Käyttäjän manipulointi kyberuhkana – haavoittuvuutena psykologiset tekijät

Nadja Liljeström

Haaga-Helia ammattikorkeakoulu
Tradenomi (AMK), tietojenkäsittely
Opinnäytetyö
2025

Tiivistelmä

Tekijä(t)
Nadja Liljeström

Tutkinto
Tradenomi, tietojenkäsittely

Raportin/Opinnäytetyön nimi
Käyttäjän manipulointi kyberuhkana – haavoittuvuutena psykologiset tekijät

Sivu- ja liitesivumäärä
58

Tämän opinnäytetyön tavoitteena oli selvittää, mitkä yksilön psykologiset piirteet voidaan mieltää haavoittuvuuksiksi käyttäjän manipuloinnin hyökkäyksissä, millaisia psykologisia menetelmiä hyökkääjä hyödyntää, sekä millaisia vaiheita tällainen tarkoin suunniteltu ja kohdennettu hyökkäys sisältää. Työn tarkoituksena oli luoda lukijalle selkeä kuva kyberuhista, joissa olennainen elementti on ihmisen psykologiaan vetoavien menetelmien hyödyntäminen.

Opinnäytetyö toteutettiin kevään 2025 aikana narratiivisena kirjallisuuskatsauksena, jossa tavoitteena on tehdä havaintoja ja yhteenvetoja aiemmin julkaistuista tutkimuksista. Tutkimuksen aihe rajattiin seuraavien tutkimuskysymysten avulla:

- Mitkä psykologiset tekijät voidaan nähdä haavoittuvuuksina kyberturvallisuuden kontekstissa?
- Mitä psykologisia menetelmiä käyttäjän manipuloinnin hyökkäyksissä hyödynnetään?
- Mitä vaiheita ja psykologisia menetelmiä kohdennettu käyttäjän manipuloinnin hyökkäys sisältää?

Työn tietoperustassa lukijalle avattiin kyber- ja tietoturvallisuuden käsitteet, sekä esiteltiin yleisimmät käyttäjän manipuloinnin uhat, joita organisaation henkilöstö työtehtävissään kohtaa. Myös tutkimusmenetelmän, eli narratiivinen kirjallisuuskatsauksen määritelmä avattiin lukijalle.

Työn empiirisessä osassa käytiin läpi kyberturvallisuuden kontekstissa haavoittuvuuksiksi miellettävät psykologiset tekijät, sekä käyttäjän manipuloinnin hyökkäyksissä hyödynnettävät psykologiset menetelmät. Empiirisessä osassa myös perehdyttiin kohdennetun käyttäjän manipuloinnin hyökkäyksen vaiheisiin, käyttäen esimerkkinä BEC-huijausta ja teknisen tuen huijausta.

Tutkimusaineistona käytettyjen aiempien tutkimusten perusteella oli havaittavissa, että käyttäjän manipuloinnin hyökkäyksissä keskitytään huomattavasti enemmän psykologisiin haavoittuvuuksiin kuin teknisen suojauksen murtamiseen. Tästä tehtiin johtopäätös, että käyttäjän manipuloinnin hyökkäyksiin on olennaista varautua juuri henkilöstön kouluttamiseen ja tietoisuuden lisäämiseen panostamalla.

Tutkimuksessa havaittiin myös jatkotutkimustarpeita, kuten hyökkäyksen onnistumiseen johtavien tekijöiden tutkiminen. Tämä edellyttäisi myös sitä, että näistä tapauksista puhuttaisiin enemmän julkisesti. Myös organisaation toimintamalleihin olisi hyvä kiinnittää huomiota, ja tutkia varsinkin kohteena olleen yksilön kokemusta toteutuneiden uhkien tapauksessa, kun organisaation työntekijä joutuu käyttäjän manipuloinnin hyökkäyksen uhriksi työtehtävissään.

On myös huomioitava, että teknologian kehittyessä myös rikolliset tulevat hyödyntämään kehittynyttä teknologiaa hyökkäyksissään luodakseen entistä uskottavampia huijauksia, joten myös hyökkäysmenetelmien kehittyminen teknologian myötä tulee olemaan tulevaisuudessa erityisen tärkeä tutkittava aihealue.

Asiasanat
käyttäjän manipulointi, kohdennettu tietojenkalastelu, psykologinen haavoittuvuus, BEC-huijaus, kyberuhka

Sisällys

1 Johdanto

Nykypäivänä organisaatioissa digitalisoituminen ottaa suuria harppauksia ja etätyöt yleistyvät. Palvelut ja liiketoiminnan kannalta kriittiset tiedot ovat siirtyneet ja siirtyvät enenevissä määrin verkkoon ja pilveen. Lähes koko yhteiskunta on jollain tavalla sidoksissa internetiin.

Työntekijät, ihmiset, ovat olennainen osa organisaatioiden toimintaa ja digitaalisten viestintävälineiden ollessa suuressa roolissa organisaation arjessa todennäköinen kohde jatkuvasti kehittyville digiajan tietoturva- ja kyberuhille, kuten huolellisesti suunnitelluille ihmisen psykologisia haavoittuvuuksia hyödyntäville manipulointiyrityksille sekä tietojenkalastelulle. Näiden lisäksi erinäisistä inhimillisistä tekijöistä, kuten väsymyksestä tai huolimattomuudesta, johtuvat inhimilliset virheet ovat yksi hyökkääjän onnistumiselle altistava tekijä.

Rikolliset ja huijarit ovat kautta aikojen hyödyntäneet inhimillisyyttä ja tunteisiin vetoamista pyrkiessään tavoitteeseensa ja käyttävät häikäilemättä esimerkiksi ihmisen myötätuntoon ja auttamisenhaluun vetoavia psykologisia keinoja saadakseen haluamansa (Järvinen 2022, 77). Konstit ovat monet, kun verkkorikollinen pyrkii ohjailemaan kohteensa toimintaa kohti haluttua tavoitetta. Tehosteena tavoitteen saavuttamiseen käytetään usein esimerkiksi luottamusta herättävää auktoriteettiasemaa ja kiireeseen vetoamista tai jopa suoraa uhkailua. (F-Secure 2024a.)

Rikolliset toimijat, kuten rahaa havittelevat huijarit, ihmisten henkilö- ja maksukorttitietojen perässä olevat rikolliset tai kyseenalaista tiedustelutoimintaa harjoittavat tahot, ovat muun maailman tavoin siirtäneet toimintansa verkkoon. Verkossa tapahtuva rikollinen toiminta on myös kansainvälistynyt vuosien varrella, sillä verkon yli toimiminen tarjoaa myös rikollisille tahoille suuremman pelikentän ilman maantieteellisiä rajoituksia (Järvinen 2022, 17).

Tämä tarkoittaa sitä, ettei Suomen maantieteellisesti syrjäinen sijainti ole mikään este kansainvälisen rikollisen toiminnan kohteeksi joutumiselle, sillä verkon kautta fyysisessä maailmassa toisella puolella maapalloa oleva rikollinen on vertauskuvallisesti aivan kulman takana. (Järvinen 2022, 34; Hyppönen 2021, 44)

1.1 Tutkimuksen tavoite ja rajaukset

Tämän opinnäytetyön tavoitteena on muodostaa ajantasainen katsaus, jossa kartoitetaan organisaation henkilöstöön kohdistuvia kyberuhkia, jotka hyödyntävät käyttäjän manipuloinnin keinoja. Tarkoituksena on selvittää, mitkä psykologiset ja inhimilliset tekijät lisäävät organisaation haavoittuvuutta kohdennettua käyttäjän manipulointia sisältäviä kyberuhkia kohdatessa, sekä mitä psykologisia menetelmiä rikolliset hyödyntävät näitä hyökkäyksiä toteuttaessaan.

Tietoperustassa avataan yleisimpiä kyberuhkia, jotka kohdistuvat organisaation henkilöstöön ja joissa keskeisenä elementtinä on käyttäjän manipulointi, eli psykologisten menetelmien hyödyntäminen.

Opinnäytetyön aihepiiriin perehtyessä nousi esiin, että monessa asiayhteydessä on hieman epäselvää, milloin on kyse tietoturvasta ja milloin taas kyberturvallisuudesta, joten selkeyden vuoksi tietoperustassa lukijalle avataan myös näiden kahden termin määritelmät ja eroavaisuudet.

Tutkimuksen tavoitteena on selvittää kuvailevan kirjallisuuskatsauksen menetelmin, mikä tekee kohdennetuista käyttäjän manipuloinnin hyökkäyksistä erityisen vaarallisia. Tutkimuskysymysten avulla selvitetään, mistä eri vaiheista tällainen hyökkäys muodostuu ja mitä ovat ne psykologiset haavoittuvuudet ja menetelmät, joita hyödyntämällä nämä hyökkäykset valitettavan usein onnistuvat varotoimenpiteistä, koulutuksesta ja tietoisuudesta huolimatta.

Tutkimus rajattiin seuraavien tutkimuskysymysten avulla:

- Mitkä psykologiset tekijät voidaan nähdä haavoittuvuuksina kyberturvallisuuden kontekstissa?
- Mitä psykologisia menetelmiä käyttäjän manipuloinnin hyökkäyksissä hyödynnetään?
- Mitä vaiheita ja psykologisia menetelmiä kohdennettu käyttäjän manipuloinnin hyökkäys sisältää?

Tutkittavaa aihetta lähestytään erityisesti psykologisesta näkökulmasta, ja pyritään selvittämään, mitä ovat ne psykologiset haavoittuvuudet ja menetelmät, joita hyödyntämällä kohdennettu käyttäjän manipuloinnin hyökkäys toteutetaan onnistuneesti, vaikka kohdetta olisi valmennettu kohtaamaan tällaisia hyökkäyksiä. Tutkimuskysymyksillä pyritään psykologisten hyökkäysmenetelmien lisäksi selvittämään, mitä eri vaiheita tällainen huolellisesti suunniteltu ja tarkoin kohdennettu käyttäjän manipuloinnin hyökkäys, kuten esimerkiksi BEC-hyökkäys, yleensä sisältää.

Opinnäytetyön aihe on rajattu niin, että työssä keskitytään organisaation henkilöstön työtehtävissään kohtaamiin kohdennettuihin kyberuhkiin, jotka sisältävät psykologisen vaikuttamisen keinoja. Tästä syystä tämän opinnäytetyön aiherajauksen ulkopuolelle jäävät tieto- ja kyberturvallisuudesta ne osa-alueet, jotka eivät liity olennaisesti organisaation henkilöstöön kohdistuviin käyttäjän manipuloinnin keinoja sisältäviin uhkiin. Opinnäytetyössä ei siis käsitellä kyberturvallisuuden osa-alueita, jotka koskevat maanpuolustusta, kriittisen infrastruktuurin suojaamista, teknisiä ratkaisuja tai informaatiovaikuttamista. Tietoturvan osalta rajauksen ulkopuolelle jäävät muun muassa tekniset ratkaisut, ohjelmistot, sekä organisaation järjestelmiin kohdistuvat tietoturva- ja kyberuhat.

Tämän opinnäytetyön tietoperusta on rakennettu sekä painetun materiaalin, että internet-lähteiden pohjalta. Asiantuntijoiden julkaisema kirjallisuus on toiminut tietoperustan runkona, jota on päivitetty ajankohtaisella tiedolla internet-lähteistä. Tähän ratkaisuun on päädytty siksi, että

opinnäytetyön aihealueessa on tietyt perusasiat, jotka säilyvät vuodesta toiseen melko muuttumattomina, mutta kokonaisuus, kuten esimerkiksi hyökkäys-, varautumis- ja puolustusmenetelmät, kehittyy jatkuvasti. Käytetyt lähteet ovat suomen- ja englanninkielisiä.

1.2 Keskeiset käsitteet

Informaatiovaikuttaminen – Levitettävää informaatiota tuotetaan, muokataan tai rajoitetaan pyrkimyksenä vaikuttaa kohteen mielipiteeseen, käsitykseen tai toimintaan (Turvallisuuskomitea 2018, 29).

Kriittinen infrastruktuuri – Yhteiskunnan arkea ja elintärkeitä toimintoja ylläpitävät perusrakenteet, palvelut ja niihin liittyvät toiminnot. Kriittistä infrastruktuuria ovat esimerkiksi energian tuotanto, liikenne ja logistiikka, vesi- ja jätehuolto, siirto- ja jakelujärjestelmät sekä tieto- ja viestintäjärjestelmät. (Turvallisuuskomitea 2018, 26.)

Kyber – Sana ”kyber” (tai cyber) on käytössä digitaalisen ympäristön, kuten tietotekniikan ja tietoverkkojen aihepiirissä, yhdyssanan määriteosana, liittyen merkityssisällöltään digitaalisessa muodossa olevaan tietoon tai digitaaliseen ympäristöön. Kyber-sanan alkuperäksi mielletään kreikan kielen sana ”kybereo”, joka tarkoittaa ”ohjata”, ”opastaa” tai ”hallita”. (Turvallisuuskomitea 2018, 21.)

Kyberrikollisuus – Viestintäverkkoja ja tietojärjestelmiä hyödyntävä tai hyökkäyksensä niihin kohdistava rikollisuuden muoto, jossa kohteena voi olla valtio, organisaatio tai yksityishenkilö (Turvallisuuskomitea 2018, 26).

Kyberturvallisuus – Toimenpiteet ja toiminta, joilla pyritään tunnistamaan, varautumaan ja ehkäisemään uhkia, jotka kohdistuvat digitaalisen ja verkottuneen yhteiskunnan tai organisaation digitaalisen ympäristön turvallisuuteen ja toimintojen häiriöttömään jatkuvuuteen. Kyberturvallisuuden käsite pitää sisällään myös uhkan toteutumisen vaikutusten minimoinnin ja riskin toteutumisen jälkeisen sietokyvyn takaamisen. Käsite pitää sisällään myös tietoturvan huomioimisen, sillä usein digitaalisen ympäristön häiriytyminen aiheutuu toteutuneesta tietoturvauhasta. Kyberturvallisuudessa myös tietoturvallinen toiminta on olennaisessa roolissa, sillä digitaalisen ympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhasta. (Turvallisuuskomitea 2018, 22.)

Kyberturvallisuudella tarkoitetaan tässä opinnäytetyössä organisaatiossa työskentelevien henkilöiden valppautta, toimintatapoja ja asenteita, joiden pyrkimyksenä on havaita ja torjua verkkorikollisten manipuloinnin keinoja sisältävät hyökkäysyritykset.

Kyberuhka – Digitaaliseen ympäristöön tai järjestelmään kohdistuva mahdollinen haitallinen tapahtuma tai kehityskulku, esimerkiksi tietoturvauhka, joka toteutuessaan vaarantaa järjestelmän toiminnan (Turvallisuuskomitea 2018, 25).

Kyberuhkalla tarkoitetaan tässä opinnäytetyössä rikollisten toimijoiden toteuttamia hyökkäyksiä, joiden tavoitteena on saavuttaa rikollista hyötyä, kuten rahaa tai pääsy arvokkaaseen tai arkaluontoiseen tietoon tai organisaation järjestelmiin. Hyökkäyksen kohteena on organisaatiossa työskentelevä henkilö tai henkilöt. Hyökkäyksissä hyödynnetään käyttäjän manipuloinnin keinoja, joilla vedotaan ihmisen tunteisiin, sekä hyödynnetään inhimillisiä tekijöitä, kuten väsymystä tai huolimattomuutta.

Käyttäjän manipulointi (social engineering) – Epärehellinen pyrkimys, jossa tavoitteena on saavuttaa taloudellista hyötyä, pääsy järjestelmiin tai arkaluontoiseen tietoon. Rikollinen edistää tavoitteensa saavuttamista tekeytymällä henkilöksi tai hyväksikäyttämällä henkilöä, jolla on oikeus tavoiteltuun tietoon. Kohteeksi organisaatiossa voi valikoitua yksittäinen tai useampi henkilö. (Turvallisuuskomitea 2018, 19.) Hyökkäyksissä hyödynnetään usein tietoa ihmisen käyttäytymisestä, sekä psykologisia ja inhimillisyyteen vetoavia elementtejä. Social engineering -termistä voidaan käyttää myös seuraavia suomenkielisiä ilmaisuja: henkilön manipulointi, sosiaalinen manipulointi, vaikuttaminen tai hämääminen (F-Secure 2024a.)

Tietoturva – Toiminta ja toimenpiteet, joilla pyritään varmistamaan ja suojaamaan tiedon saatavuus eheys ja luottamuksellisuus. Tietoturva kattaa myös fyysisen ulottuvuuden, eli esimerkiksi asianmukaisen kulunvalvonnan ja tilojen lukituksen, sekä fyysisten asiakirjojen turvallisen ja huolellisen käsittelyn, säilyttämisen ja hävittämisen. Myös laitteiden, ohjelmistojen ja tietoliikenteen turvaaminen, kuten esimerkiksi ohjelmistojen päivittäminen sekä palomuurin, virustorjuntaohjelmien ja varmenteiden käyttö, ovat tietoturvaa. (Turvallisuuskomitea 2018, 15.)

Tietoturvalla tarkoitetaan tässä opinnäytetyössä sitä, että tiedon luottamuksellisuus, eheys ja saatavuus suojataan ja taataan esimerkiksi salasanojen ja käyttäjätunnusten oikeaoppisella käsittelyllä ja säilyttämisellä, sekä valppaalla toiminnalla esimerkiksi tilanteissa, joissa pyydetään arkaluontoista tietoa tai käyttäjätunnuksia. Tässä työssä keskitytään näkökulmaan, kuinka organisaation työntekijä omalla toiminnallaan noudattaa tietoturvallisen toiminnan periaatteita.

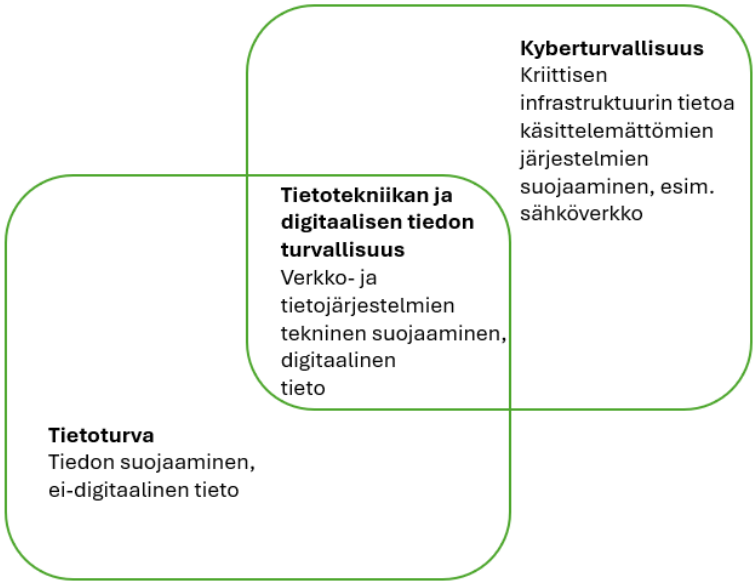
2 Kyberturvallisuus ja tietoturva organisaatioissa

Tämän luvun tarkoituksena on selkeyttää, mitä käsitteillä kyberturvallisuus ja tietoturva tarkoitetaan. Digiajan uhkista ja niihin varautumisesta puhuttaessa termit tietoturva ja kyberturvallisuus menevät usein keskenään sekaisin.

Niillä sinänsä onkin osittain sama tarkoitus, eli suojata dataa sekä varmistaa tietojärjestelmien toiminta. Kuitenkin osa-alueet, jotka tietoturva ja kyberturvallisuus kattavat, eriävät toisistaan. (Järvinen 2018, 14.)

Tietoturva kattaa digitaalisen tiedon lisäksi myös fyysisessä muodossa olevan tiedon suojaamisen. Tietoturvassa olennaista on tiedon suojaaminen niin, että siihen pääsee käsiksi vain kyseistä tietoa käsittelemään tai katselemaan oikeutetut henkilöt. Tämän lisäksi tietoturvalla taataan, että tieto on saatavilla silloin kun sitä tarvitaan, ja ettei oikeudeton taho pääse muuttamaan tallennettua tietoa. Kyberturvallisuus puolestaan keskittyy nimenomaan digitaalisten uhkien torjumiseen, kuten tietojärjestelmien ja laitteiden suojaamiseen verkkoympäristössä. (F-Secure 2023; Järvinen 2018, 14.)

Kuten kuva 1 havainnollistaa, näillä kahdella on siis yhteinen rajapinta, joka suojaa muun muassa digitaalista tietoa ja tietoa käsitteleviä järjestelmiä noudattaen tietoturvan periaatteita ja käyttäen kyberturvallisuuden menetelmiä. Seuraavissa alaluvuissa käsitellään tätä aihealuetta perusteellisemmin.

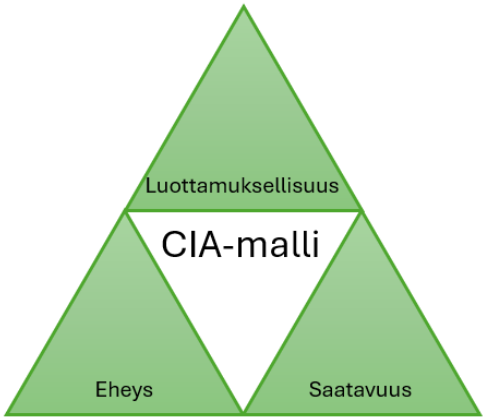


Kuva 1. Tietoturvan, tietotekniikan ja digitaalisen tiedon sekä kyberturvallisuuden suhde mukaillen Venn-diagrammia (mukaillen Ekqvist, Kiuru, Satopää & Vanharanta 2024, 15; Jyväskylän yliopisto s.a)

2.1 Tietoturvan määritelmä

Tietoturvallisuudesta, eli lyhyemmin ilmaistuna tietoturvasta puhuttaessa tarkoitetaan pyrkimystä suojata tietoja, tiedostoja ja yksittäisiä koneita verkkoympäristössä. Muun muassa tiedostojen varmuuskopiointi, ohjelmien päivittäminen sekä käyttöoikeuksien rajoittaminen ja tiedon suojaaminen salasanalla kuuluvat tietoturvan piiriin. (Järvinen 2018, 14; F-Secure 2023.) Tietoturvalla suojataan digitaalisessa muodossa olevan tiedon ja järjestelmien lisäksi myös fyysistä tietoa ja laitteita, sekä varmistetaan, ettei kukaan asiaton pääse suojattuun tietoon käsiksi (F-Secure 2023).

Tietoturvan tavoitteen tiivistämiseen (kuva 2) käytetään usein ilmaisua C-I-A (suomeksi L-E-S), joka muodostuu sanoista confidentiality eli luottamuksellisuus, integrity eli eheys ja availability eli saatavuus. Luottamuksellisuudella tarkoitetaan sitä, että tieto suojataan niin, etteivät ulkopuoliset pääse näkemään tai muokkaamaan tietoa. Eheys merkitsee sitä, että tieto pysyy sellaisena kuin se on tallennettu, niin ettei se muutu esimerkiksi vahingon tai tahallisen teon seurauksena. Saatavuudella tietoturvasta puhuttaessa tarkoitetaan taas sitä, että tieto on saatavilla silloin kun sitä tarvitaan. Saatavuuden takaamiseksi tulee varmistaa laitteiston vikasietoisuus ja kartoittaa esimerkiksi tulipalo- ja vesivahinkoriskit. (Järvinen 2022, 13–15.)



Kuva 2. CIA-malli kuvaa tietoturvan kolmea keskeistä periaatetta eli luottamuksellisuutta, eheyttä ja saatavuutta (Confidentiality, Integrity, Availability) ja niiden suhdetta toisiinsa (mukaillen Ekqvist ym. 2024)

Tietoturvalla pyritään tiivistetysti ilmaistuna siis siihen, että vain tiedon käsittelyyn tai katselemiseen oikeutetut henkilöt pääsevät katselemaan tai muokkaamaan tietoa ilman käyttökatkoja tai -esteitä. Tietoturvan avulla myös varmistetaan, että tieto säilyy sellaisena kuin se on tallennettu, ilman että tieto katoaa tai muuttuu esimerkiksi vahingon tai ulkopuolisen tahon toimien seurauksena. (Järvinen 2022, 13–15.)

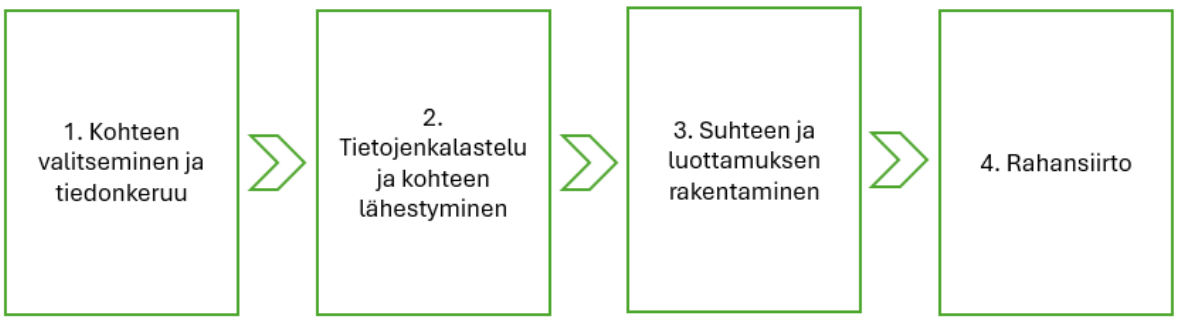
2.2 Kyberturvallisuuden määritelmä

Kyberturvallisuudella tarkoitetaan sitä, että tietoturvaa hyödyntäen suojataan ja varmistetaan kaikkien yhteiskunnan peruspalveluiden toiminta arjessa. Koska kaikki normaalin arjen ylläpitämiseen tarvittavat palvelut, kuten tietoliikenneyhteydet, sähkön ja veden jakelu, liikenteenohjaus, terveydenhuolto, sekä kauppa ja logistiikka, ovat jotenkin sidoksissa tietojärjestelmiin ja -verkkoihin, pienilläkin yhteiskunnan toimivan arjen kannalta kriittiseen infrastruktuuriin kohdistuvilla häiriöillä voi olla suuria, jopa henkeen ja terveyteen kohdistuvia seurauksia. (Järvinen 2018, 14; Järvinen 2022, 16.)

Nykypäivänä tietotekniikkaa käytetään myös välineenä sodankäynnissä, joten kyberturvallisuuden käsite kattaa myös sotilaallisen ulottuvuuden. Koska elintärkeä infrastruktuuri on tietojärjestelmistä riippuvainen, niiden puolustaminen ja suojaaminen ulkoisia uhkia vastaan on vähintään yhtä tärkeää kuin valtion fyysisten rajojen aseellinen puolustaminen. Kyberturvallisuudesta puhuttaessa uhkiksi luetaan myös informaatiovaikuttamisen keinot, joissa tavoitteena on ohjailla kansan yleistä mielipidettä tai toimintaa haluttuun suuntaan. (Järvinen 2018, 14–15.)

3 Yleisimmät organisaation henkilöstöön kohdistuvat kyberuhat

Tässä luvussa keskitytään käymään läpi työn rajauksen mukaisesti niitä kyberuhkia, joissa olennaisena osana on käyttäjän manipuloinnin keinot, ja jotka kohdistuvat organisaation henkilöstöön. Näissä rikollista hyötyä tavoittelevissa menetelmissä yhdistävänä tekijänä on usein se, että usein niissä hyödynnetään manipuloinnin keinoja monipuolisesti yhdistellen. Rikollinen saattaa vedota kohteensa tunteisiin, kuten auttamisenhaluun tai myötätuntoon, tai esimerkiksi johtajaksi tekeytyneenä luoda kiireen tuntua, jonka lisäksi sekoittaa pakkaa vielä lisää painostamalla kohdetta työtehtävässä epäonnistumisen uhalla (Kyberturvallisuuskeskus 2023a).



Kuva 3. BEC-hyökkäyksen vaiheet (mukaillen Fbi s.a.)

On melko tavanomaista, että kehittyneemmissä, kohdennetuissa käyttäjän manipuloinnin hyökkäyksissä yhdistellään manipulaation keinojen lisäksi elementtejä eri hyökkäysmuodoista. Käyttäjän manipuloinnin hyökkäys voi siis olla huolellisesti suunniteltu kokonaisuus (kuva 3), joka saattaa sisältää hyvin perusteellista kohteen tutkimista (vaihe 1), puhelimitse tai sähköpostitse tapahtuvaa tietojenkalastelua ja kohdennettuja tietojenkalasteluviestejä (vaihe 2), manipulointia, uskottavan oloista ja luottamusta herättävää viestittelyä väärennetyillä lähettäjän tiedoilla sekä lähestymistä auktoriteettiasemassa (vaihe 3). (F-Secure 2024a; Fbi s.a.) Hyökkäyksen kaikkien vaiheiden tavoitteena on rahansiirto rikollisen hallinnoimalle tilille (vaihe 4) (Fbi s.a.).

3.1 Tietojenkalastelu (Phishing) ja sen variaatiot

”Perusmuotoisella” tietojenkalastelulla tarkoitetaan usein laajassa mittakaavassa toteutettua rikollisen toimijan toimintaa, jonka pyrkimyksenä erinäisin keinoin kohdettaan, kuten organisaation työntekijää, harhaan johtamalla saada haltuunsa esimerkiksi kohteen käyttäjätunnukset. Näitä haltuunsa saamiaan käyttäjätunnuksia rikollinen käyttää päästäkseen käsiksi arvokkaisiin tietoihin tai

yrityksen järjestelmiin, motiivinaan useimmiten taloudellisen hyödyn saavuttaminen. (Kyberturvallisuuskeskus 2020b, 4.)

Rikollinen saattaa lähestyä kohdettaan esimerkiksi lähettämällä huijausviestin jonkun todellisuudessakin olemassa olevan, mahdollisesti kohteen tunteman tai yleisesti tunnetun, organisaation nimissä. Tämä huijausviesti saattaa olla ulkoasultaan hyvinkin samanlainen, kuin mitä se organisaatio käyttää, jonka taholta rikollinen uskottelee kohdettaan lähestyvänsä. Tällainen viesti saattaa sisältää esimerkiksi jotain kohteen maksuvälineisiin liittyvää tiedustelua pankin nimissä ja vaikkapa linkin väärennetylle verkkopankin kirjautumissivulle. Rikolliset toimijat käyttävät viestihuijauksissaan sähköpostiviestien lisäksi myös muita viestintäkanavia, kuten tekstiviestejä ja eri pikaviestimiä. (Kyberturvallisuuskeskus 2020b, 4.)

Tietojenkalastelua on valeviestien lisäksi myös haitallisten linkkien levittäminen internetsivustoille, kuten sosiaalisen median sivustot. Tietojenkalastelulinkkien avulla pyritään erehdyttämään sivuston käyttäjiä esimerkiksi väärennetylle kirjautumissivulle, pyrkimyksenä saada haltuun huijaussivustolle eksyneen käyttäjätunnukset. (Kyberturvallisuuskeskus 2020b, 4.)

Kun käyttäjä on syöttänyt käyttäjätunnuksensa ja salasanansa oikeaksi luulemallaan sivustolla, on mahdollista että ”kirjautumisen” jälkeen käyttäjä ohjataan sille aidolle sivustolle, jolle käyttäjä alun perinkin olettaa kirjautuneensa. Näin rikollinen pyrkii viimeistelemään tekonsa siten, ettei huijauksen uhri välttämättä edes huomaa tunnustensa joutuneen rikollisen haltuun. (Järvinen 2022, 54.)

Tietojenkalasteluviesteillä pyritään tavoittamaan mahdollisimman suuri joukko potentiaalisia kohteita, joiden kautta rikolliset voivat päästä käsiksi arvokkaisiin tietoihin ja taloudellisiin resursseihin. Tavoitteena on usein saada haltuun esimerkiksi mahdollisimman suuri määrä sähköpostiosoitteita käyttäjätunnuksineen, joiden avulla rikolliset voivat kirjautua tilille ja etsiä esimerkiksi organisaation laskutukseen liittyviä tietoja. Näitä aitoja laskutustietoja hyödynnetään valelaskujen luomiseen, joiden uskottavuutta pyritään parantamaan hyödyntämällä jo olemassa olevia laskuja. Lisäksi rikolliset voivat lähettää kaapatulta tililtä valelaskuja suoraan tilin omistajan kontakteille huijauksen onnistumisen maksimoimiseksi. Varastetuilla käyttäjätunnuksilla on myös mahdollisuus päästä käsiksi yrityssalaisuuksiin, mikä lisää organisaation maine- ja turvallisuusriskejä. Tietojenkalastelun seurauksena voi siis olla taloudellisten menetysten lisäksi myös merkittäviä mainehaittoja ja mahdollisia sanktioita, jos esimerkiksi henkilötietoja vuotaa tunnusten vääriin käsiin joutumisen seurauksena. (Kyberturvallisuuskeskus 2020a, 6; Kyberturvallisuuskeskus 2020b, 4.)

3.1.1 Kohdennettu tietojenkalastelu (Spear Phishing)

Kohdennettu tietojenkalastelu (Spear Phishing, keihäskalastelu) on tietojenkalastelun tarkemmin kohdennettu muoto, jossa rikollinen valitsee kohteensa huolellisesti ja räätälöi huijausviestit

kohteestaan hankkimiensa taustatietojen perusteella. Toisin kuin perinteisessä tietojenkalastelussa, jossa viestejä lähetetään massoittain satunnaisille vastaanottajille, kohdennetun tietojenkalastelun kohde voi olla esimerkiksi jonkin tietyn organisaation henkilöstö tai yksittäinen henkilö tietystä organisaatiosta, kuten esimerkiksi organisaation hallituksen jäsen tai joku vastaava henkilö, jolla on käyttäjätunnukset ja pääsyoikeudet rikollista toimijaa kiinnostavaan tietoon. (Kyberturvallisuuskeskus 2020a, 6; Kyberturvallisuuskeskus 2020b, 4.)

Kohdennetussa tietojenkalastelussa käytetään usein käyttäjän manipuloinnin keinoja ja tarkoituksena on saada kohde uskomaan, että viesti on peräisin luotettavalta taholta. Rikollinen toimija voi esimerkiksi esiintyä kohteen kollegana, esihenkilönä tai tunnettuna palveluntarjoajana, kuten pankin edustajana. (Kyberturvallisuuskeskus 2020b, 4.)

Viestit voivat vaikuttaa tulevan esimerkiksi organisaation sisäisestä sähköpostista tai pankilta. Ne saattavat sisältää haitallisen linkin, jolla kohde ohjataan väärennetylle kirjautumissivulle. Kohde saattaa luulla kirjautuvansa aidolle sivustolle, kuten sähköpostiin tai yrityksen sisäiseen järjestelmään, mutta todellisuudessa hänen käyttäjätunnuksensa ja salasanansa päätyvät rikollisen haltuun. Näin rikollinen voi saada luvattoman pääsyn esimerkiksi organisaation tietojärjestelmiin, mikä voi johtaa tietovuotoihin, taloudellisiin menetyksiin tai järjestelmien manipulointiin. (Järvinen 2022, 54; Kyberturvallisuuskeskus 2020a, 6; Kyberturvallisuuskeskus 2020b, 4.)

Kohdennettu tietojenkalastelu menetelmänä pyrkii hyödyntämään kohteen luottamusta tämän tuntemaan tahoon, jolloin kohde ei välttämättä osaa epäillä viestin aitoutta tai kyseenalaistaa sen sisältöä. Seurauksena kohdennetun tietojenkalastelun kohteeksi joutuneelle organisaatiolle voi aiheutua vakavia tietoturvauhkia, kuten luvattomia järjestelmään tunkeutumisia, yrityssalaisuuksien paljastumisia sekä mahdollisia mainehaittoja. (Kyberturvallisuuskeskus 2020a, 6; Kyberturvallisuuskeskus 2020b, 4.)

3.1.2 Johtotason henkilöön kohdistettu kohdennettu tietojenkalastelu (Whaling)

Whaling-hyökkäys eli ”valastelu” tai ”valaanpyynti” on kohdennetun tietojenkalastelun muoto, jossa hyökkäyksen kohteena on erityisesti organisaation johtotason henkilö, kuten esimerkiksi toimitusjohtaja tai muu organisaatiossa korkeassa asemassa työskentelevä henkilö, eli niin sanottu ”iso kala” (F-Secure 2024b; Microsoft s.a.).

Näille hyökkäyksille on tyypillistä se, että rikolliset näkevät huomattavan paljon vaivaa valitessaan kohdetta ja tehdessään perusteellista taustatutkimusta mahdollisimman vakuuttavan huijausviestin luomiseksi (F-Secure 2024b). Onnistuessaan whaling-hyökkäys voi aiheuttaa organisaatiolle huomattavia taloudellisia menetyksiä sekä mainehaittaa (F-Secure 2024b; Microsoft s.a.).

3.1.3 Huijauspuhelut (Vishing)

Termillä vishing, joka muodostuu englannin kielen sanoista ”voice” ja ”phishing”, tarkoitetaan huijauspuheluita, eli petosmuotoa, jossa rikollinen tekeytyy luotettavaksi tahoksi, kuten esimerkiksi pankin, it-tuen tai työnantajan edustajaksi tavoitteenaan saada organisaation työntekijä paljastamaan arkaluotoista tietoa, kuten käyttäjätunnuksia, salasanoja, pankki- tai henkilötietoja (F-Secure 2024b; F-Secure 2024c). Hyökkäys voidaan kohdistaa esimerkiksi tiettyyn maantieteelliseen alueeseen, jolloin tavoitellaan lisäuskottavuutta esiintymällä esimerkiksi paikallisen pankin nimissä (F-Secure 2024c).

Huijauspuheluissa hyödynnettäviä manipuloinnin keinoja ovat esimerkiksi kiireeseen vetoaminen ja nopeaan toimintaan painostaminen. Uhria saatetaan painostaa esimerkiksi käyttäjätunnusten lukitsemisella, jolloin uhri saattaa langeta toimimaan nopeasti ilman harkintaa. Myös auktoriteettiasemaa hyödynnetään häikäilemättä, rikollinen saattaa lähestyä uhria esimerkiksi viranomaisena tai terveydenhuollon edustajana esiintyen. Huijauspuheluissa on yleistä myös tekniikka, jossa uhrille soitetaan niin lyhyt puhelu, ettei tähän ehdi vastata. Näin uhri houkutellaan soittamaan takaisin numeroon, jolloin puhelusta saattaa tulla kallis lasku. (F-Secure 2024.)

Nykyteknologiaa hyödynnetään myös entistä uskottavampien huijauspuheluiden luomiseen. Soittajana voi siis olla ihan oikea ihminen tai vaihtoehtoisesti puhe voi olla tekstistä puheeksi -ohjelmalla tuotettua tai tekoälyn avulla luotua. (F-Secure 2022a.)

Yleistä huijauspuheluissa on myös se, että rikolliset hyödyntävät teknisiä keinoja väärentääkseen puhelinnumeron tai soittajan tunnuksen. Näin he pyrkivät myös hankaloittamaan käyttämiensä numeroiden jäljittämistä. (F-Secure 2024; Järvinen 2022, 257.)

Rikolliset ovat yleensä saaneet uhrin puhelinnumeron käsiinsä esimerkiksi tietomurron yhteydessä tai tietojenkalastelun avulla. Huijauspuheluita hyödynnetään usein myös osana laajempaa huijausprosessia. (F-Secure 2024c.)

3.1.4 Tekstiviesti- ja pikaviestintietojenkalastelu (Smishing)

Smishing on tietojenkalastelun muoto, jossa rikollinen lähestyy kohdettaan erityisesti tekstiviestin (SMS, Short Message Service) välityksellä, tai pikaviestimien, kuten WhatsApp, Facebook Messenger, Signal tai Telegram, välityksellä (F-Secure 2022b). Termi ”smishing” muodostuu lyhenteestä ”SMS” ja tietojenkalastelua tarkoittavasta termistä ”phishing” (F-Secure 2022a; F-Secure 2022b).

Viestien pyrkimyksenä on saada kohde luovuttamaan arkaluontoista tai henkilökohtaista tietoa, jota hyödynnetään rikollisen hyödyn saavuttamiseen. Viestit voivat myös sisältää esimerkiksi linkin haitalliselle verkkosivustolle tai esimerkiksi pyynnön vahvistaa salasana, luottokorttinumero tai puhelinnumero. (F-Secure 2022b.)

Viestejä voidaan lähettää rikollisen toimesta myös olemassa oleviin viestiketjuihin (F-Secure 2022a; Järvinen 2022, 257). Tällöin viestissä oleva haitallinen linkki tai pyyntö paljastaa arkaluontoista tietoa näyttää tulevan tutulta lähettäjältä (F-Secure 2024b).

Smishing-viesteissä hyödynnetään manipuloinnin keinoja, kuten tunteisiin vetoamista tai kiireen luomista. Uhria voidaan houkutella esimerkiksi palkinnolla, lahjalla tai yllätyksellä, jonka lisäksi häntä painostetaan toimimaan tietyn rajoitetun ajan puitteissa. (F-Secure 2022b.)

Huijaustekstiviestien tunnistaminen voi olla haastavaa, sillä ne pyritään suunnittelemaan niin, että ne jäljittelevät aidon lähettäjän aitoja viestejä. Huijausviestin tunnistamista hankaloittaa myös se, että nykyään tietojenkalasteluviestejä ei välttämättä enää pysty tunnistamaan kömpelöstä kieliasusta tai kirjoitusvirheistä. (F-Secure 2022b.) Uhrin voi olla todella haastavaa tunnistaa rikollisen lähettämä aidon näköinen saapumisilmoitus, joka on lähetetty esimerkiksi Postin tai kuljetuspalvelun nimissä, varsinkin jos viesti vastaanotetaan jo olemassa olevaan viestiketjuun. (F-Secure 2022b; Järvinen 2022, 257.)

Smishing-viesti, jossa uhria lähestytään tekstiviestillä, ei ole niin sanottu perinteinen verkkorikollisuuden muoto, kuten esimerkiksi tietojenkalastelusähköpostit (F-Secure 2022b). Vaikka uhri olisikin valppaana sähköpostitse tapahtuvan tietojenkalastelun varalta, ei hän välttämättä osaa varautua tekstiviestin välityksellä tapahtuvaan tietojenkalasteluun (F-Secure 2022a).

3.2 Toimitusjohtajahuijaus (CEO Fraud) variaatioineen

Toimitusjohtajahuijaus (CEO Fraud) on käyttäjän manipuloinnin keinoja hyödyntävä menetelmä, jossa rikollinen esiintyy organisaatiossa johtotehtävissä tai korkeassa asemassa työskentelevänä henkilönä, kuten toimitusjohtajana, talouspäällikkönä tai organisaation lakiasioista vastaavana henkilönä. (Järvinen 2022, 224.) Rikollinen lähestyy maksutoimeksiannon muodossa organisaation taloushallinnosta tai laskujen maksamisesta vastaavaa henkilöä esimerkiksi sähköpostitse, pyrkien manipuloimaan tätä suorittamaan kiireellisen rahansiirron rikollisen antamilla väärillä maksutiedoilla. (Järvinen 2022, 224; Kyberturvallisuuskeskus 2020b, 4.)

Suurta taloudellista hyötyä tavoittelevat rikolliset tekevät usein huolellista pohjatyötä selvittäessään perusteellisesti organisaation rakennetta sekä tapoja toimia ja kommunikoida. Kun rikollinen on selvittänyt, miten organisaation johtohenkilöt puhuttelevat henkilökuntaa, tai mikä on heidän

tapansa allekirjoittaa viestit, tätä kerättyä tietoa hyödynnetään mahdollisimman vakuuttavan huijausviestin luomisessa. (Järvinen 2022, 224.)

Kun organisaation rakennetta on ensin selvitelty perusteellisesti, huijauksessa on helppo hyödyntää psykologisia keinoja, kuten luottamusta tuttuun henkilöön. Kun viesti näyttää tulevan luotettavaksi oletetulta henkilöltä, kuten esihenkilöltä tai taholta, jonka määräysten noudattaminen kuuluu työnkuvaan, viesti toimii tavallaan kuin käsky, jota noudatetaan kyselemättä. Luotettavaksi tahoksi tekeytymiseen hyödynnetään myös sähköpostiosoitteen väärentämisen mahdollistavaa tekniikkaa, jolloin vastaanottajalle näyttää siltä, että viesti on tullut tutulta lähettäjältä. (Järvinen 2022, 224.) On myös mahdollista, että rikollinen on saanut haltuunsa esittämänsä lähettäjän käyttäjätunnukset ja kaapannut käyttäjätilin, jolloin viesti tulee aidosta osoitteesta (Kyberturvallisuuskeskus 2023a; Rikosuhripäivystys s.a.).

Toimitusjohtajahuijauksissa sähköposti ei siis ole ainoa lähestymistapa, vaan rikollinen voi lähestyä kohdettaan myös esimerkiksi väärennettyä numeroa hyödyntämällä tekstiviestitse. Vastaanottajan laitteessa näyttää siltä, että viestin on lähettänyt tuttu lähettäjä. Koska numero on väärennetty, viesti näkyy vastaanottajan laitteessa samassa viestiketjussa, jossa aikaisemmat aidotkin viestit ovat. (Järvinen 2022, 224.)

Tyypillisesti huijausviesti on huolellisesti muotoiltu vaikuttamaan mahdollisimman aidolta, noudattaen organisaation sisäistä viestintätapaa, kieliasua ja allekirjoituksia (Kyberturvallisuuskeskus 2020b, 4; Rikosuhripäivystys s.a.). Viestissä voidaan esimerkiksi pyytää kiireellistä maksusuoritusta valelaskuun, jossa olevat maksutiedot ohjaavat varat rikollisen hallinnoimalle tilille. Usein viestin sävy on painostava ja viestissä vedotaan esimerkiksi kiireeseen, jotta kohde keskittyy maksun suorittamiseen, eikä niinkään ehdi epäillä viestin aitoutta. (Kyberturvallisuuskeskus 2023a; Rikosuhripäivystys s.a.)

Viestissä voidaan myös vedota luottamuksellisuuteen ja asian salassa pitämiseen. Kohdetta voidaan kehottaa pitämään annettu maksutoimeksianto omana tietonaan, ettei esimerkiksi tieto ”yrityskaupasta” pääse leviämään. (Hyppönen 2021, 113; Järvinen 2022, 224.)

Merkkejä, joista tällaisen huijauksen tunnistaa, ovat edellä mainittujen kiireen luomisen ja luottamuksellisuuteen vetoamisen lisäksi esimerkiksi kehotus ohittaa normaalit varmistusprosessit valelaskua maksaessa, epäilystä herättävä tilinumero tai lähettäjän osoite (Rikosuhripäivystys s.a.).

Rikolliset myös hyödyntävät huijauksissaan johtotehtävissä työskentelevien henkilöiden loma-aikoja, sekä tilanteita, joissa työntekijä vaihtuu. On myös mahdollista, että organisaation avainhenkilöiden aikatauluja tiedustellaan organisaation vaihdepuhelimesta tai assistentilta. Myös esimerkiksi nimitysuutisia seuraamalla rikollinen voi selvittää, milloin uusi johtaja aloittaa, tai johtajan

aikatauluja selvittelemällä varmistaa, että tämä on esimerkiksi lennolla, ja näin ajoittaa hyökkäyksen mahdollisimman otolliseen ajankohtaan, jotta maksutoimeksiannolle ei ole mahdollista saada varmistusta esimerkiksi puhelimitse. (Järvinen 2022, 225.)

Rikolliset myös hyödyntävät hetkiä, jolloin on yleistä, ettei ihminen ole valppaimmillaan, kuten esimerkiksi perjantai-iltapäivät, jolloin monen mieli on jo tulevassa viikonlopussa. Mahdollisesti myös henkilöt, joilta rahasiirtoja tulisi varmistaa, ovat voineet lähteä jo viikonlopun viettoon. Myös vakituisen henkilöstön lomakausi ja näinä aikoina työskentelevät harjoittelijat ja kesätyöntekijät ovat otollinen kohde rikollisille, sillä on mahdollista, että uudet ja kokemattomat työntekijät eivät ole harjaantuneet tunnistamaan mahdollisia huijausyrityksiä. (Järvinen 2022, 225.)

3.3 Valelasku tai laskutushuijaus

Rikollisen lähettämille valelaskuille tyypillistä on, että lasku vaikuttaa päällisin puolin aidoilta ja esimerkiksi yhteistyökumppanin lähettämältä. Tarkemmin silmäiltynä vastaanotetusta valelaskusta kuitenkin käy ilmi, että esimerkiksi laskutettava palvelu tai tuote on sellainen, jota vastaanottaja ei ole koskaan tilannut. Valelaskuja voidaan lähettää massapostituksena, jolloin rikollinen toivoo, että osa vastaanottajista maksaa laskun esimerkiksi epähuomiossa. Jos rikollisen junailema maksutoimeksianto on lähetetty organisaation sisäisesti esimerkiksi vastaanottajan esimiehen nimissä, on yleistä, että maksua pyritään vielä nopeuttamaan kehottamalla maksutoimeksiannon saanutta ohittamaan normaalit vahvistuskäytännöt. (Kyberturvallisuuskeskus 2022.) Valelaskun voi paljastaa myös edellisestä vastaanotetusta laskusta poikkeava, muuttunut tilinumero (Järvinen 2022, 243). Näissä tapauksissa muutetut maksutiedot ohjaavat maksut rikollisen hallinnoimalle tilille (Kyberturvallisuuskeskus 2020c).

Rikollinen voi myös ottaa yhteyttä organisaatioon palveluntarjoajan tai yhteistyökumppanin nimissä, ja pyytää muutosta laskutustietoihin, kuten esimerkiksi tilinumeroon (Kyberturvallisuuskeskus 2020b). Yhteydenotto voi tapahtua sähköpostin lisäksi esimerkiksi puhelimitse tai kirjeitse (Kyberturvallisuuskeskus 2020c).

3.4 Sähköpostihuijaus eli BEC-huijaus (BEC-fraud, BEC-scam)

BEC-huijauksella (Business E-mail Compromise, BEC-fraud, BEC-scam) tarkoitetaan huijauksia, jotka tehdään pääsääntöisesti murretun sähköpostitilin avulla. Rikollinen lähettää murretulta tililtä esimerkiksi talousosastolle vilpillisen maksutoimeksiannon. (Hyppönen 2021, 110; Järvinen 2022, 226.) BEC-huijauksen ydinajatuksena on löytää organisaatiosta muun muassa sähköpostiliikennettä seuraamalla ne henkilöt, joiden vastuulla on organisaation rahaliikenne. Sähköpostiliikenteen seuraamisen lisäksi rikolliset hyödyntävät hyökkäystä valmistellessaan avainhenkilöiden

henkilöllisyyden kartoittamisessa esimerkiksi LinkedIniä ja internetissä olevia rekrytointi-ilmoituksia. (Hyppönen 110–111.)

Perusteellisen selvitystyön jälkeen rikolliset lähestyvät kohdettaan esimerkiksi toimitusjohtajan, talousjohtajan tai hallituksen jäsenen roolissa esiintyen, joko sähköpostitse tai puhelimitse (Hyppönen 2021, 111). On myös mahdollista, että rikollinen lähestyy talousasioista vastaavaa organisaation työntekijää yhteistyökumppanin nimissä (Kyberturvallisuuskeskus 2022).

Sähköpostitse lähetetyn vilpillisen maksutoimeksiannon uskottavuutta voidaan pyrkiä tehostamaan sähköpostiviestien lisäksi uskottavan kuuloisen henkilön soittamalla puhelulla (Kyberturvallisuuskeskus 2022).

Rikolliset tavoittelevat BEC-hyökkäyksissä yleensä mahdollisimman suurta taloudellista hyötyä, mutta ei ole tavatonta, että hyökkäyksen kohteeksi joutuu myös pienempi organisaatio (Järvinen 2022, 226).

Onnistuneissa huijauksissa taloudelliset menetykset ovat usein huomattavan suuria. Rikolliset panostavat BEC-huijaukseen tekemällä valmisteluja jopa useiden viikkojen ajan. (Hyppönen 2021, 111.) Manipulaation keinoja ei säästellä, vaan kohteen harkintakykyä pyritään heikentämään vetoamalla tunteisiin, luomalla kiirettä ja hyödyntämällä auktoriteettiasemaa (Kyberturvallisuuskeskus 2022).

Viesteissä voidaan käyttää tehokeinoina aggressiivisuutta tai suostuttelua, sekä kiireelliseen, ulkopuoliselle taholle suoritettavaan maksusuoritukseen painostamista (Hyppönen 2021, 111). Maksutoimeksiannon yhteydessä voidaan myös ilmaista melko painokkaastikin, esimerkiksi sisäpiirilistalle lisäämiseen vedoten, ettei maksutoimeksiannosta saa puhua edes kollegoille (Hyppönen 2021, 113).

Myös ajankohta pyritään valitsemaan näissä huijauksissa tarkasti, ja huijauksissa hyödynnetäänkin esimerkiksi loma-aikoja (Kyberturvallisuuskeskus 2022).

Järvinen (2022) kertoo eräästä tapauksesta, jossa rikolliset aloittivat selvittelytyön murtauduttuaan erään organisaation työntekijän sähköpostitilille. He selvittivät, millaisia yrityksen sisäiset käytännöt ovat, jonka jälkeen he loivat valheellisen, tavarantilausta koskevan viestiketjun toimitusvahvistuksineen. Viestiketju sisälsi aidon näköiset asiakirjat tilausprosessista. Tämän jälkeen viestiketju toimitettiin talousosastolle, liitteenään viesti, että ostolasku tulisi maksaa, jotta tilaus lähtisi liikkeelle. Toinen maksun hyväksyneistä henkilöistä oli hyökkäyksen kohteena olleen organisaation talouspäällikkö. (Järvinen 2022, 227.)

Jälkeenpäin huijauksen kohteeksi joutuneessa organisaatiossa huomattiin, että maksuun liittyvät asiakirjat ja tapahtumien kokonaisuus sisälsivät piirteitä, joiden olisi pitänyt herättää epäilys. Näitä epäilyttäviä merkkejä olivat tilinumero, joka ei toiminut, jolloin se piti vaihtaa. Tilinumeron toimimattomuutta perusteltiin käynnissä olevalla tilintarkastuksella. Myös tilauksessa olleet tavarantoimittajien nimet olivat outoja ja maksua pyrittiin jouduttamaan erilaisilla verukkeilla. (Järvinen 2022, 227.)

Toinen BEC-huijauksen kulkua hyvin kuvaava esimerkkitapaus liittyi Järvisen (2022) mukaan erääseen asiantuntijaorganisaatioon, jonka taloushallinnon palvelut oli ostettu tilitoimistolta. Organisaation laskut toimitettiin tilitoimistolle, joka tiliöi laskut ja siirsi ne maksuohjelmaan, josta asiakasorganisaation maksuista vastaava taho kävi hyväksymässä laskut maksuohjelmasta maksuun. (Järvinen 2022, 228.)

Tammikuussa 2019 asiakasorganisaation johtajien sähköpostiosoitteesta oli tullut tilitoimistolle ulkomaalaisia ostolaskuja noin 700 000 euron arvosta. Tilitoimistossa työskentelevä kirjanpitäjä varmisti asiakasorganisaation edustajalta epätavallisten laskujen oikeellisuuden. Asiakasorganisaation edustaja vahvisti laskut oikeiksi. Saamansa vahvistuksen jälkeen kirjanpitäjä siirsi kyseiset laskut järjestelmään, jossa maksut hyväksyttiin johtajien tunnuksilla. (Järvinen 2022, 228.)

Tapauksessa kävi myöhemmin ilmi, että rikolliset olivat murtautuneet organisaation johtotason henkilöiden sähköpostitileille ja käyttäneet murrettuja tilejä tilitoimiston kanssa viestittelyyn. Tapauksen aikaan käytössä ollut maksuohjelmisto oli lähettänyt vieraasta IP-osoitteesta kirjautumista koskevia varoitusviestejä johtajien sähköpostiin, mutta rikolliset olivat ohjanneet viestit kansioon, josta ei aktiivisesti seurattu saapuneita viestejä. Tähän samaiseen kansioon oli ohjattu myös tilitoimiston lähettämät vahvistuspyynnöt, joihin rikolliset olivat myös vastanneet organisaation johtajien nimissä. (Järvinen 2022, 228.)

4 Tutkimuksen toteutus

Tässä luvussa kuvataan opinnäytetyön tutkimusmenetelmä, aineiston hakuprosessi ja valintaperusteet sekä analysoinnin menetelmät. Opinnäytetyö toteutetaan narratiivisena kirjallisuuskatsauksena, jonka tavoitteena on kartoittaa ja analysoida kohdennettuja käyttäjän manipuloinnin keinoja osana organisaation työntekijään kohdistuvia kyberuhkia. Tutkimuksessa selvitetään miksi nämä kyberuhkat ovat niin vaarallisia, mitä psykologisia keinoja niissä hyödynnetään, ja miksi hyökkäykset onnistuvat koulutuksesta ja tietoisuudesta huolimatta. Tutkimuksessa myös kartoitetaan, mistä elementeistä nämä hyökkäykset koostuvat.

Narratiivinen kirjallisuuskatsaus valikoitui tutkimusmenetelmäksi, koska sitä hyödyntämällä on mahdollista muodostaa ajankohtainen kokonaiskuva tutkittavasta ilmiöstä hyödyntämällä aiheesta aiemmin tehtyjä tutkimuksia. Aikaisempien tutkimusten tuloksia yhdistämällä on myös mahdollista tehdä aihealueesta uusia johtopäätöksiä, sekä havaita jatkotutkimuksen tarpeita.

Tutkimusprosessin läpinäkyvyyden varmistamiseksi luvussa käsitellään aineiston valintakriteerit, rajaukset ja analysointitavat, jotta tutkimuksen luotettavuutta ja toistettavuutta voidaan arvioida.

4.1 Tutkimusmenetelmän kuvaus

Tämän työn tutkimusmenetelmäksi on valittu narratiivinen kirjallisuuskatsaus (engl. narrative review). Kyseisestä menetelmästä käytetään myös nimitystä kuvaileva kirjallisuuskatsaus (Vilkka 2023, luku 1.2.1).

Narratiivinen kirjallisuuskatsaus on yksi traditionaalisista katsaustyypeistä. Menetelmän käytössä tavoitteena ei ole ensisijaisesti selvittää ilmiön yleisyyttä, vaan kartoittaa, mitä ilmiöstä on jo aikaisemmin tutkittu, mitkä ovat sen keskeiset käsitteet ja millaisia yhteyksiä näiden käsitteiden välillä on. (Vilkka 2023, luku 1.2.1.)

Narratiivisen kirjallisuuskatsauksen avulla voidaan tarkastella aiheen historiallista kehitystä, sekä kuvata tutkimusasetelmia ja teorioita, joita on käytetty aiemmissa tutkimuksissa. Menetelmää voidaan hyödyntää paitsi aiempien tutkimusten tiivistämiseen, myös uuden kokonaisnäkemyksen muodostamiseen hajanaisesta tiedosta. Se auttaa jäsentämään epäyhtenäistä tietoa johdonmukaiseksi kokonaisuudeksi. Lisäksi narratiivinen kirjallisuuskatsaus tarjoaa kattavan yleiskuvan käsiteltävästä ilmiöstä ja sen tutkimuksellisesta tilasta, minkä myötä voidaan tunnistaa myös mahdollisia jatkotutkimuksen tarpeita. (Vilkka 2023, luku 1.2.1; Salminen 2023, 8.)

Kirjallisuuskatsaus on tutkimusmenetelmä, jossa aineistona käytetään aiemmin toteutettuja tutkimuksia (Vilkka 2023, luku 1.1.1). Vaikka kuvaileva kirjallisuuskatsaus ei tarjoa analyyttisintä

tulosta, tutkimuskysymysten avulla on mahdollista muodostaa tutkittavasta aiheesta ajantasainen kokonaiskuva (kriittisesti tarkasteltu synteesi), jonka muodostaminen ei aina ole mahdollista pelkästään tieteellisen kirjallisuuden pohjalta (Vilkka 2023, luku 1.1.1; Salminen 2023, 9).

Kuvailevan kirjallisuuskatsauksen johtopäätökset pohjautuvat alkuperäiseen korkealaatuiseen tutkimustyöhön. Kuvaileva kirjallisuuskatsaus tunnistaa, arvioi ja tiivistää asiantuntijoiden laatiman valmiin ja jo julkaistun tutkimusaineiston, joten menetelmänä se on systemaattinen, täsmällinen ja toistettavissa oleva. (Salminen 2023, 4.)

4.2 Tutkimusaineiston haku ja valintakriteerit

Aineiston haussa hyödynnettiin HH Finnan artikkelihakua. Hakusanoina käytettiin seuraavia yhdistelmiä: ”BEC fraud”, ” Business Email Compromise”, ”social engineering cyber threats”, ja ”social engineering psychological cyber threat”. Lisäksi haetut artikkelit rajattiin vertaisarvioituihin artikkeleihin, jotka on julkaistu vuoden 2020 jälkeen. Näin pyrittiin varmistamaan, että käytetty aineisto on mahdollisimman tuoretta.

Artikkeleita valittaessa luettiin tiivistelmä, sekä silmäiltiin otsikot ja artikkeli läpi, jotta voitiin varmistaa, että artikkeli käsittelee tutkimuskysymysten rajaamaa aihetta ja vastaa tutkimuskysymyksiin syvällisesti.

Aineistoon valittiin neljä tutkimusta, jotka käsittelevät käyttäjän manipuloinnin määrittelyä, sekä hyökkäysten psykologista puolta, sekä kaksi tutkimusta, jotka keskittyvät BEC-hyökkäyksiin. Näin pyrittiin varmistamaan, että ensinnäkin kirjallisuuskatsauksessa käytettävä materiaali vastaa tutkimuskysymyksiin, sekä toiseksi, että käyttäjän manipuloinnin hyökkäyksestä kokonaisuutena saadaan mahdollisimman kokonaisvaltainen ja syvällinen ymmärrys. BEC-hyökkäys hyökkäysmenetelmänä valikoitui katsauksessa tarkemmin läpikäytäväksi sen vaarallisuuden ja ajankohtaisuuden vuoksi, sekä myös sen vuoksi, että tietoperustaa kootessa ja materiaaliin perehtyessä juuri BEC-hyökkäyksistä ei löytynyt kovin paljoa julkaistua, yhtenäistä tietokirjallisuutta. BEC-hyökkäys on kokonaisuus, joka yleensä muodostuu useammasta käyttäjän manipuloinnin menetelmästä, joten myös tästä syystä se oli hyvä valinta, kun tarkoituksena oli tarkastella kehittyneemmän, kohdennetun käyttäjän manipuloinnin hyökkäyksen rakennetta.

5 Tulokset

Tässä luvussa käydään läpi havainnot, joita tutkimusaineistosta tehtiin tutkimuskysymysten perusteella tietoperustan luvussa 3 esiteltyihin käyttäjän manipuloinnin kyberuhkiin peilaten. Näiden havaintojen perusteella on todettavissa, että ihmisellä on useita psykologisia piirteitä, joita voidaan pitää kyberturvallisuuden kontekstissa haavoittuvuuksina.

Luvussa avataan lukijalle termin ”käyttäjän manipulointi” määritelmä hieman pintaa syvemmältä. Kirjallisuuskatsaukseen valituissa tutkimuksissa oli hyödynnetty myös joitain melko tunnettuja psykologisia luokitteluja ja viitekehyksiä, kuten esimerkiksi persoonallisuustyyppien ”peruselementtejä” kuvaava Big Five-luokittelu, sekä Cialdinin kuusi vaikuttamisen periaatetta. Näistä molemmista viitekehyksistä on hyötyä, kun määritellään lähestymistapoja, joilla voidaan tehokkaimmin vaikuttaa kullekin persoonallisuustyypille ominaisiin piirteisiin, eli myös näitä molempia viitekehyksiä avataan lukijalle tässä luvussa.

5.1 Käyttäjän manipulointi – määritelmä

Kyberturvallisuuden kontekstissa käyttäjän manipulointi on monitieteinen tutkimusalue, joka yhdistää muun muassa tietojenkäsittelytieteen, kyberturvallisuuden, psykologian, sosiaalipsykologian, kognitiotieteen, neurotieteen ja aivotutkimuksen näkökulmia (Wang ym. 2021, 11906).

Käyttäjän manipulointi on toimintaa, jossa manipulaation, vaikuttamisen ja petoksen avulla pyritään saamaan henkilö, joka on usein organisaation työntekijä, suostumaan pyyntöön, johon yleensä liittyy tiedon luovuttamista tai jonkin toimenpiteen suorittaminen hyökkääjän eduksi. Käyttäjän manipulointi voi olla jotakin niin yksinkertaista kuin puhelinkeskustelu, tai paljon monimutkaisempaa, kuten teknistä haavoittuvuutta hyödyntävällä verkkosivulla vierailu, jonka seurauksena hyökkääjä saa pääsyn tietokoneelle. (Wang ym. 2020, 85099.)

Käyttäjän manipuloinnin hyökkäys voi siis olla yksinkertainen puhelinsoitto, jossa esiinnytään sisäpiiriläisenä ja saadaan haluttu tieto ilman, että tarvitsee ohittaa virustorjuntaohjelmia tai murtaa palomuureja teknisellä osaamisella. Toisaalta hyökkäys voi olla myös kehittyneempi, tehokkaampi ja aggressiivisempi, kun siihen yhdistetään uutta teknologiaa ja kehittyneitä uhkia. (Wang ym. 2020, 85103.)

Kyberturvallisuuden kontekstissa käyttäjän manipulointi on kohteen inhimillisten haavoittuvuuksien, kuten hyväuskoisuuden, uteliaisuuden, mukautuvuuden, ahneuden, laiskuuden, intuitiivisen päätöksenteon ja automaattisten toimintamallien, hyväksikäyttöä (Wang ym. 2020. 85106).

5.2 Big Five – persoonallisuuspiirteet haavoittuvuuksina

Big Five -mallia voidaan kuvata persoonallisuuspiirteiden ”perustana”. Mallissa on määritelty ihmisen perustavanlaatuiset psykologiset piirteet, joita voidaan hyödyntää esimerkiksi psykologisten haavoittuvuuksien kartoittamisessa kyberturvallisuuden kontekstissa.

Big Five -piirteet muodostavat laajasti tutkitun ja käytetyn mallin ihmisen persoonallisuuserojen ymmärtämiseksi. Big Five -malli tarjoaa vahvan psykologisen viitekehyksen käyttäjän manipuloinnin hyökkäyksissä hyödynnettävien psykologisten haavoittuvuuksien kartoittamiseen. (Longtchi ym. 2024, 215.)

Nämä persoonallisuuden piirteet kuvaavat yksilöiden ainutlaatuisuutta ja erilaisuutta persoonallisuuspiirteidensä osalta. Esimerkiksi toiset ihmiset ovat tavallisesti tarkempia ja huolellisempia yksityiskohtien suhteen kuin toiset, ja jotkut ihmiset ovat taas varovaisempia kuin toiset. (Longtchi ym. 2024, 218.)

Big Five -mallia on käytetty ihmisen persoonallisuuden perustan ja käyttäytymisen tutkimisessa eri kielissä ja kulttuureissa vuosikymmenten ajan, joten viitekehystä voidaan pitää luotettavana välineenä, kun tutkitaan persoonallisuuspiirteiden vaikutusta ihmisten haavoittuvuuteen käyttäjän manipuloinnin hyökkäysten yhteydessä (Longtchi ym. 2024, 215).

Big Five -mallin mukaan persoonallisuuden peruspiirteet ovat ”Avoimuus”, ”Tunnollisuus”, ”Ekstroversio”, ”Sovinnollisuus” ja ”Neuroottisuus” (Longtchi ym. 2024, 214–215).

Avoimuus (*Opennes*) viittaa yksilön aktiiviseen mielikuvitukseen ja mielenkiintoon uusia ideoita tai asioita kohtaan (Longtchi ym. 2024, 215). Avoimuudella kuvataan yksilön aktiivista mielikuvitusta ja oivalluksia. Voimakkaasti avoimia piirteitä omaavat yksilöt ovat usein uteliaita maailmaa ja muita ihmisiä kohtaan. He ovat innokkaita oppimaan uusia asioita, nauttivat uusista kokemuksista ja ovat seikkailunhaluisia ja luovia. Voimakkaasti avoin yksilö on erityisen altis phishing-hyökkäyksille. (Longtchi ym. 2024, 219.)

Persoonallisuudeltaan avoimet yksilöt ovat avoimia uusille kokemuksille. Käyttäjän manipuloinnin hyökkäyksissä he ovat muita alttiimpia (perifeeriselle) suostuttelulle, tunteisiin vetoamiselle ja kognitiivista dissonanssia, eli sisäistä ristiriitaa hyödyntäville vaikutusmekanismeille. (Wang ym. 2021, 11904.)

Tunnollisuus (*Conscientiousness*) viittaa yksilön harkitsevaisuuteen, impulssikontrolliin ja tavoitteelliseen käyttäytymiseen (Longtchi ym. 2024, 215). Tunnollisuudella kuvataan yksilön taipumusta ajatteluun, impulssien hallintaan ja tavoiteorientoitunutta käytöstä. Korkean määrän tunnollisuutta

omaavat yksilöt ovat yleensä järjestelmällisiä, tarkkoja yksityiskohtien suhteen, itsekurin omaavia, tavoiteorientoituneita ja taitavia suunnittelijoita. Tunnollinen yksilö huomioi myös oman käytöksensä vaikutukset muihin ihmisiin. On myös olemassa tutkimus, jonka tulokset osoittavat, että erittäin tunnolliset ihmiset ovat vähemmän alttiita spear phishing -hyökkäyksille. (Longtchi ym. 2024, 219.)

Persoonallisuudeltaan tunnolliset yksilöt saattavat olla alttiimpia käyttäjän manipuloinnin hyökkäyksissä muun muassa vastuullisuuteen, sitoutumiseen ja johdonmukaisuuteen vetoaville, sekä auktoriteettia hyödyntäville vaikutusmekanismeille (Wang ym. 2021, 11904).

Ekstroversio (*Extraversion*) viittaa siihen, kuinka sosiaalinen, määrätietoinen, puhelias ja tunteitaan ilmaiseva yksilö on (Longtchi ym. 2024, 215). Ekstroversiolla kuvataan yksilön taipumusta olla sosiaalinen, itsetietoinen, puhelias ja tunteitaan ilmaiseva. Korkean määrän ekstroversion piirteitä omaava yksilö on ulospäin suuntautunut ja saa energiaa sosiaalisista tilanteista. On olemassa tutkimus, joka osoittaa, että ekstroversio, avoimuus ja taipumus sovinnollisuuteen lisäävät yksilön alttiutta phishing-sähköposteille. (Longtchi ym. 2024, 219.)

Persoonallisuudeltaan ulospäinsuuntautuneet yksilöt ovat alttiimpia käyttäjän manipuloinnin hyökkäyksissä muun muassa samankaltaisuuden, miellyttävyyden ja mukautuvuuden vaikutusmekanismeille (Wang ym. 2021, 11904).

Sovinnollisuus (*Agreeableness*) viittaa yksilön luottamukseen sidoksissa oleviin tekijöihin, altruismiin, ystävällisyyteen, hellyyteen ja prososiaalisiin (muut huomioiva, empaattinen) käyttäytymismalleihin (Longtchi ym. 2024, 215). Sovinnollisuudella (tai mukautuvuudella) kuvataan yksilön piirteitä, jotka liittyvät luottamukseen, altruismiin, ystävällisyyteen, kiintymykseen ja muihin prososiaalisiin käytösmalleihin. Eräs tutkimus osoittaa, että korkea määrä sovinnollisuuteen pyrkiviä piirteitä tekee ihmisistä alttiita phishing-hyökkäyksille. (Longtchi ym. 2024, 219.)

Persoonallisuudeltaan sovinnollisuuteen taipuvaiset yksilöt ovat käyttäjän manipuloinnissa alttiita muun muassa ryhmävaikutusta, sosiaalista validointia, vastavuoroisuutta, sekä ”jalka oven väliin”-tekniikkaa hyödyntäville vaikutusmekanismeille (Wang ym. 2021, 11904).

Neuroottisuus (*Neuroticism*) viittaa yksilön taipumukseen mielialanvaihteluihin ja emotionaaliseen epävakauteen (Longtchi ym. 2024, 215). Neuroottisuudella kuvataan yksilön mielialaa ja emotionaalista epävakautta. Korkean neuroottisuuden omaavat henkilöt kokevat usein mielialanvaihteluita, ahdistusta, ärtyneisyyttä ja surullisuutta. Korkea neuroottisuus tekee yksilöistä alttiimpia phishing-hyökkäyksille. (Longtchi ym. 2024, 219.)

Persoonallisuudessaan korkean neuroottisuuden omaavat yksilöt ovat käyttäjän manipuloinnin hyökkäyksissä alttiimpia pelkoa herättäville, arvioinnin pelkoa, vastuuntunnon hajaantumista ja deindividuaatiota (yksilöllisuuden tunteen menettäminen ryhmässä) hyödyntäville vaikutusmekanismeille (Wang ym. 2021, 11904).

5.3 Cialdinin kuusi vaikuttamisen periaatetta – psykologiset menetelmät verkkorikollisen aseena

Robert B. Cialdini on määritellyt kuusi vaikuttamisen periaatetta, joita voidaan hyödyntää vaikuttamisen ja manipulaation välineenä, kun pyritään ohjailemaan ihmistä toimimaan automaattisesti ja ilman tietoista harkintaa (Cialdini 2009, Introduction).

Vaikka suostuttelun ammattilaiset käyttävät tuhansia eri taktiikoita saadakseen ihmiset suostumaan, voidaan sanoa, että suurin osa näistä suostuttelutekniikoista kuuluu Cialdinin määritelmän mukaisesti kuuteen peruskategoriaan. Jokaisessa kategoriassa on perustavanlaatuinen psykologinen periaate, joka ohjaa ihmisen käyttäytymistä ja tekee niihin vetoavista suostuttelutaktiikoista tehokkaita. (Cialdini 2009, Introduction.)

Cialdinin kuusi vaikuttamisen periaatetta ovat ”Pitäminen” (Liking), ”Vastavuoroisuus” (Reciprocity), ”Ryhmään mukautuminen ja muiden seuraaminen” (Social Proof), ”Sitoutuminen ja johdonmukaisuus” (Commitment and Consistency), ”Auktoriteetti” (Authority) ja ”Niukkuus” (Scarcity) (Longtchi ym. 2024, 214).

Nämä psykologisiin tekijöihin vaikuttamisen periaatteet ovat vakiintuneet tutkimuskäytössä, erityisesti myynnin ja markkinoinnin kontekstissa. Ne ovat relevantteja myös käyttäjän manipuloinnin kontekstissa, sillä hyökkäyksissä hyödynnetään suostuttelun keinoja laajasti. (Longtchi ym. 2024, 214.)

Cialdinin määritelmän mukaiset kuusi vaikuttamisen periaatetta määritellään seuraavasti:

- **Pitäminen** (*Liking*) – Yksilö pitää helpommin henkilöstä, jota hän pitää miellyttävänä tai jolla on yhteisiä uskomuksia (Longtchi ym. 2024, 214).
- **Vastavuoroisuus** (*Reciprocity*) – Yksilö saattaa tuntea tarvetta maksamaan takaisin saamansa palvelus (Longtchi ym. 2024, 214).
- **Ryhmään mukautuminen, muiden seuraaminen** (*Social Proof*) – Yksilöllä on tarve mukautua ryhmään tai seurata muiden näyttämää esimerkkiä (Longtchi ym. 2024, 214).
- **Sitoutuminen ja johdonmukaisuus** (*Commitment and Consistency*) – Yksilöllä on tarve toimia johdonmukaisesti sekä pysyä aiemmin antamassaan lupauksessa (Longtchi ym. 2024, 214).

- **Auktoriteetti** (*Authority*) – Yksilö on taipuvainen noudattamaan asiantuntijan tai ylemmän tahon toimintakehotusta (Longtchi ym. 2024, 214).
- **Niukkuus** (*Scarcity*) – Yksilö arvostaa asioita, jotka ovat harvinaisia, joiden saatavuus on rajoitettu tai joita on vain vähän tarjolla (Longtchi ym. 2024, 214).

5.4 Mitkä psykologiset tekijät voidaan nähdä haavoittuvuuksina kyberturvallisuuden kontekstissa?

Tässä alaluvussa vastataan ensimmäiseen tutkimuskysymykseen, jonka avulla pyrittiin kartoittamaan yksilön psykologisia piirteitä tai toimintamalleja, sekä inhimillisiä tekijöitä, jotka voidaan nähdä kyberturvallisuuden näkökulmasta käyttäjän manipuloinnin hyökkäyksessä hyödynnettävinä haavoittuvuuksina. Havaintojen tekemisen viitekehyksenä on käytetty tietoperustan luvussa 3 käsiteltyjä käyttäjän manipuloinnin uhkia.

Kyberturvallisuuden kontekstissa jotkin liialliset tai väärässä tilanteessa ilmenevät yksilölliset positiiviset ominaisuudet voivat johtaa negatiivisiin seurauksiin. Yksilölliset piirteet, kuten muun muassa ystävällisyys, hyväntahtoisuus, nöyryys, kohteliaisuus, ujous, välinpitämättömyys, ylimielisyys tai kateus voivat siis muodostua käyttäjän manipuloinnin hyökkäyksissä hyödynnettäväksi haavoittuvuudeksi. (Wang ym. 2021, 11904.)

Kyberturvallisuuden kontekstissa yksilön haavoittuvuuksien hyväksikäyttö on käyttäjän manipuloinnin (social engineering) olennainen ominaisuus. Riippumatta käytetyistä menetelmistä tai taidoista, hyökkääjät hyödyntävät jossain määrin ihmisen haavoittuvuutta, jotta hyökkäys lopulta onnistuisi. (Wang ym. 2020, 85106.)

Huolellisesti valmisteltu käyttäjän manipuloinnin hyökkäys voi onnistua jopa niiden keskuudessa, jotka pitävät itseään tietoisina käyttäjän manipuloinnin tekniikoista, puhumattakaan käyttäjistä, joilla on alhainen tietoturvatietoisuus. Sosiaalisissa verkostoissa ja internetissä oleva runsas taustatieto voidaan vapaasti kerätä tarkkojen kohteiden kartoittamiseksi ja kohdistetun käyttäjän manipuloinnin hyökkäyksen valmistelemiseksi. (Wang ym. 2020, 85102.)

Huolellisesti suunnitellulla ja oikeaan aikaan ajoitetulla viestillä on mahdollista saada käytännössä kuka tahansa klikkaamaan vaarallista linkkiä, sillä jokainen ihminen on jostakin asiasta utelias, kiinnostunut, tai sellaisessa elämäntilanteessa, että viestin sisältö ja konteksti osuvat kohdalleen (Wang ym. 2020, 85102).

5.4.1 Välinpitämättömyys

Välinpitämättömyys (Individual indifference) kuvaa yksilön mielenkiinnon puutetta jotakin tehtävää kohtaan. Eräs tutkimus osoittaa, että pitkäkestoinen välinpitämättömyys turvallisuutta kohtaan voi synnyttää riskialttiin toimintakulttuurin, joka voi olla altis käyttäjän manipuloinnin hyökkäyksille. Tämä tutkimus osoittaa myös, että organisaatioissa esiintyy vaihtelevia käsityksiä kyberturvallisuuden tärkeydestä. Tämä näkyy työntekijöiden, mukaan lukien johdon ja joskus jopa myös turvallisuushenkilöstön, välinpitämättömyytenä kyberturvallisuuden käytäntöjä ja toimintatapoja kohtaan. (Longtchi ym. 2024, 219.)

Kun työntekijä on välinpitämätön työnsä suhteen, tulee eteen haasteita esimerkiksi tietoturvan osalta, varsinkin silloin kun tietoturvan saralla ”oikaistaan” käytännöissä ja turvatoimia ei noudateta (Wang ym. 2021, 11903). Välinpitämättömät ihmiset eivät välttämättä ole kiinnostuneita turvallisuusriskeistä (Wang ym. 2021, 11904).

5.4.2 Kyberturvallisuuden kannalta kyseenalainen asennoituminen

Piittaamattomuus säännöistä (Freewheeling) kuvaa yksilön halukkuutta ohittaa sääntöjä tai käytäntöjä, sekä taipumusta toimia rajoituksetta tai estoitta. Tällainen käytös voi lisätä alttiutta käyttäjän manipuloinnin hyökkäyksille. Erään raportin mukaan kyberrikolliset voivat toimia säännöistä piittaamatta kehitellessään innovatiivisia hyökkäyksiä, kun taas puolustavalla osapuolella ei ole samaa vapautta byrokratian ja sääntöjen vuoksi. Tämä tarkoittaa sitä, että liian huoleton suhtautuminen puolustuksen puolella saattaa vahingossa altistaa organisaation kyberhyökkäyksille. (Longtchi ym. 2024, 219.)

Ylimielinen yksilö saattaa olla välinpitämätön turvallisuuspolitiikan suhteen (Wang ym. 2021, 11904). Liikaa omiin toiveisiinsa keskittyvä *itsekeskeinen* yksilö on alttiimpi manipuloinnille ja voi tehdä heikkoja päätöksiä (Wang ym. 2021, 11903).

Riskiä voi lisätä myös *liiallinen luottaminen itseen,* eli yksilön taipumus olla liiankin varma itsestään ja erityisesti kyvystään havaita tietojenkalastelua. Tilannetta voidaan korjata koulutuksen ja harjoittelun avulla. Tämä psykologinen piirre voi korreloida itseluottamuksen kanssa. (Longtchi ym. 2024, 221.)

Laiskuudella tarkoitetaan sitä, että henkilö voi olla haluton tekemään tarvittavaa työtä tai näkemään vaivaa estääkseen turvallisuusuhan (Wang ym. 2021, 11903). Yksilö osoittaa siis vapaaehtoista haluttomuutta käyttää vaadittua määrää energiaa, jotta saisi tehtävänsä suoritettua. Eräs tutkimus osoittaa, että laiskuus tekee ihmisestä haluttoman tekemään tarvittavaa työtä, tai näkemään vaivaa

pienentääkseen riskejä. Tämä lisää alttiutta käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 220.)

Tottelemattomuus kuvaa henkilön haluttomuutta totella auktoriteettia tai noudattaa sääntöjä. Tämä voi altistaa käyttäjän manipuloinnin hyökkäyksille. Vaikka yleisesti tiedetään, että luottavaiset ja tottelevaiset ihmiset ovat alttiimpia käyttäjän manipuloinnin hyökkäyksille, on vähemmän tunnettu tieto, että myös yksilön tietoista tottelemattomuutta voidaan hyödyntää hyökkäyksissä. (Longtchi ym. 2024, 218.)

5.4.3 Tietoisuuden puute ja inhimilliset tekijät

Tietoisuuden puute, eli tilanne, jossa työntekijällä ei ole tietämystä arkaluontoisen tiedon arvosta tai turvallisuudesta, on riski turvallisuuden kannalta. Sekä tietoisuuden puute että kokemattomuus lisäävät turvallisuusriskiä. (Wang ym. 2021, 11903.)

Kun yksilö ei kiinnitä tarpeeksi huomiota tietoturvaympäristöön tai mieti mahdollisia turvallisuusriskejä, puhutaan *huolimattomuudesta* tai *ajattelemattomuudesta* (Wang ym. 2021, 11903).

Huolimattomuus kuvaa tilannetta, jossa henkilö epäonnistuu tehtävänsä asianmukaisessa suorittamisessa, aiheuttaen tietomurron (security breach). Erään tutkimuksen mukaan 27% tietomurroista johtuu työntekijän tai alihankkijan huolimattomuudesta, etenkin kun kyseessä on etäyhteys organisaation sisäverkkoihin. Muut tutkimukset osoittavat, että huolimattomuus on pääasiallinen syy siihen, että käyttäjistä tulee phishing-hyökkäysten uhreja. (Longtchi ym. 2024, 219.)

Epäjärjestemällisyys (Disorganization) kuvaa yksilön taipumusta toimia ilman ennakkosuunnittelua tai sallia sitä, että hänen ympäristössään on epäjärjestystä tai sotkuisuutta. Nämä olosuhteet voivat vaikuttaa heikentävästi yksilön kykyyn havaita hyökkäyksiin viittaavia poikkeamia tai vihjeitä ja näin lisätä heidän alttiuttaan käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 219.)

Kognitiivisella saituruudella (Cognitive miser) tarkoitetaan henkisten oikoteiden käyttämistä päätöksentekoprosessissa, eli tilannetta, jossa ajatteluun käytetään resursseja hyvin säästellen. Esimerkiksi tilanteen kiireellisyys tai monimutkaisuus voi saada yksilön ”oikaisemaan” päätöksentekoprosessissaan, jolloin päätöksenteko on nopeaa, mutta virheille altista. (Longtchi ym. 2024, 220.)

Hajamielisyys kuvaa sitä, kuinka paljon yksilön huomio voi harhautua pois käsillä olevasta tehtävästä. Eräs tutkimus osoittaa, että työntekijöiden hajamielisyys on yhteydessä emotionaaliseen uupumukseen, joka vaikuttaa negatiivisesti työtehoon. Tutkimukset osoittavat, että hajamieliset ihmiset saattavat klikata phishing-linkkejä, koska eivät kiinnitä huomiota siihen, mitä ovat parhaillaan tekemässä. Lisäksi tutkimukset osoittivat, että osallistujat eivät välttämättä edes huomanneet tai

tarkistaneet esimerkiksi varoitusta siitä, että vastaanotettu sähköposti on lähetetty ulkoisesta lähteestä. (Longtchi ym. 2024, 221.)

Uteliaisuus kuvaa yksilön halua tietää jotain. Verkkorikollinen hyödyntää kohteen uteliaisuutta suostuttelutekniikkana kohteen houkuttelussa saadakseen tämän tekemään virhearviointeja tai huonoja päätöksiä. (Longtchi ym. 2024, 220.)

Luottamusalttius on piirre, joka vaikuttaa siihen, kuinka suuri alttius yksilöllä on luottaa muihin ilman aiempaa tietoa heistä. Ihmiset eroavat toisistaan luottamusalttiudessa kehityskokemusten, persoonallisuuden ja kulttuuritaustan perusteella. Hyökkääjä voi tunnistaa kohteen luottamusalttiuden, mutta ei yleensä pysty suoraan vaikuttamaan siihen. Siksi hyökkääjä pyrkii vaikuttamaan tilanteeseen ja esittämään itsensä luotettavana manipuloidakseen uhrin luottamukseen perustuvia reaktioita. (Wang ym. 2021, 11901.)

5.4.4 Voimakkaat tunteet, kuten pelko, ahneus ja kateus

Pelko ja voimakkaat tunteet voidaan nähdä haavoittuvuutena. Hyökkääjä voi herättää pelkoa esimerkiksi uhkailemalla tai syyllistämällä, tai luomalla kohteelle työtehtävissä epäonnistumisen pelon tunteen. Voimakkaat tunteet heikentävät ajattelua ja voivat johtaa huonoihin päätöksiin. (Wang ym. 2021, 11903.)

Pelko kuvaa yksilön uskomusta siitä, että jotakin kivuliasta, vaarallista tai uhkaavaa voi tapahtua. Pelko on universaali, inhimillinen tunne ja pelkoa herättävät tilanteet laukaisevat voimakkaan välttämisreaktion sekä käyttäytymisessä että kognitiivisessa käsittelyssä (ajattelussa). Eräs tutkimus osoittaa, että käyttäjän manipuloinnin hyökkäykset ovat tehokkaita ihmisiin, jotka kokevat pelkoa vaikutusvaltaisia henkilöitä kohtaan. Pelkoa on mahdollista käyttää myös yhtenä huijausviestien vaikuttamisen tekniikkana. (Longtchi ym. 2024, 221–222.)

Ahneus kuvaa yksilön voimakasta halua saada jotakin, erityisesti varallisuutta, valtaa tai ruokaa. Ahneutta hyödynnetään usein phishing-sähköposteissa, ja se yhdistyy usein tarpeeseen. Hyökkääjä siis tietää, mitä kohde tarvitsee, ja esittää sen syöttinä. Jotkut tutkijat pitävät ahneutta inhimillisenä rajoitteena verrattaessa ihmiskeskeistä ja teknologiapohjaista tietoturvaa, eli mitä ahneempi ihminen on, sitä todennäköisemmin hän joutuu käyttäjän manipuloinnin hyökkäysten uhriksi. (Longtchi ym. 2024, 221.)

Myös *kateus* on voimakas tunne, jonka avulla yksilö voidaan johdatella tietojenkalasteluansaan (Wang ym. 2021, 11904).

5.4.5 Impulsiivisuus, itsehillinnän puute ja kärsimättömyys

Impulsiivisuudella kuvataan yksilön taipumusta toimia ilman suurempaa harkintaa. Eräs tutkimus on osoittanut, että matalan impulsiivisuuden omaavat tutkimukseen osallistuneet olivat vähemmän alttiita phishing-hyökkäyksille. (Longtchi ym. 2024, 219.) Voimakas impulsiivisuus ihmisen toiminnassa voidaan nähdä haavoittuvuutena, sillä vähemmän impulsiiviset käyttäjät ovat varovaisempia ja arvioivat petolliset viestit todennäköisemmin vaaralliseksi (Wang ym. 2021, 11903).

Itsehillinnällä kuvataan yksilön kykyä säädellä päätöksentekoprosessejaan voimakkaiden tunteiden tai halujen edessä. Itsehillinnän puute altistaa yksilön verkkohuijarin uhriksi joutumiselle. Yksilöt, joilla on alhainen itsehillintä, ovat taipuvaisempia ottamaan riskejä käyttäjän manipuloinnin hyökkäysten tapahtuessa. (Longtchi ym. 2024, 219.)

Kärsimättömyydellä kuvataan yksilön turhautumista tämän odottaessa tiettyä tapahtumaa tai turhautumista siihen, kuinka kauan tehtävän suorittamiseen kuluu aikaa. Kärsimätön yksilö voi olla alttiimpi käyttäjän manipuloinnin hyökkäyksille, etenkin keskittyessään välittömän palkinnon saamiseen. (Longtchi ym. 2024, 219.)

5.4.6 Myönteisiksi mielletyt piirteet ja kokemukset, kuten empatia, sympatia ja luottamus

Myös myönteisiksi mielletyt piirteet, kuten *myötätunto* ja *auttamisenhalu* voivat aiheuttaa riskejä kyberturvallisuuden kannalta. Apua tarvitsevan esittäminen on osoittautunut kerta toisensa jälkeen tehokkaaksi keinoksi huijauksissa. (Wang ym. 2021, 11904.)

Hyökkääjä pyrkii usein herättämään yksilössä voimakkaita tunteita. *Sympatia* kuvaa tunnetilaa, jossa yksilö pystyy ymmärtämään toisen henkilön henkisen tai emotionaalisen tilan, vaikkei itse välttämättä koe samaa tunnetta. Tunteisiin, kuten sympatiaan vetoaminen voi altistaa yksilön käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 222.)

Empatia kuvaa tunnetilaa, jossa yksilö ymmärtää omien kokemustensa pohjalta toisen ihmisen henkisen tai emotionaalisen tilan ilman, että välttämättä kokee itse samaa tunnetta. Huijarit hyödyntävät usein empatiaa herättäviä vaikuttamisen tekniikoita saavuttaakseen tavoitteensa. (Longtchi ym. 2024, 222.)

Myös *kohteliaisuus*, etenkin fyysisessä maailmassa, voi olla riski turvallisuudelle, sillä joku, joka pitää ovea auki perässä kulkevalle kohteliaisuuttaan, voi aiheuttaa turvallisuusriskin (Wang ym. 2021, 11904).

Luottamus (Trust) kuvaa ihmisluonteen taipumusta luottaa toisiin ihmisiin tai uskoa heihin. Mitä luottavaisempi yksilö on, sitä alttiimpi hän on käyttäjän manipuloinnin hyökkäyksille. Tämä ei ole

yllättävää, sillä luottamuksen luominen on yksi käyttäjän manipuloinnin hyökkäysten avainelementeistä. Lisäksi ihmiset, jotka ovat alttiita luottamaan muihin, päätyvät todennäköisemmin huijauksen uhriksi. Eräs tutkimuksen mukaan luottavaiset ihmiset ovat alttiimpia käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 219.)

Kunnioitus (Respect) kuvaa yksilön arvostusta toista kohtaan ja kuvastaa sitä, kuinka arvokkaana tai tärkeänä toista pidetään. Henkilö ei esimerkiksi osaa kyseenalaistaa ystävän lähettämää epäilyttävän linkin sisältävää sähköpostia, koska arvostaa suhdetta ystäväänsä. (Longtchi ym. 2024, 218.)

Alistuvuus (Submissiveness) kuvaa sitä, kuinka valmis yksilö on mukautumaan auktoriteettiin tai toisten tahtoon. Erään tutkimuksen mukaan korkea alistuvuus aiheuttaa korkean alttiuden phishing-sähköposteille. (Longtchi ym. 2024, 220.) Myös esimerkiksi ujot ihmiset ovat tottelevaisempia auktoriteettia kohtaan (Wang ym. 2021, 11904).

Emotionaalinen sitoutuminen (Affective commitment) kuvaa sitä, että emotionaalisesti sitoutunut yksilö on herkempi ottamaan riskejä ja kiintymys myös lisää tottelevaisuutta, vaikka kiintymys ei suoranaisesti vähentäisikään koettua riskiä tai lisäisi koettua luottamusta (Longtchi ym. 2024, 224).

5.4.7 Haavoittuvassa tilassa oleva yksilö

Haavoittuvuus (Vulnerability) kuvaa yksilön tarvetta erityiselle huolenpidolle, tuelle tai suojelulle iän, vamman tai hyväksikäytön tai laiminlyönnin riskin vuoksi. Eräs tutkimus pyrki tunnistamaan ne, joilla on suurempi riski joutua käyttäjän manipuloinnin hyökkäyksen uhriksi. Tämä tutkimus osoitti, että työntekijät, jotka olivat työskennelleet organisaatiossa vuoden tai sitä lyhyemmän ajan, ovat 52,07% alttiimpia spear phishing -hyökkäyksille kuin organisaatiossa kahdeksan vuotta työskennelleet, joiden alttiusprosentti oli 23,19%. (Longtchi ym. 2024, 219.)

Yksinäisyys (Loneliness) kuvaa yksilön subjektiivista kokemusta tämän toivoman ja todellisen sosiaalisen kumppanuuden, yhteyden tai läheisyyden välillä. Yksinäisyyttä hyödynnetään hyökkäyksissä usein, sillä yksilön kokemus ulkopuolisuudesta muihin nähden tekee tästä alttiimman hyökkäyksille. Hyökkääjät hyödyntävät yksinäisyydestä kumpuavaa huomion kaipuuta, erityisesti iäkkäiden kohdalla. Eräs tutkimus myös osoitti, että yksinäisyys on yhteydessä ongelmalliseen internetin käyttöön, jota käyttäjän manipuloinnin hyökkäykset voivat hyödyntää. (Longtchi ym. 2024, 222.)

Toivottomuus (Hopelessness) kuvaa yksilön mielentilaa, jossa vallalla ovat epätoivo, toivon puute, tunne siitä, ettei asioiden parantamiseksi ole mitään tehtävissä, tai epätoivoinen olo siitä, ettei pysty vaikuttamaan epäkohtiin työyhteisössä. Tässä tilassa olevat yksilöt ovat erityisen alttiita hyökkäyksille, joissa tarjotaan valheellista toivoa. (Longtchi ym. 2024, 222.)

5.4.8 Työpaikkakulttuuriin ja organisaatiorakenteeseen liittyvät psykologiset tekijät

Työpaikan kulttuuriin ja organisaatiorakenteeseen liittyvät psykologiset tekijät ovat olennaisia haavoittuvuuden näkökulmasta, sillä erilaiset työympäristöt voivat johtaa vaihtelevaan stressitasoon, työntekijöiden sitoutumiseen ja lojaaliuteen. Hyökkääjä voi hyödyntää työpaikalla tapahtuvia asioita kohdistaessaan hyökkäyksen organisaatiossa työskentelevään henkilöön. (Longtchi ym. 2024, 222.)

Työkuorma (Workload) kuvaa työmäärää, joka henkilöllä on. Eräs kolmen sairaalan 488 työntekijälle toteutettu kysely osoittaa, että suurempi työkuorma kasvattaa todennäköisyyttä klikata phishing-linkkejä. Toinen tutkimus osoittaa, että yksilön kokema henkinen kuormitus aiheuttaa muistivajetta, mikä vaikeuttaa oikeiden ja tekaistujen viestien erojen havaitsemista, lisäten alttiutta hyökkäyksille. (Longtchi ym. 2024, 222.)

Stressi on seurausta fyysisestä, emotionaalisesta tai psykologisesta rasituksesta. Tutkimukset osoittavat, että stressaantunut yksilö on vähemmän tehokas huomaamaan epäilyttäviä viestejä ja on alttiimpi käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 222.)

Kiire (Busyness) kuvaa tilaa, jossa yksilöllä on liikaa tehtävää, riippumatta varsinaisesta työmäärästä. Kiireinen yksilö ei kiinnitä huomiota yksityiskohtiin ja kiireen myötä yksilön kognitiivinen käsittelykyky voi heikentyä, mikä lisää alttiutta phishing-sähköposteille. (Longtchi ym. 2024, 222.)

Kiire (Hurry) voi näkyä myös tehtävää suoritettaessa tilanteessa, jossa henkilö kiirehtii saadakseen tehtävän valmiiksi. Kiireessä yksilö voi laiminlyödä turvallisuuteen liittyviä käytäntöjä ja lukea sähköpostit keskittymättä niihin syvällisesti. Tämä lisää alttiutta käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 222.)

Tunnepohjainen sitoutuminen (Affective commitment) kuvaa työolosuhteissa yksilön emotionaalista kiintymystä organisaatioon. Eräs tutkimus osoittaa, että korkea tunnepohjainen sitoutuminen voi sumentaa objektiivista ajattelua ja altistaa käyttäjän manipuloinnin hyökkäyksille, kun yksilö keskittyy liikaa organisaation miellyttämiseen. (Longtchi ym. 2024, 222.)

Tottuminen (Habitation) kuvaa tilannetta, jossa yksilö työtehtävissään toistaa samaa tehtävää ja turtuu tehtävän toistamiseen. Eräs tutkimus käyttäjien reaktioista turvallisuusvaroituksiin osoittaa, että varoituksiin turtuneet ihmiset kiinnittävät niihin vähemmän huomiota. Tottuminen siis lisää alttiutta hyökkäyksille. (Longtchi ym. 2024, 222–223.)

Kyynisyys (Cynisism) kuvaa taipumusta hyväksyä muiden vahingoittaminen oman edun vuoksi. Eräs tutkimus osoittaa, että epämiellyttävän esimiehen alaisuudessa työskentely voi johtaa

kyynisyyteen erityisesti tyytymättömien työntekijöiden keskuudessa. Tätä voidaan hyödyntää käyttäjän manipuloinnin hyökkäyksissä. (Longtchi ym. 2024, 223.)

Heikko luottamus omiin kykyihin halutun lopputuloksen saavuttamisessa voi ilmetä haavoittuvuutena. Luottamus omiin kykyihin on tärkeä ominaisuus ihmisen toiminnassa, ja vaikuttava tekijä henkilön sähköpostikäyttäytymisessä. Heikko luotto itseen ja omiin kykyihin tekee yksilöstä alttiimman phishing-hyökkäyksille. (Longtchi ym. 2024, 223.)

5.5 Mitä psykologisia menetelmiä käyttäjän manipuloinnin hyökkäyksissä hyödynnetään?

Tässä alaluvussa käsitellään toisen tutkimuskysymyksen perusteella tehtyjä havaintoja. Tutkimusaineistosta nostettiin esiin erityisesti ne psykologiset menetelmät, joilla on selkeä yhteys tietoperustan luvussa 3 käsiteltyihin käyttäjän manipuloinnin hyökkäyksen menetelmiin. Menetelmien läpikäymisessä ja ryhmittelemisessä on hyödynnetty löyhästi mukaillen Cialdinin vaikuttamisen periaatteita.

5.5.1 Samankaltaisuus, miellyttävyys ja auttamisenhalu (Cialdini: Liking)

Yksilöllä on taipumus pitää enemmän itsensä kanssa samankaltaisista ihmisistä kuin itsestään eroavista. *Samankaltaisuus*, kuten samoista asioista pitäminen tai samankaltaiset ajatukset, edistää vastapuolen kokemista miellyttävänä, mikä lisää auttamisenhalua. Myös fyysinen viehättävyys voi vaikuttaa auttamisenhaluun. Hyökkääjän toiminta on tehokkaampaa, jos hän käyttää lähestymistapaa, joka mukailee kohteen mielipiteitä ja asenteita, sillä ristiriidat voivat vähentää suostuttelun tehoa. Pehmeä ja yhteisymmärrystä korostava lähestymistapa edesauttaa yhteistyötä. (Wang ym. 2021, 11897.)

Yksilöllä on taipumus suhtautua myönteisesti henkilöön, johon tällä on muodostunut suhde ja toisen pyyntöihin suostuminen on todennäköisempää, jos tämä vaikuttaa ystävälliseltä tai tutulta. Tätä piirrettä voidaan hyödyntää hyökkäyksessä luomalla kohteen houkuttelemiseksi profiili, joka vaikuttaa luotettavalta tai ystävälliseltä. (Longtchi ym. 2024, 218.)

5.5.2 Vastavuoroisuus ja sosiaalisen vaihdon teoria (Cialdini: Reciproty)

Sosiaalisen vaihdon teoria (Social exchange theory) osoittaa, että ihmiset vaihtavat aineellisten hyödykkeiden, kuten rahan, lisäksi myös sosiaalisia hyödykkeitä, kuten rakkautta, palveluksia, tietoa ja asemaa. Päätöksiin ja käyttäytymiseen, kuten avun vastaanottamiseen ja ”takaisin maksamiseen”, vaikuttaa kustannusten ja hyötyjen arviointi, joko tietoisesti tai tiedostamatta. Hyvään tulisi vastata hyvällä, eli jos joku tekee ihmiselle palveluksen, hänen oletetaan tekevän vastapalvelus. On yleistä sisäistää käytösmalli, jossa toisen osoittamaan hyvyyteen ja apuun tulisi vastata

annettua palvelusta vastaavalla tavalla. Sosiaalisissa vuorovaikutustilanteissa toiminnan pitäisi olla vastavuoroista, eli palveluksia tulisi antaa tasapuolisesti puolin ja toisin. Jos apua vastaanotetaan ilman vastinetta, se rikkoo vastavuoroisuuden normia. (Wang ym. 2021, 11898–11899.)

Vastavuoroisuus (Reciprocity) kuvaa yksilön taipumusta pyrkiä maksamaan saamansa palvelus takaisin. Ihmiselle on luontaista kokea velvollisuutta maksaa saamansa palvelus takaisin, vaikka palveluksen antaneen osoittama pyyntö olisi täysin eri suurusluokassa kuin aiemmin vastaanotettu palvelus. Tämä asettaa vastapalvelusta pyytävän henkilön edulliseen asemaan. (Longtchi ym. 2024, 218.)

Vastavuoroisuutta hyödynnetään esimerkiksi käänteisessä käyttäjän manipuloinnin hyökkäyksessä, hyökkääjä aloittaa tekemällä ”palveluksen” esimerkiksi järjestelmänvalvojana tai IT-tuen edustajana. Hän luo tilanteen, jossa kohde joutuu pyytämään apua, ja odottaa, että esimerkiksi uusi työntekijä pyytää apua teknisessä ongelmassa. Uhrin pyydettyä apua, hyökkääjä hyödyntää tilanteen pyytämällä vastapalvelusta. Tämä edesauttaa hyökkäyksen onnistumista, sillä uhrin odotetaan noudattavan vastavuoroisuuden normia ja täyttävän oman osuutensa sosiaalisessa vaihdossa. (Wang ym. 2021, 11899.)

Myös *henkilökohtaisuuksien paljastaminen* (Self-disclosure) edesauttaa vastavuoroisuutta ja luottamuksellisen suhteen rakentamista. Sosiaalisen suhteen rakentumisessa ihmisen avoimuus synnyttää vastavuoroista avoimuutta, eli yksilö on alttiimpi kertomaan itsestään enemmän ihmiselle, joka on vuorovaikutuksessa avoimesti jakanut ajatuksiaan ja tunteitaan. Yksilö kokee mielihyvää tullessaan valituksi sellaiseksi henkilöksi, jolle uskalletaan avautua. Ihmiset pitävät henkilöistä, jotka kertovat avoimesti itsestään. Avoin itseilmaisu vahvistaa luottamuksellista suhdetta ja helpottaa sosiaalista vuorovaikutusta. Kun toiminta (avautuminen) on vastavuoroista, se saa ihmisen pitämään vastapuolesta vielä enemmän. (Wang ym. 2021, 11899.)

Quid pro quo, eli “jotain vaihdossa jostakin”, on psykologinen tekniikka, jolla hyökkääjä pyrkii ohjailemaan kohteen ottamaan riskejä suuren palkkion, kuten rahan tai ilmaisten palveluiden, tai häpeän välttämisen toivossa. Se hyödyntää vastavuoroisuuden, ahneuden ja toivottomuuden psykologisia piirteitä. Hyökkääjä voi myös esiintyä virkavallan edustajana ja pyrkiä manipuloimaan kohdetta maksamaan esimerkiksi laittomasta sisällöstä, jottei tätä pidätettäisi laittoman sisällön hallussapidosta. Esimerkiksi niin kutsutuissa nigerialaishuijauksissa hyödynnetään tekniikkaa, jossa kohteelle luvataan suuri summa rahaa, jos hän ensin maksaa itse pienen summan. (Longtchi ym. 2024, 224.)

5.5.3 Ryhmään mukautuminen ja muiden seuraaminen (Cialdini: Social Proof)

Ryhmävaikutuksella ja mukautumisella (Group influence and conformity) tarkoitetaan sitä, että yksilö on altis mukautumaan ryhmässä vallitsevaan mielipiteeseen joko todellisen tai kuvitellun ryhmäpaineen seurauksena. Tämä tarkoittaa yksilön käyttäytymisen tai mielipiteen mukautumista ryhmässä vallalla olevan kannan mukaiseksi. Mukautumiseen vaikuttavat useat tekijät, kuten ryhmän koko, yksimielisyys, yhteenkuuluvuuden tunne, sekä se kuinka julkisesti yksilö ilmaisee kantansa. Jo pieni ryhmäkoko voi aiheuttaa merkittävää mukautumista yksilön taholta, ja vaikutus voimistuu ryhmäkoon kasvaessa. Ryhmän yksimielisyyden väheneminen heikentää yksilön mukautumista, vahvan yhteenkuuluvuuden kokemuksen taas voimistaessa sitä. Yksilö mukautuu ryhmän vallalla olevaan kantaan erityisesti silloin, kun hänen reaktionsa tapahtuu julkisesti. (Wang ym. 2021, 11898.)

Ryhmään mukautumisella (Social proof) voidaan kuvata myös yksilön taipumusta kopioida muiden toimintaa riippumatta kopioitavan toiminnan ”oikeellisuudesta”. Jos enemmistö näyttää esimerkkiä huonosta tietoturvakäyttäytymisestä, yksilö saattaa omaksua käytösmallin siksi, että muutkin käyttäytyvät samalla tavalla. (Longtchi ym. 2024, 218.)

Yksilö saattaa mukautua ryhmän toimintaan joko saadakseen hyväksyntää (*normatiivinen vaikutus*) tai saadakseen tärkeää tietoa (*informatiivinen vaikutus*) (Wang ym. 2021, 11898).

Normatiivisen vaikutuksen (Normative influence) taustalla on hyväksytyksi tulemisen halu, sosiaalisista suhteista kiinnipitäminen tai ryhmäpaineen välttäminen. Sosiaalisten normien rikkominen voi johtaa ryhmän ulkopuolelle jäämiseen, joka on useimmille ihmisille henkisesti kivuliasta. Henkistä epämukavuutta välttääkseen yksilö mukautuu ryhmään toisinaan tiedostamattaankin, joka voi johtaa jopa vaarallisten käyttäytymismallien, kuten päihteiden käytön tai varastelun, omaksumiseen. Normatiivisen vaikutuksen kontekstissa ryhmän hyväksyntä on merkityksellisempää kuin oikein toimiminen. (Wang ym. 2021, 11898.)

Informatiivisen vaikutuksen (Informational influence) taustalla on ihmisen pyrkimys löytää oikea ratkaisu tai välttää tuntemattomia riskejä. Yksilö usein olettaa, että ryhmän toiminta on todennäköisesti oikein ja riskittömämpää. Tämä oletus saa heidät mukautumaan ryhmän kanssa samankaltaiseen käyttäytymiseen, uskomuksiin tai päätöksiin. Yksilö määrittelee tällöin oikean selvittämällä, mitä ryhmä oletetusti pitää oikeana. (Wang ym. 2021, 11898.)

Käyttäjän manipuloinnin hyökkäyksissä hyökkääjä pyrkii rakentamaan tilanteet siten, että pystyy hyödyntämään sekä normatiivista että informatiivista vaikutusta kohteen toiminnan ohjailussa (Wang ym. 2021, 11898).

Sivustakatsojan efektillä (Bystander effect) tarkoitetaan ilmiötä, jossa yksilö on vähemmän halukas auttamaan hätätilanteessa, jos paikalla on muitakin. Mitä enemmän tilanteella on sivustakatsojia, sitä todennäköisempää on, että kukaan ei puutu tilanteeseen, sillä tilanteessa oletetaan jonkun muun auttavan. Tämä on seurausta *vastuun hajaantumisesta*, eli kun oletettu vastuu jakaantuu useamman ihmisen kesken, yksilö tuntee vähemmän painetta kantaa vastuuta. (Wang ym. 2021, 11900.)

Yksilöllisyyden menettämisellä (deindividuaatio) tarkoitetaan ryhmätilanteissa tapahtuvaa ilmiötä, jossa yksilö kadottaa tietoisuuden omasta identiteetistään ja alkaa toimia ryhmän normien mukaan. Anonymiteetti, suuri väkijoukko ja häiritsevät tekijät, kuten melu tai pimeys, voivat lisätä tätä ilmiötä. Tämä ohjaa yksilön toimimaan ryhmän mukana tavalla, jolla ei normaalisti toimisi, koska ei kokisi toimintaa vastuullisena. (Wang ym. 2021, 11900.)

Käyttäjän manipuloinnin hyökkäyksissä, kuten tietojenkalastelussa, hyökkääjä käyttää hyväkseen tällaisia psykologisia ryhmäkäyttäytymiseen liittyviä ilmiöitä luomalla esimerkiksi tilanteita, joissa uhri toimii ryhmäpaineen tai vastuun hajaantumisen vaikutuksesta tavalla, joka vaarantaa kyberturvallisuuden (Wang ym. 2021, 11900).

Jos esimerkiksi yksilöllä on uskomus siitä, että tärkeä henkilö tai ryhmä hyväksyy tai tukee tietynlaista käyttäytymistä, tämä uskomus saattaa ohjata yksilön käyttäytymään tietyllä tavalla. Tämä aiheuttaa usein työpaikalla sosiaalista painetta ja saattaa johtaa phishing-viestin klikkaamiseen. Tämä tekijä on sidoksissa siihen, miten yksilö on huolissaan siitä, mitä muut hänestä ajattelevat. (Longtchi ym. 2024, 223.)

5.5.4 Itsestä annetun vaikutelman hallinta, sitoutuminen ja johdonmukaisuus (Cialdini: Commitment and Consistency)

Ihminen pyrkii luontaisesti luomaan itsestään *myönteisen vaikutelman* sekä muille että itselleen. Tähän motivoi tarve tuntea itsensä paremmaksi, sosiaalisten tai materiaalisten hyötyjen saavuttaminen, sekä sosiaalisen identiteetin vahvistaminen. Yksilö muokkaa käytöstään vaikuttaakseen *johdonmukaiselta ja luotettavalta*. Tämän takia, välttääkseen vaikuttamasta epäjohdonmukaiselta, yksilö pyrkii muovaamaan toimintansa vastaamaan aiemmin osoittamaansa asennetta tai antamaansa lupausta, niin että toiminta ei olisi aiemman toiminnan kanssa ristiriidassa. (Wang ym. 2021, 11899.)

Sisäisen ristiriidan (kognitiivinen dissonanssi) teorian mukaan yksilö tuntee epämukavuutta kokiessaan samanaikaisesti kaksi keskenään ristiriitaista ajatusta, uskomusta tai arvoa. Yksilö pyrkii tällöin vähentämään ajattelun ja toiminnan välisen ristiriidan herättämää epämukavuutta muuttamalla joko ajatteluaan tai käyttäytymistään. (Wang ym. 2021, 11899.)

Yksilön tarve *johdonmukaisuuteen* (Consistency) voi siis johtaa siihen, että yksilö myöntyy pyyntöön tai pysyy lupauksessaan tai valinnassaan välttääkseen ristiriidan aikaisemman ja nykyisen toiminnan välillä (Wang ym. 2021, 11899). Tämä *sitoutuminen* (Commitment) aiempiin päätöksiin voi siis vaikuttaa tuleviin päätöksiin hyökkäykselle edullisella tavalla (Longtchi ym. 218).

”Jalka oven väliin”-efektiksi (Foot-in-the-door) kutsutaan tekniikkaa, jolla yksilö saadaan suostumaan suureen pyyntöön pyytämällä ensin pientä palvelusta (Wang ym. 11899). Tämä psykologinen tekniikka pyrkii saamaan myöntävän vastauksen suureen pyyntöön johdattelemalla kohdetta suostumaan ensin pieneen pyyntöön. Tekniikka hyödyntää *johdonmukaisuuden* (Consistency) piirrettä. (Longtchi ym. 2024, 224.)

Yksilön pyrkiessä antamaan johdonmukaisen kuvan itsestään pieneen palvelukseen suostuminen johtaa todennäköisemmin myös suurempaan palvelukseen suostumiseen. Yksilön pyrkiessä johdonmukaiseen toimintaan välttääkseen ristiriitaa aiemman toimintansa ja nykyisen toiminnan välillä, voidaan esimerkiksi auttamishalua hyödyntää myös käyttäjän manipuloinnin hyökkäyksissä, sillä pieni suostumus avaa portin myös suuremmille myönnytyksille. (Wang ym. 2021, 11899–11900.)

5.5.5 Auktoriteetti (Cialdini: Authority)

Auktoriteetilla (Authority) kuvataan valtaa tai valta-asemaa yksilöön nähden (Longtchi ym. 2024, 218). Ihmisillä on taipumus osoittaa automaattista alistumista auktoriteettihahmojen käskyihin. Useissa kulttuureissa ihmiset opetetaan uskomaan auktoriteetteihin, asiantuntijoihin ja tuttuihin henkilöihin, sillä näihin rooleihin yhdistetään uskottavuus, luotettavuus ja matala riski. (Wang ym. 2021, 11897.)

Auktoriteetin ja siihen liittyvien symbolien on todettu laukaisevan yksilön alistumista, sekä itsenäisen ajattelun ja rationaalisen käyttäytymisen tukahduttamista. Joillain yksilöillä ilmenee myös heikompaa tarkkaavaisuutta viestin sisällön suhteen, kun sen oletetaan tulevan luotettavasta lähteestä. (Wang ym. 2021, 11897.)

Voimakas reagointi auktoriteettiin selittää myös sen, miksi käyttäjän manipuloinnin hyökkäyksissä hyödynnetään auktoriteettia, asiantuntemusta ja uskottavuutta kuvastavia symboleita, kuten univormuja, tunnuksia, asiantuntijoiden käyttämää erikoiskieltä ja sisäpiirin termejä (Wang ym. 2021, 11897).

Valta-asemaa hyödynnetään erityisesti spear phishing -hyökkäyksissä, kun kohteen halutaan paljastavan arkaluonteista tietoa. Tutkimuksissa on myös todettu, että mitä tottelevaisempi yksilö on

auktoriteettia kohtaan, sitä haavoittuvaisempi tämä on käyttäjän manipuloinnin hyökkäyksille. (Longtchi ym. 2024, 218.)

5.5.6 Niukkuus (Cialdini: Scarcity)

Niukkuudella (Scarcity) kuvataan hyödykkeen tai palvelun puutetta tai harvinaisuutta (Longtchi ym. 2024, 218). Tekemällä asiasta harvinainen tai vaikeasti saatava voidaan vaikuttaa yksilöön muuttamalla hänen käsitystään arvosta, herättää tunteita ja lisätä motivaatiota. Yksilö kokee mahdollisuudet arvokkaammiksi, kun ne ovat harvinaisempia. Resurssien rajallisuudella voidaan luoda vaikutelma vaikeasta saatavuudesta, suuremmasta kilpailusta tai valinnanvapauden rajallisuudesta. Yksilö siis arvostaa harvinaisia asioita, usein jopa liioitellen niiden arvoa. (Wang ym. 2021, 11900.)

Yksilö haluaa saada resurssin haltuunsa entistä voimakkaammin, jos kokee sen arvokkaaksi tai pelkää jäävänsä ilman, vaikka resurssin rajallisuus olisi vain tilapäistä tai jopa keinotekoista. Motivaatiota resurssin tavoitteluun voidaan lisätä herättämällä voimakkaita tunteita, kuten pelkoa, ahdistusta, halua tai ahneutta. (Wang ym. 2021, 11900.)

Käyttäjän manipuloinnin hyökkäyksissä, erityisesti tietojenkalastelussa, hyökkääjä houkuttelee kohdetta klikkaamaan linkkiä korostamalla, että tarjolla oleva asia on harvinainen tai rajattu (Wang ym. 2021, 11900).

Tätä psykologista tekijää hyödynnetään phishing-sähköpostien lisäksi laajasti verkkohuijauksissa. Usein niukkuuden lisäksi hyödynnetään myös auktoriteettia, jotta kohde saadaan toimimaan hyökkääjän haluamalla tavalla. (Longtchi ym. 2024, 218.)

5.5.7 Aikapaine, kiire

Aikapaine (Time pressure) vaikuttaa ihmisen loogiseen ajatteluun. Kun ihminen joutuu käsittelemään suurta määrää tietoa rajoitetun ajan puitteissa, tarkempaa tarkastelua vaativiin viesteihin saatetaan vastata hätiköidysti. Aikapaine voi myös laukaista tunnetiloja, kuten vihaa, jännitystä tai ahdistusta, joilla on ajattelua heikentävä vaikutus. Hyökkääjä voi pyrkiä tarkoituksellisesti ylikuormittamaan kohteen ajattelua liiallisella määrällä harhaanjohtavaa tietoa ja luomalla kiireen tuntua. Tällöin kohteen ajatteluprosessi häiriintyy ja käyttäytyminen muuttuu haavoittuvammaksi. (Wang ym. 2021, 11900.)

Kiireen tuntua (Urgency) luomalla hyökkääjä pyrkii luomaan tilanteen, jossa vaaditaan välitöntä toimintaa tai jossa on selkeä aikapaine. Näin hyökkääjä pyrkii heikentämään hyökkäyksen tunnistamisen todennäköisyyttä. Tämä psykologinen tekniikka vetoaa kognitiiviseen saituruuteen, pelkoon ja huolimattomuuteen. (Longtchi ym. 2024, 223–224.)

5.5.8 Luottamuksen luominen ja hyödyntäminen

Luottamus (Trust) on olennainen tekijä, kun ennustetaan yksilön alttiutta käyttäjän manipuloinnin hyökkäyksille, ja monissa tapauksissa hyökkääjä pyrkiikin vakuuttamaan olevansa luotettava henkilö. Luottamuksella tarkoitetaan sitä, että luottava osapuoli on valmis olemaan haavoittuvainen luottamansa osapuolen toimille ja olettaa, että luotettu osapuoli suorittaa tietyn toiminnon, joka on tärkeä luottavalle osapuolelle, riippumatta siitä onko luottavalla osapuolella kykyä valvoa tai hallita luotetun osapuolen toimintaa. Luottaminen on siis ennen kaikkea riskin ottamista. (Wang ym. 2021, 11900–11901.)

Yksi merkittävä syy siihen, miksi hyökkääjä panostaa juuri *luottamuksen luomiseen*, voi olla positiivinen korrelaatio, joka vallitsee luottamuksen, auttamisvalmiuden, suhteiden ja tiedon jakamisen välillä. Juuri vahvan luottamuksen rakentaminen edesauttaa käyttäjän manipuloinnin hyökkäyksen toteutumista, vaikka kohde tiedostaisi luottamisen riskit. Luottamuksen rakentamiseen vaikuttavat tekijät ja huijaukseen vaikuttavat tekijät ovat parametreja, joita hyökkääjä haluaa hallita toteuttaakseen käyttäjän manipuloinnin hyökkäyksen. (Wang ym. 2021, 11900–11901.)

Luottamussuhde (Trusted relationship) on psykologinen tekniikka, joka hyödyntää olemassa olevaa luottamussuhdetta, ja käyttää hyväkseen auktoriteetin, kunnioituksen ja luottamuksen (authority, respect, trust) piirteitä. Hyökkääjä voi esimerkiksi esiintyä LinkedInissä rekrytoijana ja ottaa yhteyttä työnhakijoihin. BEC-hyökkäyksissä tätä tekniikkaa käytetään esihenkilön ja alaisen välisen luottamussuhteen hyödyntämisessä hyökkäyksen tarkoituksiin. (Longtchi ym. 2024, 224.)

Personointi (Personalization) tarkoittaa psykologista tekniikkaa, joka hyödyntää henkilökohtaista tietoa viestin muotoilemiseksi yksilöllisesti kohteelle osoitetuksi, pyrkimyksenä herättää luottamusta. Tekniikka hyödyntää eri yksilöiden erilaisia persoonallisuuden piirteitä ja psykologisia tekijöitä lisätäkseen hyökkäyksen onnistumisen todennäköisyyttä. (Longtchi ym. 2024, 224.)

Kiintymyssuhteen hyödyntäminen (Affection trust) on psykologinen tekniikka hyödyntää kiintymyssuhteen luomista kohteeseen. Se hyödyntää emotionaalisen (tunnepohjaisen) sitoutumisen (Affective commitment) psykologista piirrettä. Kiintynyt yksilö ottaa herkemmin riskejä ja on tottelevaisempi, vaikka kiintymyksen kokemus ei lisäisikään luottamuksen kokemusta. (Longtchi ym. 2024, 224.)

5.5.9 Harhauttaminen: Totuuden muuntelu, kertomatta jättäminen, valehtelu, petollisuus

Petos on yleensä tarkoituksellista ja strategista toimintaa, jonka petoksen tekijä suunnittelee huijatakseen toista osapuolta. IDT-teorian (Interpersonal Deception Theory, IDT) mukaan petoksessa hyödynnetään tyypillisesti kolmea keinoa, jotka ovat valehtelu, olennaisen tiedon salaaminen ja

aiheen väistely. Petollisessa viestinnässä lähettäjä harjoittaa strategisia toimia hallitakseen ja manipuloidakseen tietoa, käyttäytymistä ja imagoaan huijatakseen vastaanottajaa. (Wang ym. 2021, 11901.)

Valetarina (Pretexting) on psykologinen tekniikka, joka pyrkii lisäämään kohteen sitoutumista hyökkääjään hyödyntämällä valheellisen tarinan avulla luotua luottamusta. Valetarinaa voidaan hyödyntää käyttäjän manipuloinnissa viittaamalla ajankohtaisiin, esimerkiksi uutisissa mainittuihin tapahtumiin. (Longtchi ym. 2024, 223.) Hyökkääjä voi myös sepittää valheellisen tarinan henkilöllisyydestään päästäkseen käsiksi tietoon, johon hänen esittämänsä henkilö on oikeutettu (Choi 2023, 11).

Toisena henkilönä esiintyminen (Impersonation) on psykologinen tekniikka, joka perustuu valheellisen henkilöllisyyden esittämiseen kohteen suostumuksen lisäämiseksi hyödyntämällä auktoriteettia, kunnioitusta ja luottamusta (authority, respect, trust). Hyökkääjä hyödyntää valheellista henkilöllisyyttä kohteen houkutteluun tai vakuuttamiseen, ja esimerkiksi BEC-hyökkäyksessä hyökkääjä esittää organisaation johtotehtävissä työskentelevää ja pyytää kohdetta siirtämään rahaa tilille, joka on hyökkääjän hallussa. (Longtchi ym. 2024, 223.)

Visuaalinen harhautus (Visual deception) on psykologinen tekniikka, joka hyödyntää visuaalisilla elementeillä harhauttamista luottamuksen luomiseksi. Tällä tekniikalla vedotaan esimerkiksi luottamukseen ja tottumisen piirteisiin (trust, habituation). Tässä tekniikassa hyödynnetään esimerkiksi väärennettyjä URL-osoitteita, jotka silmämääräisesti näyttävät aidoilta. (Longtchi ym. 2024, 223.)

5.5.10 Suostuttelu ja houkuttelu

Suostuttelu (Persuasion) on psykologinen tekniikka, joka rohkaisee tietynlaiseen käyttäytymiseen hyödyntämällä pitämisen (Liking), vastavuoroisuuden (Reciprocity), ryhmään kuulumisen (Social proof), johdonmukaisuuden (Consistency) ja auktoriteetin kunnioittamisen (Authority) menetelmiä, joilla vedotaan psykologisiin piirteisiin. Tämän tekniikan tehokkuus riippuu siitä, mitä piirteitä tarkalleen hyödynnetään, sekä muista tekijöistä, kuten iästä ja pyynnön tyypistä. (Longtchi ym. 2024, 223.)

Kannustimia ja motivaattoreita (Incentive and motivator) käytetään ”palkintoina”, kun kohdetta pyritään kannustamaan toivottuun käyttäytymiseen tai pyynnön noudattamiseen. Kannustimena voi olla ulkoisia tekijöitä, kuten rahaa, kun taas motivaattoreilla pyritään luomaan sisäistä palkitsevuuden tunnetta. Tekniikka vetoaa sympatiaan, empatiaan, yksinäisyyteen sekä auktoriteettien uhmaamiseen. (Longtchi ym. 2024, 223.)

Houkutinvaikutus (Decoy effect) on psykologinen tekniikka, jossa tarkoituksena on saada kohde uskomaan, että hänelle on annettu erityisen hyvä tarjous, kuten huomattavasti markkinahintaa

edullisempi tuote. Tuotetta ei lopulta koskaan toimiteta, vaikka se olisi maksettu etukäteen. Tämä tekniikka hyödyntää luottamusta, niukkuutta (scarcity), emotionaalista sitoutumista ja impulsiivisuutta. (Longtchi ym. 2024, 224.)

5.6 Mitä vaiheita ja psykologisia menetelmiä kohdennettu käyttäjän manipuloinnin hyökkäys sisältää?

Tässä alaluvussa perehdytään kolmannen ja viimeisen tutkimuskysymyksen avulla kehittyneen ja kohdennetun käyttäjän manipuloinnin hyökkäyksen prosessin vaiheisiin. Prosessin vaiheita kuvataan perehtymällä esimerkkitapausten, BEC-hyökkäyksen ja teknisen tuen hyökkäyksen, vaiheisiin. Luvussa syvennytään myös tietoperustan luvussa 3 käsiteltyihin hyökkäystyyppeihin ja niissä hyödynnettäviin psykologisiin menetelmiin.

Kyberturvallisuuden näkökulmasta käyttäjän manipuloinnin hyökkäyksissä yksi selkeästi erottuva ominaisuus on sosiaalinen vuorovaikutus. Hyökkäys voidaan toteuttaa joko teknisin tai ei-teknisin keinoin. (Wang ym. 2020, 85107.)

Sosiaalisella vuorovaikutuksella tarkoitetaan viestintää tai yhteistä toimintaa, jossa on mukana kaksi tai useampia ihmisrooleja. Vuorovaikutuksen tyyppejä voi olla monia eri kriteerien mukaan:

- suora tai epäsuora (henkilökohtainen vuorovaikutus reaalimaailmassa tai vuorovaikutus verkon kautta),
- reaaliaikainen tai ei-reaaliaikainen (puhelinkeskustelu tai sähköposti),
- aktiivinen tai passiivinen (käänteinen käyttäjän manipulointi). (Wang ym. 2020, 85105.)

Tietoturvan aihealueella termi käyttäjän manipulointi viittaa laajasti verkkorikollisten käyttämiin tekniikoihin, joiden avulle he hankkivat arkaluontoista tietoa tai houkuttelevat kohteen suorittamaan toimia, jotka voivat vaarantaa organisaation tietojärjestelmän. Käyttäjän manipulointi kattaa monenlaisia haitallisia tekniikoita, kuten tietojenkalastelun (phishing), valheellisen henkilöllisyyden käytön (pretexting), houkuttelun (baiting), quid pro quon (vastapalveluksen hyödyntäminen) ja seuraamalla pääsyn rajoitetulle alueelle (tailgating). (Wang ym. 2020, 85101.)

5.6.1 Hyökkäysprosessi yleisesti

Wang kollegoineen (2021, 11896) määrittelee käyttäjän manipuloinnin hyökkäysprosessin kulun yleistettynä seuraavasti:

Vaihe 1. Hyökkääjä laatii suunnitelman, joka sisältää hyökkäyksessä käytettävät hyökkäysmenetelmät, joiden tarkoituksena on hyödyntää kohteen inhimillisiä haavoittuvuuksia ja näin saavuttaa tietyt tavoitteet hyökkäyksessään (Wang ym. 2021, 11896).

Vaihe 2. Kun hyökkääjä on onnistunut hyödyntämään haavoittuvuutta ja saanut kohteen toimimaan haluamallaan tavalla, kohteesta tulee uhri ja tämän toiminta johtaa hyökkäyksen seurauksiin (Wang ym. 2021, 11896).

Vaihe 3. Hyökkääjä tarkastelee syntyneitä seurauksia suhteessa asetettuihin tavoitteisiin tehdäkseen päätöksen mahdollisista jatkotoimista (Wang ym. 2021, 11896).

5.6.2 Psykologiset tekniikat eri hyökkäystyypeissä

Käyttäjän manipuloinnin hyökkäyksissä jokainen hyökkäystyyppi hyödyntää yhtä tai useampaa psykologista menetelmää vedotakseen yhteen tai useampaan psykologiseen piirteeseen (Longtchi ym. 2024, 235). Tähän on koottu tietoperustan luvussa 3 käsiteltyjen hyökkäystyyppien psykologiset elementit.

Perusmuotoisessa tietojenkalastelussa (phishing) lähetetään phishing-sähköposteja ilman tiettyä ennalta määriteltyä kohdetta toivoen, että osa vastaanottajista lankeaa ansaan. Näitä viestejä ei ole mitenkään personoitu. On yleistä, että phishing-sähköpostiviesti sisältää houkuttimen (jolla vedotaan ahneuden psykologiseen piirteeseen) ja hyökkääjän toiveena on, että joku tarttuu siihen. (Longtchi ym. 2024, 226.) Houkuttelevan ”palkinnon” tai jonkin muun motivoivan tekijän lisäksi perusmuotoisessa tietojenkalastelussa voidaan hyödyntää kiireellisyyttä, toisena henkilönä esiintymistä, valetarinaa sekä quid pro quo -tekniikkaa (Longtchi ym. 2024, 234).

Kohdennetussa tietojenkalastelussa (spear phishing) tietojenkalasteluviesti sisältää yksilöllisesti kohteelle muotoillun viestin, jossa kohdetta puhutellaan tämän nimellä ja tittelillä. Hyökkäys voi hyödyntää yksilöllisesti muotoiltua viestintää (personointi) ja esiintymistä toisena henkilönä (Impersonation), joilla vedotaan auktoriteettia (Authority) kunnioittavaan psykologiseen piirteeseen. Hyökkääjä on valmis näkemään vaivaa tämän hyökkäystyypin toteuttamiseksi ja pyrkii luomaan tilanteen, jossa kohde uskoo hyökkääjän olevan vaikutusvaltainen henkilö, ja pyrkii toimimaan nopeasti tämän ohjeiden mukaisesti. (Longtchi ym. 2024, 226.) Spear phishing -hyökkäyksissä hyödynnettäviä menetelmiä ovat viestin visuaalisilla elementeillä harhaanjohtaminen sekä viestin yksilölliseksi muotoileminen (personointi), kiireen luominen, palkitseminen (Incentive & motivator), suostuttelu, quid pro quo -tekniikka ja valetarina (Longtchi ym. 2024, 234).

Johtotason henkilöön kohdennetussa tietojenkalastelussa (whaling) kohteelle lähetettävä sähköpostiviesti muistuttaa spear phishing -viestiä siltä osin, että viestin sisältö on kohdistettu nimenomaan kyseiselle henkilölle. Kuitenkin, toisin kuin spear phishing -viesti, joka voi olla kohdennettu kenelle tahansa organisaatiossa, whaling-viesti on kohdistettu erityisesti johtoportaan edustajalle, kuten toimitusjohtajalle. Whaling-hyökkäyksessä käytettäviä tekniikoita ovat viestin yksilölliseksi muotoileminen (personointi) sekä esiintyminen toisena henkilönä (Impersonation). Hyökkääjä pyrkii

vetoamaan kohteen luottamukseen ja näin saada kohteen olemaan luottavaisempi sähköpostiviestin sisältöä kohtaan. (Longtchi ym. 2024, 226–227.) Whaling-hyökkäyksessä hyödynnettäviä menetelmiä ovat lisäksi kiireen luominen ja visuaalisten elementtien avulla harhauttaminen (Longtchi ym. 2024, 234).

BEC-hyökkäyksessä (Business E-mail Compromise) hyödynnetään sähköpostiviestejä organisaatioita vastaan kohdistamalla viestit tietyille henkilöille, jotka työskentelevät organisaatiossa. Kohteelle lähetetään sähköpostiviesti väärennetystä osoitteesta ja viestin lähettänyt hyökkääjä tekeytyy esimerkiksi toimitusjohtajaksi tai tutuksi, luotetuksi asiakkaaksi. (Longtchi ym. 2024, 227.) BEC-hyökkäyksessä hyödynnetään toisena henkilönä esiintymistä, kiireen luomista, visuaalista harhautusta ja viestien personointia, joilla pyritään herättämään kohteessa luottamusta ja hyödyntämään luottamussuhdetta (Longtchi ym. 2024, 235).

Käänteinen käyttäjän manipulointi (Reverse social engineering) on hyökkäystapa, jossa pyritään ensin voittamaan uhrin luottamus ja vasta sitten toteutetaan varsinainen hyökkäys. Hyökkäyksessä ohjaillaan käyttäjä ottamaan itse ensiksi yhteyttä hyökkääjään, joka käyttää tilaisuutta hyväkseen edistääkseen omaa tavoitettaan. Hyökkäystapaa kutsutaan käänteiseksi käyttäjän manipuloinniksi siksi, että hyökkääjä luo tilanteen, joka saa uhrin ottamaan yhteyttä häneen. (Longtchi ym. 2024, 228.) Hyökkäyksen uskottavuuden parantamiseksi voidaan hyödyntää valetarinaa (Pretexting) (Longtchi ym. 2024, 235). Tämä hyökkäys hyödyntää luottamussuhteeseen ja kiireellisyyteen perustuvia psykologisia tekniikoita, joilla pyritään herättämään kohteessa luottamusta (Longtchi ym. 2024, 228).

Vishing-hyökkäyksessä hyödynnetään VoIP-puheluita luotettavana tai tuttuna tahona esiintymiseen. Hyökkääjä voi yhdistää vishing-hyökkäykseen auktoriteetin (Authority) ja niukkuuden (Scarcity) psykologisia tekijöitä, jotta kohde uskoisi hänen olevan luotettava. Puhelun sisällössä pyritään huijaamaan kohde tekemään vahingollisia toimia hyökkääjän hyödyksi. Hyökkääjä voi myös väärentää numeron, josta soittaa, niin että puhelu vaikuttaa tulevan luotettavalta henkilöltä tai yritykseltä. (Longtchi ym. 2024, 230.) Vishing-hyökkäyksessä hyödynnetään kiireen luomista, palkinnolla houkuttelua, suostuttelua, esiintymistä toisena henkilönä, valetarinoita sekä personointia (Longtchi ym. 2024, 235). Hyökkäyksessä käytetyillä menetelmillä pyritään vetoamaan yksilön luottamukseen ja mukautuvuuteen (Agreeableness) (Longtchi ym. 2024, 230).

Smishing-hyökkäyksessä hyödynnetään mobiilisovelluksia ja lähetetään viestejä, joissa esiinnytään toisena henkilönä ja joissa pyritään houkuttelemaan kohdetta paljastamaan arkaluontoista tietoa hyökkääjälle. Hyökkääjä voi myös väärentää numeron, josta ottaa kohteeseen yhteyttä, jolloin kohteen on vaikeampi havaita olevansa hyökkäyksen kohteena. Jopa ne henkilöt, jotka eivät yleensä vastaa tuntemattomiin viesteihin, saattavat olla alttiita smishing-viesteille, jotka näyttävät

tulevan tutulta lähettäjältä. (Longtchi ym. 2024, 230.) Smishing-hyökkäyksessä hyödynnetään kiireen luomista, palkinnolla houkuttelua (Incentive & motivator), suostuttelua, esiintymistä toisena henkilönä, personointia, valetarinaa sekä houkutusvaikutusta (Longtchi ym. 2024, 235). Näillä tekniikoilla pyritään vetoamaan auktoriteetin kunnioittamiseen, luottamukseen, ahneuteen ja impulsiivisuuteen (Longtchi ym. 2024, 230).

5.6.3 Teknisen tuen hyökkäyksen vaiheet

Yksi yleisimmistä käyttäjän manipuloinnin hyökkäysmuodoista on niin sanottu teknisen tuen huijaus. Hyökkääjä voi esimerkiksi huijata kohteen uskomaan, että tämän tietokoneessa on ongelma, kuten virus tai hidas suorituskyky, ja tarjota apua maksua vastaan. Hyökkääjä voi ottaa suoraan yhteyttä uhriin puhelimitse tai kiinnittää kohteen huomion ponnahdusikkunalla, joka näyttää käyttöjärjestelmän ilmoitusikkunalta. Ilmoituksessa voidaan väittää, että tietokone on saastunut, ja tarjotaan tukea puhelimitse. Jos kohde soittaa ilmoitettuun numeroon, hyökkääjä esiintyy käyttöjärjestelmän julkaisseen tahon teknisen tuen työntekijänä. (Choi 2023, 7.)

On myös mahdollista, että hyökkääjä käyttää käänteistä käyttäjän manipulointia, ja saa muovattua olosuhteet sellaisiksi, että kohde itse ottaa hyökkääjään yhteyttä (Wang ym. 2021, 11899).

Teknisen tuen hyökkäyksen kulku voi olla esimerkiksi seuraavanlainen, mukaillen Wangin ja kollegoiden artikkelissaan esille tuomia vaiheita (Wang ym. 2021, 11906):

Vaihe 1 – Kohteen lähestyminen. Hyökkääjä lähestyy kohdetta, kuten uutta työntekijää, lähettämällä IT-tuen nimissä sähköpostia väärennetystä osoitteesta. Viestissä kerrotaan, että lähiaikoina tullaan suorittamaan verkon testausta, josta mahdollisesti seuraavien verkko-ongelmien ilmetessä pyydetään ottamaan yhteyttä viestissä olevaan (hyökkääjän) numeroon. (Wang ym. 2021, 11906.)

Vaihe 2 – Oikeanlaisen tilanteen luominen. Viestin lähetettyään hyökkääjä aiheuttaa verkkovian ja odottaa kohteena olevan työntekijän yhteydenottoa (Wang ym. 2021, 11906).

Vaihe 3 – Käänteinen käyttäjän manipulointi, tietämättömyyden hyödyntäminen. Hyökkääjä laskee sen varaan, ettei uusi työntekijä ole vielä ehtinyt tutustua kollegoihinsa, eikä välttämättä kokemattomuuttaan vielä tiedä tai ole sisäistänyt kaikkia organisaation käytäntöjä. Kun verkossa ilmenee (hyökkääjän aiheuttama) vika, uusi työntekijä soittaa viestissä ilmoitettuun IT-tuen numeroon. (Wang ym. 2021, 11906.)

Vaihe 4 – Vastavuoroisuus, Foot-in-the-door. IT-tukihenkilönä esiintyvä hyökkääjä auttaa ongelman ratkaisemisessa ja tämän jälkeen pyytää vilpittömästi pientä ”palvelusta”. Tämä ”palvelus” olisi, että uusi työntekijä täyttäisi lyhyen kyselyn, jonka täyttämiseen ”menee vain hetki” ja jota

hyödynnetään turvallisuustietoisuus- ja koulutusohjelman kehittämisessä uusille työntekijöille. Pyynnön yhteydessä IT-tuen edustajana esiintyvä hyökkääjä kertoo, että lähes 80% työntekijöistä on jo täyttänyt kyselyn. (Wang ym. 2021, 11906.)

Vaihe 5 – Luottamusta herättävä viestintä, paineen luominen, ryhmään mukautumisen tarve. ”Uusien työntekijöiden turvallisuustietoisuus- ja koulutusohjelma” -termillä ja vilpittömällä äänensävyllä luodaan luottamusta, ja ”vain pieni hetki”, joka kyselyn täyttämiseen luvataan menevän, lisätään uuden työntekijän halua olla avulias. Painetta kyselyyn vastaamiseen lisää se, että ”80% prosenttia työntekijöistä on jo täyttänyt kyselyn” (ryhmävaikutus, kognitiivinen vinouma). (Wang ym. 2021, 11906.)

Vaihe 6 – Vastapalvelus, ryhmäpaine, itsestä annetun mielikuvan hallinta. Uusi työntekijä haluaa antaa hyvän ensivaikutelman itsestään osoittamalla kykynsä yhteistyöhön ja tehokkaaseen toimintaan. Uuden työntekijän osoittama suostuvaisuus, auttamisenhalu ja mukautuminen liittyvät käytösmalliin, jossa pyritään hallitsemaan itsestä annettua mielikuvaa tai vaikutelma. Vastavuoroisuuden normi vaikuttaa uuden työntekijän harkintaan, ja koska ”IT-tuki” auttoi ongelman ratkaisemisessa, uusi työntekijä antaa myönteisen vastauksen ja sitoutuu vastaamaan kyselyyn. (Wang ym. 2021, 11906.)

Vaihe 7 – Sitoutuminen ja johdonmukaisuus. Hyökkääjä saa uuden työntekijän sitoutumaan kyselyyn vastaamiseen (Wang ym. 2021, 11906).

Vaihe 8 – Luottamuksen luominen, luottamussuhteen hyödyntäminen. Rehellisyyttä ja hyväntahtoisuuden kuvaa korostetaan tavanomaisella keskustelulla salasana- ja sähköpostiturvallisuuskäytännöistä. Näin hyökkääjä pyrkii saavuttamaan korkean luottamustason. (Wang ym. 2021, 11906.)

Vaihe 9 – Ryhmäpaine, luottamus, sitoutuminen ja johdonmukaisuus, vastuun hajautuminen, sisäisen ristiriidan välttäminen. Kaiken tämän jälkeen lause ”Meidän täytyy tietää salasanasi arvioidaksemme uusien työntekijöiden turvallisuustietoutta” ei herätä enää niin suurta huolta kuin sen pitäisi. ”80 % työntekijöistä on jo tehnyt tämän” johtaa vastuuntunnon hämärtymiseen. Lisäksi sitoutumisen ja johdonmukaisuuden käytösmallit ”pakottavat” kohteena olevan uuden työntekijän jatkamaan tietojen antamista sisäistä ristiriitaa välttääkseen. (Wang ym. 2021, 11906.)

Vaihe 10 – Luottamussuhteen hyödyntäminen. Huolta lievennetään korostamalla, että kyseessä on turvallinen toimenpide ilman vaaraa, ja ilmaisemalla, että salasanan tarkastaminen on turvallisuuteen liittyvä rutiini, jonka avulla uusien mitataan työntekijöiden tietoturvatietoisuutta. Tässä vaiheessa hyökkääjä on käyttänyt suuren joukon psykologiaan vetoavia menetelmiä ja hyödyntänyt psykologisia haavoittuvuuksia. (Wang ym. 2021, 11906.)

Vaihe 11 – Hyökkäyksen onnistuminen. Kohteena oleva uusi työntekijä paljastaa lopulta salasanansa IT-tukena esiintyvälle hyökkääjälle uskoen, että se on rutiinimenettely (Wang ym. 2021, 11906).

5.6.4 BEC-hyökkäyksen vaiheet

BEC-hyökkäykset onnistuvat usein tehokkaasti kohdennetun käyttäjän manipuloinnin ansiosta, ja näissä hyökkäyksissä pyritään ohittamaan tekniset suojauskeinot vaikuttamalla henkilökohtaisiin suhteisiin (Cross & Gillett 2020, 871).

Julkisesti saatavilla olevien materiaalien avulla hyökkääjä analysoi esimerkiksi niiden henkilöiden kirjoitustyylejä, joina he aikovat esiintyä. BEC-hyökkäystä suunnittelevat rikolliset voivat viettää viikkoja tai kuukausia tutkimalla kohteena olevaa organisaatiota tai sen työntekijöitä. Tällaiset kohdennetut hyökkäykset vievät siis prosessina kokonaisuudessaan huomattavasti aikaa, mutta hyökkäyksen lopputulos on yleensä myös vaikutukseltaan melko suuri. Huijauksen onnistumisen todennäköisyys kasvaa suhteessa siihen tiedon määrään, jota hyökkääjä onnistuu organisaatiosta keräämään. (Cross & Gillett 2020, 871.)

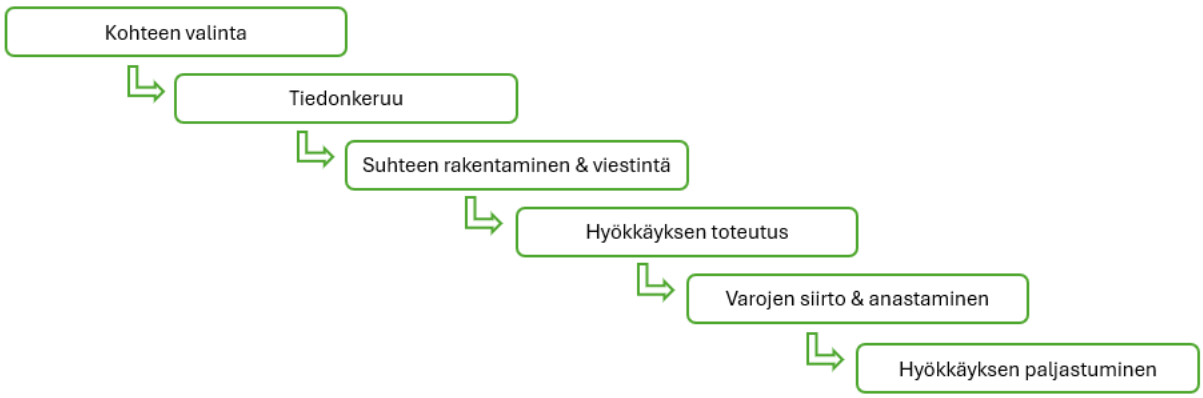
BEC-huijauksessa hyökkääjä voi hyödyntää organisaation olemassa olevia suhteita esimerkiksi liikekumppaneihin tai tavarantoimittajiin. Hyökkääjä esiintyy työntekijänä, tavarantoimittajana tai muuna luotettavana liiketoimintaan liittyvänä henkilönä saadakseen haltuunsa varoja, tilinumeroita, pääsykoodeja tai muuta arkaluontoista tietoa. Tyypillistä on, että kohdetta pyydetään siirtämään rahaa rikoksentekijän hallinnoimalle tilille. (Cross & Gillett 2020, 872.)

Hyökkääjän kyky esiintyä uskottavasti henkilönä tai organisaationa riippuu useista tekijöistä. Hyökkääjä voi esimerkiksi kaapata aidon sähköpostitilin tai luoda uuden tilin, joka muistuttaa suuresti aitoa osoitetta. On myös todennäköistä, että hyökkääjä räätälöi viestinsä kyseisen organisaation erityispiirteiden mukaan. Tämä voi tarkoittaa esimerkiksi ylimmän johdon matkasuunnitelmien tai yrityksen toimintatapojen tutkimista. (Cross & Gillett 2020, 873.)

BEC-hyökkäyksen menestys perustuu monien yksinkertaisten tekniikoiden tehokkaaseen hyödyntämiseen. Vaikka hyökkääjä voi käyttää hyökkäyksensä tukena myös monimutkaisia teknisiä keinoja, suurin osa käytetyistä menetelmistä on luonteeltaan yksinkertaisia ja nojaa tehokkaaseen käyttäjän manipulointiin. Hyökkäyksissä hyödynnetään erityisesti auktoriteettia ja kiireellisyyden tunteen luomista. (Cross & Gillett 2020, 873–874.)

Hyökkäys onnistuu, jos rikoksentekijä onnistuu kohdistamaan toimintansa tarkasti kohteen tiettyihin haavoittuvuuksiin tai heikkouksiin. Tämän mahdollistamiseksi hyökkääjä voi tehdä perusteellista tutkimusta organisaatiosta ja siihen liittyvistä henkilöistä, jolloin hyökkäyksessä osataan rakentaa

uskottava huijaus. Tällainen räätälöity lähestymistapa perustuu tietomurroista, tilikaappauksista ja julkisesti saatavilla olevista lähteistä, kuten sosiaalisesta mediasta tai organisaation verkkosivuilta, kerättyyn tietoon. Kun hyökkääjä on perehtynyt organisaation toimintaan, hän voi laatia erittäin vakuuttavia ja uskottavia sähköposteja, jotka todennäköisemmin saavat kohteen toimimaan halutulla tavalla. (Cross & Gillett 2020, 874.)



Kuva 4. BEC-hyökkäyksen vaiheet (mukaillen Saud Al-Musib ym. 2023, 500–501)

Kuvassa 4 on havainnollistettu BEC-hyökkäyksen kulku. Saud Al-Musib ja kollegat (2023, 500–501) kuvaavat artikkelissaan BEC-hyökkäyksen kulkua seuraavasti:

Vaihe 1. Kohteen valinta – Hyökkääjä valitsee organisaation, johon kohdistaa hyökkäyksen (Saud Al-Musib ym. 2023, 500–501).

Vaihe 2. Tiedonkeruu – Hyökkääjä etsii tietoa yrityksestä, hyödyntäen esimerkiksi sosiaalista mediaa tai nettisivuja tai jopa puhelinsoittoa, saadakseen yksityiskohtaista tietoa, jota hyödyntää luottamuksen rakentamisessa (Saud Al-Musib ym. 2023, 500–501).

Vaihe 3. Suhteen rakentaminen ja viestintä – Hyökkääjä lähestyy kohdetta (henkilöä, joka hallinnoi rahaliikennettä) luotettavan ja uskottavan oloisella viestillä, joka näyttää tulevan toimitusjohtajalta tai talousosaston johtajalta. Viestittely saattaa jatkua jopa viikkojen ajan, jotta hyökkääjä saa luottamuksen rakennettua. (Saud Al-Musib ym. 2023, 500–501.)

Vaihe 4. Hyökkäyksen toteutus – Kun kohteen luottamus on saavutettu, hyökkääjä pyytää kiireellistä ja salaista rahansiirtoa. Summa on usein sellainen, ettei se herätä epäilyksiä, ja pyyntö voidaan naamioida joksikin hankinnaksi. Maksutoimeksiannon antanut ”johtaja” ei myöskään ole

puhelimitse tavoitettavissa, koska hän on ”kokouksessa” tai ”matkoilla”. (Saud Al-Musib ym. 2023, 500–501.)

Vaihe 5. Varojen siirto ja anastaminen – Rahat siirretään hyökkääjän ulkomaiselle pankkitilille, jonka omistajakin on todennäköisesti tuntematon (Saud Al-Musib ym. 2023, 500–501).

Vaihe 6. Hyökkäyksen paljastuminen – Hyökkäys paljastuu todennäköisesti vasta siinä vaiheessa, kun rahat ovat jo hyökkääjän hallussa (Saud Al-Musib ym. 2023, 500–501).

5.7 Yhteenveto tuloksista

Tässä alaluvussa käydään läpi tutkimusaineistosta tutkimuskysymysten perusteella ja tietoperustassa läpikäytyihin hyökkäysmenetelmiin pohjautuen esiin nousseet havainnot.

5.7.1 Haavoittuvuuksiksi miellettävät psykologiset tekijät

Ensimmäisen tutkimuskysymyksen tavoitteena oli selvittää, mitkä psykologiset tekijät voidaan nähdä haavoittuvuutena kyberturvallisuuden kontekstissa. Tutkimusaineistosta tutkimuskysymyksen perusteella tehtyjen johtopäätösten pohjalta voidaan sanoa, että kyberturvallisuuden kontekstissa haavoittuvuuksina voidaan nähdä yksilölliset psykologiset ja inhimilliset tekijät, jotka voivat tehdä yksilöstä alttiimman manipuloinnille. Eri hyökkäystyypeissä käytetään tarkoituksellisesti eri psykologisia vaikutuskeinoja, joilla tavoitellaan hyökkäyksen kohteelta reaktiota, kuten auktoriteetin kunnioittamista, pelkoa, kiireen kokemuksen heikentämää harkintakykyä, auttamisen halua ja luottamuksen tunnetta. Näillä keinoilla pyritään vaikuttamaan hyökkääjälle edullisesti siihen, miten kohteena oleva yksilö havainnoi, ajattelee ja toimii.

Auktoriteettia kunnioittavat psykologiset piirteet voidaan nähdä haavoittuvuutena erityisesti niissä hyökkäyksissä, joissa hyökkääjä pyrkii esiintymään esimerkiksi organisaation johtoportaan edustajana, kuten toimitusjohtajahuijauksessa, BEC-huijauksessa ja spear phishing-hyökkäyksessä.

Myös kiireen luominen yhdisti useita hyökkäystyyppejä, joten inhimillinen reagoiminen kiireen tunteeseen voidaan nähdä kyberturvallisuuden kontekstissa haavoittuvuutena. Erityisesti auktoriteettiasemasta asetettu kiireen tuntu vaikuttaa olevan tehokas menetelmä hallita kohteen toimintaa (F-Secure 2024). Tutkimusaineistosta tehdyistä havainnoista kävi ilmi, että kiire voi laskea yksilön kykyä harkita ja ajatella (Longtchi ym. 2024, 220; Wang ym. 2021, 11900). Luomalla kiireen tuntua hyökkääjä pyrkii vetoamaan esimerkiksi ihmisen haluun tehdä hyvä vaikutus esihenkilöön tekemällä työnsä hyvin ja tehokkaasti tilanteessa, jossa odotetaan ripeää toimintaa. Kiireen luominen vaikuttaa olevan hyökkääjää hyödyntävä menetelmä esimerkiksi perusmuotoisessa tietojenkalastelussa, kun kohteena olevaa painostetaan toimimaan asettamalla aikarajoja, sekä smishing- ja

vishing-hyökkäyksissä esimerkiksi rajoittamalla ”palkinnon” lunastamisajankohtaa. Myös toimitusjohtaja- ja BEC-huijauksissa kiireellinen maksutoimeksianto vaikuttaa olevan erityisen olennainen osa hyökkäystä.

Ihmisellä on taipumus olla vähemmän tarkkaavainen, kun viesti tulee oletetusti tutulta taholta (Järvinen 2022, 224; Wang ym. 2021, 11897). Niinkin inhimillinen ja normaali piirre, kuin tuttuun tai luotettavaksi oletettuun tahoon luottaminen voidaan nähdä kyberturvallisuudessa haavoittuvuutena. Luottamuksen luominen ja hyödyntäminen vaikuttaa tutkimusaineiston perusteella olevan hyvin olennainen osa kohdennetun käyttäjän manipuloinnin hyökkäyksiä. Luottamusta pyritään luomaan ja hyödyntämään huolellisesti suunnitelluissa hyökkäyksissä hyvin monitahoisesti. Hyökkääjä on tehnyt läksynsä, ja pyrkii viestinnässään herättämään luottamusta viestin ulkoasusta aina tekstin sisältöön ja esittämänsä henkilön kirjoitustyyliin. Hyökkääjä pyrkii myös kartoittamaan kohteensa ympäristöstä ne henkilöt, joilla on auktoriteettiasema suhteessa kohteeseen, tai ne henkilöt, joita kohteen voidaan selvitystyön perusteella päätellä pitävän luotettavana, kuten esimerkiksi yhteistyökumppania. Luottamusta pyritään hyödyntämään erityisesti toimitusjohtajahuijauksessa, BEC-huijauksessa, spear phishing- ja whaling-hyökkäyksissä.

5.7.2 Käyttäjän manipuloinnin hyökkäyksissä hyödynnettävät psykologiset menetelmät

Toisen tutkimuskysymyksen avulla pyrittiin kartoittamaan, mitä psykologisia menetelmiä käyttäjän manipuloinnin hyökkäyksissä hyödynnetään. Tutkimusaineistosta pystyi selkeästi havaitsemaan, että käyttäjän manipuloinnin hyökkäyksissä hyödynnettävien psykologisten menetelmien yhdistävänä tekijänä on tarkoitus ohjailla kohteen toimintaa vetoamalla yksilöllisiin psykologisiin piirteisiin. Näitä hyökkäyksissä hyödynnettäviä psykologisia menetelmiä ovat esimerkiksi ryhmäpaineen hyödyntäminen, kiireen luominen, pelottelu, tunteisiin vetoaminen sekä luottamuksen vaiheittainen rakentaminen ja hyödyntäminen. Näissä menetelmissä nousi vahvasti esiin totuuden muuntelu, valheellisen luottamussuhteen luominen, sekä myönteisinä pidettyjen ominaisuuksien hyödyntäminen. Kohteeseen ja tämän toimintaympäristöön perusteellisesti perehtymällä hyökkääjä voi joiltain osin varmistaa sen, että käytettävät psykologiset menetelmät on mahdollista optimoida hyödyntämään kohteeksi valitun yksilön yksilöllisiä persoonallisuuden piirteitä ja toimintamalleja.

Tutkimusaineiston perusteella tehtyjen havaintojen mukaan ryhmäpainetta hyödynnetään luodessa tilannetta, jolla painostetaan käyttäjää toimimaan tietoturvan vaarantaen uskoessaan, että myös muut ovat toimineet samalla tavalla (Longtchi ym. 2024, 218; Wang ym. 2021, 11898). Ryhmäpainetta voidaan siis hyödyntää esimerkiksi huijauspuhelussa, jossa kohteelle kerrotaan lähes kaikkien muiden työntekijöiden suorittaneen jonkin toiminnon, jota häneltä nyt odotetaan (Wang ym. 2021, 11906). Samaa logiikkaa voidaan hyödyntää painostaessa kohdetta klikkaamaan

tietojenkalasteluviestiä uskottelemalla, että enemmistö organisaatiossa on suorittanut toiminnon, johon linkkiä klikkaamalla päätyy.

Hyökkääjä voi pyrkiä esimerkiksi auktoriteettiasemalla herättämään tunteita, kuten pelkoa tai kunnioitusta. Tutkimusaineiston mukaan voimakas tunnetila, kuten pelko esimerkiksi työtehtävissä epäonnistumisesta voi vaikuttaa voimakkaasti yksilön harkintakykykyyn (Wang ym. 2021, 11903). Työtehtävissä epäonnistumisen pelon luominen vaikuttaa tutkimusaineiston perusteella olevan melko yleinen elementti auktoriteettiasemaa hyödyntävissä hyökkäyksissä, kuten BEC- ja toimitusjohtajahuijauksissa ja laskutushuijauksissa. Pelkoa voidaan pyrkiä hyödyntämään myös smishing-hyökkäyksissä kohteen toimintaa ohjailevana elementtinä (Longtchi ym. 2024, 221–222).

5.7.3 Kohdennetun käyttäjän manipuloinnin hyökkäyksen vaiheet

Kolmannen tutkimuskysymyksen avulla haluttiin selvittää, millaisia vaiheita kohdennettu käyttäjän manipuloinnin hyökkäys sisältää. Tutkimusaineistona olleissa artikkeleissa hyökkäyksen vaiheet kuvattiin melko samankaltaisina. Kohdennetut käyttäjän manipuloinnin hyökkäykset sisältävät useita vaiheita. Niillä on tietty, melko samanlainen, perusrakenne, vaikka käytetyt tekniset ja psykologiset menetelmät, sekä hyökkäyksen kohde vaihtuvat. Tutkimusaineistosta kootun tiedon perusteella vaiheet etenevät yleisesti ottaen seuraavasti:

- kohteen valinta ja selvitystyö,
- luottamuksen rakentaminen ja viestien vaihto kohteen kanssa,
- luottamuksen hyödyntäminen ja toimintaan ohjaaminen,
- hyökkäyksessä tavoitellun hyödykkeen, kuten rahojen tai käyttäjätunnusten, haltuun saaminen.

Hyökkäyksen eri vaiheissa hyödynnetään kussakin vaiheessa optimaalisinta psykologista menetelmää. Esimerkiksi luottamuksen rakentamisen vaiheessa hyökkääjä pyrkii luomaan itsestään omalla toiminnallaan ja viestinnällään mahdollisimman luotettavan vaikutelman. Kiireen tunnun luomisella pyritään poissulkemaan kohteelta mahdollisuus ajatella ja harkita toimintaansa. Myös se on yleistä, että hyökkääjä tavalla tai toisella lavastaa tilanteen ja olosuhteet niin, että kohde itse ottaa yhteyttä hyökkääjään.

Myös tietoperusta tukee tutkimusaineistosta tehtyjä havaintoja kohdennetun käyttäjän manipuloinnin hyökkäyksen suunnitelmallisuudesta ja hyökkääjän huolellisesta perehtymisestä kohteeseensa. Erityisen suunnitelmallista toiminta vaikuttaa olevan toimitusjohtaja-, BEC- ja whaling-huijauksissa, joissa hyökkääjä tekee perusteellista selvitystyötä ennen kuin lähestyy kohdettaan, hyödyntäen kaikkea haltuunsa saamaa tietoa aina organisaation nettisivujen ja LinkedIn-julkaisujen tietojen hyödyntämisestä jopa kuukausia kestävään organisaation sähköpostiliikenteen tarkkailuun (F-Secure 2024b; Hyppönen 110–111; Järvinen 2022, 224;).

6 Pohdinta

Tässä luvussa tehdään johtopäätöksiä tutkimuksessa havaituista tuloksista, sekä tarkastellaan tutkimuksessa havaittuja aihepiiriin liittyviä jatkotutkimuksen tarpeita. Luvussa tehdään myös yhteenveto tutkimusprosessista, sekä käsitellään myös omaan oppimisprosessiin sisältyneet haasteet, onnistumiset ja havainnot.

6.1 Johtopäätökset

Tutkimustulosten perusteella voidaan todeta, että kohdennetun käyttäjän manipuloinnin hyökkäysten menetelmissä on olennaista manipuloinnin keinojen kohdistaminen yksittäisiin ihmisiin. Kyberuhilta suojautuminen vaatii siis teknisten toimenpiteiden lisäksi myös järjestelmiin sidoksissa olevien ihmisten valmentamista kohtaamaan uhkia, jotka vetoavat psykologisiin ja inhimillisiin piirteisiin. On myös hyvä huomioida, että tietoa tällaisista uhista ja merkeistä, joista ne voi tunnistaa, on hyvä levittää laajemminkin yhteiskunnassa. Kohdennetun käyttäjän manipuloinnin tai tietojenkalastelun hyökkäykset eivät ole uhka pelkästään suurille organisaatioille, vaan myös pienemmät organisaatiot tai yksityishenkilöt voivat olla hyökkääjälle potentiaalisia kohteita.

Yksi syy, miksi nämä huijausmenetelmät ovat niin tehokkaita on se, että ne ovat kehittyneet pitkän ajanjakson aikana. Psykologisia toiseen ihmiseen vaikuttamisen menetelmiä on hiottu vuosisatojen saatossa, ja huijareita on ollut jo kauan ennen harppausta digitaaliseen yhteiskuntaan. Lisäksi nämä menetelmät hyödyntävät usein kunniallisina ja arvostettavina pidettäviä piirteitä, kuten auttamisenhalua, empatiaa ja halua hoitaa työnsä hyvin.

Hyökkäystavoissa on havaittavissa selkeitä yhtäläisyyksiä. Etenkin kohdennetuissa käyttäjän manipuloinnin hyökkäyksissä kohteesta otetaan perusteellisesti selvää, ennen kuin tätä lähestytään. Valmistelut tehdään huolellisesti ja onnistumisen eteen voidaan nähdä paljonkin vaivaa, tästä esimerkkinä pitkäjänteinen toiminta luottamussuhteen luomiseksi hyökkääjän ja kohteen välille. Tämä vaikuttaa olevan toinen vahva tekijä hyökkäysten onnistumisen taustalla. Hyökkääjä ikään kuin ”sulautuu” ympäristöönsä ennen ”loppuhuipennusta”.

Kohdennettujen käyttäjän manipuloinnin hyökkäysten ydin vaikuttaa olevan ennemminkin psykologinen kuin tekninen. Hyökkäyksissä vaikuttaa olevan melko vahvasti yhdistävänä tekijänä juuri manipuloinnin keinot, joiden tunnistamiseen olisi syytä kiinnittää organisaatioissa huomiota.

Organisaatioiden olisikin siis hyvä panostaa jatkuvaan ja yksilöä palkitsevaan tietoisuuden lisäämiseen ja koulutukseen. Uuden ajan kyberuhkilta suojautumisessa voisi pitää hyvänä lähtökohtana sitä, että organisaation henkilöstön valmius tunnistaa manipulaation piirteitä olisi entistä keskeisempi osa nykyaikaista organisaation kyberturvallisuutta.

Cross ja Gillings (2020) käsittelivät BEC-hyökkäyksiä käsittelevässä tutkimuksessaan myös rikoksen uhriksi joutuneen yksilön kokemuksia ja sitä, kuinka kohteena tahtomattaan ollut yksilö usein asetetaan yksin vastuuseen tällaisista huomattavista hyökkäyksen jälkeisistä taloudellisista seurauksista. On olemassa useampi tapaus, joissa inhimillisellä virheellä on ollut mittavia seurauksia, joista vastuun ottaminen ja henkisten seurausten käsittely on jäänyt täysin yksilön vastuulle. (Cross & Gillings 2020, 875–876.)

Hyökkäyksen kohteeksi joutuneessa organisaatiossa työskentelevän, itsekin kohteeksi ja uhriksi joutuneen yksilön kokemus on erittäin tärkeä näkökulma esille nostettavaksi. Rikoksen uhriksi joutuu organisaation lisäksi myös kohteena tahtomattaan ollut yksilö. Tällaisen rikoksen uhrilla on usein kannettavanaan työtehtävässään epäonnistumisen taakan lisäksi myös syyllisyyttä ja häpeää. Organisaatioiden käytäntöjä kohdennetun käyttäjän manipuloinnin uhriksi joutuessa olisikin siis hyvä tarkastella myös siitä näkökulmasta, että yksilö, jota hyödyntämällä hyökkäys on onnistunut, on myös uhri, jonka inhimillinen virhe on seurausta hyvin järjestelmällisesti toteutetusta manipulaatiosta. Hyvin tärkeää hyökkäyksen uhriksi joutuneen yksilön inhimillisen kohtelun lisäksi näissä tilanteissa olisi myös nähdä ne tekijät, jotka ovat johtaneet hyökkäyksen onnistumiseen, jotta niiden avulla voitaisiin kehittää puolustusta tulevaisuudessa.

6.2 Kehittämisehdotukset ja suositukset jatkotutkimukselle

Tutkimusaineiston perusteella voidaan todeta, että yksilön päätöksentekoon ja käyttäytymiseen vaikuttavat tekijät ovat teknisen suojauksen lisäksi keskeinen osa-alue kyberturvallisuudessa etenkin kohdennettuihin manipuloinnin hyökkäyksiin varautumisen osa-alueella.

Yksi lähestymistapa ”inhimillisen” suojauksen tehokkuuden lisäämiseen voisi olla se, että ihminen nähtäisiin riskin sijaan osana hyökkäyksiin varautumisen ja puolustuksen mekanismeja. Kuten tietoturvaohjelmistoja, myös ihmisen osaamista tulisi päivittää säännöllisesti.

On toki ymmärrettävää, että ihminen, jolla on heikko tekninen osaaminen, voi kokea erityisen kuormittavana kaiken tietotekniikkaan tai tietoturvaan liittyvän ”ylimääräisen”. Myös erinäisistä tekijöistä johtuvat asenteen haasteet lisäävät riskejä huomattavasti. Olisi siis hyvä tutkia, onko mahdollista löytää keinoja, joilla tietoturvalle asennoitumisellaan tietoisesti tai tiedostamatta riskejä aiheuttava yksilö saataisiin muuttamaan asennettaan tietoturvallisempaan suuntaan. Suhtautumiseen vaikuttanee vahvasti ainakin se, jos yksilö kokee tietoturvaan panostamisen lisäävän kuormitusta. Myös sitä olisi hyvä tutkia, olisiko organisaatiossa mahdollista ja kannattavaa luoda olosuhteet, joissa tietoturvalliseen toimintaan panostaminen on palkitsevaa.

Myös organisaatiokulttuuriin ja yksilön kokonaiskuormitukseen on siis hyvä kiinnittää huomiota. Kun yksilöllä on liikaa kuormitusta, se heikentää kykyä havaita tai torjua uhkia. Usein

ylikuormittunut yksilö oireilee muutenkin kuin unohtelemalla asioita ja pitkäaikainen ylikuormitus voi vaikuttaa myös työn tuottavuuteen. Tietojärjestelmissäkin on huomioitu tilanteet, joissa suorituskyky ylittyy. Laitteistot on suojattu ylikuormittumiselta, ja turvamekanismina laitteesta voidaan ajoissa katkaista virta esimerkiksi ylikuumenemisen varalta.

Yhteiskunnassa on myös melko yleinen taipumus, muuallakin kuin kyberturvallisuuden saralla, piilotella virheitä tai hävetä rikoksen uhriksi joutumista. Erityisesti rikoksen uhreiksi joutuneilla yksilöillä on yleistä, että häpeä ja trauma aiheuttavat tapahtuneen kieltämistä tai piilottelua, rikoksen tyypistä riippumatta. Kuten monilla elämänalueilla, myös kyberturvallisuuden saralla, erityisesti niistä tilanteista, joissa jokin on mennyt pieleen ja hyökkäys on onnistunut, voidaan oppia eniten. Tämän takia olisi ensiarvoisen tärkeää tuoda enemmän esille onnistuneita hyökkäyksiä ja tutkia syitä, miksi hyökkäys on onnistunut.

Cross ja Gillett nostivat tutkimuksessaan esille, miten vakavia henkisiä seurauksia yksityishenkilölle aiheutuu petoksen uhriksi joutumisesta ja mainitsivat, että vastaavia seurauksia ei ole paljoa tutkittu yritysmaailmassa (Cross & Gillett 2020, 875–876).

Onnistuneiden hyökkäysten saralla olisi siis myös hyvä kiinnittää huomiota yksilöön, joka on sattunut organisaatiossa käyttäjän manipuloinnin hyökkäyksen uhrin epäonniseen asemaan työtehtävissään. Olisi hyvä tutkia, millainen tämän yksilön kokemus on itse tapahtumasta, mitä tästä voisi oppia, ja miten uhriksi joutunut organisaatio kohtelee työntekijää, joka on tapahtumaketjussa myös uhrin asemassa. On myös kiinnitettävä huomiota siihen, yleisesti ottaenkin, että joissain tapauksissa rikoksen tekijä nimenomaan hyötyy rikoksen salailusta. Nopea reagointi tapahtuneen jälkeen saattaa siis vaikuttaa olennaisesti hyökkäyksen seurausten laajuuteen, jos esimerkiksi rahansiirrot pystytään keskeyttämään. Tiedon lisääminen auttaa myös muita organisaatioita olemaan entistä tehokkaammin varuillaan hyökkäysten varalta. Organisaation maineen kannalta on toki ymmärrettävää, ettei tietomurroista tai rikoksen uhriksi joutumisesta kovin vapaaehtoisesti tehdä julkista tietoa.

Yhteenvetona voikin siis sanoa, että ihmisten tietoisuus kyberrikollisten käyttämistä psykologisista keinoista kyberturvallisuuden osa-alueena on erittäin kriittinen. Varautuminen ja suojautuminen vaatii koko yhteiskunnalta, niin yksilöiltä kuin organisaatioiltakin, jatkuvaa kehittymistä ja valppautta. Rikolliset eivät lepää laakereillaan, vaan heidän käyttämänsä menetelmät kehittyvät jatkuvasti.

Tulevaisuuden tutkimuksessa on myös hyvä huomioida tekoälyn kehittyminen ja sen rikollisille tarjoamat mahdollisuudet kehittää jatkuvasti tehokkaampia ja uskottavampia välineitä hyökkäysten toteuttamiseen.

6.3 Yhteenveto tutkimusprosessista

Opinnäytetyön tarkoituksena oli luoda ajantasainen katsaus organisaation henkilöstöön kohdistuviin kohdennetun käyttäjän manipuloinnin uhkiin. Painopisteenä tutkimuksessa oli selvittää hyökkäysten psykologinen puoli, eli inhimilliset haavoittuvuudet ja psykologiset menetelmät, joilla näitä haavoittuvuuksia hyödynnetään hyökkäyksen eri vaiheissa.

Ilmiön tarkastelulle määriteltiin tietoperustassa teoreettinen viitekehys, eli kyberuhat, joissa olennaisena elementtinä on käyttäjän manipulointi, ja jotka kohdistuvat organisaation työntekijään tämän työtehtävien puitteissa. Uhkat pyrittiin rajaamaan niin, että esille nostettiin ne uhat, joissa hyökkääjä lähestyy kohdetta yksilönä ja hyökkäys sisältää hyökkääjän ja kohteen välistä vuorovaikutusta. Tietoperustassa tällaisiksi uhiksi määriteltiin tietojenkalastelu, spear phishing, whaling, vishing, smishing, toimitusjohtajahuijaus, valelasku ja BEC-huijaus. Perusmuotoinen tietojenkalastelu ei täysin täytä tätä rajausta, mutta otettiin mukaan, koska menetelmän avaaminen oli tarpeen kohdennettujen tietojenkalastelun menetelmien määrittelyssä.

Opinnäytetyön empiirisessä osassa tarkasteltiin kuvailevan kirjallisuuskatsauksen menetelmin tietoperustassa määriteltyyn viitekehykseen peilaten organisaation henkilöstöön kohdistuvissa kohdennetun käyttäjän manipuloinnin hyökkäyksissä hyödynnettäviä psykologisia menetelmiä, sekä psykologisia ja inhimillisiä piirteitä, joita kyberturvallisuuden näkökulmasta voidaan pitää haavoittuvuuksina.

Kirjallisuuskatsauksessa haettiin vastausta seuraaviin tutkimuskysymyksiin:

- Mitkä psykologiset tekijät voidaan nähdä haavoittuvuuksina kyberturvallisuuden kontekstissa?
- Mitä psykologisia menetelmiä käyttäjän manipuloinnin hyökkäyksissä hyödynnetään?
- Mitä vaiheita ja psykologisia menetelmiä kohdennettu käyttäjän manipuloinnin hyökkäys sisältää?

6.4 Tutkimuksen eettisyys ja luotettavuus

Tutkimuksen luotettavuuden ja läpinäkyvyyden takaamiseksi tutkimusaineiston kerääminen dokumentoitiin niin, että se on täysin toistettavissa. Tutkimusaineistoksi valittiin tieteellisiä, vertaisarvioituja artikkeleita, joiden ajankohtaisuus varmistettiin tekemällä melko tiukka rajaus hakuehtoihin julkaisuajankohdan suhteen. Näin pyrittiin takaamaan, että tehtävä tutkimus pohjautuu ajankohtaiseen ja luotettavaan materiaaliin.

Tutkimuksen luotettavuuden arvioinnissa otettiin huomioon, että käytetty tutkimusaineisto oli melko suppea, jonka voidaan katsoa heijastuvan johtopäätösten yleistettävyyteen. Valittu aineisto kuitenkin täytti kirjallisuuskatsauksen vaatimukset ja sen perusteella pystyttiin muodostamaan syvällinen,

ajantasainen ja kattava kuva käyttäjän manipuloinnin hyökkäysten vaiheista ja psykologisista elementeistä.

Haasteeksi termien luotettavuuden saralla havaittiin erityisesti BEC-hyökkäyksen ja toimitusjohtajahuijauksen määritelmien epäyhtenäisyys eri lähteissä, etenkin työn tietoperustaa rakentaessa. Koska virallisia määritelmiä ei ole, näiden kahden termin välinen rajanveto oli hieman hankalaa, sillä useissa lähteissä kyseiset termit oli määritelty melko vaihtelevasti. Opinnäytetyön tietoperustaa varten näiden kahden termin kohdalla piti nähdä siis hieman enemmän vaivaa, jotta termit sai määriteltyä selkeästi niin, että kyseisten hyökkäystapojen ominaispiirteet ovat selkeästi ja mahdollisimman totuudenmukaisesti erotettavissa. Melko laajan tutkimustyön perusteella tässä työssä päädyttiin rajaamaan ja määrittelemään kyseiset hyökkäystavat useassa lähteessä mainittujen yhtenevien ominaispiirteiden perusteella, eli painottamaan sitä, että toimitusjohtajahuijauksessa korostuu auktoriteettiaseman hyödyntäminen ja kiireellinen maksutoimeksianto, ja BEC-huijauksessa keskeistä taas on organisaation sähköpostiliikenteen seuraaminen ja/tai hyödyntäminen. Kuitenkin työn edetessä ja kokonaisuuden selkeytyessä oli havaittavissa, että kohdennetun käyttäjän manipuloinnin hyökkäykset ovat monissa tapauksissa teonkuvaukseltaan melko toistensa kaltaisia ja hyökkäystyypit muistuttavat hyvin paljon toisiaan. Rajanveto juuri tiettyjen ominaisuuksien osalta oli siis looginen valinta, kun haluttiin selkeyttää näiden kahden termin lisäksi myös muiden kohdennetun käyttäjän manipuloinnin hyökkäystyyppien määrittelyä.

Myös toinen työn aiheen kannalta olennainen, termien määrittelyyn liittyvä haaste ilmeni psykologian termien käännöstyössä. Tämä oli kuitenkin haaste enemmänkin vain ajankäytön kannalta, sillä psykologian termeistä on olemassa suurilta osin viralliset suomenkieliset määritelmät ja kattavasti suomenkielistä aineistoa. Käännöstyö pyrittiin siis tekemään työn kaikissa vaiheissa huolellisesti ja termit useammasta lähteestä tarkistaen niin, että käsitteiden merkitys säilyy käännöksessä.

Prosessin kaikissa vaiheissa, aineiston haussa, käsittelyssä ja analysoinnissa, noudatettiin hyvän tieteellisen käytännön menettelytapoja. Tutkimustyön kaikissa vaiheissa huomioitiin rehellisyys, objektiivinen näkökulma ja tiedon esittämistapa, läpinäkyvyys ja jäljitettävyys, sekä käytettyjen lähteiden erityisen huolellinen merkitseminen. Koko tutkimusprosessin kulku ja työn eri vaiheet dokumentoitiin huolellisesti.

6.5 Oma oppiminen

Opinnäytetyöni rakentaminen lähti liikkeelle väitteen ”ihminen on tietoturvan heikoin lenkki” pohjalta. Aiheen valintaan vaikutti vahvasti mielenkiintoni kyberturvallisuuteen ja psykologiaan, sekä inhimilliseen näkökulmaan digiajan turvallisuudessa. Halusin saada lisää ymmärrystä siitä, miksi juuri yksilöön kohdistetut hyökkäykset onnistuvat, varsinkin niissä tapauksissa, joissa kohteena

oleva henkilö on koulutettu ja tietoinen uhista. Tällaiset ihmiseen kohdistuvat kyberuhat ovat merkityksellinen tutkimuksen kohde, sillä nyky-yhteiskunnassa lähes jokainen yksilö on tavalla tai toisella digitaalisten sovellusten ja palvelujen käyttäjä. Jos tällaisia räätälöityjä hyökkäyksiä havainnoimaan koulutettu henkilö voi joutua huijauksen uhriksi, mitä tämä tarkoittaa laajemmassa mittakaavassa esimerkiksi yksilölle, jolla ei ole vastaavaa koulutustaustaa tai ymmärrystä? Halusin siis selvittää, mitkä ovat ne tekijät ihmisessä, jotka nähdään haavoittuvuuksina kyberturvallisuudessa.

Opinnäytetyöprosessi syvensi merkittävästi ymmärrystäni kahdelta tieteenalalta, kyberturvallisuudesta ja ihmisen psykologiasta. Olin yllättynyt, kuinka voimakkaasti nämä kaksi tieteenalaa käyttäjän manipuloinnin hyökkäyksissä kytkeytyvät toisiinsa. Opinnäytetyöni aiheen monitieteinen luonne edellytti siis opinnäytetyöprosessin aikana perehtymistä sekä kyberturvallisuuteen, eli hyökkäysten menetelmiin, että niihin kytkeytyviin psykologisiin tekijöihin rinnakkain. Tämä auttoi hahmottamaan sitä, miten positiivisiksikin mielletyistä inhimillisistä tekijöistä voi muodostua haavoittuvuuksia kyberturvallisuuden näkökulmasta katsottuna.

Koen, että valitsemaani aihepiiriin perehtyminen laajensi ymmärrystäni valtavasti ja auttoi käsittämään, kuinka merkittävä ja nopeasti kehittyvä osa-alue esimerkiksi ainoastaan kohdennettu tietojenkalastelu on kyberturvallisuuden kannalta. Yllätyin myös siitä, kuinka laaja ja moniulotteinen aihealue käyttäjän manipuloinnin psykologinen puoli on ja aiheeseen syvemmin perehdyttyäni ymmärsin, kuinka keskeisessä roolissa ihmisen ajattelu, päätöksenteko ja toiminta ovat käyttäjän manipuloinnissa. Ennakko-oletusteni mukaan tutkimuksista myös ilmeni, että yksilön asenteilla ja käytösmalleilla on huomattava vaikutus tietoturvallisuuteen.

Psykologisiin tekijöihin perehtyminen lisäsi huomattavasti ymmärrystäni ihmisen käyttäytymis- ja ajatusmalleista. Oli mielenkiintoista havaita, kuinka ”oikeista naruista vetelemällä” yksilön toimintaa on mahdollista ohjailla huomattavan paljon ja näin saada esimerkiksi myös älykäs ja harkitsevainen yksilö haksahtamaan huijaukseen. Koen myös, että ihmisen psykologiaan perehtyminen on antanut uuden näkökulman ja uudenlaista ymmärrystä ympäristöni toiminnan tarkasteluun, sekä myös itselleni ymmärrystä ja työkaluja laajempaan itseni ja ajatteluni kehittämiseen.

Aineiston keräämisen prosessi kehitti taitojani luotettavan lähdemateriaalin löytämisessä ja sen kriittisessä analysoinnissa. Kahden tieteenalan, kyberturvallisuuden ja psykologian, yhdistäminen myös opetti konkreettisesti tarkastelemaan aihetta useammasta näkökulmasta. Kirjoitusprosessin aikana koen saaneeni huomattavaa varmuutta kirjoittajana. Opinnäytetyöprojektin edetessä myös havahduin siihen, kuinka sekä tiedonhausta että kirjoittamisesta tuli työn edetessä jatkuvasti sujuvampaa.

Opinnäytetyön tutkimusaineiston läpikäyminen tarjosi minulle myös mahdollisuuden syventää englannin kielen taitoani, erityisesti psykologian termien osalta. Näiden termien avaaminen ja kääntäminen suomen kielelle edellytti itsenäistä tiedonhakua ja vertailua eri lähteiden välillä, koska tavoitteena oli säilyttää käsitteiden alkuperäinen merkitys käännöksen yhteydessä. Tehtävä olisi ollut huomattavasti helpompi, jos minulla olisi ollut jo valmiiksi omaksuttuna esimerkiksi suomenkielinen psykologian alan termistö, eli kääntämisprosessi syvensi kielitaidon lisäksi omaa ymmärrystäni myös psykologian termistöstä ja aihepiiristä.

Minulla on hyvin luontainen taipumus itsenäiseen työskentelyyn ja olen melko voimakkaasti itseohjautuva työskentelyssäni. Näistä piirteistä oli ehdottomasti hyötyä koko prosessin ajan. Sain opinnäytetyöprosessin aikana arvokasta käytännön oppia ja vinkkejä aikatauluttamisesta ja suuren kokonaisuuden jäsentämisestä pienemmiksi tehtäviksi. Huomasin myös, että oman työn esittely ja muiden töiden kommentoiminen, sekä vastavuoroinen kanssaopiskelijoiden kannustaminen virkisti mieltä ja avasi uusia näkökulmia opinnäytetyöprosessiin ja työskentelytapoihin. Koen itse, että palautteen ja uusien näkökulmien saaminen virkistää huomattavasti omia ajatuksia ja sitä kautta koko prosessia.

Huomasin myös, että motivaation ylläpitäminen on hyvä huomioida tällaisessa pitkäkestoisessa prosessissa. Koin siis hetkiä, jolloin jo tehty työ tuntui täysin hallitsemattomalta kokonaisuudelta. Paras lääke näihin hetkiin ja motivaation ylläpitämiseen oli kerta toisensa jälkeen yksinkertaisesti vain aloittaa tekeminen, pienin askelin ja kerta toisensa jälkeen.

Tähän tutkimusaiheeseen perehtyminen oli minulle valtavan mielenkiintoinen tutkimusmatka. Haastetta tarjosi oma vähäinen tausta psykologian saralla, mutta aiheeseen syventyminen oli erittäin palkitsevaa. Saatuani tämän opinnäytetyön ja tutkimusprosessin loppusuoralle minulle jäi tunne, että olen tässä aihepiirissä päässyt perehtymään vasta ”jäävuoren huippuun”. Tämä havainto vahvisti ajatustani siitä, että tämä osa-alue kyberturvallisuudesta on juuri se, jonka ymmärrystä ja osaamista haluan myös tulevaisuudessa syventää.

Jälkikäteen arvioituna tutkimuksen rajausta olisi voinut kaventaa huomattavasti. Tämä olisi mahdollistanut syvällisemmän perehtymisen esimerkiksi johonkin tiettyyn hyökkäystyyppiin. Koen kuitenkin, että olen tämän työn osalta saavuttanut asettamani tavoitteet. Tavoitteenani oli koota kohdennetun käyttäjän manipuloinnin kyberuhkien psykologisesta puolesta eheä ja looginen kokonaisuus, jota voi hyödyntää tarkemmin rajatuissa jatkotutkimuksissa.

Pelkästään käyttäjän manipuloinnin aihepiiri kattaa valtavan määrän tutkimisen arvoisia aiheita. Huijausmenetelmien tekninen puoli on jatkuvasti kehittynyt teknologian rinnalla. Paperilaskujen aikaan esimerkiksi laskutushuijaus toteutettiin varastamalla paperinen lasku postilaatikosta ja

muuntelemalla sitä. Puhelinlinjojen kehittyessä huijarit iskivät puhelinlinjojen kautta, pysytellen teknologian ”aallonharjalla”. Nykyisin hyökkäykset kohdistuvat sähköisiin järjestelmiin. Tulevaisuudessa taas tekoäly mahdollistaa uusien työkalujen, kuten äänen ja videon, hyödyntämisen huijauksissa. Kuitenkin tietty yhdistävä tekijä on ollut mukana näissä huijauksissa kautta aikojen riippumatta hyödynnettävästä teknologiasta. Nimittäin se, että keskiössä on manipuloinnin keinot ja ihminen.

Lähteet

Choi, Y. 2023-12-21. Social Engineering Cyber Threats. Journal of global awareness, 4(2), s. 1–12. Luettavissa: https://www.proquest.com/docview/2931772575/fulltextPDF/AE987E734B86476EPQ/1?accountid=27436&sourcetype=Scholarly%20Journals. Luettu: 26.4.2025.

Cialdini, R. B. 2009. Influence. HarperCollins Publishers. E-kirja. Luettu: 20.4.2025.

Cross, C. & Gillett, R. 2020-10-25. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. Journal of Financial Crime, 27(3), s. 871–884. Luettavissa: https://www.proquest.com/docview/2454034150/fulltextPDF/2C7E8FB6358B45A3PQ/1?accountid=27436&sourcetype=Scholarly%20Journals. Luettu: 25.4.2025.

Ekqvist, J., Kiuru, M., Satopää, P. & Vanharanta, J. 2024. Kyberturvallisuus, Tieto- ja kyberturvallisuuden perusteet. Luettavissa: https://aoe.fi/api/v1/download/file/tietojakyberturvallisuudenperusteet-1734439309016.pdf. Luettu: 2.2.2025.

Fbi s.a. Business Email Compromise. Luettavissa: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise. Luettu: 12.4.2025.

F-Secure 2022a. Mitä on tietojenkalastelu eli phishing? Näin verkkourkinta toimii. Luettavissa: https://www.f-secure.com/fi/articles/what-is-phishing. Luettu: 22.3.2025.

F-Secure 2022b. Mitä on smishing? Luettavissa: https://www.f-secure.com/fi/articles/what-is-smishing. Luettu: 20.3.2025.

F-Secure 2023. Mitä on kyberturvallisuus? Luettavissa: https://www.f-secure.com/fi/articles/what-is-cyber-security. Luettu: 2.3.2025.

F-Secure 2024a. Mitä on käyttäjän manipulointi? Luettavissa: https://www.f-secure.com/fi/articles/what-is-social-engineering. Luettu: 21.2.2025.

F-Secure 2024b. Mitä on kohdennettu tietojenkalastelu eli spear phishing? Luettavissa: https://www.f-secure.com/fi/articles/spear-phishing. Luettu: 17.3.2025.

F-Secure 2024c. Mitä ovat huijauspuhelut? Luettavissa: https://www.f-secure.com/fi/articles/what-is-vishing. Luettu: 2025-03-20.

Hyppönen, M. 2021. Internet. Werner Söderström Osakeyhtiö. Helsinki. Luettu: 7.3.2025.

Jyväskylän yliopisto s.a. Mitä on tietoturva? Luettavissa: https://www.jyu.fi/fi/yliopistopalvelut/digipalvelut/palvelut/tietoturva/mita-on-tietoturva. Luettu: 9.3.2025.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Docendo Oy. Jyväskylä. Luettu: 6.2.2025.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Kauppakamari. Helsinki. E-kirja. Luettu: 25.1.2025.

Kyberturvallisuuskeskus 2020a. Yrityksen hallituksen vastuu. Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. Helsinki. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf. Luettu: 1.2.2025.

Kyberturvallisuuskeskus 2020b. Pienyritysten kyberturvallisuusopas. Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. Helsinki. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf. Luettu: 1.2.2025.

Kyberturvallisuuskeskus 2020c. Huijauslaskut. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Huijauslaskut_FI_2020%20%28002%29.pdf. Luettu: 28.4.2025.

Kyberturvallisuuskeskus 2022. Laskutushuijaukset lisääntyvät kesäisin – näin suojaudut huijauksilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/laskutushuijaukset-lisaantyvat-kesaisin-nain-suojaudut-huijauksilta. Luettu: 21.2.2025.

Kyberturvallisuuskeskus 2023a. Näin suojaudut nettihuijaukselta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta?toggle=Yleisimm%C3%A4t%20huijaustavat. Luettu: 21.2.2025.

Longtchi, T. T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A. & Xu, S. 2024-03-01. Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey. Proceedings of the IEEE, 112(3), s. 210–246. Luettavissa: https://ieeexplore-ieee-org.ezproxy.haaga-helia.fi/stamp/stamp.jsp?tp=&arnumber=10493072. Luettu: 21.4.2025.

Microsoft s.a. Mitä on tietojenkalastelu? Luettavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-phishing. Luettu: 9.3.2025.

Rikosuhripäivystys s.a. Toimitusjohtajahuijaus. Luettavissa: https://www.riku.fi/nettihuijaus/identiteettivarkaus/toimitusjohtajahuijaus/. Luettu: 21.2.2025.

Salminen, A. 2023. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja joihinkin hallintotieteellisiin sovelluksiin. 2. tarkistettu painos. Vaasan yliopisto. Vaasa. E-kirja. Luettu: 25.2.2025.

Saud Al-Musib, N., Mohammad Al-Serhani, F., Humayun, M. & Jhanjhi, N. 2023. Business email compromise (BEC) attacks. Materials today: proceedings, 81, s. 497–503. Luettavissa: https://www-sciencedirect-com.ezproxy.haaga-helia.fi/science/article/pii/S2214785321027425/pdfft?md5=0980444fe446fa0faedc6c6e532b952b&pid=1-s2.0-S2214785321027425-main.pdf. Luettu: 24.4.2025.

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Sanastokeskus TSK ry. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. Luettu: 19.2.2025.

Vilkka, H 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Art House Oy. Helsinki. E-kirja. Luettu: 12.2.2025.

Wang, Z., Sun, L. & Zhu, H. 2020. Defining Social Engineering in Cybersecurity. IEEE access, 8, s. 85094–85115. Luettavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9087851. Luettu: 23.4.2025.

Wang, Z., Zhu, H. & Sun, L. 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE access, 9, s. 11895–11910. Luettavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9323026. Luettu: 19.4.2025.