetty ja siitä seuraa oikeustapaus, mahdollisia rikosnimikkeitä ovat muun muassa petos, maksuvälinepetos, kunnianloukkaus, yksityisyyselämää loukkaavan tiedon levittäminen.

Myös tutkitut tapaukset liittyivät edellä mainittuihin rikosnimikkeisiin. Tapauksessa 1 (alastonkuvat) vastaajaa syytettiin yksityiselämää loukkaavan tiedon levittämisestä.

> Vaadin vastaajalle rangaistusta seuraavasta rikoksesta: 1. Yksityisyyselämää loukkaava tiedon levittäminen (Helsingin käräjäoikeus, R 09/5097).

Tapauksessa 2 (Donnerin nimellä luotu huijaustili) kyseessä oli edellä mainitun rikosnimikkeen lisäksi kunnianloukkaus.

> Donnerin asianajajan Antti Hemmon mukaan tutkintapyynnön syynä on kunnianloukkaus ja yksityiselämää loukkaavan tiedon levittäminen (Seppälä, 25.3.2013).

Tapauksessa 3 (blogi-kirjoitukset) tekijöiden syyksi luettiin kaikkiaan seitsemän törkeää kunnianloukkausta, kiihottaminen kansanryhmää vastaan ja uskonrauhan rikkominen.

> A ja B ovat kumpikin osaltaan syyllistyneet törkeään kunnianloukkaukseen (Tampereen käräjäoikeus, R 07/3284).

> Rikoslain 24 luvun 10 §:n 1 kohdan mukaan törkeä kunnianloukkaus edellyttää, että valheellinen tieto tai vihjaus esitetään joukkotiedotusvälineitä käyttämällä tai muutoin toimittamalla tieto tai vihjaus lukuisten ihmisten saataville (Tampereen käräjäoikeus, R 07/3284).

Neljännessä tapauksessa (kiristys) kyseeseen tulee aikuisen kohdalla kiristys ja kunnianloukkaus ja 16–17 vuotiaan kohdalla rikosnimike on sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen.

> Rikosnimikkeet aikuisen henkilön ollessa asianomistajana olisivat perusmuodoissaan kiristys ja kunnianloukkaus. 16-17 -vuotiaan asianomistajan kohdalla lisäksi sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen. (Antikainen, 17.12.2013.)

Rikokset eivät ole palveluriippuvaisia, vaan yhtä hyvin toisen kunniaa voi loukata tai levittää hänestä tietoa niin blogissa kuin Twitterissä ja Facebookissa.

Vaikutus voi olla valtava, sillä palveluissa on satoja tuhansia käyttäjiä ja julkaisut leviävät salamannopeasti. Tapauksessa 3 (blogi-kirjoitukset) blogit on käsitetty joukkoviestintävälineinä, ja rikoksen tekemisen aikaan joukkoviestintävälineiden käyttö kunnianloukkauksessa on tehnyt rikoksesta rangaistavampaa (törkeä rikos). Vuonna 2014 voimaantulleessa laissa (Laki rikoslain muuttamisesta 879/2013) joukkoviestintävälineitä ei enää mainita törkeän rikoksen tunnusmerkistössä.

6.4.2 Motiivi ja aiheutunut haitta

Identiteettivarkauden ja tietojen kalastelun määritelmään kuuluu olennaisena osana aiheutunut taloudellinen tai muu haitta tai hyökkääjän näkökulmasta katsottuna saavutettu etu. Myös tutkittavissa tapauksissa oli havaittavissa tämän ehdon täyttyminen tavalla tai toisella. Tapauksessa 1 (alastonkuvat) tekijä halusi aiheuttaa uhrille häpeää ja nolostumista julkaisemalla tästä arkaluontoisia kuvia uhrin ystävien nähtäville. Uhri oli tekijän mukaan velkaa tälle, ja tekijän tavoitteena oli tällä tavoin pakottaa velka maksetuksi. On epäselvää, maksoiko uhri velkansa vai ei.

> Vastaaja oli pyytänyt [asianomistajaa] maksamaan takaisin hänelle lainaamansa rahat. Kun vastaaja ei ollut saanut suoritusta, hän oli lähettänyt painostusmielessä tekstiviestejä [asianomistajalle], jotta saisi lainaamansa rahat takaisin. (Helsingin käräjäoikeus, R 09/5097.)

> Viestien tarkoitus oli painostaa [asianomistajaa] maksamaan velkansa mutta [vastaaja] ei toteuttanut uhkauksiaan [julkaista alastonkuvia Facebookissa]. (Helsingin käräjäoikeus, R 09/5097.)

Tapauksessa 2 (Donnerin nimellä luotu huijaustili) tarkoituksena oli niin ikään vain uskotella muille, että Twitter-tilin julkaisujen takana todellakin on Jörn Donner itse. Tapaus ei vaikuta niinkään kiusanteolta, sillä tekijä ei missään vaiheessa haukkunut Donneria.

> Me kunnioitamme Jörn Donneria. Tarkoituksemme ei ole aiheuttaa pahaa mieltä […], tilinhaltija kirjoitti iltakymmenen jälkeen. (Seppälä, 25.3.2013.)

Eräässä uutisessa kirjoitettiin, että huijaustiliä voisi melkein pitää jopa kunnianja ihailunosoituksena Donneria kohtaan. Huijausprofiilin kirjoitukset olivat maltillisia, joten sinänsä aiheutunut haitta jäi pieneksi. Tilanne voisi kuitenkin myös olla päinvastainen, jolloin julkisuuden henkilön ja poliitikon oma ura voisi kärsiä jonkun toisen kirjoitusten takia. Tekijä voisi väittää ja esittää esimerkiksi radikaaleja mielipiteitä ja suuren seuraajamäärän takia muut ihmiset voisivat uskoa ne oikean henkilön sanomiksi.

Tapaus 3 (blogi-kirjoitukset) tilanne on juuri edellä kuvatun kaltainen. Tekijät ovat kirjoittaneet toisten henkilöiden nimissä jyrkkiä mielipiteitä, kehottaneet rikoksiin ja herjanneet muita ihmisiä. Tällaisella kirjoittelulla voi olla kauaskantoiset seuraukset. Vaikka tuomiota koskevan asiakirjan mukaan kyseiset blogi-sivut on pyydetty poistettaviksi, karu totuus on, ettei kerran Internettiin

laitettua asiaa välttämättä saa koskaan täysin kitketyksi pois. Tuomiosta ei käynyt ilmi, miten moni ehti kirjoitukset nähdä.

Tapaus 4 (kiristys) on ainoa tutkituista tapauksista, jossa tekijän tarkoitus on ollut selkeästi saavuttaa taloudellista hyötyä, minkä lisäksi uhrille aiheutetaan henkistä kärsimystä. Videoiden avulla tekijä on yrittänyt kiristää jopa lähes tuhat euroa tapauksesta riippuen.

> Nettipoliisi Jutta Antikainen kertoo Facebookissa uudesta ilmiöstä, jossa huijataan pahaa-aavistamattomat käyttäjät noloon tilanteeseen, ja heiltä kiristetään suuria summia (Ilta-Sanomat, 17.12.2013).

> Minun [asianomistajan] pitää maksaa huomiseen mennessä 800 euroa tai hän jakaa videon kaikille FB-kavereilleni ja julkaisee sen uudelleen (Antikainen, 17.12.2013).

Kuten perinteisille rahaa pyytäville nigerialaiskirjeille ja romanssihuijauksille on tyypillistä, rahat viedään mutta mitään ei tule takaisin. Todennäköisesti sama pätee myös tässä, eli vaikka uhri olisikin maksanut vaaditun summan, video olisi silti voinut lähteä leviämään julkisesti.

Jokaisessa tapauksessa pyrittiin saavuttamaan joko taloudellista tai muuta hyötyä, tai aiheuttamaan uhrille taloudellista tai esimerkiksi henkistä haittaa. On epäselvää, saiko kukaan tekijöistä lopulta taloudellista hyötyä, vaikka kahdessa tapauksessa siihen pyrittiinkin.

6.4.3 Tutkinta

Kahdessa tapauksessa epäiltyä ei joko tuomittu tai tutkinta lopetettiin syyttäjän toimesta. Tapauksessa 1 (alastonkuvat) IP-osoitetta ei selvitetty, vaikka tekijä olisikin todennäköisesti osoitteen avulla saatu selville. Asianomistaja oli lähettänyt alastonkuvia myös toiselle henkilölle, joten täyttä varmuutta huijausprofiilin luojasta ei ollut. Toisaalta taitava rikollinen voi käyttää esimerkiksi Torverkkoa (The Onion Router), joka mahdollistaa anonyymin liikkuminen Internetissä niin, ettei käyttäjän tekemisistä ja sijainnista jää tietoja. Tällaisessa tilanteessa IP-osoitetta on erittäin hankala saada selville.

> [Asianomistaja] oli lähettänyt valeprofiiliin liitetyt valokuvat yhdelle ulkopuoliselle henkilölle sen lisäksi, että kertomansa mukaan oli lähettänyt kyseiset kuvat myös [vastaajalle]. (Helsingin käräjäoikeus, R 09/5097.)

Tapauksessa 2 (Donnerin nimellä luotu huijaustili) tutkinta lopetettiin, sillä kustannukset olisivat olleet korkeat suhteessa vaivannäköön, eikä edes perusteellinen tutkinta takaa sitä, että tekijä olisi joutunut vastuuseen.

> Poliisi perustelee tutkinnan lopettamista kustannussyillä. Tutkinnan johtajan mukaan kulut ovat selvässä epäsuhteessa tutkittavan asian laatuun ja siitä mahdollisesti tulevaan rangaistukseen. Asiassa pitäisi muun muassa tehdä oikeusapupyyntö Yhdysvaltoihin, koska viestit oli kirjoitettu yhdysvaltalaisella sivustolla. Poliisin arvion mukaan edes perusteellinen esitutkinta ei takaisi sitä, että joku joutuisi rikosoikeudelliseen vastuuseen. (Salokorpi, 16.5.2013.)

Televalvontalaki on keskeisessä osassa siinä, miksi IP-osoitteita ei ole selvitetty tapauksessa 1 j 2. Laki määrittelee tarkasti televalvonnan edellytykset. Lain mukaan muun muassa teleoperaattoreilla on velvollisuus luovuttaa tietoja poliisille, mikäli tietoja yksittäistapauksessa tarvitaan poliisille kuuluvan tehtävän suorittamiseksi. Poliisilla on rikoksen estämiseksi tai paljastamiseksi oikeus kohdistaa televalvontaa muun muassa teleliittymään ja telepäätelaitteeseen, jos on perusteltua olettaa epäillyn syyllistyneen esimerkiksi automaattiseen tietojenkäsittelyjärjestelmään kohdistuvaan rikokseen, huumausainerikokseen tai rikokseen, jonka ankarin rangaistus on vähintään neljä vuotta vankeutta. (Laki poliisilain muuttamisesta 525/2005.) Tapauksessa 1 ja 3 televalvonnan edellytykset eivät ole täyttyneet, joten teleoperaattoreilta ei ole saatu tietoja.

Tulevaisuudessa identiteettivarkaudesta tuomittava korkein rangaistus on sakko, mikäli eduskunta hyväksyy lainmuutoksen esitetyssä muodossa. Rikoksesta tulee aiheutua vähäistä suurempaa haittaa, jotta siitä tuomitaan. Sosiaalisen median palvelut rikospaikkana voivat olla haastavia, sillä palveluntarjoajat ovat rekisteröityneet muihin maihin kuin Suomeen ja niiden palvelimia on yleensä ympäri maailman. Usein uhri on eri maassa kuin rikollinen saati palveluntarjoaja. Oikeusapupyyntö tulee osoittaa siihen valtioon, johon palveluntarjoaja on rekisteröitynyt. Oikeusapupyynnön voi tehdä oikeusministeriö, tuomioistuin, syyttäjäviranomainen ja esitutkintaviranomainen. Lain mukaan (Laki kansainvälisestä oikeusavusta rikosasioissa 5.1.1994/4) kansainväliseen oikeusapuun kuuluu muun muassa rikosasian käsittelyyn liittyvien asiakirjojen tiedoksianto, todistajien kuuleminen, asiakirjojen ja esine- ja muiden todisteiden hankkiminen, vastaanottaminen ja toimittaminen sekä asiantuntijoiden kuuleminen. Oikeusapupyynnössä tulee määrittää esimerkiksi viranomainen, joka on tehnyt pyynnön, henkilöt, joita pyyntö koskee, kuvaus rikollisesta teosta ja todisteista sekä selvitettävistä asioista ja lainkohdat, joihin teon rangaistavuus perustuu. Oikeusapupyyntö mahdollistaa rikoksen kannalta olennaisten tietojen saamisen ja rikoksen selvittämisen sellaisessa tilanteessa, jossa rikos ylittää maan rajat.

Suomessa rikoksesta epäillyllä on oikeus vaieta (Laki esitutkintalain muuttamisesta 818/2014). Tämä tarkoittaa sitä, ettei epäillyn tarvitse omalla toiminnallaan myötävaikuttaa mahdollisen rikoksen selvittämiseen (itsekriminointisuoja). Siten epäillyn ei tarvitse kertoa poliisille esimerkiksi käyttäjätunnuksia käyttämäänsä sosiaalisen median palveluun. Ainakin Facebook luovuttaa käyttäjätiliin liittyviä tietoja palvelun käyttöehtojen ja Yhdysvaltojen lain mukaisesti. Luovutettavia tietoja ovat muun muassa käyttäjän nimi, palvelun käyttöaika, sähköpostiosoitteet, luottokorttitiedot ja viimeisimmässä sisään- tai uloskirjautumisessa käytetyt IP-osoitteet, mikäli ne ovat tiedossa. Kansainvälisissä oikeudenkäyntiprosesseissa edellytyksenä on oikeusapupyyntö tai keskinäinen sopimus, jotta käyttäjätilin sisältö paljastetaan. (Facebook, 2015a.)

6.5 Yhteenveto

Tässä luvussa esitettiin tutkimuksen tulokset. Ensimmäisessä alaluvussa kuvattiin käytettyjä tietojen kalastelukeinoja, joiden piirteitä oli tutkittavissa tapauksissa havaittavissa. Useassa tapauksessa oli hyödynnetty toisen henkilön nimellä tehtyä profiilia ja käyttäjän manipulointia.

Toisessa alaluvussa kuvailtiin sitä, missä tekijä oli kerännyt tietonsa ja mikä uhrin suhde tekijään oli. Esimerkiksi kuuluisista henkilöistä on helpompi löytää tietoa Internetistä kuin täysin tuntemattomasta. Palveluita käytettiin myös tietojen keräämiseen.

Kirjallisuuden perusteella oletettiin, että tapauksissa nousi esiin Facebook ja Twitter, sillä nämä ovat suosituimmat ja tunnetuimmat palvelut, joten todennäköisesti näissä tapahtuu myös rikoksia. Näin kävikin, mutta myös muita palveluita käytettiin. Joukkoon mahtui blogi- ja videopalvelu sekä Internetin anonyymi chat-palvelu, jossa voi nimettömästi keskustella toisten henkilöiden kanssa. Ei voi siis olettaa, että rikoksia tehtäisiin pelkästään maailmanlaajuisissa ja isoissa palveluissa, vaan myös pienemmät palvelut ovat aivan yhtä riskialttiita. Lukumäärällisesti rikosten määrä toki voi erota eri palvelujen välillä, mutta mikään palvelu ei ole hyökkäyksiltä täydellisesti turvassa.

Koska identiteettivarkaus ei vielä ole rikos Suomessa, vaan kyseeseen tulee jokin muu rikosnimike, katsottiin tarpeelliseksi kuvailla lyhyesti niitä rikoksia, joita sosiaalisen median palveluissa voi tehdä. Lisäksi kerrottiin motiivista ja aiheutuneesta haitasta. Tietojen kalastelulle ja identiteettivarkaudelle on olennaista, että joko tekijä itse saavuttaa jotain tai aiheuttaa uhrille joko taloudellista tai muuta haittaa. Tämä näkyi myös tutkituissa tapauksissa, vaikkakin vain yhdessä tapauksessa tavoiteltiin selkeästi taloudellista hyötyä. Yleensä tarkoituksena oli pilailla toisen kustannuksella tai yrittää nolostuttaa tämä. Alaluvussa kerrottiin myös hieman syistä, joiden takia joistain rikoksista ei ole tuomittu tai tutkintaa edes aloitettu. Sosiaalisen median palveluiden palvelimet sijaitsevat ulkomailla, joten jotta esimerkiksi huijausprofiilin takana oleva IP-osoite saataisiin selville, tulisi palvelimen sijaintimaahan tehdä oikeusapupyyntö. Toisinaan kustannukset ja vaivannäkö ja laki eivät kohtaa saavutettua hyötyä, jolloin on katsottu paremmaksi olla jatkamatta tutkintaa ja lopettaa se siihen.

Tapaukset esittivät kukin hyvin erilaisen näkökulman identiteettivarkaudesta sosiaalisen median palveluissa, vaikka tapauksissa on myös paljon samaa. Erilaisuus vain osoittaa, ettei identiteettivarkautta voi laittaa yhteen muottiin. Osaltaan käytäntö tuki kirjallisuuden antamaa kuvaa aiheesta, mutta oli myös asioita, jotka eivät menneet esitetyllä tavalla. Olisi ollut mielenkiintoista tutkia tapauksia, joissa hyödynnetään monimutkaisia keinoja, mutta tutkimukseen ei saatu yhtään sellaista tapausta. Voi myös olla, ettei ainakaan Suomessa kovin vaativia keinoja ole edes käytetty identiteettivarkauteen sosiaalisessa mediassa.

7 POHDINTA

Tässä luvussa esitetään lyhyesti tutkimuksen tulokset ja tehdään niistä johtopäätöksiä. Lisäksi pohditaan, missä yhteydessä tutkimusta voi hyödyntää.

7.1 Tulokset ja johtopäätökset

Tutkimuksessa tarkasteltiin kirjallisuuden perusteella tehtyjen kysymysten kautta tutkittavia oikeus- ja muita tapauksia. Teorian perusteella luotiin kuusi havaintoa, jotka jollain tavalla kuvaavat identiteettivarkauden ja tietojen kalastelun toteutumista ja ympäristöä, jossa hyökkäys ja rikos tapahtuivat.

Kaikilta osin kirjallisuuden ja käytännön antamat kuvat identiteettivarkaudesta ja sosiaalisesta mediasta eivät vastanneet toisiaan. Tapauksissa oli käytetty muutamaa hyökkäyskeinoa, jotka eivät olleet teknisesti kovin vaativia. Tämä oli oletettavaa, sillä tekniset keinot vaativat toisinaan enemmän osaamista, eivätkä ole niin helposti toteutettavissa. Jos tapauksia olisi ollut useampia, olisivat myös hyökkäyskeinot todennäköisesti vaihdelleen enemmän. Kirjallisuudessa esiteltiin monipuolisesti sekä yksinkertaisia että monimutkaisia hyökkäysmenetelmiä, mutta teknisten hyökkäysten piirteitä ei ollut havaittavissa tutkittavissa tapauksissa.

Useimmissa tapauksissa tekijä oli nähnyt kohtuullisen vähän vaivaa hyökkäyksen ja rikoksen onnistumiseksi. Sosiaalisen median palveluissa on helppo luoda profiili toisen nimellä. Tarkoituksena oli saada tapauksesta riippuen joko yksittäiset henkilöt tai jopa tuhannet ihmiset uskomaan profiilin aitouteen. Tapauksissa oli samankaltaisuuksia, mutta myös eroavaisuuksia. Luottamuksen määrä ja tarkoitus vaihtelivat eri tapauksissa. Donnerin tapauksessa tekijän ei tarvinnut luoda kovin läheistä luottamusta muihin käyttäjiin, mutta kiristystapauksessa (tapaus 4) luottamus oli ratkaisevassa asemassa rikoksen onnistumisen kannalta.

Kirjallisuuskatsauksessa esiteltiin erilaisia tekijöitä, jotka vaikuttavat luottamuksen syntymiseen sosiaalisessa mediassa. Tutkittavien tapausten määrä oli

pieni, mutta muutamia tekijöitä oli silti nähtävissä. Esiintulleita luotettavuuden tekijöitä olivat ainakin kuuluisuus, hyvä kirjoitustaito ja kyvykkyys. Kahdessa tapauksessa hyödynnettiin kuuluisien ja vaikutusvaltaisten henkilöiden identiteettejä, ja varsinkin Donnerin tapauksessa luotettavuuden tekijät korostuivat. Monet siteerasivat ja kommentoivat vale-Donnerin tviittejä olettaen tämän olevan oikea Jörn Donner. Kirjallisuudessa esiteltiin paljon enemmän luotettavuuteen vaikuttavia tekijöitä, ja luultavasti muitakin tekijöitä olisi voitu havaita, jos tutkittujen tapausten määrä olisi ollut suurempi ja monipuolisempi. Vaikka kuuluisaan henkilöön luotetaan, esittää kirjallisuus myös, ettei julkisuuden henkilöltä tullutta kaveripyyntöä hyväksytä kovin usein. Ajatusmalli lienee se, että julkisuuden henkilöä voi seurata ja häneen voi ottaa kontaktia, mutta on epäilyttävää, jos kuuluisa henkilö yrittää ottaa yhteyttä tavalliseen ihmiseen.

Suuri osa tieteellisestä materiaalista käsittelee tutkittua aihetta Facebookin ja Twitterin näkökulmasta. Sen sijaan tutkituissa tapauksissa paljastui myös muita palveluita, joita hyödynnetään tietojen kalastelussa ja identiteettivarkauksissa. Mikään palvelu ei ole täysin turvassa rikollisuudelta, ja on väärin olettaa, että vain tunnetuimmat ja suosituimmat palvelut ovat rikollisten kohteena. Toki on todennäköistä, että isoissa ja kansainvälisissä palveluissa tapahtuu lukumäärällisesti enemmän rikoksia kuin pienissä ja tuntemattomammissa palveluissa.

Yleinen suuntaviiva tutkituissa tapauksissa on se, että varsinaisesti identiteettivarkaus ei ole ollut pääasiana rikoksessa, vaan toisen henkilön identiteetin turvin on tehty muita rikoksia. Todennäköisesti sama trendi tulee myös jatkumaan tulevaisuudessa. Identiteettivarkaus tulee luultavasti olemaan vain rikos, jonka avulla tehdään muita rikoksia eli se on osa laajempaa kokonaisuutta, vaikka siitä voidaankin tuomita omana rikoksenaan.

Sosiaalisen median palveluissa ja ylipäätään Internetissä tapahtuvissa rikoksissa on se piirre, että tekijä voi olla tuhansien kilometrien päässä. Virtuaalirikollisuus on kasvanut rajusti viime vuosina ja se tulee olemaan iso uhka myös tulevaisuudessa. Rikosten tutkimista vaikeuttaa se, että useat sivustot eivät ole suomalaisia, vaan niiden palvelin sijaitsee jossain muussa maassa. Tutkinnan kannalta rikosten selvittely on paitsi haastavaa myös aikaa vievää, sillä kotimaisella viranomaisella ei ole valtuuksia mennä ulkomaan maaperälle, vaan esimerkiksi sosiaalisen median palveluilta hyödyntävien rikosten tutkinnassa tulee tehdä oikeusapupyyntö kyseisen valtion viranomaisille. Pienissä ja vähäpätöisissä rikoksissa ei edes nyt mennä niin pitkälle, sillä saavutettu hyöty on pieni verrattuna kustannuksiin ja vaivannäköön. Lisäksi laki määrää muun muassa televalvonnan edellytyksistä, eikä sitä saa tehdä ilman lupaa. Tutkituissa tapauksissa kahdessa ei selvitetty esimerkiksi IP-osoitetta, jolla rikoksiin syyllistynyt olisi todennäköisesti saatu kiinni. Toisaalta taitava virtuaalirikollinen pystyy huijaamaan myös tässä asiassa, joten edes perusteellinen tutkinta ei aina takaa sitä, että syyllinen löytyy.

Käyttäjän manipulointi näyttäytyi isossa osassa kaikissa tapauksissa. Tämä oli ennustettavissa, sillä lähes kaikissa tietojen kalasteluhyökkäyksissä tällä on jokin rooli. Kaikissa tapauksissa näkyi myös selkeästi tavoiteltu tai aiheutet-

tu hyöty/haitta. Taloudellista hyötyä tavoiteltiin kahdessa tapauksessa, vaikka onkin epäselvää, saivatko tekijät lopulta tavoittelemaansa taloudellista etua.

Monet ovat varmasti törmänneet joskus eri palveluissa selkeisiin huijausprofiileihin. Tällaisen profiilin takana eivät aina välttämättä ole rikolliset tarkoitusperät, vaan tekijä haluaa vain vähän pitää hauskaa ja pilailla. Varsinkin julkisuuden henkilöistä saattaa löytyä jopa kymmeniä huijausprofiileita. Useimmiten näistä kuitenkin näkee heti, etteivät ne ole oikean henkilön luomia. Monen palvelun tarjoama profiilin vahvistamistoiminto edesauttaa oikean profiilin tunnistamista. Pian voimaantulevan identiteettivarkauslaki ei edelleenkään kiellä näiden valeprofiilin luomista. Keskeistä on, että profiilista näkyy selkeästi, että se on tehty pilailutarkoituksessa eikä tarkoitus ole erehdyttää saati aiheuttaa muille haittaa tai saavuttaa itse taloudellista etua. Julkisuuden henkilöiden tulee kestää lähtökohtaisesti enemmän arvostelua verrattuna tavallisiin kansalaisiin. Kaikista huijausprofiileista on siten hyödytöntä tehdä rikosilmoitusta, sillä tapauksia luultavasti tulisi tuhansia. Vaikka julkinen työ asettaakin henkilön eri asemaan, ei kenenkään henkilökohtaisten ominaisuuksien haukkuminen ja perättömien väitteiden kirjoittaminen silti ole suotavaa. Internettiä on totuttu pitämään anonyymina paikkana, jossa voi päästää suuttumuksensa valloilleen ja kirjoittaa radikaalitkin mielipiteet sanoja säästelemättä. Tosiasia silti on, että rikokseen voi syyllistyä myös Internetissä, eikä siellä siksi kannata julkaista mitään, mitä ei olisi valmis sanomaan myös kasvotusten.

Tällä hetkellä poliisilla ei ole oikeuksia esimerkiksi poistaa huijausprofiilia tai muuta materiaalia sosiaalisen median palveluista. Poliisi voi pyytää profiilin poistamista, kuten kuka tahansa kansalaisista. Myös nettipoliisi korostaa tätä, sillä heidän toimenkuvaansa kuuluu asioiden seuraaminen ja tarvittaessa puuttuminen ja jatkotoimenpiteet, (Poliisi, 2015.) Nettipoliisit eivät siis moderoi sivustoja ja poista haitallista materiaalia suoraan. Tehokkain keino onkin ottaa suoraan itse yhteyttä palvelun ylläpitoon ja raportoida epäilyttävästä profiilista. Joissain palveluissa, esimerkiksi Facebookissa ilmoituksen voi tehdä huijausprofiilin sivulla vain nappia painamalla.

Karu totuus on, ettei huijausprofiileita koskaan pystytä kitkemään täysin mistään. Tärkeää onkin selvittää, mitä tarkoitusta varten profiili on luotu. Selvästi viattomaan pilailuun tehty profiili saattaa piristää useiden käyttäjien päivää ilman, että siitä koituu kenellekään hankaluuksia tai pahaa mieltä eikä minkään rikoksen tunnusmerkistö täyty.

7.2 Tutkimuksen hyödyntäminen

Tämä tutkimus kuvaa yleisimpiä tietojen kalastelutekniikoita ja niiden toteuttamista. Näiden lisäksi on toki muitakin sekä teknisesti vaativampia keinoja että myös tutkielmassa kuvattuja helpompia ”jokamiehen” keinoja. Tutkielmassa on haluttu ensisijaisesti tuoda esille ne keinot, joilla paitsi tietojen kalastelu, myös identiteetin varastaminen on helppoa.

Tutkielmaa voi hyödyntää identiteettivarkauksia, tietojen kalastelua ja sosiaalista mediaa käsittelevissä yhteyksissä niin tutkimuksen kuin käytännönkin kannalta. Tutkielman aihe on tullut osittain Victim Support for Identity Theft -projektista (VISIT-projekti), jossa tutkitaan identiteettivarkauksia ja keinoja niiden ehkäisemiseen. Vaikka projekti käsittää myös muita Internetissä tapahtuvia tietojen kalastelutekniikoita ja identiteettivarkauksia, on sosiaalisen median näkökulma hyvä lisä siihen – onhan palveluihin rekisteröityneitä yhteensä jo miljardeja maailmassa. Identiteettivarkauksiin liittyy myös taloudellinen puoli, sillä menetys voi olla suuri. Nykyaikana perinteisten nigerialaiskirjeiden rinnalle ovat tulleet romanssihuijaukset, joissa rakkauteen vedoten pyritään saamaan rahaa uhrilta.

Tutkielmaa on kirjoitettu samaan aikaan kuin kirjoittaja on työskennellyt VISIT-projektissa. Projekti on edesauttanut tutkielman kirjoittamista ja antanut sille uusia näkökulmia, ja vastaavasti varsinkin tutkielman käsitteellinen osuus on hyödyttänyt projektia.

Paitsi tutkimuksen kannalta, tutkielmasta on hyötyä myös käytännön tasolla sosiaalisen median palveluiden käyttäjille. Tutkielma tarjoaa katsauksen siihen, mitä piirteitä sosiaalisen median palveluiden kautta tehdyillä identiteettivarkauksilla on ja millaisia keinoja rikosten toteuttamiseen, identiteettivarkauksiin ja tietojen kalasteluun on olemassa. Tutkittavat tapaukset olivat luonteeltaan kovin erilaisia, vaikka yhteisiä tekijöitä löytyikin. Kukin tapaus tuo erilaisen näkökulman identiteettivarkauteen ja sosiaaliseen mediaan, mikä osoittaa, ettei ilmiö toistu täysin samanlaisena. Tutkielmaan ei ole edes yritetty sisällyttää kaikkia keinoja, vaan on haluttu keskittyä niihin, jotka ovat helpoimmin toteutettavissa ja joihin käyttäjät itse voivat varautua. Tutkielmassa on haluttu tuoda esiin tekijöitä, jotka ovat yleisiä muun muassa huijausprofiileissa ja asioita, joihin käyttäjä huomaamattaan saattaa uskoa. Koska käyttäjän manipulointi on keskeisessä osassa hyökkäysten ja rikosten taustalla, käyttäjien tulisi kiinnittää huomiota omaan ajatteluunsa ja toimintaansa sosiaalisen median palveluissa.

8 YHTEENVETO

Tämän tutkimuksen tarkoituksena oli selvittää, miten sosiaalisen median palveluita voidaan hyödyntää identiteettivarkauksissa ja tietojen kalastelussa. Tutkielman ensimmäinen osa koostui teoriasta, jossa käsiteltiin aihetta pääasiassa tieteellisten lähteiden kautta. Kirjallisuuskatsauksessa kuvattiin ensin identiteettivarkauden määritelmän pohjana toimivia käsitteitä ja eri tahojen laatimia määritelmiä. Koska identiteettivarkaus ei vielä ole rikos Suomessa, sovellettiin eri määritelmiä tutkielman kannalta sopivaksi yhteiseksi käsitteeksi, joka kattaa ne rikokset, joissa voidaan hyödyntää väärää identiteettiä.

Kirjallisuuskatsauksessa käsiteltiin lisäksi erilaisia menetelmiä, joilla identiteetti voidaan varastaa. Osa menetelmistä perustuu ihmisen luontaisen käyttäytymisen hyödyntämiseen. Tätä kutsutaan käyttäjän manipuloinniksi. On myös olemassa tietojen kalastelumenetelmiä, jotka vaativat teknistä osaamista. Tähän tutkielmaan valikoitui ne keinot, joista löytyy eniten tietoa, jotta mahdollistettaisiin monipuolinen kuva jokaisesta hyökkäystyypistä. Keinoja on myös paljon lisää ja uusia kehitetään jatkuvasti. Koska ihmisen luontaista käyttäytymistä vastaan on vaikea suojautua virusturvaohjelmilla, on haluttu tuoda erityisesti esiin juuri tätä hyödyntävät tekniikat, sillä niitä hyödynnetään tulevaisuudessakin laajasti.

Empiirinen osuus toteutettiin teoriaa testaavasta näkökulmasta. Kirjallisuuskatsauksen teorian perusteella luotiin identiteettivarkautta, tietojen kalastelua ja sosiaalisen median palveluita koskevia havainnoivia kysymyksiä. Koska kirjallisuuskatsauksessa käytettiin useita eri lähteitä ja siten teorian takana seisoo enemmän kuin yksi kirjoittaja, voitiin sen perusteella luoda puolueettomia ja perusteltuja oletuksia. Teorian pohjalta luotujen kysymysten avulla tarkasteltiin käytännön tapauksia. Empiirisen osan aineistona oli sekä oikeustapauksia että uutisia.

Kirjallisuuskatsauksen luoma kuva identiteettivarkauden ja sosiaalisen median välisestä suhteesta vastasi osittain hyvin käytännön tapauksiin, mutta myös eroavaisuuksia löytyi. Valitettavasti tutkittujen tapausten määrä oli pieni johtuen tapausten hankintaan liittyvistä kirjoittajasta riippumattomista vaikeuksista. Kuitenkin tutkielmaa varten saatiin kerättyä sinänsä monipuolinen

joukko tapauksia, joista löytyi sekä samankaltaisuutta että eroavaisuuksia. Jo näin pieni määrä tapauksia tuo aivan erilaisia näkökulmia identiteettivarkauteen sosiaalisessa mediassa.

Tutkituissa tapauksissa oli nähtävissä viitteitä käyttäjän manipulaatiosta ja huijausprofiileista. Tämä oli oletettavaa, sillä sosiaalisen median palvelut mahdollistavat väärällä nimellä esiintymisen. Vaikka palveluiden käyttöohjeissa kielletäänkin huijausprofiilit, on nykyisillä toimintatavoilla ja resursseilla kieltoa hankala valvoa muuten kuin koneellisesti. Tässä vaaditaankin käyttäjien aktiivisuutta raportoida ylläpidolle epäilyttävistä profiileista.

Lisäksi tutkimuksessa havaittiin, että rikospaikkoina olivat Facebook, Twitter, Blogspot, Skype ja Youtube. Facebook ja Twitter ovat suosituimpia ja tunnetuimpia palveluita, joten oli oletettavaa, että näissä tapahtuisi myös rikoksia, mutta rikollisuus ei todellakaan rajoitu pelkästään näihin palveluihin, kuten tutkimuksessa huomattiin.

Omien henkilökohtaisten tietojen pitäminen julkisesti saatavilla helpottaa identiteetin varastamista. Varsinkin julkisuuden henkilöistä on saatavilla paljon tietoa, ja tutkituissa tapauksissa peräti kahdessa oli käytetty tunnettuja ihmisiä. Toisinaan huijausprofiili voi olla hankala erottaa aidosta, varsinkin jos tietyllä nimellä löytyy vain yksi ainoa profiili eivätkä profiilin julkaisut eroa nähtävästi siitä, mitä oikea henkilö sanoisi.

Jatkotutkimuksessa olisi mielenkiintoista selvittää, miltä tilanne näyttää identiteettivarkauslain astuttua voimaan vuoden 2015 syksyllä. Kun laki on voimassa, väheneekö esimerkiksi toisen henkilön nimellä tehtyjen profiilien määrä sosiaalisessa mediassa. Sosiaalisen media on kansainvälisen ja henkilökohtaisen luonteensa takia mielenkiintoinen rikospaikka. Olisikin kiinnostavaa tutkia, millaisilla keinoilla identiteettivarkautta ja muuta rikollisuutta voisi sosiaalisessa mediassa vähentää sekä palveluntarjoajan että käyttäjän oman toiminnan kautta, ja onko se edes mahdollista. Tässä tietojärjestelmätiede kohtaa psykologian, sillä ihmismieltä ei suojata palomuurilla ja virusturvalla. Lisäksi jatkotutkimuksena voisi selvittää, eroavatko erityyppiset palvelut toisistaan rikollisuuden suhteen. Työnhakuun ja ammatilliseen osaamiseen keskittyvät palvelut eroavat viihteellisistä palveluista, mutta tähän tutkimukseen ei saatu aineistoa ensiksi mainitusta palvelutyypistä.

Identiteettivarkaudessa on varsinaisen varkauden sijaan lähes aina kyse informaation kopioimisesta eli rikollinen kopioi tietoa uhrista tämän tietämättä tarkoituksenaan hyödyntää tietoa edelleen. Pelkän nimen kopioimisella voi saada valtavaa tuhoa aikaiseksi uhrin elämässä. Internettiä on totuttu pitämään anonyymina paikkana, jossa jokainen saa olla juuri sitä, mitä haluaa ja puhua suunsa puhtaaksi. Sosiaalisen median palveluita käytetään jatkossakin rikosten tekemiseen eikä rikollisuutta saada koskaan kitkettyä täysin pois virtuaali- tai fyysisestä elämästä. Omalla toiminnalla ja tarkkaavaisuudella voi vaikuttaa paljon siihen, miten turvassa on. Oma identiteetti ei ole myytävissä, lainattavissa tai toisen ihmisen käytettävissä. Jokaisella on yksinoikeus olla itsensä.

LÄHTEET

Aggarwal, A., Rajadesingan, A. & Kumaraguru, P. (2012). PhishAri: Automatic realtime phishing detection on Twitter. Teoksessa *Proceedings of 2012 eCrime Researchers Summit (eCrime 2012)* (s. 554–266). IEEE.

Ahmadinejad, S. H., Anwar, M. & Fong, P. W. L. (2011). Inference attacks by third-party extension to social network systems. Teoksessa *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (s. 2824–2287). IEEE.

Ahmed, F. & Abulaish, M. (2012). An MCL-based approach for spam profile detection in online social networks. Teoksessa *Proceedings of 2012 IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom 2012)* (s. 6024–2608). Washington, DC: IEEE Computer Society.

Algarni, A., Xu, Y. & Chan T. (2014). Social engineering in social netowrking sites: The art of impersonation. Teoksessa *Proceedings of the 2014 IEEE International Conference on Services Computing (SSC 2014)* (s. 7974–2804). Washington, DC: IEEE Computer Society.

Bhumiratana, B. (2011). A model for automating persistent identity clone in online social network. Teoksessa *Proceedings of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011)* (s. 6814–2686). Washington, DC: IEEE Computer Society.

Beck, K. (2011). Analyzing tweets to identify malicious messages. Teoksessa *Proceedings of 2011 IEEE International Conference on Electro/Information Technology (EIT)* (s. 1874–2191). IEEE.

Benenson, Z., Girard, A., Hintz, N. & Luder, A. (2014). Susceptibility to url-based internet attacks: Facebook vs. e-mail. Teoksessa *Proceedings of 2014 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (s. 6044–2609). IEEE.

Buchanan, T & Whitty, M.T. (2014). The online dating romance scam: causes and consequences of victimhood . *Psychology, Crime & Law, 20(3),* 2614–2283.

Cashion, J. & Bassiouni, M. (2011). Protocol for mitigating the risk of hijacking social networking sites. Teoksessa *Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2011)* (s. 3244–2331). IEEE.

Chu, Z., Gianvecchio, S. Wang, H. & Jajodia, S. (2012). Detecting automation of Twitter accounts: Are you a human, bot or cyborg?. *IEEE Transactions on Debendable and Secure Computing, 9(6),* 8114–2824.

De Paula, A. (2010). Security aspects and future trends of social networks. *The International Journal of Forensic Computer Science, 2010(1),* 604–279.

Devmane, M. & Rana, N. (2014). Detection and prevention of profile cloning in online social networks. Teoksessa *Proceedings of 2014 Recent Advances and Innovations in Engineering (ICRAIE 2014)* (s. 10594–21063). IEEE.

DuPaul, N. (2014). Man in the middle (MITM) attack. Haettu 6.12.2014 osoitteesta http://www.veracode.com/security/man-middle-attack

Erlandsson, F., Boldt, M. & Johnson, H. (2012). Privacy threats related to user profiling in online social networks. Teoksissa *Proceedings of 2012 International Conference on Privacy, Security, Risk and Trust (PASSAT)* ja *Proceedings of 2012 International Conference on Social Computing (SocialCom)* (s. 8384–2842).

Euroopan komissio. (2012). *Study for an impact assessment on a proposal for a new legal framework on identity theft.* Centre for Strategy & Evaluation Services.

Euroopan unioni. (2013). Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU. Haettu 3.2.2015 osoitteesta http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32013L0040&from=FI

Facebook. (2015a). Tietoja lainvalvontaviranomaisille. Haettu 5.4.2015 osoitteesta https://fi-fi.facebook.com/safety/groups/law/guidelines/

Facebook. (2015b). Tietojenkäyttökäytäntö. Haettu 5.4.2015 osoitteesta https://fi-fi.facebook.com/about/privacy

Forss, M. (2014). *Fobban sosiaalisen median selviytymisopas.* Helsinki: CrimeTime.

Haddadi, H. & Hui, P. (2010). To add or not to add: Privacy and social honeypots. Teoksessa *Proceedings of 2011 IEEE International Conference on Communications Workshops (ICCW 2010)* (s. 3214–2325). IEEE.

Helsingin poliisilaitos. (2014). Identiteettivarkaudet. Haettu 5.12.2014 osoitteesta https://www.poliisi.fi/poliisi/helsinki/home.nsf/pages/4AA4B4D403026EC2C2257A7E0034F614?opendocument Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. uud. painos). Helsinki: Tammi.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2007). *Tutki ja kirjoita* (13. uud. painos). Helsinki: Tammi.

Huber, M., Mulazzani, M., & Weippl, E. (2011*). Friend-in-the-middle attacks* (Technical Report TR-SBA-Research-0710-01). SBA Research.

Huber, M., Mulazzani, M., Kitzler, G., Goluch, S. & Weippl, E. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. *EEE Internet Computing, 15(3)*, 284–234.

Jin, L., Takabi, H. & Joshi, J. (2011). Towards active detection of identity clone attacks on online social networks. Teoksessa *Proceedings of the first ACM conference on Data and application security and privacy* (s. 274–238). New York, NY: ACM.

Joshi, Y., Das, D. & Saha, S. (2009). Mitigating man in the middle attack over Secure Sockets Layer. Teoksessa *Proceedings of 2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA 2009)* (s. 188–192). Piscataway, NJ: IEEE.

Järvinen, P. & Järvinen, A. (2004 & 2011). Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Kansalaisyhteiskunnan tutkimusportaali. (2014). Sosiaalinen media. Haettu 5.12.2014 osoitteesta http://kans.jyu.fi/sanasto/sanat-kansio/sosiaalinen-media

Kaplan, A. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons, 53(1),* 59–68.

Khayyambashi, M. & Rizi, F. (2013). An approach for detecting profile cloning in online social networks. Teoksessa *Proceedings of the 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security* (s. 76–87). IEEE.

Kirves, A. (2002, 2. maaliskuuta). Social engineering: mitä se on?. Haettu 19.1.2015 osoitteesta http://www.digitoday.fi/tietoturva/2002/03/08/social-engineering-mita-se-on/20029075/66

Kontaxis, G., Polakis, I., Ioannidis, S. & Markatos, E. (2011). Detecting social network profile cloning. Teoksessa *Proceedings of 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops 2011)* (s. 295–300). IEEE.

Laki esitutkintalain muuttamisesta 818/2014. (2014). Valtion säädöstietopankki Finlex. Haettu 5.4.2015 osoitteesta http://www.finlex.fi/fi/laki/alkup/2014/20140818

Laki kansainvälisestä oikeusavusta rikosasioissa 5.1.1994/4. (1994). Valtion säädöstietopankki Finlex. Haettu 5.4.2015 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1994/19940004

Laki poliisilain muuttamisesta 525/2005. (2005). Valtion säädöstietopankki Finlex. Haettu 5.4.2015 osoitteesta http://www.finlex.fi/fi/laki/alkup/2005/20050525

Laki rikoslain muuttamisesta 879/2013. (2013). Valtion säädöstietopankki Finlex. Haettu 5.4.2015 osoitteesta http://www.finlex.fi/fi/laki/alkup/2013/20130879

Lawler, J. & Molluzzo, J. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the Internet. *Journal of Information Systems Applied Research 3(12)* 1–18.

Lin, P.C. & Huang, P.M. (2013). A study of effective features for detecting long-surviving Twitter spam accounts. Teoksessa *Proceedings of 2013 15th International Conference on Advanced Communications Technology (ICACT 2013)* (s. 841–846). IEEE.

Mahmood, S. (2012). New privacy threats for Facebook and Twitter users. Teoksessa *2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)* (s. 164–169). Washington, DC: IEEE Computer Society.

Mahmood, S. & Desmedt, Y. (2012). Your Facebook activated friend or cloaked spy. Teoksessa *Proceedings of 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops 2012)* (s. 367–373). IEEE.

Mitnick, K. & Simon, W. (2002). The art of deception: Controlling the human element of security. Indianapolis: Wiley Publishing.

Mouton, F., Malan, M., Leenen, L. & Venter, H. (2014). Social engineering attack framework. Teoksessa *Proceedings of 2014 Conference on Information for South Africa* (s. 170–178).

Oikeusministeriö. (2014, 13. marraskuuta). Tietoverkkorikoksia koskeviin säännöksiin muutoksia – Identiteettivarkaus rangaistavaksi itsenäisenä rikoksena. Haettu 3.12.2014 osoitteesta http://oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2014/11/tietoverkkorikoksiakoskeviinsaannoksiinmuutoksia-identiteettivarkausrangaistavaksiitsenaisenarikoksena.html

Okuno, T., Ichino, M., Kuboyama, T. & Yoshiura, H. (2011). Content-based de-anonymization of tweets. Teoksessa *Proceedings of 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2011)* (s. 53–56). Washington, DC: IEEE Computer Society.

Peng, W., Li, F., Zou, X. & Wu, J. (2012). Seed and grow: An attack against anonymized social networks. Haettu 24.1.2015 osoitteesta http://cs.iupui.edu/~pengw/doc/pub/peng2012seed-n-grow-slides.pdf

Peng, W., Li, F., Zou, X. & Wu, J. (2014). A two-stage deanonymization attack against anonymized social networks. *IEEE Transactions on computers, 63(2),* 290–301.

Poliisi. (2015). Poliisit sosiaalisessa mediassa. Haettu 4.4.2015 osoitteesta https://www.poliisi.fi/tietoa_poliisista/poliisit_sosiaalisessa_mediassa

Rizi, F., Khayyambashi, M. & Kharaji, M. (2014). A new approach for finding cloned profiles in online social networks. *International Journal of Network Security, 2014(6)*, 25–37.

Sanzgiri, A., Hughes, A. & Upadhyaya, S. (2013). Analysis of malware propagation in Twitter. Teoksessa *IEEE 32nd International Symposium on Reliable Distributed Systems (SRDS)* (s. 195–204). Washington, DC: IEEE Computer Society.

Sharma, M., Mishra, N. & Sharma, S. (2013). Prevention of traffic analysis attack in friend in the middle using dummy traffic approach. Teoksessa *Proceedings of 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC 2013)* (s. 62–69). IEEE.

Sisäasiainministeriö. (2010). Sisäministeriön julkaisu 32/2010: Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Haettu 5.12.2014 osoitteesta http://www.intermin.fi/julkaisu/322010?docID=24918

Sivanesh, S., Kavin, K. & Hassan, A.A. (2013). Frustrate Twitter from automation: How far a user can be trusted?. Teoksessa *Proceedings of 2013 International Conference on Human Computer Interactions (ICHCI 2013)* (s. 97–101). IEEE.

Valtioneuvosto. (2014). HE 232/2014: Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muutamisesta ja eräiksi siihen liittyviksi laeiksi. Haettu 3.2.2015 osoitteesta https://www.finlex.fi/fi/esitykset/he/2014/20140232.pdf

Watters, P.A (2009). Why do users trust the wrong messages? A behavioural model of phishing. Teoksessa *Proceedings of the 4th annual Anti-Phishing Working Groups eCrime Researchers Summit* (s. 1–7). IEEE.

Wondracek, G., Holz, T., Kirda, E. & Kruegel, C. (2010). A practical attack to de-anonymize social network users. Teoksessa *Proceedings of 2010 IEEE Symposium on Security and Privacy (SP 2010)* (s. 223–238). Washington, DC: IEEE Computer Society.

LIITE 1 TAPAUKSEN 2 AINEISTO

ESS: Jörn Donnerin Twitter-tili on huijausta

Jörn Donnerin useissa medioissa siteerattu Twitter-tili ei ole Donnerin, kertoo Etelä-Suomen Sanomat. Lehden mukaan tilin twiittejä on julkaistu lehdistössä siellä täällä.

Donner-tuntijoiden mukaan on näyttänyt siltä, että tviitit ovat heikkoja Donner-mukaelmia. Donner on vahvistanut epäilyn Etelä-Suomen Sanomille.

"En ole koskaan kuullutkaan tällaisesta Twitteristä", hän sanoo lehdelle.

Twitter-tilin voi perustaa kuka tahansa, ja monella julkisuuden henkilöillä on tekaistuja tilejä. Joidenkin tunnettujen henkilöiden tilin aitous on varmistettu, mutta Donnerin tilillä varmennetta ei ole.

Donnerin nimissä olevan tilin motto on "Elämä on suurta parodiaa, kuten myös tämä".

Helsingin Sanomat julkaisi sunnuntaisivullaan viikon twiittinä yhden kyseisen tilin julkaisuista.

Keskiviikkona tilille oli ilmestynyt seuraava viesti: "Oikea Jörn. Väärä Jörn. Yhtä ja samaa. Jos oikea on oikeampi ja näin haluaa, ojennamme tämän tilin hänelle mielellään ja veloituksetta."

Tili on perustettu 7. helmikuuta. Sillä on ollut yli 2 000 seuraajaa, ja ”Donnerin” tviittejä on kommentoinut muun muassa ministeri Alexander Stubb (kok).

Lähde: Helsingin Sanomat. (2013, 13. maaliskuuta). ESS: Jörn Donnerin Twitter-tili on huijausta. Haettu 22.2.2015 osoitteesta
http://www.hs.fi/kulttuuri/a1363142933112

Jörn Donner teki Twitter-huijarista tutkintapyynnön

Jörn Donner on tehnyt asianajajansa välityksellä poliisille tutkintapyynnön kummallisesta Twitter-tilistä.

Joku tai jokin ryhmittymä aloitti Finlandia-palkitun kulttuuripersoonan nimissä yhteisöpalvelu twitterin jo reilu vuosi sitten.

Vasta viime perjantaina Jörn Donner, 80, reagoi ja otti yhteyttä asianajajaan, joka on nyt tehnyt poliisille tutkintapyynnön.

– Itse en ole edes käynyt twitterissä, en edes katsomassa, mitä nimissäni sinne on kirjoitettu.

Donner on närkästynyt siitä, että hänen henkilöllisyytensä on varastettu.

– Ihmisten henkilöllisyyttä ei noin vain voi viedä. Monet - jopa Alexander Stubb - ovat luulleet, että siellä kirjoittelen minä.

Donnerin asianajaja Antti Hemmon mukaan tutkintapyynnön syynä on kunnianloukkaus ja yksityiselämää loukkaavan tiedon levittäminen.

"Ei ole väärää Donneria"

Donnerin nimissä on twiitattu ahkerasti. Reilussa vuodessa hän tai ryhmä "henkilöllisyyden varastajia" on kirjoittanut lähes 200 twiittiä. Seuraajia vale-Donner on saanut jo yli 2000.

Twiittejä tupsahteli vielä maanantaina tihenevään tahtiin. Mysteerikirjoittaja on muuttanut Donnerin Twitter-profiiliin julkisen kuvauksen, jossa myönnetään, että tekaistu tili on "suurta parodiaa". Aikaisemmin Twitter-tililtä ei käynyt ilmi, että kyseessä olisi Donnerina esiintyvä henkilö eikä Donner itse.

Twiittaaja tai useat twiittaajat kritisoivat maanantain aikana myös useassa twiitissä oikean Donnerin tekemää tutkintapyyntöä.

– Harkitsemme tutkintapyyntöä Mr Jörn Donnerin tutkintapyynnöstä. Se on aiheeton ja perätön. Sillä ei ole menestymisen edellytyksiä.

– Seuraajani ovat pelästyneet "oikean" Jörn Donnerin ilman menestymisen mahdollisuuksia tekemästä tutkintapyynnöstä. Pakenevatko he Siperiaan? tilillä kirjoitetaan.

Maantai-iltana Twitteri-huijarin kelkka kuitenkin kääntyi. Donnerin kuva vaihtui piirrosmammuttiin, ja profiilinimi Jörn Donnerista Jorn Donneriksi.

– Me kunnioitamme Jörn Donneria. Tarkoituksemme ei ole aiheuttaa pahaa mieltä. Korjaamme nyt tilin nimi- ja kuvatiedot vastaamaan tunnusta, tilinhaltija kirjoitti iltakymmenen jälkeen.

Lähde: Seppälä, A. (2013, 25. maaliskuuta). Jörn Donner teki Twitter-huijarista tutkintapyynnön. Haettu 22.2.2015 osoitteesta
http://www.iltalehti.fi/uutiset/2013032516828848_uu.shtml

Jörn Donnerin Twitter-valetilin tutkinta lopetetaan

Jörn Donnerin nimissä tehtyä väärää Twitter-tiliä seurasi noin 2 000 ihmistä.

Jörn Donnerin nimissä tehdyn väärän Twitter-tilijutun esitutkinta lopetetaan. Poliisi perustelee tutkinnan lopettamista kustannussyillä. Tutkinnanjohtajan mukaan kulut ovat selvässä epäsuhteessa tutkittavan asian laatuun ja siitä mahdollisesti tulevaan rangaistukseen.

Asiassa pitäisi muun muassa tehdä oikeusapupyyntö Yhdysvaltoihin, koska viestit oli kirjoitettu yhdysvaltalaisella sivustolla. Poliisin arvion mukaan edes perusteellinen esitutkinta ei takaisi sitä, että joku joutuisi jutussa rikosoikeudelliseen vastuuseen.

Myöskään tärkeä yleinen tai yksityinen etu ei vaadi syytteen nostamista.

Tuntematon ihminen perusti Jörn Donnerin nimissä Twitter-tilin ja kirjoitti sinne noin 170 viestiä. Valetilin viestejä ehdittiin siteerata melko laajasti.

Päätöksen esitutkinnan lopettamisesta teki syyttäjä.

Lähde: Salokorpi, J. (2013, 16. toukokuuta). Jörn Donnerin Twitter-valetilin tutkinta lopetetaan. Haettu 22.2.2015 osoitteesta
http://yle.fi/uutiset/jorn_donnerin_twitter-valetilin_tutkinta_lopetetaan/6644275

LIITE 2 TAPAUKSEN 4 AINEISTO

Jutta Antikaisen Facebook-päivitys (17.12.2013)

”Törmäsin netissä mukavaan naiseen, jonka kanssa pidimme yhteyttä web-kameran välityksellä. Pidimme kevyttä kivaa, jossa näkyi paljasta pintaa. Tyyppi tuntui luotettavalta ja hyväksyin hänet Facebook-kaverikseni. Tämän jälkeen hän kertoi tallentaneensa videon ja se oli jo julkaistu YouTubessa. Minun pitää maksaa huomiseen mennessä 800 euroa tai hän jakaa videon kaikille FB-kavereilleni ja julkaisee sen uudelleen. Mitä teen, että video ei leviä nettiin?”

Ensisijainen ohjeistukseni on, että ÄLÄ MAKSA ja ole yhteydessä poliisiin. Rikosnimikkeet aikuisen henkilön ollessa asianomistajana olisivat perusmuodoissaan kiristys ja kunnianloukkaus. 16-17 -vuotiaan asianomistajan kohdalla lisäksi sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen.

Tämänkaltaisia yhteydenottoja on tullut minulle muutamia ja toimintatapa on ollut sama. Kontakti on syntynyt anonyymissa chatissa, mistä tekijä on pyytänyt siirtymään skypeen. Skype-yhteyden pätkimisen tai jonkun muun syyn verukkeella on siirrytty Facebookiin, minkä kautta tekijä on saanut tietoonsa kaverit, sukulaiset, työpaikat jne. Tämän jälkeen asianomistajalle on lähetetty YouTube-linkki jo julkaistusta videomateriaalista ja pyydetään maksamaan X euroa pikaisella aikataululla tai materiaali leviää.

Tekotapa vaikuttaa varsin ammattimaiselta ja nopealla tsekkauksella erään jutun osalta löysin tekijältä eri palveluista kymmeniä samanlaisia videoita.
Nettipoliisilta kysytään usein, että mitkä ovat uusimpia ilmiöitä sosiaalisessa mediassa. Olisiko tämä nyt sitten yksi niistä?

Lähde: Antikainen, J. (2013, 17. joulukuuta). Haettu 22.2.2015 osoitteesta
https://www.facebook.com/jutta.antikainen/posts/796930540324543

Poliisi varoittaa: Uusi seksikiristyshuijaus leviää Suomessa

Poliisi kertoo Facebookissa uudesta huolestuttavasta someilmiöstä, jossa kiristetään rahaa seksichatin julkaisulla uhaten.

Nettipoliisi Jutta Antikainen kertoo Facebookissa uudesta ilmiöstä, jossa huijataan pahaa-aavistamattomat käyttäjät noloon tilanteeseen, ja heiltä kiristetään suuria summia.

Toiminnassa käytetään hyväksi verkon keskustelupalstoja, Skypeä ja Facebookia. Ensin uhrin kanssa avataan keskustelu chatissa, jonka jälkeen siirrytään Skypeen eroottiseen videokeskusteluun.

Kun paljasta pintaa on näkynyt tarpeeksi, siirretään viestintä Facebookin puolelle. Tekosyynä käytetään Skype-yhteyden pätkimistä tai muuta vastaavaa veruketta.

Facebookista kerätään tietoa uhrin perheestä, ystävistä ja työnantajasta. Tämän jälkeen lähetetään linkki Youtube-videoon, joka sisältää kaiken aiemmin kuvatun materiaalin. Samalla uhataan, että jos uhri ei maksa pikaisella aikataululla kiristäjän vaatimaa summaa, materiaali leviää.

Kymmeniä samankaltaisia videoita.

Antikainen kertoo, että yhteydenottoja on tullut muutama, ja toimintatapa on aina sama. Tekotapaa Antikainen kommentoi ammattimaiseksi.

Poliisi kertoo, että yksittäisessä tutkitussa tapauksessa on löytynyt samalta kiristäjältä jopa kymmeniä samankaltaisia videoita.

Lähde: Ilta-Sanomat. (2013, 17. joulukuuta). Poliisi varoittaa: Uusi seksikiristyshuijaus leviää Suomessa. Haettu 22.2.2015 osoitteesta
http://www.iltasanomat.fi/digi/art-1288633408238.html