Sosiaalisen manipuloinnin menetelmät tietoturvahyökkäyksissä

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Kesäkuu 2026
Vilho Saarinen

TURUN YLIOPISTO
Tietotekniikan laitos

Vilho Saarinen: Sosiaalisen manipuloinnin menetelmät tietoturvahyökkäyksissä

LuK-tutkielma, 26 s.
Tietojenkäsittelytiede
Kesäkuu 2026

Sosiaalinen manipulointi on yksi keskeisimmistä haasteista tietoturvallisuudessa. Ihminen on usein heikoin lenkki vahvoja teknologisia suojauskeinoja hyödyntävissä tietojärjestelmissä. Hyökkääjät käyttävät tätä heikkoutta hyväkseen erilaisilla psykologisilla manipulaatiokeinoilla ja huijauksilla. Kuka tahansa taustastaan riippumatta voi joutua tällaisen hyökkäyksen kohteeksi ja oikein kohdistettuna ne voivat aiheuttaa jopa miljoonien eurojen edestä vahinkoa. Koska kaikki ihmiset ovat potentiaalisia kohteita, on tärkeää tunnistaa mitkä tekijät lisäävät hyökkäysten onnistumisen todennäköisyyttä.

Tutkielma on toteutettu kirjallisuuskatsauksena ja sen tarkoituksena on selvittää millaisia sosiaalista manipulaatiota hyödyntäviä hyökkäyksiä on olemassa ja mitä ihmisten psykologisia ominaisuuksia niissä hyödynnetään. Tämän lisäksi tutkitaan mitä suojauskeinoja yrityksillä on käytössään, sekä arvioidaan niiden tehokkuutta ja mahdollisia rajoitteita.

Tutkimuksen perusteella sosiaalisessa manipuloinnissa hyödynnetään usein suostuttelun periaatteita, sekä kohteen tunnetiloja. Erityisen altistava tekijä on heikko asenne tietoturvallisuutta kohtaan. Pelkkä koulutus ja tietoisuus sosiaalisen manipulaation uhasta ei merkittävästi auta suojautumaan siltä, vaan tarvitaan myös vahva minäpystyvyyden tunne, eli kokemus omasta kyvykkyydestään selvitä hyökkäystilanteista.

Asiasanat: Sosiaalinen manipulointi, kyberturvallisuus, phishing, huijaukset, petos, tietoturva suojauskeinot, psykologiset tekijät

Sisällys

1 Johdanto

Ihmistä pidetään yleisesti tietoturvan heikoimpana lenkkinä. Teknisesti hienostuneinkin järjestelmä on altis sille, että sen ihmiskäyttäjät toimivat huolimattomasti ja mahdollistavat näin useat erilaiset hyökkäykset. Nämä käyttäjiin kohdistuvat hyökkäykset hyödyntävät usein ihmispsykologian tuntemusta pelkän teknologisen osaamisen sijaan. Niitä voidaan kuitenkin yhtä lailla hyödyntää sähköisiin tietojärjestelmiin murtautumisessa. [1]–[5]

Englannin kielessä näistä tietojärjestelmän käyttäjiin kohdistettavista hyökkäyksistä käytetään vakiintunutta termiä ”social engineering”. Suomen kielessä ei ole yhtälailla vakiintunutta termiä, mutta samaan konseptiin voidaan viitata esimerkiksi termeillä ”käyttäjän manipulointi” tai ”sosiaalinen manipulointi”. Tässä tutkielmassa käytetään termiä sosiaalinen manipulointi viittaamaan samaan käsitteeseen kuin englanniksi tehtäisiin termillä social engineering.

Tutkielmassa sosiaalisella manipulaatiolla viitataan psykologisia menetelmiä hyödyntäviin hyökkäyksiin, joissa hyökkääjä pyrkii saamaan kohteeltaan arvokasta tietoa, kuten käyttäjätunnuksia, henkilötietoja tai muuta informaatiota, jota hyökkääjä voi hyödyntää tulevissa tietoturvahyökkäyksissä kohdetta vastaan. Tieto viedään joko kohteen ymmärtämättä, tai uhri huijataan paljastamaan sen hyökkääjälle vapaaehtoisesti. [1], [4]–[7]

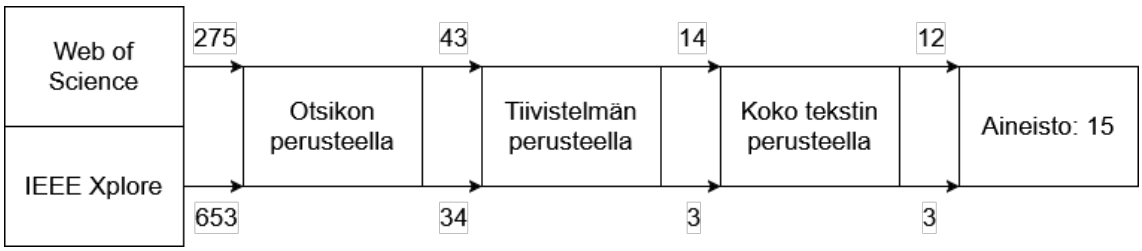
Tutkielman tarkoituksena on selvittää, millaisia eri sosiaalista manipulaatiota hyödyntäviä tietoturvahyökkäyksiä on olemassa ja mihin psykologisiin tekijöihin näi-

den hyökkäysten tehokkuus perustuu. Tämän lisäksi pyritään selvittämään millaisia keinoja yritykset voivat hyödyntää minimoidakseen sosiaalisesta manipulaatiosta aiheutuvan riskin. Aineiston perusteella pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

TK1: Miksi sosiaalisen manipulaation menetelmät ovat niin tehokkaita tietoturvahyökkäyksissä?

TK2: Miten yritykset voivat pyrkiä suojautumaan sosiaaliselta manipuloinnilta?

Tutkielma on toteutettu kirjallisuuskatsauksena. Hakutietokannoiksi valikoituivat Web of Science ja IEEE Xplore. Molempiin tietokantoihin hyödynnettiin hakulauseketta *social engineering AND (cyber* OR "information security") AND ("defen?e" OR protect*)*. Lausekkeella pyrittiin rajaamaan tuloksia jotka käsittelevät nimenomaan sosiaalista manipulaatiota tietoturvakontekstissa ja ottavat myös kantaa hyökkäyksiltä suojautumiseen. Tiedonhakuprosessi on esitetty kaaviossa 1.1.



Kaavio 1.1: Tutkielman tiedonhakuprosessi

Web of Science -tietokannasta hakutuloksia oli yhteensä 275, joista valittiin otsikon perusteella tarkasteluun 43. Valinnassa pyrittiin ottamaan mukaan artikkeleita, joissa pääpaino oli nimenomaan sosiaalisessa manipuloinnissa tai psykologian vaikutuksessa tietoturvallisuudessa. Tiivistelmän perusteella tarkempaan käsittelyyn valittiin 14. Valinnassa painotettiin artikkeleita, joissa oli tietoa sosiaalisen manipuloinnin menetelmistä, suojautumiskeinoista tai taustalla vaikuttavista psykologisista tekijöistä. Valinnasta karsittiin pois yli kymmenen vuotta vanhat artikkelit. Koko tekstin perusteella artikkeleista valikoitui mukaan 12. Pois jäävistä artikkeleista toi-

sessa oli rikkinäinen linkki ja toinen ei ollut tutkimuskysymysten kannalta hyödyllinen. IEEE Xploresta löytyi alkuun 653 lähdettä. Yllä mainittujen valintakriteerien mukaisesti näistä valittiin tutkittavaksi otsikon perusteella 27 artikkelia. Tiivistelmän perusteella valittiin kolme, jotka kaikki valittiin myös koko tekstin perusteella tutkielmaan.

Tutkielman toisessa luvussa käydään läpi taustatietoja sosiaalisesta manipuloinnista, sekä esitellään esimerkkejä aiemmin suoritetuista hyökkäyksistä ja niiden aiheuttamasta vahingosta. Luvussa kolme käydään aineistoon pohjautuen läpi millaisiin tyyppeihin sosiaalista manipulaatiota hyödyntävät hyökkäykset voidaan jakaa, millaisia psykologisia periaatteita niiden toteutuksessa voidaan hyödyntää, sekä esitellään mahdollisia puolustautumiskeinoja sosiaalista manipulaatiota vastaan ja arvioidaan niiden tehokkuutta. Luvussa neljä käydään läpi pohdintaa liittyen aineistoon ja löytöihin. Luvussa viisi esitellään yhteenveto tutkielman löydöistä.

2 Taustaa

2.1 Sosiaalinen manipulointi

Sosiaalisella manipuloinnilla ei ole täysin yksiselitteistä määritelmää. Laajimmillaan sen voidaan ajatella tarkoittavan kaikkea sellaista psykologiaa hyödyntävää toimintaa, jolla pyritään vaikuttamaan kohteen päätöksentekoon ja toimintaan, jotta saadaan tämä toimimaan omaa etuaan vastaan [6], [8]–[10]. Käsitettä käytetään yleensä modernin tietoturvallisuuden yhteydessä, mutta erilaisia huijauksia ja muuta salakavalaa toimintaa on hyödynnetty läpi ihmiskunnan historian [1]. Tietoturvakontekstissa sosiaalisella manipuloinnilla tarkoitetaan usein nimenomaan sellaisia psykologisia hyökkäyksiä, joissa kohde saadaan tajuamattaan tai vapaaehtoisesti paljastamaan arvokkaita tietoja, kuten käyttäjätunnuksia tai henkilötietoja Hyökkäykset voidaan toteuttaa sekä verkon välityksellä että paikan päällä. [1], [4], [5], [7]. Koska hyökkäykset eivät välttämättä ole aina sähköisiä, on mielekkäämpää puhua niistä tietoturvauhkana kyberuhan sijaan.

Sosiaalista manipulaatiota hyödyntävät hyökkäykset ovat tietoturva-alalla yleinen ja tunnettu ongelma, joiden uhriksi voi joutua kuka tahansa. Tästä syystä onkin olemassa paljon ohjeita siihen, miten hyökkäyksiin voi varautua. Esimerkiksi tietoturva yhtiö F-Secure kannustaa varovaiseen toimintaan. Ei kannata klikata epäilyttäviä linkkejä eikä ladata tuntemattomia tiedostoja. Samoin on järkevää varmistaa toisen henkilön henkilöllisyys ennen kuin luovuttaa tietojaan ja tällöinkään ei tu-

le antaa esimerkiksi kirjautumistietoja. Tuntemattomia muistitikkuja tai vastaavia laitteita ei pidä yhdistää koneeseensa. Yhtiö suosittelee myös tietoturvaohjelmien sekä erityisesti julkisissa verkoissa VPN-ohjelmien käyttöä. [11]

Myös Suomen poliisilla on ohjeistus sosiaaliselta manipulaatiolta suojautumiseen. Poliisi ei käytä termiä sosiaalinen manipulointi, mutta suuri osa siihen kuuluvista menetelmistä lasketaan petosrikoksiksi. Poliisi kehottaa ihmisiä varomaan tarjouksia jotka kuulostavat kohtuuttoman hyviltä ja pohtimaan todellisia motiiveja niiden takana. Erityisesti kannattaa varoa mikäli joku lupaa lähes ilmaista rahaa, tai kertoo sinun voittaneen kilpailussa mihin et koskaan osallistunut. Epäilyttäviin viesteihin ei yleisesti kannata vastata ja etenkään tilinumeroita tai passitietoja ei tule ikinä luovuttaa tuntemattomille. Mikäli epäilee joutuneensa petoksen uhriksi Poliisi kehottaa tekemään rikosilmoituksen ja olemaan tarvittaessa yhteydessä pankkiinsa. Mahdollisuus tekijöiden kiinnisaamiseen voi olla joissain tapauksissa kuitenkin pieni. [12]

2.2 Suostuttelun periaatteet

Sosiaalista manipulaatiota hyödyntäviä hyökkäyksiä on pyritty tutkimaan useamman olemassa olevan näkökulman kautta, joista yksi on ”Suostuttelun periaatteet”-malli (engl. Principles of Persuasion). [2], [10] Mallin on kehittänyt yhdysvaltalainen psykologi Robert Cialdini [13] ja siihen kuuluu kuusi periaatetta, jotka on alunperin tarkoitettu kuvaamaan markkinoinnissa käytettäviä psykologisia keinoja, joita hyödyntämällä mainonnan yleisöstä tulisi mahdollisimman todennäköisesti maksavia asiakkaita. Nämä periaatteet ovat hyödyllisiä myös sosiaalista manipulaatiota tutkittaessa [2], [10]. Periaatteet esitellään seuraavissa kappaleissa.

Pitäminen (engl. liking) viittaa siihen, että ihmiset ovat tyypillisesti halukkaampia olemaan tekemisissä toisen kanssa, jos tämä on kohtelias, avulias ja ystävällinen. Samoin auttaa, jos toisella vaikuttaa olevan samoja mielipiteitä tai hän

kuuluu samaan ryhmään. [13] Niin markkinoinnissa kuin sosiaalisessa manipuloinnissakin tämä mukavuuden ja samankaltaisuuden tunne voi olla tietoisesti luotu illuusio. [2], [10]

Vastavuoroisuus (engl. reciprocity) viittaa siihen, että henkilö haluaa todennäköisesti tehdä vastapalveluksen, jos hän kokee, että hänen vuokseen on tehty jotain. Markkinnoinnissa tämä näkyy esimerkiksi siinä, että ihmiset saattavat ostaa ennemmin tuotetta, jota saivat kokeilla ilmaiseksi kilpailevien tuotteiden sijaan. [13] Tietojenkalastelussa periaatetta voidaan hyödyntää esimerkiksi laatimalla viesti, jossa esitetään, että kohteen eteen on tehty jotain ja hänen täytyy tehdä vain jokin pieni palvelus vastineeksi. Tämä näennäisesti pieni palvelus voi olla esimerkiksi jonkin tiedon antaminen. [2], [6], [10]

Muiden esimerkki (engl. social proof) viittaa siihen, että ihmiset haluavat yleensä kuulua joukkoon ja toimia samalla tavalla kuin muutkin. Ihmiset ovat myös valmiimpia ottamaan riskejä, jos vaikuttaa että monet muut ovat jo ottaneet saman riskin. [13] Sosiaalista manipulaation näkökulmasta tätä voidaan hyödyntää esimerkiksi esittämällä, että monet ovat lähteneet mukaan johonkin projektiin tai sijoitusmahdollisuuteen, joka on todellisuudessa huijaus.

Johdonmukaisuus (engl. consistency) viittaa siihen, että henkilö todennäköisesti tekee asioita samantapaisesti kuin on ennenkin tehnyt, tai kuten on luvannut tehdä. [13] Tätä hyödynnetään esimerkiksi Watering hole-hyökkäyksissä. Jos saadaan tunnistettua sivu, jota henkilö on käyttänyt usein voidaan olettaa, että hän käy siellä jatkossakin. [2], [5], [10]

Niukkuus (engl. scarcity) viittaa siihen, että tyypillisesti ihmiset antavat enemmän arvoa asioille, joita on rajatusti, tai joita on saatavilla vain rajoitetun aikaa. [13] Tietojenkalastelussa tätä pyritään usein hyödyntämään esimerkiksi huijausmainoksissa. Kohteella ei ole aikaa jäädä pohtimaan onko kyseessä aito mainos vai ei, sillä tarjous loppuu pian. [2], [10]

Auktoriteetti (engl. authority) viittaa siihen, että ihmiset noudattavat useammin ohjeistusta, jos se tulee lähteeltä joka koetaan luotettavaksi. Tämä voi olla virkavalta, valtion virallinen viestintä tai vain joku kohteen läheinen. [13] Tätä on hyödynnetty huijauksissa, joissa huijarit esittävät viestitse esimerkiksi poliisia ja käskevät kohdetta antamaan heille pankkitietonsa. [2], [10]

2.3 Esimerkkejä sosiaalista manipulaatiota hyödyntäneistä hyökkäyksistä

Sosiaalista manipulaatiota on hyödynnetty lukuisissa eri hyökkäyksissä, usein yhdessä teknisten hyökkäyskeinojen kanssa. Osan tällaisista hyökkäyksistä aiheuttama vahinko voidaan laskea miljoonissa euroissa.

Vuonna 2014 amerikkalainen sairausvakuutus yhtiö Anthem (nykyiseltä nimeltään Elevance) joutui suuren tietomurron kohteeksi. Tietomurron yhteydessä hyökkääjät saivat varastettua lähes 80 miljoonan asiakkaan terveystiedot. Yhdysvaltain oikeusministeriön arvion mukaan hyökkäyksen takana saattoi olla kiinalainen hakkeriryhmä. Hakkerit saivat pääsyn tietokantaan kohdennetulla tietojenkalasteluhyökkäyksellä. Anthemin työntekijöille lähetettiin sähköposti, jossa olevaa linkkiä klikkaamalla työntekijä antoi tietämättään pääsyn koneeseensa ja järjestelmänvalvojan tunnuksiinsa. Tietomurrossa varastettujen tietojen joukossa oli muun muassa vakuutustietoja, sosiaaliturvatunnuksia, syntymäaikoja, koti- ja sähköpostiosoitteita sekä työllisyystietoja. Vuonna 2017 Anthem joutui maksamaan sovintona 115 miljoonaa dollaria uhrien suojelemiseksi identiteettivarkaudelta. [14]

Maailmanlaajuisesti eniten vahinkoa aiheuttaneena kyberhyökkäyksenä pidetään usein vuonna 2017 iskenyttä NotPetya-haittaohjelmaa. Hyökkäys lähti liikkeelle Ukrainasta, jossa virus alkoi erittäin nopealla tahdilla leviämään koneelta koneelle, tuhoten samalla kaikki laitteelta löytyvät tiedot. Viruksen takana on arvioitu ole-

van venäläinen hakkeriryhmä Sandworm ja hyökkäyksen uskotaan liittyneen vuonna 2014 alkaneeseen Ukrainan ja Venäjän väliseen konfliktiin Krimin alueella. Virus alkoi lopulta levitä itsenäisesti, mutta hyökkäyksen käynnistyksessä hyödynnettiin sosiaalista manipulaatiota. Niin kutsutussa Watering hole-hyökkäyksessä hakkerit ensin hyödynsivät haavoittuvuutta M.E.Doc-ohjelmassa, jotta saivat lisättyä NotPetya-viruksen siihen. Tunnetusti lähes kaikki ukrainalaiset yritykset käyttivät M.E.Docia veroasioiden käsittelyyn, joten oli vain ajan kysymys että virus leviäisi ohjelman mukana yritysten koneille. Hyökkäys ei rajoittunut vain Ukrainaan, vaan levisi ympäri maailmaa tuhoten koneiden tiedot mennessään. Maailmanlaajuisesti hyökkäyksen uskotaan tehneen jopa 10 miljardia dollaria vahinkoa. [15]

Suuria tappioita voi aiheuttaa myös vähemmän teknisesti hienostuneilla hyökkäyksillä. Vuonna 2019 Toyotan ajoneuvokomponentteja valmistava osa Toyota Boshoku huijattiin lähettämään 4 miljardia jeniä eli noin 37 miljoonaa dollaria väärään osoitteeseen. Ennen hyökkäystä hakkerit olivat käyttäneet aikaa tunnistaakseen yhtiön luotettavia kauppakumppaneita. Yhden näistä nimissä Toyota Boshokun talous- ja kirjanpito-osaston työntekijöille lähetettiin täysin aidonnäköinen sähköposti, jossa kehotettiin välittämään rahasumma annetulle pankkitilille. [16]

Samantapaisen hyökkäyksen kohteeksi joutui myös Las Vegasissa sijaitseva kasinohotelli MGM Vuonna 2023. Hakkeriryhmät Scattered Spider ja ALPHV selasivat MGM:n työntekijöitä LinkedIn-verkostoitumispalvelussa, etsien sopivaa henkilöä jota impersonoida. Sopivan henkilön löydyttyä hakkerit soittivat kasinon työntekijöiden IT-tukeen ja onnistuivat suostuttelemaan tukihenkilön luovuttamaan heille kirjautumistunnukset. Tunnusten avulla hakkerit pääsivät käsiksi kasinon järjestelmiin ja lamauttivat ne lunnasohjelmalla (engl. ransomware). Kasinon rahapelikoneet, hotellin sähköiset avainkortit, hotellin ja ravintolan varauspalvelut, sekä sähköpostijärjestelmät olivat kaikki useamman päivän poissa toiminnasta. MGM noudatti yleistä

ohjeistusta olla maksamatta lunnaita, mutta koki silti lähes 100 miljoonan dollarin tappiot, sekä merkittävää mainehaittaa. [17]

Sosiaalisen manipulaation vaara ei rajoitu pelkästään suurin yrityksiin, vaan on jatkuva uhka yksittäisillekin ihmisille myös Suomessa. Esimerkiksi YLE uutisoi vuonna 2025 satojen tuhansien huijaustekstiviestien aallosta, joissa on esimerkiksi esitetty verottajaa tai vastaanottajan lasta. Viestien tarkoituksena on ollut kaapata uhrin pankkitunnukset tai huijata heidät lähettämään rahaa. [18]

3 Sosiaalisen manipuloinnin menetelmät tutkimusaineistossa

3.1 Tutkimuksen aineisto

Tässä luvussa esitellään kirjallisuuskatsauksen tulokset. Tutkimusta varten kerätty aineiston on esitetty taulukossa 3.1. Se on jaettu neljään pääteemaan, jotka ovat hyökkäystyyppien luokittelu (HT1), hyökkäystyyppien psykologinen perusta (HT2), suojauskeinojen luokittelu (SK1) ja suojauskeinojen arviointi (SK2). HT1 käsitellään alaluvussa 3.2, HT2 alaluvussa 3.3, SK1 alaluvussa 3.4.1 ja Sk2 alaluvussa 3.4.2.

3.2 Hyökkäystyyppien luokittelu

Sosiaalista manipulointia hyödyntäviä tietoturvahyökkäyksiä on lukuisia, mutta ne kaikki tyypillisesti noudattavan suurin piirtein samoja vaiheita. Hyökkääjä aloittaa keräämällä taustatietoja yhdestä tai useammasta kohteestaan. Kerättyjen tietojen perusteella hyökkääjä valitsee sopivan menetelmän luodakseen luottamussuhteen kohteeseensa ja hyökkäyksen onnistuessa kohde huijataan luovuttamaan esimerkiksi kirjautumistunnukset tai arvokkaita henkilötietoja. Hyökkääjä pyrkii tämän jälkeen peittämään jälkensä ja hyödyntämään saamaansa tietoa. [1], [3], [7], [9]

Taulukon 3.1 teeman HT1 aineistojen perusteella hyökkäystyyppien kategorisointiin ei ole samalla tavalla vakiintunutta mallia. Hyökkäykset voidaan luokitella yksin-

Taulukko 3.1: Kirjallisuustaulukko

Kirjoittajat & Vuosi	HT1: Hyökkäys-tyyppien luokittelu	HT2: Hyökkäys-tyyppien psykologinen perusta	SK1: Suojaus-keinojen luokittelu	Sk2: Suojaus-keinojen arviointi
Aldawood, H. & Skinner, G. (2018) [19]			x	x
Cazares, M. et al. (2023) [20]	x	x		
Grassegger, T. (2021) [8]		x	x	
Greavu-Şerban, V. et al. (2025) [21]				x
Kamruzzaman, A. (2023) [1]	x			
Kaushalya, S. et al. (2018) [7]	x		x	
Khadka, K. et al. (2023) [6]		x		
Lee, D. (2023) [22]		x		x
Longtchi, T. et al. (2024) [2]	x	x		
Lopes, A. et al. (2022) [9]				x
Montañez, R. et al. (2020) [10]		x		x
Nowakowski, W. (2025) [3]	x			
Sámson, N. & Tick, A. (2024) [4]	x			x
Wiemken, M. et al. (2025) [23]	x	x		
Zaoui, M. et al. (2024) [5]	x		x	

kertaisesti tunnettujen manipulointimenetelmien alalajeiksi [7] tai jakaa ne yleisesti ihmis- ja ohjelmistopohjaisiin. [1], [4] Aineiston perusteella kattavin luokittelumalli on Zaoui et al. [5] esittämä Sosiaalisen manipulaation taksonomia (engl. Taxonomy of Social Engineering Attacks). Mallissa hyökkäykset luokitellaan ympäristön, lähestymistavan sekä menetelmän tai alustan (engl. medium) mukaan. Ympäristö viittaa siihen, tapahtuuko hyökkäys paikan päällä vai etäältä. Lähestymistavalla tarkoitetaan sitä, hyödynnetäänkö psykologista manipulointia vai fyysistä läheisyyttä kohteeseen. Menetelmä tai alusta viittaa niihin taktiikoihin, ohjelmistoihin tai laitteisiin joita hyökkääjä hyödyntää. [5] Seuraavissa alaluvuissa esitellään erilaisia sosiaalista manipulaatiota hyödyntäviä hyökkäysmenetelmiä Zaoui et al. [5] mallin mukaan.

3.2.1 Paikan päällä tapahtuvat hyökkäykset

Paikan päällä tapahtuvat hyökkäykset hyödyntävät lähestymistapanaan fyysistä läheisyyttä. Näiden hyökkäysten menetelmiin kuuluu fyysinen kulku tiloissa, kanssakäyminen ihmisten kanssa, tarkkailu sekä tavaroiden vieminen. [5] Vaikka näissä hyökkäyksissä ollaankin tarvittaessa tekemisissä muiden ihmisten kanssa, pääasiallisena tavoitteena on kiinnittää mahdollisimman vähän huomiota itseensä. Toisin kuin etähyökkäyksissä, jos hyökkääjän toiminta herättää epäilystä hän voi olla suoraan itse vaarassa. Hänellä täytyykin siis olla hyvät näyttelijän taidot ja tuntemus sosiaalinormeista. Valmistautumiseen kuuluu sopivan taustatarinan kehittäminen sekä mahdollisen valeasun hankkiminen. [3]

Tailgating eli luvaton seuraaminen on fyysisen maailman menetelmä, jossa hyökkääjä tunkeutuu tiloihin, joihin hänellä ei pitäisi olla pääsyä seuraamalla henkilöä, jolla on kulkuoikeudet. Hyökkääjä voi esimerkiksi väittää olevansa eksyksissä tai esittää jotain ulkopuolista henkilöä kuten lähettiä tai huoltomiestä, jolla olisi kuitenkin syytä päästä tiloihin. Menetelmässä hyödynnetään ihmisten taipuvaisuutta olla kohteliaita ja pitää ovia auki muille. [1], [5]

Shoulder surfing eli olan yli tarkkailu tarkoittaa menetelmää, jossa hyökkääjä fyysisesti katselee salaa toista henkilöä tämän syöttäessä tunnuksia, kuten PIN-koodeja tai salasanoja. Näin kerätyillä tunnuksilla hyökkääjä voi joko tunkeutua fyysisiin tiloihin tai digitaalisiin järjestelmiin. [5]

Dumpster diving eli roskien tonkiminen on menetelmä, jossa hyökkääjä käy fyysisesti läpi kohteena olevan tahon roskia tai muita materiaaleja, jotka ovat menossa hävitettäväksi. Monet eivät tajua, että näiden materiaalien joukossa voisi olla mitään arvokasta, mutta väärin hävitetyistä papereista, tallennusvälineistä tai tietokoneista voi löytyä paljonkin hyökkääjälle hyödyllistä tietoa. [3], [5]

3.2.2 Etäältä tapahtuvat hyökkäykset

Etähyökkäykset hyödyntävät lähestymistapanaan psykologista manipulointia, joka voi perustua kohteen mielenkiintoon, ahneuteen, pelkoon tai kiireen tunteeseen. Alustana hyökkäyksille voivat toimia nettisivut, sähköposti, ohjelmistot, tekstiviestit ja puhelut, eli käytännössä kaikki tavat joilla ihmiset pystyvät kommunikoimaan etäältä. Kohteen tunteisiin ja ajatteluun pyritään hienovaraisesti vaikuttamaan, jotta tämä toimisi hyökkääjän toiveiden mukaisesti. [5]

Phishing eli tietojenkalastelu on yksi yleisimmistä sosiaalisen manipulaation muodoista [23]. Tyypillinen tietojenkalasteluyritys etenee siten, että hyökkääjä lähettää kohteilleen viestin, joka on tekaistu näyttämään esimerkiksi luotettavan tahon, kuten pankin tai tunnetun yrityksen, lähettämältä. Viestissä on usein linkki aidon näköiselle kirjautumissivulle, johon kirjautuessaan huijauksen kohteeksi joutuneen henkilön tiedot kaapataan. [5], [23]

Tietojenkalastelulla on lukuisia alatyyppejä, jotka määrittyvät kohteiden ja käytettyjen alustojen mukaan. Kohdennettu tietojenkalastelu (engl. spear phishing) tarkoittaa kalastelua, joka on kohdistettu tiettyyn ryhmään tai henkilöön. [5], [20] Jos kohteena on erityisen korkean profiilin uhri voidaan puhua tietojen valastelusta (engl. whaling). Phishingillä voidaan viitata kaikkiin tietojenkalastelun muotoihin, mutta useimmiten sähköpostitse tapahtuviin hyökkäyksiin. Nimenomaan tekstiviestitse tapahtuvia hyökkäyksiä voidaan kutsua termillä smishing (SMS phishing) [5] ja puhelimessa puhuen tapahtuvia termillä vishing (voice phishing) [5], [20].

Watering hole eli vesikuoppahyökkäyksessä hyökkääjä tunnistaa jonkin nettisivun tai ohjelman, jota kohde käyttää usein. Hyökkääjä voi tartuttaa tälle nettisivulle tai ohjelmalle haittaohjelmia, jotka leviävät uhrille tämän vieraillessa sivustolla tai ladatessa uusia päivityksiä. [2], [5]

Quid pro quo eli ”jotain jostain” on menetelmä, jossa hyökkääjä tarjoaa jotain palvelua esimerkiksi arvokkaita tietoja vastaan. Hyökkääjä voi esimerkiksi esittää

IT-tukihenkilöä ja luvata auttaa uhria tämän tietokoneongelmien kanssa, kunhan vain saa tämän käyttäjätunnuksen ja salasanan. [5]

3.2.3 Hybridihyökkäykset

Hybridihyökkäyksiin lasketaan ne hyökkäykset, jotka sisältävät sekä lähi- että etävaiheita tai jotka pystyy toteuttamaan paikan päällä tai etänä. Näiden hyökkäystyyppien kategorisointi voi olla välillä vaikeaa, sillä samoissa hyökkäyksissä voidaan käyttää useampia menetelmiä, jolloin niiden tarkat rajat hämärtyvät.

Pretexting eli taustatarinan käyttö on kasvotusten tai verkon välityksellä hyödynnettävä menetelmä, jossa hyökkääjä keksii tarinan tai tekaistun identiteetin saadakseen uhrin luottamuksen. [3] Hyökkääjä voi esimerkiksi esittää olevansa joku uhrin luottama henkilö, kuten tuttava, esimies tai viranomainen. Uhri luulee olevansa tekemisissä tämän oikean henkilön kanssa ja luovuttaa helpommin tietojaan. [5] Määritelmän mukaan esimerkiksi klassinen romanssihuijaus, jossa huijari esittää haluavansa suhteeseen uhrin kanssa saadakseen tältä rahaa tai muita palveluksia, laskettaisiin pretexting-hyökkäykseksi.

Baiting eli houkuttelu on hyökkäys, jossa hyökkääjä huiputtaa kohteen tekemään jotain haitallista houkuttelevien valheiden avulla. Hyökkääjä voi esimerkiksi jättää yleiselle paikalle muistitikun, jolla väitetysti olisi jotain kiinnostavaa. Mikäli uhri kiinnittää muistitikun tietokoneeseensa, sille latautuu haittaohjelmia. [5]

Käänteinen sosiaalinen manipulointi on menetelmä, jossa hyökkääjä luo tilanteen, jolla saa uhrin ottamaan yhteyttä häneen. Hyökkääjä voi esittää ammattilaista tai muuta luotettavaa tahoa, jonka puoleen kohde voi kääntyä esimerkiksi tietokoneongelmien kanssa. Todellisuudessa hyökkääjä on voinut itse aiheuttaa kohteen ongelmat ja vain odottaa että tämä kääntyy häneen puoleensa, jotta voi luoda luottamussuhteen. [5]

3.3 Hyökkäystyyppien psykologinen perusta

Sosiaalinen manipulaatio on pääasiassa ihmispsykologian hyväksikäyttöä, joten on tärkeää ymmärtää mitä kaikkia ihmiskognition osa-alueita hyökkääjät voivat hyödyntää. Taulukon 3.1 teeman HT2 lähteiden perusteella voidaan tunnistaa hyökkäysten tehokkuuteen vaikuttavia psykologisia tekijöitä.

Cialdinin periaatteita voidaan pitää lähtökohtana sille, miten keskiverto ihminen tyypillisesti ajattelee ja käyttäytyy. Ne ovat perusoletuksia, joiden voidaan ajatella olevan voimassa henkilöstä ja tilanteesta riippumatta. Niillä onkin siis tärkeä vaikutus myös sosiaalisessa manipuloinnissa ja niiden merkitys on erityisen suuri tarkkaan kohdistetuissa hyökkäyksissä [6], [20]. Sosiaaliseen manipulaatioon keskittyvässä kirjallisuudessa on kuitenkin huomioitu näiden yleispätevien ominaisuuksien lisäksi myös yksilöllisiä tekijöitä, jotka vaikuttavat henkilön alttiuteen jäädä hyökkäysten uhriksi. [2], [10]

Yritykset ovat erityisen arvokkaita kohteita tietoturvahyökkäyksille, joten on hyödyllistä määritellä niitä tekijöitä, jotka tulee huomioida erityisesti työpaikoilla [2]. Lyhyellä aikavälillä näitä tekijöitä ovat esimerkiksi työtaakka, kiire ja pitkittynyt stressi. Mikäli töitä on paljon tehtävänä lyhyessä ajassa, yksittäisiin työtehtäviin keskitytään todennäköisesti vähemmän huolellisesti. Henkilö saattaa myös sivuuttaa tekijät, jotka eivät liity ensisijaiseen tehtävään. Tietoturvallisuus on yleensä toissijainen tehtävä. [10] Tällöin esimerkiksi tietojenkalasteluviesti voi jäädä tunnistamatta tai tietoturvaohjeistuksen mukainen salasananvaihto tekemättä. [2], [10]

Hyökkäyksissä voidaan myös käyttää hyväksi työntekijän asennetta työpaikkaansa kohtaan [2], [22]. Virallisen työsopimuksen lisäksi työntekijöillä ja -antajilla on molemmilla oletuksia siitä, mitä vastuuta osapuolilla on toisiaan kohtaan. Esimerkiksi työnantajan oletuksiin kuuluu, että työntekijä hoitaa tehtävänsä parhaan kykynsä mukaan. Työntekijän oletuksiin voi kuulua, että jos hän työskentelee pitkään ja ahkerasti hän voi saada palkankorotuksia tai ylennyksiä. Jos työntekijä kokee,

että häntä on kohdeltu epäreilusti, eli ”psykologista sopimusta” on rikottu, ei hän myöskään koe yhtä suurta vastuuta työnantajaa kohtaan. Parhaatkin tekniset tietoturvaratkaisut ovat turhia, jos työntekijöillä ei ole motivaatiota käyttää niitä. [22] Pahimmassa tapauksessa työntekijä saattaa olla jopa valmis aiheuttamaan vahinkoa yritykselle oman hyötynsä takia. Työntekijä on tällöin erityisen arvokas Quid pro quo-hyökkäyksille, joissa hän saattaa esimerkiksi vuotaa yrityksen tietoja rahaa vastaan. [2], [22] Toisaalta myös äärimmäisen positiivista suhdetta voidaan käyttää hyväksi jos työntekijä jää uhriksi sellaisessa hyökkäyksessä, jossa luvataan jotain erityisen hyödyllistä yritykselle. [2]

Tunnetiloilla on suuri vaikutus siihen, miten ihminen käyttäytyy. Henkilö saattaa esimerkiksi helpommin tehdä huonosti harkittuja päätöksiä tai tietoturvavirheitä niiden takia. [2], [23] Kohteen tunteisiin vaikuttaminen onkin siis tärkeä väline myös sosiaalisessa manipuloinnissa. Hyökkäyksissä yleisimmin hyödynnettyihin tunteisiin kuuluvat pelko ja ahneus [2]. Toisaalta koehenkilötutkimuksissa on havaittu, että erityisesti vihaisuus aiheuttaa virheitä tehtävässä, jossa yritetään tunnistaa aitoja sähköpostiviestejä tietojenkalasteluyrityksistä [23]. Hyökkääjät voivat myös pyrkiä laatimaan hyökkäyksen siten, että saisivat uhrin tuntemaan sympatiaa tai empatiaa heitä kohtaan. [2] Erityisen ikävät tunteet kuten yksinäisyys tai toivottomuus voivat helposti altistaa ihmisen sellaisille huijauksille, joissa luvataan jotain mikä helpottaisi hänen oloaan [2]. Pahasta yksinäisyydestä kärsivä henkilö voi helpommin jäädä esimerkiksi romanssihuijauksen kohteeksi.

Yksilölliset erot vaikuttavat siihen miten altis ihminen on sosiaaliselle manipuloinnille ja mitkä hyökkäykset toimivat häneen parhaiten. Erityisesti persoonallisuuden vaikutusta on tutkittu paljon esimerkiksi tarkastelemalla Big Five -persoonallisuusmallin listaamien ominaisuuksien (avoimuus, tunnollisuus, ekstraversio, hyväntahtoisuus ja neuroottisuus) vaikutusta henkilön alttiuteen sosiaaliselle manipuloinnille [2], [10]. Longtchi et al. [2] toteavat että korkea tunnollisuus, eli

harkitsevaisuus ja hyvä itsekuri, auttaa suojaamaan kohdennettua tietojenkalastelua vastaan. Korkeat määrät muita ominaisuuksia ennustavat taas huonompaa kykyä tunnistaa tietojenkalasteluyritykset. Montañez et al. [10] toteutettamassa kirjallisuuskatsauksessa kuitenkin huomataan, että eri tutkimusten tulokset liittyen Big Five -ominaisuuksien vaikutukseen ovat usein keskenään ristiriitaisia. Persoonallisuuden todellisesta vaikutuksesta ei siis voida olla täysin varmoja ilman jatkotutkimuksia.

Taustatekijät, kuten sukupuoli tai kulttuuri, eivät itsessään vaikuta henkilön kyvykkyyteen tunnistaa sosiaalista manipulaatiota. Erityisesti kohdennettujen hyökkäysten kannalta nämä ovat kuitenkin asioita joita huomioida, jotta hyökkäys saadaan laadittua mahdollisimman toimivaksi kohdeyleisöä vastaan. [10]

Voisi kuvitella, että tietoisuus sosiaalisesta manipulaatiosta olisi erityisen tehokasta sitä vastaan suojautumisessa. Tutkimusten perusteella pelkän tietoisuuden merkitys on kuitenkin rajallinen. [8], [10] Ihmisillä on taipumus yliarvioida osaamisensa sellaisilla aihealueilla, joista he todellisuudessa tietävät vain hieman. Tätä taipumusta kutsutaan Dunning-Kruger -efektiksi. [10]

HT2-lähteiden perusteella yksi selkeästi hyödyllisimmistä ominaisuuksista sosiaalista manipulaatiota vastaan on vahva minäpystyvyyden tunne (engl. self-efficacy). Ominaisuudella viitataan henkilön kokemaan kykyyn selvitä yllättävistä tilanteista, kuten sosiaalisesta manipulaatiosta. Kun henkilö kokee, että hän pystyy vaikuttamaan tilanteisiin, hän on halukkaampi yrittämään tehdä näin. Minäpystyvyyden ongelmana on kuitenkin se, että se tyypillisesti kehittyy hiljalleen henkilön kerätessä kokemusta ja kohdatessa sosiaalista manipulaatiota. [2], [10], [20]

3.4 Suojauskeinot sosiaalista manipulaatiota vastaan

Sosiaalista manipulaatiota hyödyntäviä hyökkäyksiä on vaikea torjua kokonaan. Kaikki ihmiset käyttäytyvät eri tavoilla ja samankin henkilön käytös voi vaihdella paljon työtaakan, stressitason tai vireyden perusteella. [10] On kuitenkin olemassa menetelmiä, joilla yritykset voivat pyrkiä ennaltaehkäisemään hyökkäyksiä tai vähentämään niiden aiheuttamaa vahinkoa. Taulukon 3.1 teeman SK1 lähteiden perusteella on tunnistettu neljä kategoriaa, joihin suoja- ja ennaltaehkäisemiskeinoja voidaan luokitella. Nämä kategoriat on esitetty alaluvussa 3.4.1, jossa avataan tarkemmin mitä toimenpiteitä näihin kategorioihin sisältyy. Alaluvussa 3.4.2 esitetään kirjallisuustaulukon teeman SK2 lähteiden perusteella havaittuja haasteita suojauskeinojen käyttämisessä.

3.4.1 Suojauskeinojen luokittelu

Koulutus ja tietoisuus on yksi keskeisimmistä tavoista ehkäistä tietojärjestelmien väärinkäyttöä. Sen avulla yrityksen työntekijät tulevat tietoisiksi tunnetuista hyökkäyksistä ja niiden seurauksista. Samalla he tunnistavat myös tulevat hyökkäysyritykset paremmin. [8] Koulutus voidaan toteuttaa esimerkiksi työpajojen, luentojen tai verkkopohjaisten itseopiskelumateriaalien avulla. [19]

Koulutuksen tarkka sisältö kannattaa suunnitella aina yrityksen tarpeen mukaan, mutta koulutuksissa voidaan käsitellä esimerkiksi ajankohtaisimpia sosiaalista manipulaatiota hyödyntäviä hyökkäyksiä, niiden tunnistamista ja sitä, miten tulee toimia jos on joutunut hyökkäyksen kohteeksi. [19]. Myös yleinen koulutus salasanaturvallisuudesta ja turvallisesta verkonkäytöstä auttaa ehkäisemään sosiaalisen manipulaation hyökkäyksiä. [5]

Koulutusta voidaan täydentää käytännön harjoituksilla ja passiivisella tiedottamisella. Esimerkiksi yleisesti tietomurtoyrityksiä simuloivat harjoitukset sisältävät usein sosiaalisen manipulaation menetelmiä, joten ne edesauttavat yrityksen osaamista niitä vastaan. Passiivisesti tietoisuutta voi ylläpitää esimerkiksi julisteilla tai tiedotusviesteillä. [19]

Teknisillä suojakeinoilla on tärkeä rooli kyberturvallisuudessa. Hyökkäysten kehittyessä aina hienostuneemmiksi tarvitaan myös parempia suojakeinoja. Erityisen tärkeää sosiaalista manipulaatiota vastaan on tunnistautuminen, sillä monissa hyökkäyksissä pyritään esittämään jotain toista henkilöä. Tätä edesauttavat esimerkiksi kaksivaiheisen tunnistautumisen käyttö tileillä sekä organisaation sisäinen soittajan tunnus, josta tietää että puhelu tulee toiselta työntekijältä, eikä huijarilta. [5] Erityisen arkaluontoisissa tilanteissa voidaan käyttää myös biometristä tunnistautumista, eli jotain tietyn henkilön fyysistä ominaisuutta kuten sormenjälkiä, kasvojentunnistusta tai ääntä. Biometrisen tunnistautumisen riskinä on kuitenkin kohdistetut hyökkäykset, joissa nämä tiedot onnistutaan kopioimaan. [19]

Hyökkäyksiä voidaan pyrkiä ennaltaehkäisemään erilaisilla verkossa tai sähköpostissa toimivilla suodattimilla. Näillä voidaan esimerkiksi estää vaaralliset verkkosivut ja pysäyttää tietojenkalasteluyritykset ennen kuin ihminen edes näkee niitä. [5] Sen varalta että tietojenkalastelu kuitenkin onnistuu ja tunnukset kaapataan, on organisaatiolla hyvä olla järjestelmät sisäänpääsy-yritysten ja toiminnan seuraamiseen. Tällöin murtautuminen pystytään huomaamaan nopeasti ja voidaan välttyä suurimmilta vahingoilta. [5], [7], [19] Tekoälyä voidaan hyödyntää sekä ennaltaehkäisemisetä havaitsemisvaiheessa viestintämallien analysoinnissa ja poikkeamien tunnistamisessa. [5]

Käytännöt ja toimintamallit määrittävät miten organisaation työntekijöiden oletetaan toimivan missäkin tilanteessa. Niiden avulla annetaan selkeät ohjeet ja vaatimukset siihen mitä kaikkea työntekijöiden tulee tehdä tietoturvallisuuden yllä-

pitämiseksi. [19] Yrityksellä täytyy esimerkiksi olla selkeät käytännöt siihen, mihin tietoihin kenelläkin on pääsy ja miten tätä pääsyä hallinnoidaan. Arkaluontoisten tietojen rajaaminen vain niitä tarvitseville vähentää luvattoman pääsyn riskiä. Tietojen vuotamisen uhkaa voidaan pienentää myös varmistamalla, että jokaisesta kerrasta kun tietoja on käsitelty jää merkintä. Turhan tiedon tai asiakirjojen tuhoamiseen on myös hyvä olla ohjeet, jotta niitä ei voi käydä tonkimassa roskiksesta. [5], [19] Eri tietoihin tai asiakirjoihin kohdistuvia ohjeistuksia voi selventää työntekijöille esimerkiksi salassapidettävyys luokitustasoilla [19].

Reagoinnilla ja raportoinnilla viitataan siihen, miten hyökkäystilanteissa toimitaan ja miten niitä pyritään arviomaan, jotta voidaan toimia paremmin jatkossa. Hyvän toimintasuunnitelman kanssa hyökkäys ei välttämättä ehdi tehdä niin pahaa vahinkoa kuin olisi mahdollista. Reagointia voi tehostaa varmistamalla, että on selkeä viestikanava, jota pitkin muut saadaan tietoisiksi tapahtumasta. Yritys voi myös perustaa erikoistuneen ryhmän osaajia, joiden vastuulla on reagoida sosiaaliseen manipulointiin. Erityisen tärkeää on arvioida mihin asioihin resurssit tulee priorisoida hätätilanteessa. [5] Esimerkiksi laajamittaisemmassa hyökkäyksessä voi olla tarve eristää joitain kriittisiä laitteita yrityksen muusta verkosta. [19]

3.4.2 Suojauskeinojen arviointi

Taulukon 3.1 teeman SK2 lähteiden perusteella keskeisin haaste sosiaalista manipulaatiota vastaan suojautumisessa on työntekijöiden asenne tietoturvallisuutta kohtaan. Tietoturvariskit saatetaan nähdä organisaation uhkana, ei yksittäisen henkilön [21]. Pelkkä koulutus ja tietoisuus ei itsessään riitä takaamaan turvallista toimintaa. Vaikka työntekijöillä olisi täysi ymmärrys siitä miten heidän tulisi toimia, asenteesta riippuen he eivät välttämättä vaivaudu tekemään näin. [21] Sámson ja Tick [4] havaitsivat kyselytutkimuksensa perusteella, että töissä käyty tietoturvakoulutus ei välttämättä vaikuta merkittävästi toimintaan töiden ulkopuolella. Työnte-

kijät noudattavat siis ohjeistuksia työpaikalla, mutta heidän asenteensa eivät muutu merkittävästi.

Organisaation viralliset käytännöt ja toimintamallit sekä vallitseva ilmapiiri voivat vaikuttaa merkittävästi työntekijöiden tietoturva-asenteisiin. Henkilöt, jotka kokevat että heitä ei arvosteta tai että heitä kohdellaan epäreilusti, eivät ole yhtä motivoituneita toimimaan tietoturvallisesti [22]. Käytäntöjen valvominen ja ylläpitäminen vaatii myös vastuullisuutta johtoportaalta. Jos käytännöt asetetaan huonosti, tai johtoporras välttelee vastuuta, voivat työntekijät saada huonon esimerkin, joka voi johtaa epäammattimaiseen päätöksentekoon. [4] Tietoturvaohjeistuksien noudattamisen valvomisessa on myös haasteita. Jos niitä valvotaan pelkästään ulkoisen motivaation kuten rangaistusten tai palkkioiden kautta, pitkäaikaiset vaikutukset voivat olla toivottua päinvastaiset. Työntekijät noudattavat ohjeita vain koska käsketään ja lopettavat nopeasti jos valvontaa vähennetään. [22]

Teknologisiin suojauskeinoihin turvaudutaan usein liikaa. Tietojärjestelmien tekninen tietoturva on yleensä hyvä, mutta mahdollisuus ohittaa nämä esteet sosiaalisella manipuloinnilla huomioidaan heikommin. [4], [9] Teknisten työkalujen hyödyllisyyttä rajoittaa myös niitä käyttävien ihmisten osaaminen ja asenteet, sillä parhaatkin suojakeinot ovat turhia jos niiden käyttäjät eivät toimi tietoturvallisesti. [19], [22] Joillain ihmisillä voi olla vaikeuksia pysyä jatkuvasti kehittyvän teknologian perässä. [4]

Liiallinen luotto teknologiaan voi myös itsessään aiheuttaa riskejä. Ihmiset kehittyvät sosiaalisen manipulaation tunnistamisessa kokemuksen kautta, eli mitä useammin hyökkäyksiä kohdataan, sitä heikommin ne toimivat. Jos hyökkäyksiä kohdataan harvoin, ne toimivat tehokkaammin. Mikäli suurin osa hyökkäyksistä pysäytetään teknisillä esteillä, läpi pääsevillä hyökkäyksillä voi olla vakavat seuraukset. Syntyykin dilemma siitä, miten sulkea pois mahdollisimman moni hyökkäys, mutta pitää ihmiset koko ajan valppaina hyökkäysten varalta. [10]

4 Pohdintaa

Aineiston perusteella vaikuttaa olevan yhteisymmärrys siitä, mitkä ovat suurimmat vaikeudet liittyen sosiaalisen manipulaatioon. Tarkkaa yhteistä määritelmää sosiaaliselle manipulaatiolle tai siihen kuuluville menetelmille ei kuitenkaan ole. Lähteissä [1], [4], [5], [7], [19] käytetyissä määritelmissä sosiaalisella manipuloinnilla pyritään aina varastamaan kohteelta tietoa ja hyödyntämään sitä jatkohyökkäyksissä. Lähteissä [3], [6], [8]–[10], [22] tiedon varastamista pidettiin kyllä merkittävänä tavoitteena, mutta sosiaaliseen manipulointiin tulkittiin myös yleisemmin kohteen huiputtaminen toimimaan epäturvallisesti tulevien hyökkäysten mahdollistamiseksi. Lähteissä [2], [20], [21], [23] ei määritellä käsitettä ollenkaan, vaan lukijan oletetaan tietävän mitä sillä tarkoitetaan. Määritelmät eivät ole vakavasti keskenään ristiriidassa, mutta eroavat rajauksissaan sen verran, että ei voida aina olla varmoja mitkä tapaukset mitkäkin lähteet laskisivat sosiaaliseksi manipuloinniksi. Esimerkiksi luvussa 2.3 esitetty Toyota Boshokun tapausta, jossa hyökkääjät saivat yhtiön huijattua lähettämään väärälle tilille 37 miljoonaa dollaria, ei tiukemman määritelmän mukaan laskettaisi sosiaaliseksi manipuloinniksi, koska siinä ei varastettu nimenomaan tietoa.

Vaikka tarkka täysin yhtenäinen määritelmä puuttuukin, on psykologiaa sosiaalisessa manipuloinnissa saatu tutkittua melko monesta eri näkökulmasta, jotka paikoin täydentävät toisiaan. Esimerkiksi Lee et al. [22] tutkivat työympäristön vaikutusta työntekijöiden halukkuuteen toimia tietoturvallisesti, kun taas Grassegger

ja Nedbal [8] tutkivat kuinka tällaiset taustatekijät voivat vaikuttaa henkilön toimintaan. Tietoa siitä mitä taktiikoita tai kohteiden heikkouksia hyökkäyksissä hyödynnetään on kuitenkin sovellettu rajallisesti. Ainoastaan Longtchi et al. [2] tarkastelivat sitä, mitä psykologisia tekniikoita tietyissä hyökkäyksissä käytetään ja millä suojauskeinoilla psykologisiin tekniikoihin pystytään vastaamaan. Tämän näkökulman tarkempi analyysi olisi hyödyllistä, sillä hyökkäyksissä käytetty teknologia kehittyy jatkuvasti, mutta ihmispsykologia pysyy samankaltaisena.

Niin kauan kun ihmiset ovat vastuussa tietojärjestelmien ylläpitämisestä, sosiaalisen manipulaation uhka voi olla mahdoton kitkeä kokonaan. Ongelma on monimutkainen ja siihen ei ole yleispäteviä ratkaisuja. Aineistossa kuitenkin nousee esiin kaksi tekijää joilla on erityisen suuri vaikutus alttiuteen sosiaaliselle manipuloinnille; asenne tietoturvaa kohtaan [8], [19], [22], sekä minäpystyvyyden tunne [2], [10], [20]. Minäpystyvyydellä tarkoitetaan tässä kontekstissa yhdistelmää henkilön taidoista sekä kokemasta kyvykkyydestä vastata yllättäviin ja hankaliin tilanteisiin, kuten sosiaaliseen manipulointiin. Minäpystyvyyden ja tietoturva-asenteen välillä voidaan havaita yhteys. Jos henkilöllä on heikko minäpystyvyyden tunne, hän ei koe että hänellä olisi juurikaan vaikutusvaltaa tietoturvan suhteen. Tällöin hän tekee vain minimin ja hänen asenteensa tietoturvaa kohtaan on huonompi. Henkilö jolla on hyvä minäpystyvyyden tunne pystyy panostamaan tietoturvaan enemmän ja ymmärtää paremmin mitä tekee. Minäpystyvyyden ongelmana on se, että se kehittyy yleensä pitkällä aikavälillä kokemuksen kautta. Tietoturvakoulutusta voisi kuitenkin kehittää siten, että se auttaisi kehittämään henkilön kokemusta ja kyvykkyyttä sosiaalista manipulaatiota vastaan.

Tutkimuksen aineistoon valikoitui melko tasainen jakauma konferenssipapereita sekä lehtiartikkeleita. Julkaisuissa on siis sekä tuoretta tietoa, että pidemmälle vertaisarvioituja lähteitä. Tutkielman rajoitteena on kuitenkin lähteiden määrä. Tutkielman laajuuden rajaamiseksi monta lähdettä jouduttiin sulkemaan pois. Jat-

kotutkimuksessa tärkeää olisi selvittää, miten tietoa sosiaaliseen manipulaatioon vaikuttavista psykologisista tekijöistä voitaisiin hyödyntää puolustuskeinojen suunnittelussa, sekä miten pyrkiä kehittämään ihmisten asennetta ja koettua minäpystyvyyttä tietoturvallisuuden suhteen.

5 Yhteenveto

Tässä tutkielmassa tutkittiin kirjallisuuskatsauksena sitä, miten sosiaalista manipulaatiota hyödynnetään tietoturvahyökkäyksissä. Ihmiset ovat usein tietoturvan heikoin lenkki, joten on tärkeä tunnistaa hyökkäyksissä käytettävät taktiikat ja menetelmät. Kirjallisuuskatsauksen perusteella sosiaalista manipulaatiota on tutkittu melko paljon, erityisesti sen osalta miten yritykset pystyvät suojautumaan siltä.

TK1:een vastattiin luvussa 3.3. Sosiaalista manipulaatiota hyödyntävien hyökkäysten tehokkuus perustuu suostuttelun periaatteiden sekä kohteen hyökkäykselle altistavien tekijöiden tunnistamiseen ja hyväksikäyttöön. Suostuttelun periaatteisiin kuuluu pitämisen tunteen luominen, vastavuoroisuus, muiden esimerkki, johdonmukaisuus, niukkuus ja auktoriteetti. Näiden periaatteiden hyödyntäminen auttaa vaikuttamaan lähtökohtaisesti kaikkiin ihmisiin. Yksilöllisiä vaikuttavia tekijöitä ovat lyhyellä aikavälillä stressi, kiire, työtaakka ja tunnetilat. Erityisesti tunnetiloihin pyritään hyökkäyksissä yleensä vaikuttamaan. Pidemmällä aikavälillä vaikuttavia tekijöitä ovat asenteet työpaikkaa ja tietoturvallisuutta kohtaan sekä henkilön tietoturvakoulutus. Kulttuurilla, sukupuolella ja persoonallisuudella ei aineiston perusteella ole selkeää vaikutusta alttiuteen. Ne ovat kuitenkin tekijöitä, jotka huomioidaan suunnitellessa kohdennettuja hyökkäyksiä. Erityisen suuri positiivinen vaikutus on hyvällä koetulla minäpystyvyydellä. Tätä ominaisuutta olisikin hyvä pyrkiä kehittämään erilaisilla keinoilla.

TK2:een vastattiin luvussa 3.4. Yritysten hyödyntämät suojauskeinot sosiaalista manipulaatiota vastaan voidaan jakaa neljään kategoriaan. Koulutus ja tietoisuus on tärkeä tapa varmistaa, että työntekijät tietävät mistä olla varuillaan. Yksinään sen vaikutus on kuitenkin rajallinen, sillä ihmiset ovat taipuvaisia yliarvioimaan oman osaamisensa. Riskien tunnistaminen ei myöskään takaa, että aikoo toimia täysin tietoturvallisesti. Teknisillä suojakeinoilla kuten viestisuodattimilla tai kaksivaiheisella tunnistautumisella voidaan koittaa ennaltaehkäistä hyökkäyksiä, mutta niiden tehokkuutta rajoittaa käyttäjien osaaminen. Käytännöillä ja toimintamalleilla määrätään se, miten työntekijöiden halutaan toimivan ja miten järjestelmiä hallinnoidaan. Tämä vaatii kuitenkin valvontaa, sekä työilmapiirin jossa työntekijät ovat halukkaita panostamaan ohjeiden noudattamiseen. Suunnittelemalla toimenpiteet reagointiin ja raportointiin voidaan pyrkiä pysäyttämään alkanut hyökkäys ja pohtia miten valmistautua paremmin seuraavaan.

Jatkotutkimuksessa tulee pyrkiä selvittämään, miten tuntemusta sosiaalisessa manipulaatiossa hyödynnettävistä psykologisista tekijöistä voidaan hyödyntää puolustuskeinojen suunnittelussa. Tärkeää olisi myös pyrkiä parantamaan ihmisten minäpystyvyyttä sekä erityisesti vähentämään välinpitämätöntä asennetta tietoturvaa kohtaan.

Lähdeluettelo

[1] A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang ja H. N. Thakur, "Social Engineering Incidents and Preventions", *2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023*, s. 494–498, 2023. DOI: 10.1109/CCWC57344.2023.10099202.

[2] T. T. Longtchi, R. M. Rodriguez, L. Al-Shawaf, A. Atyabi ja S. Xu, "Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey", *Proceedings of the IEEE*, vol. 112, s. 210–246, 3 maaliskuu 2024, ISSN: 15582256. DOI: 10.1109/JPROC.2024.3379855.

[3] W. Nowakowski, "Social Engineering Analysis Framework: A Comprehensive Playbook for Human Hacking", *IEEE Access*, vol. 13, s. 18 827–18 849, 2025, ISSN: 21693536. DOI: 10.1109/ACCESS.2025.3532999.

[4] N. Sámson ja A. Tick, "Digital Defense: Investigating Human Aspects of Cybersecurity", *SACI 2024 - 18th IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, s. 525–532, 2024. DOI: 10.1109/SACI60582.2024.10619840.

[5] M. Zaoui, B. Yousra, S. Yassine, M. Yassine ja O. Karim, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies", *IEEE Access*, vol. 12, s. 72 224–72 241, 2024, ISSN: 21693536. DOI: 10.1109/ACCESS.2024.3403197.

[6] K. Khadka, A. B. Ullah, W. Ma, E. M. Marroquin ja Y. Alem, "A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing", *Proceedings - 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom/BigDataSE/CSE/EUC/iSCI 2023*, s. 1631–1638, 2023. DOI: 10.1109/TRUSTCOM60117.2023.00222.

[7] S. A. Kaushalya, R. M. Randeniya ja A. D. Liyanage, "An Overview of Social Engineering in the Context of Information Security", *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences, ICETAS 2018*, heinäkuu 2018. DOI: 10.1109/ICETAS.2018.8629126.

[8] T. Grassegger ja D. Nedbal, "The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering", *Procedia Computer Science*, vol. 181, s. 59–66, tammikuu 2021, ISSN: 1877-0509. DOI: 10.1016/J.PROCS.2021.01.103.

[9] A. Lopes, L. Reis, H. S. Mamede ja A. Santos, "Information Security Threat Assessment Using Social Engineering in the Organizational Context – Literature Review", *Lecture Notes in Networks and Systems*, vol. 469 LNNS, s. 233–242, 2022, ISSN: 23673389. DOI: 10.1007/978-3-031-04819-7_24/FIGURES/2.

[10] R. Montañez, E. Golob ja S. Xu, "Human Cognition Through the Lens of Social Engineering Cyberattacks", *Frontiers in Psychology*, vol. 11, s. 528 099, syyskuu 2020, ISSN: 16641078. DOI: 10.3389/FPSYG.2020.01755/XML.

[11] F-Secure. "Mitä on käyttäjän manipulointi?", viitattu 15. kesäkuuta 2026. url: https://www.f-secure.com/fi/articles/what-is-social-engineering.

[12] "Petosrikokset", viitattu 15. kesäkuuta 2026. url: https://poliisi.fi/petosrikokset.

[13] R. Cialdini, *Influence: The Psychology of Persuasion*. William Morrow & Company, 1984.

[14] L. Danielson. "Anthem Data Breach", viitattu 15. kesäkuuta 2026. url: https://www.huntress.com/threat-library/data-breach/anthem-data-breach.

[15] D. Business. "NotPetya – The Ten Billion Dollar Worm", viitattu 15. kesäkuuta 2026. url: https://www.dna.fi/dnabusiness/blogi/-/blogs/notpetya-the-ten-billion-dollar-worm.

[16] L. Mathews. "Toyota Parts Supplier Hit By $37 Million Email Scam", viitattu 15. kesäkuuta 2026. url: https://www.forbes.com/sites/leemathews/2019/09/06/toyota-parts-supplier-hit-by-37-million-email-scam/.

[17] D. Schrader. "An Overview of the MGM Cyber Attack", viitattu 15. kesäkuuta 2026. url: https://netwrix.com/en/resources/blog/mgm-cyber-attack/.

[18] A. L. Hankaniemi. "Poliisi varoittaa massiivisesta suomalaisiin kohdistuneesta tekstiviestihuijauksesta", viitattu 15. kesäkuuta 2026. url: https://yle.fi/a/74-20150223.

[19] H. A. Aldawood ja G. Skinner, "A critical appraisal of contemporary cyber security social engineering solutions: Measures, policies, tools and applications", *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings*, heinäkuu 2018. DOI: 10.1109/ICSENG.2018.8638166.

[20] M. Cazares, W. Fuertes, R. Andrade, I. Ortiz-Garcés ja M. S. Rubio, "Protective Factors for Developing Cognitive Skills against Cyberattacks", *Electronics 2023, Vol. 12, Page 4007*, vol. 12, s. 4007, 19 syyskuu 2023, ISSN: 2079-9292. DOI: 10.3390/ELECTRONICS12194007.

[21] V. Greavu-Şerban, F. Constantin ja S. C. Necula, "Exploring Heuristics and Biases in Cybersecurity: A Factor Analysis of Social Engineering Vulnerabilities", *Systems 2025, Vol. 13, Page 280*, vol. 13, s. 280, 4 huhtikuu 2025, ISSN: 2079-8954. DOI: 10.3390/SYSTEMS13040280.

[22] D. Lee, S. L. Harjinder ja N. Michaelides, "The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation", *Technology & Work*, vol. 25, s. 273–289, 2023. DOI: 10.1007/s10111-023-00727-5.

[23] M. Wiemken, K. Hildebrandt, A. Jeworutzki ja L. Putzar, "Emotional Manipulation in Phishing Emails: Experimental Study of Affective Responses and Human Classification Errors in a Simulated Email Environment", *Proceedings of the 18th ACM International Conference on PErvasive Technologies Related to Assistive Environments, PETRA 2025*, vol. 25, s. 583–589, heinäkuu 2025. DOI: 10.1145/3733155.3736796/ASSET/5ADA8E6C-94C0-4306-A829-87179EAE6BB6/ASSETS/IMAGES/LARGE/PETRA25-85-FIG5.JPG.