Meri Kärki

KÄYTTÄJÄN ROOLI SÄHKÖPOSTIN SUOJAAMISESSA TIETOMURTOJA VASTAAN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Kärki, Meri
Käyttäjän rooli sähköpostin suojaamisessa tietomurtoja vastaan
Jyväskylä: Jyväskylän yliopisto, 2024, 32 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Clements, Kati

Tietomurrot ovat nopeasti kasvava uhka digitalisoituneessa maailmassa, jossa yhä enemmän arkaluonteista tietoa tallennetaan sähköisesti. Vaikka teknologiat kehittyvät, nykyiset toimenpiteet eivät riitä estämään tietomurtoja ja niiden haitallisia vaikutuksia. Tämä tutkielma tarkasteli käyttäjän roolia sähköpostitilien suojaamisessa tietomurtoja vastaan. Tavoitteena oli selvittää, millä keinoilla käyttäjät voivat suojata sähköpostitilejään sekä millaisia haasteita näiden keinojen käyttöön liittyy. Tutkielma toteutettiin kirjallisuuskatsauksena, jossa analysoitiin ajankohtaisia ja vertaisarvioituja tieteellisiä artikkeleita. Tulokset osoittivat, että monivaiheinen tunnistautuminen (MFA) on yksi tehokkaimmista tavoista suojata sähköpostitilejä tietomurtoja vastaan. MFA estää merkittävästi luvattomia tunkeutumisia tileille, sillä se vaatii hyökkääjältä useampien todennustekijöiden murtamista pelkän salasanan sijaan. Käyttäjien tietoturvatietoisuuden ja tietojenkalasteluhyökkäysten tunnistamiskyvyn kehittäminen, esimerkiksi pelillisten oppimisympäristöjen avulla, on keskeistä inhimillisten virheiden vähentämisessä. Lisäksi organisaatioilla on tärkeä vastuu tarjota käyttäjille kattavaa koulutusta, riittäviä resursseja ja selkeitä toimintamalleja turvallisten käytäntöjen omaksumiseksi. Tutkimuksessa nousi esiin haasteita liittyen myös järjestelmien käytettävyyteen ja käyttäjien motivaatioon. Huomiota kiinnitettiin tarpeeseen löytää tasapaino turvallisuuden ja käytettävyyden välillä, sillä liian monimutkaiset ratkaisut voivat heikentää käyttäjien sitoutumista. Tutkimuksen tulokset tarjosivat kokonaisvaltaisen kuvan sähköpostitilien suojaamisesta ja sen haasteista sekä suosituksia tietomurtojen tehokkaampaan torjuntaan.

Avainsanat: tietomurto, sähköpostiturvallisuus, tietoturva, monivaiheinen tunnistautuminen, CIA-kolmio, tietojenkalastelu

ABSTRACT

Kärki, Meri
The User's Role in Protecting Email Against Data Breaches
Jyväskylä: University of Jyväskylä, 2024, 32 pp.
Information Systems, Bachelor's thesis
Supervisor: Clements, Kati

Data breaches are a rapidly growing threat in a digitalized world where increasingly sensitive information is stored electronically. Despite advancements in technology, current measures are insufficient to prevent data breaches and their harmful impacts. This study examined the user's role in protecting email accounts against data breaches. The objective was to identify methods that users can adopt to secure their email accounts and to explore the challenges associated with implementing these methods. The study was conducted as a literature review, analyzing current and peer-reviewed scientific articles. The findings indicate that multi-factor authentication (MFA) is one of the most effective ways to protect email accounts against data breaches. MFA significantly prevents unauthorized access to accounts, as it requires attackers to break multiple authentication factors rather than just cracking a single password. Improving users' cybersecurity awareness and their ability to recognize phishing attacks, for example, through gamified learning environments, is essential in reducing human errors. Furthermore, organizations have an important responsibility to provide users with comprehensive training, sufficient resources, and clear operational models to support the adoption of secure practices. The study also highlighted challenges related to the usability of systems and user motivation. Attention was drawn to the need to find balance in security and usability, as overly complex solutions can weaken user engagement. The findings provided a comprehensive overview of email account protection and its challenges, as well as recommendations for more effective prevention of data breaches.

Keywords: data breach, email security, information security, multi-factor authentication, CIA triad, phishing

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tänä päivänä tietoa voidaan käyttää ja hyödyntää napin painalluksella, mikä herättää huolta järjestelmien suojauksesta sekä datan yksityisyydestä ja luottamuksellisuudesta (Syahreen, Hafizah, Maarop & Maslinan, 2024). Tietomurto (data breach) tarkoittaa tapahtumaa, jossa luvaton taho pääsee käsiksi arkaluonteisiin tietoihin järjestelmässä (Hassanzadeh, Biddle, & Marsen, 2021). Vaikka tiedon suojaamiseen kehitetään jatkuvasti uusia teknologioita, tietomurtojen määrä ja niiden aiheuttamat taloudelliset tappiot ovat kasvussa (Hakami & Alshaikh, 2022). Globaalin tietokannan Risk Based Securityn raportin mukaan vuonna 2020 pelkästään ensimmäisen vuosineljänneksen aikana tietomurtojen seurauksena paljastui yli 8 miljardia tietuetta (Hassanzadeh, ym., 2021).

Turvallisen verkkoympäristön kehittäminen edellyttää, että tiedot pysyvät yksityisinä, käyttäjät ovat tunnistettuja ja tiedonsiirto on turvattu hyökkäyksiltä (Yee & Zolkipli, 2021). Pelkkä teknologisten ratkaisujen kehittäminen ei kuitenkaan riitä torjumaan kyberhyökkäyksiä, eli luvattomia yrityksiä tunkeutua järjestelmiin (Basit ym., 2020). Erityisesti organisaatioissa loppukäyttäjien käyttäytymisellä on keskeinen rooli kyberturvallisuuden ylläpitämisessä (Prümmer, van Steen & van den Berg, 2024). Tietomurrot johtuvat usein inhimillisistä virheistä, minkä vuoksi ihmisiä pidetään tietoturvaketjun heikoimpana lenkkinä (Hakami & Alshaikh, 2022). Hyökkääjät hyödyntävät inhimillisiä heikkouksia tunkeutuakseen järjestelmiin ja saadakseen pääsyn luottamuksellisiin tietoihin (Hakami & Alshaikh, 2022).

Nykyään jokainen käyttää puhelinta tai tietokonetta vastaanottamaan ja lähettämään viestejä toisilleen, minkä vuoksi tietoturva on olennainen osa jokapäiväistä elämää (Yee & Zolkipli, 2021). Sähköposti on yksi keskeisimmistä ja laajimmin käytetyistä viestintävälineistä, joten sen tietoturvan varmistaminen on välttämätöntä (Altulaihan, Alismail, Rahman & Ibrahim, 2023). Sähköpostiin kohdistuu monenlaisia hyökkäyksiä, kuten tietojenkalastelua, joka on yleisin ja tehokkain tapa, jolla hyökkääjät pääsevät käsiksi organisaatioiden tietoihin (Fadziso ym., 2023). Viime vuosina sähköpostin käyttö on jatkanut kasvuaan, mikä on lisännyt tietomurtojen riskiä (Vishwakarma, 2023).

Tämän kandidaatintutkielman aiheena on käyttäjän rooli sähköpostin suojaamisessa tietomurtoja vastaan. Tavoitteena on selvittää, millaisia keinoja käyttäjät voivat hyödyntää sähköpostitilien suojaamiseen ja mitä haasteita keinojen käyttöön liittyy. Tutkielman tarkoituksena on lisätä ymmärrystä siitä, miten käyttäjät voivat suojautua tietoturvauhkilta ja parantaa sähköpostin käytön turvallisuutta, jotta tietomurtoja voitaisiin estää. Tutkimuksen tulokset voivat auttaa kehittämään parempia käytäntöjä ja koulutusta, jotta käyttäjät voivat suojata sähköpostitilinsä entistä paremmin. Tutkimuskysymys, johon tutkielma pyrkii vastaamaan, on

- Miten käyttäjät voivat suojata sähköpostitilejään tietomurtoja vastaan ja millaisia haasteita sähköpostin suojaamisen keinoihin liittyy?

Tutkielman teoreettisena viitekehyksenä hyödynnetään laajalti tunnettua CIA-mallia, jonka avulla voidaan analysoida tietoturvan keskeisiä osa-alueita: luottamuksellisuutta, eheyttä ja saatavuutta (Samons & Coss, 2014). CIA-malli tarjoaa järjestelmällisen lähestymistavan arvioida, miten eri tietoturvaratkaisut ja -toimenpiteet vaikuttavat sähköpostin turvallisuuteen. Tutkielmassa selvitetään, miten sähköpostitilien suojaamisessa voidaan turvata tietojen luottamuksellisuus, varmistaa tiedon eheys ja ylläpitää palveluiden saatavuus erityisesti tietomurtoja vastaan.

Tutkimusmenetelmänä on kirjallisuuskatsaus, jossa tarkastellaan tieteellisiä artikkeleita sähköpostitilien turvallisuudesta, kyberuhkista ja tietomurtojen torjunnasta. Aineisto on kerätty tietokannoista, kuten Web of Science ja Google Scholar. Osa lähteistä on löydetty Jykdokin kautta. Hakusanoina on käytetty muun muassa ”data breach”, ”user”, ”email security”, ”phishing” ja ”cybersecurity”. Hakuja on rajattu vuosiluvun perusteella, tavoitteena löytää uusimmat tutkimukset aiheen ympäriltä. Lukuun ottamatta muutamaa poikkeusta, tutkielman lähteet ovat vertaisarvioituja tieteellisiä artikkeleita viime vuosilta.

Tutkielma etenee siten, että aluksi käsitellään tietomurtojen ja kyberturvallisuuden peruskäsitteitä sekä analysoidaan tietomurtojen syitä ja vaikutuksia. Tämän jälkeen käsitellään sähköpostin toimintaa, siihen kohdistuvia hyökkäyksiä sekä sähköpostitilien tietoturvaa. Tutkielman pääpaino on käyttäjän roolissa sähköpostin suojaamisessa, jossa tarkastellaan sekä teknologisia ratkaisuja että käyttäjien tietoturvatietoisuutta ja -käyttäytymistä. Lopuksi esitetään yhteenveto keskeisistä löydöksistä ja pohditaan, miten sähköpostin tietoturvaa voidaan parantaa, jotta tietomurtoja voidaan ehkäistä entistä tehokkaammin.

2 TIETOMURROT UHKAAVAT JOKAISTA

Tämän luvun alussa tarkastellaan kyberturvallisuuden nykytilannetta sekä kyberhyökkäysten ja tietomurtojen käsitteitä. Luvussa kuvataan, miten teknologian kehittyminen ja sen monimutkaistuminen ovat lisänneet kyberuhkia. Luvun loppupuolella selvitetään tietomurtojen syitä ja vaikutuksia, jotka kohdistuvat niin yksilöihin, organisaatioihin kuin yhteiskuntaan laajemmin.

2.1 Kyberturvallisuus ja kyberhyökkäykset

Kyberturvallisuus voidaan määritellä yksinkertaisesti yksilön tai organisaation sähköisten tietojen suojaamiseksi luvattomalta pääsyltä (Saeed ym., 2023). Laajempana käsitteenä kyberturvallisuus on teknologioiden, menettelytapojen ja käytäntöjen kokonaisuus, jonka tarkoituksena on suojata verkkoja, laitteita, ohjelmistoja ja tietoja hyökkäyksiltä, vahingoittumiselta sekä luvattomalta pääsyltä (Fadziso, Rao Thaduri, Dekkati, Ballamudi & Desamsetti, 2023). Kyberturvallisuuden kenttä monimutkaistuu jatkuvasti laitteiden, järjestelmien ja verkkojen nopean kasvun vuoksi (Kaur, Gabrijelčič & Klobučar, 2023).

Luvattoman pääsyn yritystä kutsutaan kyberhyökkäykseksi (Saeed ym., 2023). Kyberhyökkäykset ovat verkossa tapahtuvia yrityksiä varastaa, vahingoittaa tai tunkeutua luottamuksellisiin tietoihin (Basit ym., 2020). Nykyään organisaatiot ja eri toimijat käsittelevät valtavia määriä dataa, joista merkittävä osa sisältää arkaluonteista tietoa, kuten henkilötietoja tai taloudellisia tietoja, joiden luvaton käyttö tai paljastuminen voi aiheuttaa vakavia haittoja (Fadziso ym., 2023). Kyberturvallisuuden avulla suojataan internetiin kytkettyjen laitteiden ja palveluiden tietoja, pyrkien estämään niiden joutuminen kyberhyökkäysten kohteeksi (Fadziso ym., 2023).

Teknologian nopean kasvun ja kasvaneen merkityksen myötä erilaisten hyökkäysten, kuten palvelunestohyökkäysten ja tietojenkalastelun määrä on lisääntynyt eksponentiaalisesti viimeisen vuosikymmenen aikana (Ahsan ym., 2022). Vain muutama vuosi sitten kyberturvallisuuteen kohdistuvat uhkat eivät

olleet läheskään yhtä kehittyneitä kuin nykyään, ja uhat kehittyvät ja muuttuvat koko ajan (Fadziso ym., 2023). Koska kyberhyökkäykset ovat entistä vakavampia ja yleisempiä, uhkien seuraaminen ja nopea reagointi mahdollisiin hyökkäyksiin on yhä tärkeämpää (Sun ym., 2023). Tietoisen ja turvallisen internetin käytön avulla voidaan välttää kyberuhkille altistumisen riskiä ja estää kyberrikosten uhriksi joutuminen (Kovalan ym., 2021).

Tekoälyn kehittyminen on vaikuttanut kyberturvallisuuden luonteeseen nopeasti. Tekoäly on tehokas työkalu, jonka avulla voidaan automatisoida toistuvia tehtäviä, nopeuttaa huomattavasti uhkien havaitsemista ja niihin reagointia sekä parantaa toimintojen tarkkuutta, mikä vahvistaa kyberturvallisuuden tasoa kyberhyökkäyksiä vastaan. Samalla tekoälyn kehittyminen on vaikuttanut myös hyökkäysten kehittymiseen. (Kaur ym., 2023.)

2.2 Tietomurrot

Tietomurto (data breach) on seurausta onnistuneesta kyberhyökkäyksestä, jossa hyökkääjä on päässyt käsiksi luottamuksellisiin tietoihin järjestelmässä. Tietomurron määritelmä vaihtelee, sillä joissain määritelmissä tietomurto liittyy aina tiedon varastamiseen, kun taas toisissa riittää, että tietojärjestelmään on murtauduttu. Yhteistä kaikille määritelmille on kuitenkin se, että tietomurto tarkoittaa pääsyä tietojärjestelmään ilman lupaa.

Rahman, Rohan, Pal & Kanthamanon (2021) kuvaavat tietomurron tilanteeksi, jossa järjestelmään hyökätään ja sieltä varastetaan henkilötietoja, joita voidaan käyttää yksilön tunnistamiseen. Hassanzadeh ym. (2021) puolestaan toteavat tietomurron tapahtuvan, kun luvaton osapuoli saa pääsyn luottamuksellisiin tietoihin. Suomen valtion Viestintäviraston sisäinen organisaatio, Kyberturvallisuuskeskus (2024) määrittelee tietomurron tarkoittavan luvattoman pääsyn saamista tietojärjestelmään, palveluun tai laitteeseen esimerkiksi hyödyntämällä toisen sähköpostitunnusta, jolloin hyökkääjä voi tarkastella, muokata tai käyttää tietoja ilman oikeutettua lupaa.

Tietomurto on rikos, josta säädetään Suomen rikoslaissa, ja siitä voi seurata vankeusrangaistus. Tietomurtoon syyllistyy henkilö, joka käyttää väärin toisen käyttäjätunnusta tai murtautuu tietojärjestelmään muilla keinoilla ilman lupaa. Rikoslaissa tietojärjestelmä määritellään sellaiseksi järjestelmäksi, jossa tietoja tai dataa käsitellään, varastoidaan tai siirretään sähköisesti tai muilla teknisillä keinoilla. Tietomurtoon voi syyllistyä myös ilman järjestelmään tunkeutumista. Tämä voi tapahtua käyttämällä teknistä laitetta tai muuten teknisin keinoin ohittamalla turvajärjestelyt ja hyödyntämällä järjestelmän haavoittuvuutta. Myös tietomurron yritys täyttää rikoksen tunnusmerkistön. (Rikoslaki, 1889/39.)

2.3 Tietomurtojen syyt ja vaikutukset

Tietomurrot yleistyvät ja herättävät laajaa huolta (Hassanzadeh ym., 2021). Niiden vaikutukset ulottuvat organisaatioihin, yksilöihin ja koko yhteiskuntaan (Vishwakarma, 2023). Tietomurtojen taustalla voi olla monenlaisia syitä, mutta usein niillä tavoitellaan taloudellista hyötyä tai muuta etua (Saeed, 2023). Yleensä hyökkääjät pyrkivät pääsemään käsiksi arkaluonteisiin tietoihin, niiden muuttamiseen tai poistamiseen (Fadziso ym., 2023). He saattavat kiristää rahaa käyttäjiltä tai haluavat häiritä organisaation toimintaa (Fadziso ym., 2023). Tietomurrot perustuvat yleensä järjestelmän haavoittuvuuksien onnistuneeseen hyödyntämiseen, mutta teknisten toimenpiteiden lisäksi ne nähdään laajasti johtamis- ja organisaatiotasoisena ongelmana (Schlackl, Link & Hoehle, 2022). Olennaista on ymmärtää, mitä tapahtuu ennen ja jälkeen tietomurron, eli mitkä syyt johtavat tietomurtoon ja mitä seurauksia siitä aiheutuu (Schlackl ym., 2022).

Tietomurtojen estämisen merkitystä ei voi väheksyä nykypäivän digitalisoituneessa maailmassa (Fadzoso ym., 2023). Yritykset toteuttavat riittämättömiä suojaustoimenpiteitä, mikä johtaa tietomurtoihin (Hassanzadeh ym., 2021). Tietoturvajohtaja Stephane Nappo on todennut: ”It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it” (kuluu 20 vuotta rakentaa maine ja kyberhyökkäyksellä kuluu muutama minuutti sen tuhoamiseen) (Yasin, Fatima, JiangBin, Afzal & Raza, 2024). Esimerkiksi työntekijän sähköpostitilin vaarantuminen voi antaa hyökkääjälle pääsyn organisaation arkaluontoisiin tietoihin, kuten strategisiin suunnitelmiin, taloudellisiin tietoihin tai asiakastietoihin (Adebimpe ym., 2023) Tietomurtojen seurauksena organisaatiot kärsivät merkittäviä taloudellisia menetyksiä ja heidän asiakkaidensa luottamus heikkenee (Fadziso ym., 2023).

Jo yksittäinen tietoturvaloukkaus voi johtaa miljoonien ihmisten henkilötietojen paljastumiseen (Fadziso ym., 2023). Hyökkääjän saatua haltuun esimerkiksi käyttäjän sähköpostitunnuksen ja salasanan, tili voidaan yrittää kaapata (Thomas ym., 2017). Kaapattua tiliä voidaan käyttää hyväksi monin tavoin, kuten lataamalla yksityisiä viestejä tai pyyhkimällä datan varmuuskopiot (Thomas ym., 2017). Hyökkääjä voi kohdistaa yksilöihin identiteettivarkauksia, eli henkilön tunnistetietoja käytetään luvattomasti, minkä määrä on kasvanut valtavasti (Alothman ym., 2023). Yksilön henkilötietoja voidaan käyttää esimerkiksi roskapostin levittämiseen tai vielä vahingollisempien tekojen toteuttamiseen (Thomas ym., 2017). Tietomurrot voivat aiheuttaa myös yksilöille merkittäviä taloudellisia menetyksiä (Ahsan ym., 2022).

Toimenpiteet hyökkäyksiltä suojautumiseen ovat riittämättömiä, mikä johtaa tietomurtoihin (Hassanzadeh, ym. 2021). Huolimatta hyökkäysten lisääntymisestä, julkinen kiinnostus tietomurtoja kohtaan on yllättävän vähäistä, ja monet ihmiset jatkavat palveluiden käyttöä tietomurtojen jälkeen (Hassanzadeh ym., 2021). Teknologiasta on paljon hyötyä, joten voi olla vaikea kuvitella, että laitteiden taustalla piilee vaaroja, mutta yhteiskunnan optimistisesta näkemyksestä huolimatta, uhat ovat todellisia (Fadziso ym., 2023).

3 SÄHKÖPOSTIN TIETOTURVA JA RISKIT

Tässä luvussa käsitellään sähköpostin toimintaa ja sen merkitystä digitaalisen viestinnän keskeisenä välineenä. Sen jälkeen tarkastellaan sähköpostiin kohdistuvia tietoturvauhkia, kuten tietojenkalastelua ja tilien kaappaamista. Näiden uhkien esittely luo pohjan ymmärrykselle siitä, miksi sähköpostitilien suojaaminen on välttämätöntä. Luvun loppupuolella perehdytään tietoturvan peruselementteihin CIA-kolmio-mallin avulla, joka tarjoaa selkeän viitekehyksen tietoturvan keskeisten osa-alueiden tarkasteluun.

3.1 Sähköpostin toiminta

Sähköpostijärjestelmä on maailmanlaajuisesti levinnyt tehokas digitaalinen viestintäpalvelu, joka yhdistää joustavuuden ja lähes välittömän tiedonjaon tietokoneverkossa. Sen kehittäminen alkoi yli 50 vuotta sitten, alun perin tutkijoiden ja tieteentekijöiden etäviestinnän tarpeisiin. 1990-luvulla, internetin käytön laajentuessa, sähköposti yleistyi nopeasti niin yrityksissä kuin yksityishenkilöiden keskuudessa. Nykyään sähköposti on edelleen yksi yleisimmin käytetyistä viestintämuodoista. (Altuilahan ym., 2023.)

Toisin kuin yksittäiset viestintäsovellukset, sähköposti on viestintäteknologia, jota tarjoavat useat eri palveluntarjoajat, kuten Gmail, Outlook ja Yahoo, sekä yritysten omat sähköpostijärjestelmät. Sähköpostin merkittävä etu on järjestelmien yhteensopivuus, joka mahdollistaa viestien vaihdon käyttäjien välillä palveluntarjoajasta riippumatta. Tiedon jakaminen on helppoa ja nopeaa sähköpostin välityksellä (Qashqari, Alhbshi, Alzahrani, Ghwati & Aljahdali, 2020). Viestien lisäksi sähköpostin kautta voidaan lähettää erilaisia liitetiedostoja, kuten ääni-, video- ja kuvatiedostoja, mikä laajentaa sen käyttömahdollisuuksia (Altuilahan ym., 2023). Sähköposti onkin monipuolinen työkalu ja keskeinen osa sekä henkilökohtaista että ammatillista viestintää, ja sen käyttö on laajentunut merkittävästi uusien viestintätarpeiden myötä (Vishwakarma, 2023).

Sähköpostin keskeinen ominaisuus on käyttäjän henkilökohtainen sähköpostitili. Sähköpostitilin rooli on laajentunut perinteisestä viestintävälineestä myös pääsyavaimeksi moniin muihin verkkopaleluihin. Esimerkiksi sosiaalisen median tilien luominen tai pilvipalvelujen käyttö edellyttävät usein sähköpostiosoitteen rekisteröintiä (Thomas ym., 2017; Syahreen ym., 2024). Lisäksi sähköpostitilin avulla käyttäjät voivat palauttaa unohtuneita salasanoja tai hallita muita tilejä (Thomas ym., 2017). Tämä tekee sähköpostitileistä keskeisen osan käyttäjien digitaalisen identiteetin hallintaa.

Useimmat sähköpostijärjestelmät käyttävät salasanaan perustuvaa todennusta käyttäjien tunnistamiseen (Qashqari ym., 2020). Tunnistautuminen tarkoittaa käyttäjän henkilöllisyyden varmentamista, jotta hänelle voidaan myöntää pääsy järjestelmään. Tunnistautumisprosessi alkaa käyttäjän rekisteröinnillä, jossa hän luo käyttäjätunnuksen ja salasanan. Nämä tiedot tallennetaan palvelimelle ja tarkistetaan aina kirjautumisvaiheessa (Syahreen ym., 2024). Kirjautuessaan käyttäjä syöttää käyttäjätunnuksen ja salasanan, minkä jälkeen järjestelmä vertaa näitä tietokannassa oleviin tietoihin. Jos tiedot täsmäävät, käyttäjälle myönnetään pääsy järjestelmään (Zukarnain, Muneer & Ab Aziz, 2022; Kovalan ym., 2021). Tunnistautumisen tarkoituksena on estää luvaton pääsy järjestelmään (Adebimpe ym., 2023).

3.2 Sähköpostiin kohdistuvat hyökkäykset

Sähköpostitilit sisältävät arkaluontoista tietoa, kuten henkilötietoja, salasanoja ja kirjautumistietoja, jotka ovat arvokkaita niin käyttäjille kuin hyökkääjillekin (Altuilahan ym., 2023). Sähköpostialustat ovatkin yksi yleisimmin käytetyistä kanavista kyberhyökkäysten toteuttamiseen (Gallo, Maiello, Botta & Ventre, 2021). Arviolta 43 prosenttia kaikista kirjautumisyrityksistä verkossa tehdään hakkerien toimesta, kun he yrittävät murtautua käyttäjien tileille (Ogbanufe & Baham, 2023). Jos hyökkääjä onnistuu kaappaamaan sähköpostitilin, hän voi käyttää sitä muiden palveluiden tilien hallintaan tai salasanojen palauttamiseen, mikä lisää muiden verkkopalveluiden vaarantumisriskiä (Thomas ym., 2017).

Hyökkäyksiä tehdään monin eri tavoin, kuten roskapostin lähettämisenä, tietojenkalasteluna, salakuunteluna, viestien muokkauksena, identiteettivarkauksina tai haittaohjelmien levittämisenä (Altuilahan ym., 2023). Käyttäjätiedot voivat paljastua, vaikka hyökkäys ei kohdistuisi suoraan tiettyyn sähköpostitiliin (Zeng, Lin, Pan, Tai & Zhang, 2020). Tietojen paljastuminen ei siis aina johdu suoraan käyttäjän toiminnasta, vaan sen taustalla voi olla ohjelmistojen haavoittuvuuksia tai toisen henkilön tekemä virhe. Ohjelmistojen haavoittuvuuksia voivat olla esimerkiksi suojaamattomat käyttäjätietokannat tai ohjelmistovirheet. Näitä haavoittuvuuksia hyödyntämällä hyökkääjät voivat aiheuttaa tietovuotoja tai levittää haittaohjelmia, mikä voi vaarantaa useiden käyttäjien tietoja (Thomas ym., 2017). Lisäksi sähköpostiin voidaan kohdistaa hyökkäyksiä hyödyntämällä haavoittuvia langattomia lähiverkkoja, joissa laitteiden välistä viestintää voidaan siepata ja manipuloida (Thankappan, Rifà-Pous, & Garrigues, 2022).

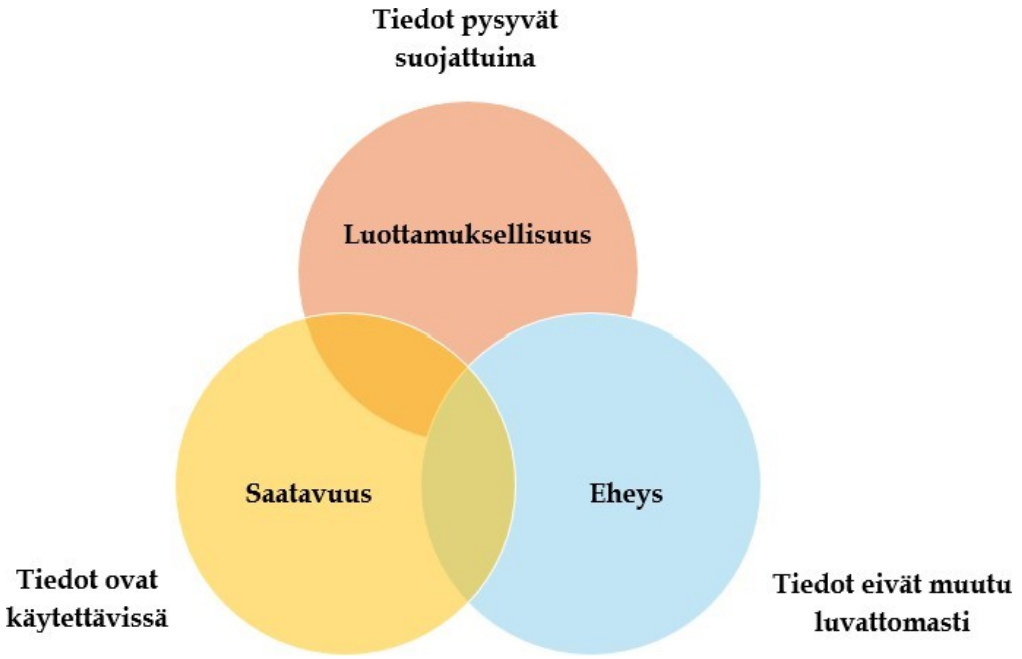
Tietojenkalastelu (phishing) on yksi tehokkaimmista ja tunnetuimmista kyberuhkista, jossa hyökkääjät pyrkivät harhauttamaan käyttäjiä antamaan heille pääsyn arkaluonteisiin tietoihin (Das, Nippert-Eng & Camp 2023; Varshney, Kumawat, Varadharajan, Tupakula & Gupta, 2024). Tietojenkalastelussa voidaan käyttää väärennettyjä verkkosivuja esimerkiksi käyttäjätunnusten, salasanojen tai luottokorttinumeroiden keräämiseen (Basit ym., 2021). Hyökkääjät lähettävät sähköpostitse linkkejä, jotka ohjaavat käyttäjät näille huijaussivustoille, joissa he voivat vahingossa antaa hyökkääjille pääsyn henkilökohtaisiin tietoihinsa (Basit ym., 2021). Jos käyttäjä ei tunnista huijausta, hyökkääjä voi saada haltuunsa käyttäjän sähköpostitilin, minkä jälkeen hän voi hallita myös muita käyttäjän verkkopalveluiden tilejä (Thomas ym., 2017).

Tietojenkalastelu on erityisen tehokas hyökkäysmuoto, koska se hyödyntää ihmisen luontaista luottamusta ja kiireen tunnetta. Hyökkääjien on helpompaa huijata käyttäjä klikkaamaan linkkiä tai avaamaan liite kuin etsiä teknisiä haavoittuvuuksia järjestelmästä, mikä tekee tietojenkalastelusta yleisimmän tavan, jolla hyökkääjät pääsevät käsiksi organisaatioon (Fadziso ym., 2023). Viswakarman (2023) mukaan jopa 25 % sähköpostin käyttäjistä on joutunut tietojenkalastelun uhriksi. Das ym. (2023) puolestaan arvioivat, että tietojenkalastelu on osasyynä 90 prosenttiin kaikista tietomurroista.

Tietojenkalasteluhyökkäyksiä tehdään laajasti, ja ne ovat kehittyneet vuosien saatossa entistä vakuuttavammiksi. Aiemmin tietojenkalasteluviestit olivat helpompia tunnistaa huijauskielen ja epäilyttävien URL-osoitteiden perusteella, mutta nykyään ne muistuttavat enemmän aitoja sähköposteja (Fadziso ym., 2023). Hyökkäykset ovat onnistuneet harhauttamaan jopa Googlen, Microsoftin ja Facebookin kaltaisissa organisaatioissa työskenteleviä kokeneita IT-ammattilaisia (Varshney ym., 2024), mikä osoittaa, kuinka vaikeaa nykyaikaisten kalasteluviestien tunnistaminen on.

3.3 CIA-malli sähköpostin tietoturvassa

Sähköpostin tullessa yhä yleisemmäksi, kyberhyökkäysten riski on kasvanut, minkä seurauksena sähköpostin tietoturvan parantaminen on tullut välttämättömäksi. Puutteellinen tietoturva altistaa sähköpostin hyökkäyksille, joiden tavoitteena on usein varastaa arkaluonteista tietoa (Altuilahan ym., 2023). Tietoturva käsittää kaikenlaisen tiedon suojelun riippumatta siitä, missä muodossa tai ympäristössä ne ovat, kattaen sekä fyysisen että digitaalisen tiedon, minkä vuoksi tietoturvaa voidaan pitää kyberturvallisuuden yläkäsitteenä. Alkhudayr, Alfarraj, Aljameeli & Elkhdiri (2019) määrittelevät, että tietoturva on tiedon ja järjestelmän sekä sellaisen laitteiston suojelemista, joka käyttää, tallentaa ja välittää tietoa, jotta tiedon eheys, luottamuksellisuus ja saatavuus ovat suojattuja. Tietoturvaa tarkastellaan usein CIA-kolmion avulla (kuva 1).



Kuva 1 CIA-kolmio (mukaillen Warkentin & Orgeron, 2020)

Erilaiset hyökkäykset, kuten tietojenkalastelu, haittaohjelmat ja haavoittuvuuksien hyödyntäminen, osoittavat, että sähköpostin suojaamiseksi on otettava huomioon useita eri näkökulmia. Yksi tunnetuimmista tietoturvan analysointimalleista on CIA-kolmio, joka koostuu kolmesta osa-alueesta: luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability) (Samons & Coss, 2014). Luottamuksellisuus varmistaa, että tiedot ovat ainoastaan luvallisten käyttäjien saatavilla, mikä suojaa tietoa luvattomalta käytöltä. Eheys tarkoittaa tiedon oikeellisuuden ja yhtenäisyyden säilyttämistä, jolloin tiedot eivät muutu luvatta. Saatavuus takaa, että tieto on käytettävissä silloin, kun käyttäjät sitä tarvitsevat (Yee & Zolkipli, 2021). Näiden kolmen osa-alueen huomioiminen on keskeistä sähköpostin suojaamisessa, jotta sähköpostitileillä olevat luottamukselliset ja arkaluontoiset tiedot, kuten henkilötiedot ja yksityinen viestintä, voidaan suojata luvattomalta pääsyltä.

CIA-kolmio esitettiin ensimmäisen kerran J. Andersonin raportissa *Computer Security Planning Study* vuonna 1972, minkä jälkeen mallia on käytetty laajasti kyberturvallisuuteen liittyvissä raporteissa, standardeissa ja muissa julkaisuissa (Ham, 2021). Vaikka CIA-malli on edelleen laajasti käytössä, se on myös saanut osakseen kritiikkiä, koska sen on katsottu olevan riittämätön nykyajan monimutkaisiin kyberturvallisuusuhkiin (Ham, 2021). Joidenkin tutkijoiden mukaan CIA-mallia tulisi laajentaa neljännellä ydintekijällä, vastuullisuudella (accountability), joka tarkoittaa kykyä jäljittää tehdyt toiminnot tiettyyn henkilöön tai prosessiin (Warkentin & Orgeron, 2020). Vastuullisuuden lisäämisen tarkoituksena on varmistaa, että jokainen toiminto kyberympäristössä voidaan liittää yksilöön tai tiettyyn prosessiin, mikä parantaa järjestelmän läpinäkyvyyttä ja jäljitettävyyttä.

4 KÄYTTÄJÄN ROOLI SÄHKÖPOSTIN SUOJAAMISESSA TIETOMURTOJA VASTAAN

Tässä luvussa käsitellään käyttäjän keinoja ja haasteita sähköpostitilien suojaamisessa tietomurtoja vastaan. Tarkastelun kohteena ovat erilaiset teknologiset ratkaisut, sekä käyttäjien tietoturvatietoisuuteen ja käyttäytymiseen liittyvät tekijät. Tutkimusten mukaan teknologiset ratkaisut muodostavat suojauksen perustan, mutta niiden tehokkuus riippuu usein käyttäjän ymmärryksestä, kyvystä tai halukkuudesta niiden soveltamiseen (Hakami & Alshaikh, 2022; Das ym., 2022; Chaudhary, 2024). Tietoturvatietoisuus, erityisesti kyky tunnistaa tietojenkalasteluviestit, on ratkaiseva tekijä kyberuhkia vastaan suojautumisessa. Luvun alussa esitetään matriisimuotoinen taulukko, joka kokoaa yhteen tärkeimmät suojauskeinot, niihin liittyvät haasteet ja keinojen vaikutukset tietoturvan kolmeen keskeiseen osa-alueeseen: luottamuksellisuuteen, eheyteen ja saatavuuteen.

Taulukko 1 Sähköpostin suojauskeinot, niihin liittyvät haasteet ja keinojen vaikutukset CIA-kolmion ulottuvuuksiin

	Luottamuksellisuus (C)	**Eheys (I)**	**Saatavuus (A)**
Vahvat salasanat Käytetään monimutkaisia ja yksilöllisiä salasanoja, jotka säilytetään turvallisesti	Estää luvatonta pääsyä tietoihin monimutkaisilla ja yksilöllisillä salasanoilla (C) (Kovalan ym., 2021; Vishwakarma, 2023)	Varmistaa, ettei salasanoja muokkaamalla voida vaikuttaa tilin tietoihin (I) (Umejiaku ym., 2023; Zukarnain ym., 2022)	Vähentää hyökkäysten riskiä, joka voisi estää pääsyn sähköpostitilille (A) (Vishwakarma, 2023)
Vahvojen salasanojen haasteet	Käyttäjät eivät vaihda salasanojaan säännöllisesti; monimutkaiset salasanat voivat unohtua tai johtaa toistuvaan käyttöön; käytettävyyden ja turvallisuuden tasapaino (Umejiaku ym., 2023; Zukarnain ym., 2022; Kovalan ym., 2021; Vishwakarma, 2023; Di Nocera ym., 2023)		

Monivaiheinen tunnistautuminen (MFA) Käytetään useita todennusmenetelmiä kirjautumisessa, kuten salasana, tekstiviestikoodi ja biometrinen tunnistus	Lisää tunnistautumistasoja, mikä vaikeuttaa hyökkääjän pääsyä järjestelmään ja suojaa varmemmin luottamuksellisia tietoja (C) (Ogbanufe & Baham, 2022)	Suojaa tietojen eheyttä estämällä järjestelmiin tunkeutumisen, mikä voi estää tietojen luvatonta muokkaamista, manipulointia tai poistamista (I) (Ogbanufe & Baham, 2022)	Parantaa saatavuutta estämällä tilin kaappauksen ja järjestelmän häiriöt; varmistaa, että vain oikeat käyttäjät voivat käyttää järjestelmää (A) (Rahman ym., 2021)
Monivaiheisen tunnistautumisen haasteet	Tietoisuuden ja koulutuksen puute; käyttäjien kokema monimutkaisuus; käytettävyys; käyttäjien motivaatio (Ogbanufe & Baham, 2022; Rahman ym., 2021; Vishwakarma, 2023; Di Nocera ym., 2023)		
Muut teknologiset ratkaisut Käytetään sähköpostin lähetyksessä tiedonsiirtoa suojaavaa salausta; käytetään tietoturvasovelluksia ja päivitetään ohjelmistot; hyödynnetään roskapostisuodatus ja tekoäly	Salaus suojaa sähköpostin tiedonsiirtoa ja sisältöä SSL/TLS-salauksella, estäen tietojen sieppaamisen; sovellusten päivittäminen suojaa tietoja haavoittuvuuksilta (C) (Syahreen ym., 2024; Vishwakarma, 2023)	Varmistaa, ettei tiedonsiirron aikana viestien sisältöä muuteta; estää roskapostin tai haitallisten liitteiden pääsyn postilaatikkoon (I) (Altuilahan ym., 2023; Gallo ym., 2021)	Pitää postilaatikon vapaana haitallisista viesteistä; pitää järjestelmät käytettävissä päivittämällä ohjelmistot ja hyödyntämällä tekoälyä uhkien havaitsemiseen (A) (Vishwakarma, 2023)
Muiden teknologisten ratkaisujen haasteet	Käyttäjien tietämättömyys teknologian käytöstä; julkisten Wi-Fi-verkkojen haavoittuvuus; roskapostisuodatuksen ja salaustekniikoiden riittämätön hyödyntäminen (Altuilahan ym., 2023; Syahreen ym., 2024; Vishwakarma, 2023)		
Tietojenkalasteluhyökkäysten tunnistaminen Opitaan havaitsemaan huijausviestit, jotka pyrkivät kalastelemaan luottamuksellisia tietoja	Ehkäisee tietojen vuotamista tunnistamalla hyökkäykset ja estäen käyttäjiä joutumasta ansaan (C) (Das ym., 2022; Desolda ym., 2021)	Estää käyttäjiä luovuttamasta tietoja ja varmistaa, että tiedot pysyvät muuttumattomina (I) (Bayl-Smith ym., 2020)	Varmistaa, että tili säilyy käyttäjän hallinnassa, eikä sen käyttö esty hyökkäysten vuoksi (A) (Sturman ym., 2024)
Tietojenkalastelun tunnistamisen haasteet	Tietoisuuden ja koulutuksen puute; hyökkäykset kehittyvät; käyttäjät yliarvioivat kykynsä tunnistaa kalastelu (Bayl-Smith ym., 2020; Das ym., 2022; Desolda ym., 2021)		

Koulutukset ja pelillisyys Opitaan tietoturvataitoja muun muassa pelillistettyjen koulutusten ja harjoitusten avulla, mikä lisää tietoisuutta ja sitoutumista	Lisää käyttäjien tietämystä ja kykyä tunnistaa hyökkäyksiä ja estää luottamuksellisten tietojen vuotamista (C) (Yasin ym., 2024; Pruemmer ym., 2024; Petrykina ym., 2021)	Parantaa tietojen suojelun ja manipuloinnin estämisen ymmärrystä, voi motivoida käyttäjiä suojautumaan uhkilta (I) (Das ym., 2022)	Parantaa valmiuksia reagoida uhkiin, jotka voisivat vaikuttaa järjestelmän saatavuuteen (A) (Varshney ym., 2024)
Koulutusten ja pelillisyyden haasteet	Koulutusmenetelmien tehokkuus vaihtelee organisaation ja käyttäjien tarpeiden mukaan; vaatii resursseja (Yasin ym. 2024; Prümmer ym., 2024)		
Organisaatioiden tuki Hyödynnetään organisaatioiden tarjoamat koulutukset, työkalut ja resurssit	Tarjoaa resursseja ja koulutusta, jotka tukevat tietojen luottamuksellisuuden suojelua (C) (Hakami & Alshaikh, 2022)	Ylläpitää turvallisia käytäntöjä ja järjestelmiä, jotka estävät tietojen muuttamisen (I) (Chaudhary, 2024)	Tukee järjestelmien toimintakykyä (A) (Chaudhary, 2024)
Organisaatioiden tuen haasteet	Työntekijöiden tietoisuus ei aina muutu toiminnaksi; organisaatiokulttuurin vaikutus; resurssien ja koulutuksen puute (Hakami & Alshaikh 2022; Vishwakarma, 2023); Chaudhary 2024; Prümmer ym., 2024)		

(Vaikutukset CIA-kolmion ulottuvuuksiin perustuvat Samonsin ja Cossin (2014) selitykseen CIA-mallista).

4.1 Teknologiset ratkaisut

Seuraavaksi matriisin sisältävät suojautumiskeinot ja niiden haasteet käsitellään tarkemmin. Salasanat ovat edelleen käytetyin tunnistautumismenetelmä digitaalisten alustojen ja palveluiden suojaamisessa, siitä huolimatta, että uusia tunnistamiseen tarkoitettuja järjestelmiä on kehitetty (Wasfi & Stone, 2023). Vahvojen salasanojen lisäksi luvussa esitellään muita teknologisia ratkaisuja, joita käyttäjä voi hyödyntää sähköpostin käytössä edistääkseen sähköpostin turvallisuutta. Tutkimusten mukaan keskeisin näistä on monivaiheinen tunnistautuminen (MFA) (Syahreen ym., 2024).

4.1.1 Vahvat salasanat

Salasanoja on käytetty suojaamaan verkossa olevia tietoja internetin alkuajoista lähtien (Kovalan ym., 2021). Salasanat ovat säilyttäneet suosionsa niiden helppokäyttöisyyden, yhteensopivuuden ja edullisuuden ansiosta (Wasfi & Stone, 2023). Tietomurtojen yleistyessä vahvojen salasanojen merkitys on korostunut, sillä jopa kolmannes tietomurroista liittyy puutteelliseen salasanojen hallintaan (Umejiaku, Dhakal & Sheng, 2023; Zukarnain ym., 2022).

Vahva salasana suojaa tehokkaasti arvaamiseen perustuvilta hyökkäyksiltä ja vähentää tilien kaappaamisen riskiä (Umejiaku ym., 2023). Kovalan ym. (2021) korostavat, että salasanat ovat yksi suurimmista tietoturvariskeistä, sillä ne ovat alttiita monenlaisille hyökkäyksille. He toteavat, että suunnitellun salasanan tulisi olla helppo muistaa, mutta vaikea murtaa. Salasanojen tulisi olla yksilöllisiä ja monimutkaisia, sisältäen sekä isoja että pieniä kirjaimia, numeroita ja erikoismerkkejä (Vishwakarma, 2023). Salasananhallintaohjelmat helpottavat monimutkaisten ja turvallisten salasanojen luomista ja hallintaa (Umejiaku, ym. 2023).

Zukarnain ym. (2022) tuovat esiin, että perinteinen salasanatodennus perustuu täysin käyttäjän muistiin, minkä vuoksi käyttäjät suosivat helposti muistettavia salasanoja, jotka ovat alttiita hyökkäyksille. Monimutkaiset salasanat puolestaan voivat olla vaikeita muistaa, mikä johtaa usein niiden vaihtamiseen ja heikentää käyttömukavuutta. Umejiaku ym. (2023) huomauttavat, että teknologian kehittyessä tasapainon löytäminen salasanaturvallisuuden ja käyttäjäystävällisyyden välille on haastavaa. Samoin Wasfi & Stone (2023) vahvistavat, että merkittävä haaste salasanojen käytössä on löytää tasapaino helposti muistettavien ja turvallisten salasanojen välillä.

Käyttäjät eivät aina vaihda salasanojaan säännöllisesti ja heillä on taipumus käyttää samoja tai lähes samoja salasanoja useilla tileillä, mikä lisää haavoittuvuutta (Viswakarma, 2023). Vishwakarman (2023) tutkimuksen mukaan vain puolet käyttäjistä kertoi vaihtavansa salasanojaan säännöllisesti. Samojen salasanojen käyttö eri palveluissa johtaa siihen, että yhden palvelun tietomurto voi vaarantaa useita tilejä. Salasananhallintaohjelmat tarjoavat työkaluja monimutkaisten ja turvallisten salasanojen luomiseen ja hallinnointiin, mutta niiden käyttämisessä on haasteita. Umejiaku ym. (2023) toteavat, että monet käyttäjät pitävät ohjelmien tuottamia salasanoja vaikeina muistaa, mikä johtaa siihen, että ne kirjoitetaan muistiin tai käytetään samoja salasanoja useilla tileillä.

Tekoälypohjaiset kielimallit, kuten ChatGPT, ovat nousseet lupaavaksi ratkaisuksi vahvojen ja helposti muistettavien salasanojen luomiseen. Koneoppimisen avulla voidaan luoda yksilöllisiä ja monimutkaisia salasanoja käyttäjän mieltymysten perusteella, mikä parantaa salasanojen turvallisuutta ja muistettavuutta (Umejiaku ym., 2023). Tutkijat kuitenkin varoittavat, että hyökkääjät voivat käyttää samoja teknologioita, mikä altistaa käyttäjät uusille riskeille (Umejiaku ym., 2023).

4.1.2 Monivaiheinen tunnistautuminen (MFA)

Autentikoinnilla eli henkilön tunnistamisella on keskeinen rooli järjestelmien suojaamisessa, mutta sitä uhkaavat yhä kehittyneemmät tilien hakkerointiyritykset (Ogbanufe & Baham, 2022). Perinteiset yksivaiheiset tunnistautumistavat, kuten pelkät salasanat, ovat alttiita monenlaisille hyökkäyksille, kuten tietojenkalastelulle ja salasanan murtamiselle (Syahreen ym., 2024; Ogbanufe & Baham, 2022). Lisäksi ohjelmistojen haavoittuvuudet voivat johtaa käyttäjätietojen paljastumiseen, mikä lisää riskejä entisestään (Zeng ym., 2020). Jos tunnistautuminen perustuu pelkästään salasanaan, sen paljastuminen voi antaa hyökkääjälle suoran pääsyn käyttäjätilille. Hyökkääjät voivat löytää keinoja murtaa jopa vahvoja salasanoja, minkä vuoksi tulisi luoda monikerroksinen suojaus (Fadzoso ym., 2023).

Monivaiheinen tunnistautuminen (MFA) on kehitetty vahvistamaan käyttäjätilien suojaa vaatimalla useita todisteita henkilöllisyyden varmistamiseksi kirjautumisen yhteydessä (Ogbanufe & Baham, 2022). Monikerroksinen suojaus vaikeuttaa järjestelmiin murtautumista, sillä hyökkääjien on läpäistävä useita turvamekanismeja (Kovalan ym., 2021; Ogbanufe & Baham, 2022). MFA:ta käytetään esimerkiksi verkkopankeissa (Qashqari ym., 2020). Viimeaikaiset tutkimukset korostavat, että MFA on tehokas keino estää käyttäjätunnuksiin ja salasanoihin perustuvien todennusjärjestelmien haavoittuvuuksia (Syahreen ym., 2024). Thomas ym. toivat jo vuonna 2017 esille, että yksinomaan käyttäjätunnuksiin ja salasanoihin perustuva todennus ei riitä suojaamaan käyttäjätilejä tehokkaasti. Qashqari ym. (2020) pitävät MFA:ta parhaana ratkaisuna salasanojen heikkoon tehoon sähköpostin suojaamisessa.

Monivaiheiseen tunnistautumiseen on kehitetty erilaisia ratkaisuja. Syahreen ym. (2024) esittävät, siihen tulisi sisällyttää kolme erilaista tunnistautumistekijää: jotain mitä tiedät (kuten salasana), jotain mitä sinulla on (kuten puhelin) ja jotain mitä olet (kuten sormenjälki). Biometriset tunnisteet, kuten sormenjälki ja kasvojentunnistus, ovat yleisesti käytettyjä menetelmiä. Ne perustuvat käyttäjän biologisen identiteetin ainutlaatuisuuteen, mikä tekee niistä erityisen turvallisia (Syahreen ym., 2024). Älypuhelimissa biometrinen tunnistus on usein helppo ottaa käyttöön, koska useimmissa laitteissa on sisäänrakennettu kamera ja sormenjälkilukija (Zukarnain ym., 2022).

Toinen yleinen ratkaisu on käyttää kertakäyttöistä koodia, joka lähetetään käyttäjän puhelimeen tai todennussovellukseen, kuten Google Authenticatoriin tai Microsoft Authenticatoriin, mikä varmistaa käyttäjän henkilöllisyyden ennen kirjautumisen hyväksymistä (Qashqari ym., 2020). Tekstiviestipohjaisessa tunnistautumisessa on kuitenkin omat riskinsä, kuten kustannukset ja mahdollisuus puhelimen tai SIM-kortin katoamiseen. Lisäksi käyttäjän puhelinnumero voi joutua huijausyritysten kohteeksi, jos se vuotaa kolmansille osapuolille (Qashqari ym., 2020).

Niistä tekijöistä, jotka motivoivat yksilöitä käyttämään monivaiheista tunnistautumista, tiedetään vielä hyvin vähän (Ogbanufe & Baham, 2022). Käyttäjät voivat kokea monivaiheisen tunnistautumisen käytön liian monimutkaisena.

Ogbanufe & Baham (2022) kuitenkin havaitsivat, että käyttäjät, jotka ennakoivat katumusta mahdollisesta tietomurrosta, ovat todennäköisemmin motivoituneita ottamaan monivaiheisen tunnistautumisen käyttöön. Tämä viittaa siihen, että tietoturvakoulutuksessa tulisi painottaa tietomurtojen seurauksia ja luoda tunnetta ennakoidusta katumuksesta, jotta käyttäjät motivoituisivat paremmin suojauskeinojen käyttöön. Tämä lähestymistapa voi parantaa verkkotilien turvallisuutta ja vähentää tietomurtojen riskiä.

4.1.3 Muut teknologiset ratkaisut

Turvalliseen sähköpostin käyttöön liittyy muitakin teknologioita, joiden tehokkaaseen hyödyntämiseen käyttäjä voi vaikuttaa. Yksi keskeinen tapa varmistaa sähköpostin lähetyksen turvallisuus on käyttää verkon suojausmekanismeja, kuten salaustekniikoita, jotka varmistavat päästä päähän -turvallisuuden käyttäjän ja palveluntarjoajan välillä (Syahreen ym., 2024). Lisäksi tietoturvasovellukset tulisi pitää ajan tasalla ja ohjelmistot tulisi päivittää säännöllisesti, jotta välttyy vanhentuneisiin ohjelmistoihin liittyviltä haavoittuvuuksilta (Vishwakarma, 2023). Käyttäjien on myös hyvä olla tietoinen roskapostisuodatuksen toiminnasta ja tekoälyn tarjoamista mahdollisuuksista sähköpostiturvallisuuden parantamisessa (Vishwakarma, 2023).

Sähköpostin salaus suojaa viestejä ja liitteitä luvattomalta pääsyltä (Vishwakarma, 2023). Altuilahan ym. (2023) korostavat, että sähköpostiyhteys on kriittinen, sillä suojaamaton yhteys palvelimeen voi paljastaa kirjautumistietoja ja mahdollistaa viestien sisällön tarkkailun. Siksi käyttäjän ja palvelimen välinen tietoliikenne tulisi aina suojata SSL- tai TSL-salauksella. Tutkijat ohjeistavat käyttäjää tarkastamaan salauksen olemassaolon osoiteriviltä: jos se alkaa https-, eikä http- merkinnällä, salaus on käytössä. Salaus voidaan toteuttaa sähköpostipalvelun omilla ominaisuuksilla, ulkopuolisilla ohjelmistoilla tai lisäosilla. Käyttäjien tulisi myös huomioida julkisiin Wi-Fi-verkkoihin liittyvät riskit, sillä suojaamattomat yhteydet altistavat tietoliikenteen sieppauksille (Altuilahan ym. 2023).

Myös roskapostisuodatus ja haitallisten liitteiden skannaus liittyvät oleellisesti sähköpostiturvallisuuteen. Suodatusominaisuudet tunnistavat epäilyttäviä viestejä ja estävät niiden pääsyn postilaatikkoon (Vishwakarma, 2023). Käyttäjien tulisi hyödyntää näitä ominaisuuksia aktiivisesti ja merkata epäilyttävät viestit roskapostiksi, mikä parantaa järjestelmän kykyä havaita ja estää tulevia uhkia (Gallo ym., 2021; Vishwakarma, 2023).

Tekoälyn hyödyntäminen on nouseva trendi. Kyberuhkien jatkuva kehittyminen on johtanut uusien ratkaisujen, kuten koneoppimisen ja käyttäytymisanalyysin käyttöönottoon. Tekoäly voi havaita ja reagoida uhkiin reaaliajassa sekä analysoida käyttäjien toimintaa mahdollisten riskien tunnistamiseksi (Vishwakarma, 2023). Nämä innovaatiot mahdollistavat tehokkaamman ja ennakoivamman suojautumisen sähköpostiin kohdistuvilta hyökkäyksiltä.

4.2 Tietoturvatietoisuus ja turvallinen käyttäytyminen

Ihmisten ymmärrys tietoturvasta ja heidän käyttäytymisensä ovat keskeisessä roolissa sähköpostin suojaamisessa tietomurtoja vastaan. Käyttäjien kyky tunnistaa ja torjua kyberuhkia riippuu pitkälti heidän saamastaan koulutuksesta sekä siitä, kuinka hyvin he pystyvät soveltamaan oppimiaan taitoja käytännössä. Tutkimukset osoittavat, että tietämättömyys ja koulutuksen puute ovat merkittäviä tekijöitä tietoturvan haavoittuvuudessa (Hakami & Alshaikh, 2022; Das ym., 2022; Chaudhary, 2024). Monet tietoturvaloukkaukset johtuvat inhimillisistä virheistä, minkä vuoksi tutkijat painottavat tietoisuuden lisäämistä keinona vähentää tietoturvariskejä (Hakami & Alshaikh, 2022).

Vaikka teknologiset ratkaisut kehittyvät jatkuvasti, ne eivät yksinään riitä ehkäisemään hyökkäyksiä. Hyökkääjät hyödyntävät inhimillisiä virheitä, kuten sosiaalista manipulointia ja sääntöjen noudattamatta jättämistä (Hakami & Alshaikh, 2022). Chaudhary (2024) korostaa, että suurin osa tietomurroista johtuu tahattomista toimista tai toimimatta jättämisestä, jotka liittyvät puutteelliseen tietoturvatietoisuuteen. Lisäksi käyttäjät usein jättävät huomiotta tietoturvavaroitukset tai ohjeet, mikä lisää heidän haavoittuvuuttaan (Petrykina, Schwartz-Chassidim & Toch, 2021). Das ym. (2022) vahvistavat, että käyttäjien tietämättömyys estää heitä tunnistamasta riskejä ja ymmärtämästä suojaustoimenpiteiden merkitystä. Alothman ym. (2023) painottavat, että erityisesti sosiaalisen median käyttäjät usein aliarvioivat tietoturvan tärkeyden.

Käyttäjien omat käsitykset ja kokemukset tietomurroista voivat vaikuttaa merkittävästi heidän käyttäytymiseensä. Hassanzadeh ym. (2021) havaitsivat, että nämä käsitykset muodostuvat usein aiempien kokemusten ja tunteiden perusteella. Tämä voi joko motivoida heitä omaksumaan parempia käytäntöjä tai estää heitä toimimasta. Heidän tutkimuksensa mukaan käyttäjien mielikuvat tietomurroista ovat perustavanlaatuisia ja niissä on aukkoja, mikä korostaa tarvetta paremmalle viestinnälle tietoisuuden lisäämiseksi. Lisäksi Hassanzadeh ym. (2021) huomauttavat, että käyttäjien ymmärrys järjestelmien toiminnasta vaikuttaa heidän kykyynsä hahmottaa tietomurtojen riskejä ja seurauksia. He esittävät, että kun ymmärretään, missä käyttäjien käsitykset ovat puutteellisia, voidaan kehittää tehokkaampaa tietoturvaviestintää, joka auttaa käyttäjiä paremmin suojaamaan tietonsa ja tunnistamaan mahdollisia uhkia.

Samoin Vishwakarma (2023) tuo esiin, että sähköpostiturvallisuuskäytäntöjen viestintä ja käyttäjien sitouttaminen ovat ratkaisevia niiden tehokkuuden kannalta. Hän selittää, että pelkkä hyvien tietoturvakäytäntöjen kehittäminen ei riitä, ellei niitä viestitä tehokkaasti käyttäjille ja elleivät käyttäjät sitoudu noudattamaan niitä. Hänen tutkimuksensa mukaan monet käyttäjät ovat tietoisia sähköpostiin kohdistuvista uhkista, mutta he eivät aina ymmärrä, miten suositellut käytännöt voivat vähentää riskejä. Käyttäjien toimintaa ohjaavat riskin koettu taso, mukavuudenhalu ja luottamus. Tutkija ehdottaa, että koulutuksella ja tehokkaalla viestinnällä voidaan parantaa käyttäjien tietoisuutta ja sitoutumista, mikä puolestaan edistää parempaa sähköpostiturvallisuutta.

4.2.1 Turvallisuuden ja käytettävyyden tasapaino

Teknologioiden käytettävyyttä sivuttiinkin tutkielmassa jo aikaisemmin käsiteltäessä teknologisia ratkaisuja. Di Noceran, Tempestinin ja Orsinin (2023) mukaan käytettävyyttä edistävä tietoturva tarkoittaa tietoturvatoimenpiteiden suunnittelua ja toteutusta siten, että niissä huomioidaan käyttäjien tarpeet, kyvyt ja käyttäytyminen. Käytettävyyden näkökulma on keskeinen osa teknologisten ratkaisujen onnistunutta hyödyntämistä, mutta usein turvallisuuden lisääminen voi heikentää järjestelmän käytettävyyttä. Järjestelmät saattavat muuttua monimutkaisemmiksi ja vähemmän intuitiivisiksi käyttäjille, kun niistä tehdään turvallisempia esimerkiksi autentikointimekanismien tai salausprotokollien avulla (Di Nocera ym., 2023).

Rahman ym. (2021) toteavat, että turvallisempien järjestelmien luominen vaikuttaa usein negatiivisesti järjestelmän käytettävyyteen ja näiden tekijöiden välille on löydettävä sopiva tasapaino. Di Noceran ym. (2023) mukaan turvallisten järjestelmien monimutkaisuus voi johtaa jyrkempään oppimiskäyrään, suurempaan ponnisteluun tehtävien suorittamisessa ja käyttäjien turhautumiseen. Vastaavasti järjestelmän, jotka painottavat käytettävyyttä, voivat altistaa käyttäjät kyberhyökkäyksille (Di Nocera ym., 2023).

Di Noceran ym. (2023) tuovat esiin, että huolimatta käytettävyyden merkityksestä, aihe on saanut vain vähän huomiota tietoturvan kehittäjien keskuudessa, sillä sitä pidetään usein vähemmän tärkeänä kuin turvallisuutta. Usein ajatellaan, että käytettävyyteen liittyvät asiat eivät vaadi erityistä asiantuntemusta, ja käytettävyys nähdään täysin erillisenä asiana kuin turvallisuus. Tämä asenne voi kuitenkin johtaa järjestelmiin, joissa inhimillisten virheiden riski kasvaa, mikä heikentää niiden turvallisuutta (Di Nocera ym., 2023).

Desolda, Ferro, Marrella ja Costabile (2021) korostavat, että järjestelmiä tulee suunnitella käyttäjäystävällisiksi, jotta ne tukevat turvallista käyttäytymistä ja vähentävät inhimillisten virheiden riskiä. Tämä voisi tarkoittaa yksinkertaisten käyttöliittymien ja selkeiden ohjeiden tarjoamista, jotka auttavat käyttäjiä navigoimaan ilman turhautumista. Käyttäjäystävällisyyttä voitaisiin tukea tarjoamalla reaaliaikaista palautetta käyttäjän toiminnasta, mikä auttaa heitä ymmärtämään, mitkä toiminnot ovat turvallisia ja mitkä voivat altistaa heidät riskeille.

4.2.2 Tietojenkalasteluhyökkäysten tunnistaminen

Käytettävyys auttaa käyttäjiä hyödyntämään teknologisia ratkaisuja, mutta tietoturvariskit, kuten tietojenkalasteluhyökkäykset, haastavat käyttäjien kykyä havaita ja torjua uhkia. Näissä tilanteissa pelkkä teknologisten työkalujen tuki ei riitä, vaan tietoisuuden ja päätöksenteon merkitys korostuu (Desolda ym., 2021). Käyttäjien tulisi olla erityisen varovaisia avatessaan viestejä tuntemattomilta lähettäjiltä, sillä ne voivat sisältää haitallisia linkkejä tai ohjelmistoja. Lisäksi heidän tulisi suhtautua epäilevästi sähköposteihin, jotka näyttävät tulevat luotettavalta taholta, kuten pankilta tai yritykseltä, mutta sisältävät yllättäviä pyyntöjä, esimerkiksi henkilökohtaisten tietojen antamiseksi (Altuilahan ym., 2023).

Das ym. (2022) havaitsivat tutkimuksessaan, että osallistujat yliarvioivat usein kykynsä tunnistaa tietojenkalasteluviestejä, riippumatta heidän teknisestä osaamisestaan. Tutkimuksen mukaan tämä korostaa koulutuksen merkitystä, sillä tekninen tausta ei yksin riitä tehokkaaseen suojautumiseen. Jatkuva koulutus ja tietoisuuden lisääminen ovat välttämättömiä, jotta käyttäjät voivat paremmin tunnistaa ja välttää tietojenkalasteluhyökkäyksiä (Das ym., 2022).

Sturman, Bell, Auton, Breakey & Wiggins (2024) tutkivat, miten tietojenkalastelutieto, vihjeiden hyödyntäminen ja päätöksentekotyylit vaikuttavat kykyyn tunnistaa tietojenkalasteluviestejä. Heidän mukaansa koulutuksessa tulisi paitsi lisätä tietoa ja kehittää turvallisia toimintatapoja, myös tarjota käyttäjille keinoja tunnistaa tietojenkalastelulle tyypillisiä vihjeitä. Bayl-Smith, Sturman & Wiggins (2020) nostavat esiin, että tällaisia vihjeitä voivat olla epäjohdonmukainen muotoilu, kirjoitusvirheet, epäilyttävä sähköpostiosoite tai epäluotettavat linkit.

Myös Desolda ym. (2021) painottavat, että käyttäjien kouluttaminen tunnistamaan tietojenkalasteluyritykset ja ymmärtämään niiden seuraukset ovat ratkaisevan tärkeää. Heidän tutkimuksensa mukaan monet käyttäjät eivät ole tietoisia tietojenkalastelun riskeistä, tai osaa tunnista sen merkkejä, mikä tekee heistä alttiimpia hyökkäyksille. Ihmiset ovat usein taipuvaisia luottamaan liikaa tuttuihin lähettäjiin tai kiireellisiin viesteihin. Lisäksi emotionaaliset tekijät, kuten pelko ja uteliaisuus, voivat saada käyttäjät toimimaan impulsiivisesti lisäten tietojenkalastelun onnistumisen todennäköisyyttä. (Desolda ym., 2021.)

4.2.3 Pelillistetyt koulutukset

Uusimpien tutkimusten mukaan pelillistetyt koulutusmenetelmät ovat osoittautuneet tehokkaiksi tietoturvakoulutuksessa. Prümmer ym. (2024) toteavat, että pelillistämisen avulla voidaan simuloida todellisia kyberturvallisuustilanteita, mikä parantaa käyttäjien sitoutumista ja oppimismotivaatiota. Tämä heidän mukaansa johtaa oppimistulosten merkittävään paranemiseen.

Yasin ym. (2024) tutkivat pelillisyyden hyödyntämistä tietojenkalastelu-hyökkäysten estämisessä. Heidän tutkimuksensa osoitti, että pelin avulla osallistujat kehittivät merkittävästi kykyään tunnistaa tietojenkalasteluviestejä. Pelaajat oppivat havaitsemaan tietojenkalastelulle tyypillisiä merkkejä ja ymmärtämään, miten heidän toimintansa voi altistaa heidät hyökkäyksille. Tulokset viittaavat siihen, että pelipohjainen oppiminen voi olla tehokas keino kouluttaa käyttäjiä tietojenkalastelun vaaroista. Petrykina ym., (2021) esitteli tutkimuksessaan Security-Robot -nimisen pelillistetyn interaktiivisen tietoturvajärjestelmän, joka palkitsee käyttäjiä tietoturvallisista toimista verkossa. He havaitsivat, että pisteiden kerääminen motivoi käyttäjiä tekemään tietoisempia päätöksiä ja vähensi haittaohjelmien lataamista.

Varshney ym., (2024) mainitsevat, että monet organisaatiot kehittävät tällä hetkellä erilaisia tietojenkalastelun tunnistus- ja ehkäisymekanismeja, joihin kuuluu käyttäjien tietoisuuden lisäämistä, koulutuksia ja simulaatioharjoituksia. Tutkijat korostavat, että yritysten tulisi hyödyntää näitä ratkaisuja työntekijöiden kouluttamisessa, jotta hyökkäyksiä voidaan estää tehokkaammin.

4.2.4 Organisaatioiden merkitys käyttäjän toiminnan tukemisessa

Organisaatioiden tulisi priorisoida sähköpostiturvallisuuskoulutusta, investoida tehokkaisiin sähköpostiturvallisuuden ohjelmistoihin ja työkaluihin sekä kehittää yrityslaajuisia käytäntöjä, jotka edistävät käyttäjien turvallisten käytänteiden omaksumista (Vishwakarma, 2023). Prümmer ym. (2024) tuovat kuitenkin esiin, että koulutusmenetelmien valinnassa on tärkeää huomioida organisaatioiden erityispiirteet ja henkilöstön osaamistaso. Toinen organisaatio hyötyy enemmän simulaatiosta, kun toisen organisaation tarpeisiin voi sopia verkkokurssi.

Qashqarin ym. (2020) mukaan yritysten tulisi tarjota selkeitä ohjeita, jotka auttavat käyttäjiä estämään hyökkäyksiä. He ehdottavat seuraavia toimia:

> ”Älä avaa liitteitä, joiden nimet vaikuttavat epäilyttäviltä tai haitallisilta, ja vältä erityisesti pakattuja ja suoritettavia tiedostotyyppejä tuntemattomilta lähettäjiltä.
>
> Ole varovainen avatessasi epäluotettavia verkkosivustoja, sillä joitakin selaimen haavoittuvuuksia voidaan hyödyntää pelkästään sivustolla vierailemalla.
>
> Älä vastaa sähköpostiviesteissä tai ponnahdusikkunoissa oleviin pankkitietojen pyyntöihin.
>
> Älä koskaan käytä mahdollisesti arkaluonteisia tietoja ponnahdusikkunassa.
>
> Useimmat kalasteluviestit sisältävät linkin. Vie hiiri linkin päälle nähdäksesi, johtavatko ne samaan URL-osoitteeseen, ja jos eivät, ilmoita viesti roskapostiksi.
>
> Älä anna arkaluonteisia henkilökohtaisia tietoja (käyttäjätunnus ja salasana) sähköpostitse.”

Chaudharyn (2024) mukaan pelkkä tiedon jakaminen ei riitä muuttamaan työntekijöiden käyttäytymistä. Sen sijaan organisaatioiden tulisi keskittyä vaikuttamaan työntekijöiden asenteisiin ja motivoimaan heitä omaksumaan turvalliset toimintatavat. Käytännön toimet, jotka perustuvat pelkkään tiedon lisäämiseen, eivät ole tehokkaita, ellei tietoa hyödynnetä päätöksenteossa ja jokapäiväisessä toiminnassa (Chaudhary, 2024).

Hakami ja Alshaikh (2022) korostavat kyberturvallisuuskulttuurin merkitystä organisaatioissa. He määrittelevät kyberturvallisuuskulttuurin joukoksi normeja, uskomuksia ja asenteita, jotka ohjaavat ihmisten toimintaa tietojärjestelmien käytössä. Hyvin kehittynyt turvallisuuskulttuuri voi merkittävästi vähentää inhimillisten tekijöiden aiheuttamia riskejä ja samalla parantaa sekä tehokkuutta että turvallisuutta. Vishwakarma (2023) huomauttaa, että sähköpostiturvallisuusstrategioiden tehokkuus riippuu vahvasti organisaation kulttuurista, johtajuudesta ja resursseista. Vaikuttaa siltä, että kyberturvallisuuskulttuuri ei ole vain tekninen tai hallinnollinen kysymys, vaan se vaatii johdon vahvaa sitoutumista ja resursseja, jotta turvallisuus voidaan integroida osaksi jokapäiväistä toimintaa.

5 YHTEENVETO

Tässä kandidaatintutkielmassa tarkasteltiin käyttäjän roolia sähköpostitilien suojaamisessa tietomurtoja vastaan. Tutkimusaiheen taustalla olivat jatkuvasti kasvava tietomurtojen määrä ja niiden laajamittaiset haitalliset vaikutukset, jotka koskevat ihan jokaista. Tutkielman tavoitteena oli selvittää, millä keinoilla käyttäjät voivat suojata sähköpostitilejään tietomurtoja vastaan ja millaisia haasteita keinojen käyttöön liittyy. Käyttäjänäkökulma valittiin tutkielman rajaukseen, koska inhimilliset tekijät ovat keskeinen osa tietoturvan haavoittuvuuksia.

Tutkimus toteutettiin kirjallisuuskatsauksena. Lähteinä käytettiin mahdollisimman uusia ja vertaisarvioituja tieteellisiä artikkeleita, jotta tutkimus perustuisi ajankohtaiseen ja luotettavaan tietoon. Aineisto kerättiin tietokannoista, kuten Web of Science, Google Scholar, ja Jykdok. Sähköpostin tietoturvaa analysoitiin hyödyntäen CIA-mallia, jonka avulla havainnollistettiin, miten eri suojauskeinot edistävät sähköpostin luottamuksellisuutta, eheyttä ja saatavuutta. Tietomurtojen torjunnassa korostuu erityisesti sähköpostin luottamuksellisuuden suojaaminen, koska sähköpostitilit sisältävät usein henkilötietoja, pääsytietoja muihin palveluihin ja organisaatioiden luottamuksellisia asiakirjoja. Luvattomien kirjautumisyritysten estäminen on keskeinen osa luottamuksellisuuden suojaamista.

Tutkielma rakentui loogisesti eteneväksi kokonaisuudeksi, joka alkoi keskeisten käsitteiden määrittelyllä ja tietomurtojen vaikutusten avaamisella. Tietomurto tarkoittaa tapahtumaa, jossa luvaton osapuoli pääsee käsiksi järjestelmän luottamuksellisiin tietoihin. Kyberturvallisuus puolestaan viittaa teknologisten, hallinnollisten ja käyttäytymiseen liittyvien toimenpiteiden kokonaisuuteen, joilla pyritään estämään tietomurtoja ja suojaamaan järjestelmiä ulkopuolisilta hyökkäyksiltä. Tutkielmassa tarkasteltiin sähköpostin toimintaa ja siihen kohdistuvia tietoturvauhkia, kuten tietojenkalastelua ja tilien kaappaamista. Näiden uhkien esittely antoi perustan ymmärtää, miksi sähköpostitilien suojaaminen on välttämätöntä. Tutkielman pääpaino oli yhteenvetoa edeltävässä luvussa, joka käsitteli käyttäjän roolia sähköpostin suojaamisessa, painottaen teknologisia ratkaisuja sekä käyttäjien tietoturvatietoisuuden merkitystä.

Tutkimuksen tulokset esitettiin taulukossa (taulukko 1), jossa kuvattiin suojauskeinot, niihin liittyvät haasteet ja vaikutukset CIA-mallin. Tulokset osoittivat, että monivaiheinen tunnistautuminen (MFA) on yksi tehokkaimmista teknologisista keinoista suojata sähköpostitilejä tietomurtoja vastaan. MFA vaikeuttaa merkittävästi luvattomia kirjautumisyrityksiä, sillä hyökkääjän on läpäistävä useampi todennustekijä pelkän salasanan sijaan. Käyttäjien tietoturvatietoisuus ja kyky tunnistaa tietojenkalasteluhyökkäykset havaittiin keskeisiksi tekijöiksi inhimillisten virheiden vähentämisessä. Pelillistettyjen oppimisympäristöjen avulla voidaan lisätä käyttäjien tietoisuutta ja parantaa heidän kykyään tunnistaa kyberhyökkäyksiä. Lisäksi organisaatioiden rooli käyttäjien tukemisessa nähtiin keskeisenä, sillä organisaatioiden tarjoamat koulutukset, resurssit ja selkeät toimintamallit edistävät käyttäjien kykyä suojata sähköpostitilejään.

Tutkimuksessa tunnistettiin myös useita haasteita, kuten käyttäjien motivaatio ja järjestelmien käytettävyys. Monimutkaiset turvajärjestelmät voivat heikentää käyttäjäkokemusta, mikä saattaa vähentää käyttäjien halukkuutta hyödyntää niitä. Lisäksi käyttäjien kyvyttömyys tunnistaa tietojenkalasteluhyökkäyksiä ja heidän taipumuksensa käyttää samoja salasanoja useilla tileillä lisäävät tietoturvariskejä. Nämä tekijät korostavat tarvetta tasapainon löytämiseksi turvallisuuden ja käytettävyyden välillä, sillä liian monimutkaiset suojaukset voivat johtaa suojauskeinojen käyttämättä jättämiseen.

Johtopäätöksenä todetaan, että sähköpostitilien suojaaminen tietomurtoja vastaan edellyttää sekä teknologisia ratkaisuja että käyttäjien tietoisuuden lisäämistä. Monivaiheinen tunnistautuminen, pelillistetty oppiminen ja tietoturvakoulutus ovat tehokkaita keinoja, mutta niiden toimivuus riippuu käyttäjien sitoutumisesta ja organisaation tarjoamasta tuesta. Turvallisuusratkaisujen tulee olla helppokäyttöisiä ja selkeitä, jotta käyttäjät motivoituvat noudattamaan niitä. Organisaatioilla on merkittävä rooli turvallisten käytäntöjen juurruttamisessa osaksi arkipäiväistä toimintaa. Suosituksena on, että organisaatiot panostavat kattavaan tietoturvakoulutukseen ja hyödyntävät pelillistettyjä oppimisympäristöjä, jotka tekevät koulutuksesta motivoivaa ja käytännönläheistä. Lisäksi suositellaan, että sähköpostin käyttäjät ottaisivat käyttöön monivaiheisen tunnistautumisen sähköpostitileillään.

Tutkielmaan liittyi myös rajoitteita. Koska tutkielman tulokset perustuvat ainoastaan olemassa olevaan aiempaan tutkimukseen, tulokset ovat riippuvaisia löydettyjen tutkimusten laadusta ja kattavuudesta, ja jotkin vielä tutkimattomat näkökulmat saattoivat jäädä huomiotta. Lisäksi käyttäytymiseen liittyvien ilmiöiden tarkastelu vaatisi syvempää empiiristä analyysia. Aineiston rajaaminen vertaisarvioituihin lähteisiin saattoi sulkea pois käytännön ratkaisuja ja kokemuksia, jotka olisivat voineet täydentää tutkimuksen johtopäätöksiä. Myös CIA-mallin käyttö asetti rajoituksia, sillä malli keskittyy yleisiin tietoturvan periaatteisiin, mutta ei huomioi esimerkiksi käyttäjien yksilöllisiä motivaatioita tai taustatekijöitä. Vastuullisuuden näkökulman lisääminen olisi voinut laajentaa mallin soveltamismahdollisuuksia. On myös mahdollista, että jokin toinen viitekehys olisi tarjonnut tarkoituksenmukaisemman näkökulman tutkielman tarkasteluun.

Jatkotutkimukselle löytyy useita mahdollisuuksia. Tärkeä tutkimusaihe olisi selvittää enemmän käyttäjien motivaatiotekijöitä monivaiheisen tunnistautumisen käyttöönotossa, jotta käytön esteitä voitaisiin poistaa ja käyttäjiä motivoida vahvempien suojausmenetelmien käyttöönottoon. Lisäksi olisi hyödyllistä tutkia tekoälyn potentiaalia sähköpostiturvallisuudessa, josta löytyi vain vähän tutkimusta. Myös organisaatiokulttuurin ja johtajuuden vaikutukset tietoturvakäytäntöjen omaksumiseen kaipaavat lisää tutkimusta.

Sähköpostitilien suojaaminen tietomurtoja vastaan on jatkuvasti kehittyvä haaste, joka edellyttää yksilöiltä ja organisaatioilta yhteisiä ponnistuksia. Tietoturvatietoisuuden lisääminen, käytännönläheinen koulutus ja monivaiheinen tunnistautuminen ovat keskeisiä keinoja, jotka voivat merkittävästi vähentää tietomurtojen riskiä. Tämä tutkielma antaa käsityksen siitä, miten käyttäjät voivat parantaa sähköpostiturvallisuuttaan ja millaisia haasteita on voitettava tietomurtojen tehokkaamman estämiseksi.

LÄHTEET

Adebimpe, L. A., Ng, I. O., Idris, M. Y. I., Okmi, M., Ku, C. S., Ang, T. F., & Por, L. Y. (2023). Systemic Literature Review of Recognition-Based Authentication Method Resistivity to Shoulder-Surfing Attacks. *Applied Sciences*, *13*(18), Article 18. https://doi.org/10.3390/app131810040

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), Article 3. https://doi.org/10.3390/jcp2030027

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information Security:A Review of Information Security Issues and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1–6. https://doi.org/10.1109/CAIS.2019.8769504

Alothman, B., Alibrahim, O., Alenezi, N., Alhashemi, A., Alhashemi, M., Almardasi, D., Khattab, O., Joumaa, C., & Khan, M. (2023). The Development of a Secure Online System to Protect Social Networking Platforms from Security Attacks. *Applied Sciences-Basel*, *13*(21), 11731. https://doi.org/10.3390/app132111731

Altulaihan, E., Alismail, A., Rahman, M. M. H., & Ibrahim, A. A. (2023). Email Security Issues, Tools, and Techniques Used in Investigation. *Sustainability*, *15*(13), 10612. https://doi.org/10.3390/su151310612

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Bayl-Smith, P., Sturman, D., & Wiggins, M. (2020). Cue Utilization, Phishing Feature and Phishing Email Detection. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, & M. Sala (Eds.), *Financial Cryptography and Data Security: FC 2020 International Workshops.* (pp. 56–70). Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_5

Chaudhary, S. (2024). Driving behavior change with cybersecurity awareness. *Computers & Security*, *142*, 103858. https://doi.org/10.1016/j.cose.2024.103858

Das, S., Nippert-Eng, C., & Camp, L. J. (2022). Evaluating user susceptibility to phishing attacks. *Information and Computer Security*, *30*(1), 1–18. https://doi.org/10.1108/ICS-12-2020-0204

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. *Acm Computing Surveys*, *54*(8), 173. https://doi.org/10.1145/3469886

Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. *Information*, *14*(12), Article 12. https://doi.org/10.3390/info14120641

Fadziso, T., Rao Thaduri, U., Dekkati, S., Ballamudi, V. K. R., & Desamsetti, H. (2023). *Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat*. https://doi.org/10.6084/m9.figshare.24189921.v1

Gallo, L., Maiello, A., Botta, A., & Ventre, G. (2021). 2 Years in the anti-phishing group of a large company. *Computers & Security*, *105*, 102259. https://doi.org/10.1016/j.cose.2021.102259

Hakami, M., & Alshaikh, M. (2022). Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study. *International Journal of Computer Science and Network Security*, *22*(4), 299–309. https://doi.org/10.22937/IJCSNS.2022.22.4.37

Ham, J. V. D. (2021). Toward a Better Understanding of "Cybersecurity." *Digital Threats: Research and Practice*, *2*(3), 1–3. https://doi.org/10.1145/3442445

Hassanzadeh, Z., Biddle, R., & Marsen, S. (2021). User Perception of Data Breaches. *Ieee Transactions on Professional Communication*, *64*(4), 374–389. https://doi.org/10.1109/TPC.2021.3110545

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A., & Pitchan, M. A. (2021). A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users. *International Journal of Advanced Computer Science and Applications*, *12*(7). https://doi.org/10.14569/IJACSA.2021.0120792

Kyberturvallisuuskeskus. (2024, 11. kesäkuuta) *Tietomurrot*. Saatavilla osoitteessa: https://www.kyberturvallisuuskeskus.fi/fi/tietomurrot

Ogbanufe, O. M. & Baham, C. (2023). Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. *Information Systems Frontiers*, *25*(2), 897–916. https://doi.org/10.1007/s10796-022-10278-1

Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers & Security*, *108*, 102270. https://doi.org/10.1016/j.cose.2021.102270

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Qashqari, A., Alhbshi, D., Alzahrani, F., Ghwati, H. & Aljahdali, A. (2020). Electronic Mail Security. *College of Journal of Computer Science and Information Security (IJCSIS),* 18(5), 46–53. Saatavilla osoitteessa https://www.academia.edu/43236738/Electronic_Mail_Security.

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. *The 12th International Conference on Advances in Information Technology*, 1–11. https://doi.org/10.1145/3468784.3468789

Rikoslaki 39/1889. Finlex. Saatavilla osoitteessa: https://finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), Article 16. https://doi.org/10.3390/s23167273

Samonas, S., & Coss, D. (2014). The CIA Strikes Back. Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information Systems Security, 10(3),* 21-45. Saatavilla osoitteessa: https://www.jissec.org/Contents/V10/N3/V10N3.html

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4), 103638. https://doi.org/10.1016/j.im.2022.103638

Sturman, D., Bell, E., Auton, J., Breakey, G. & Wiggins, M. (2024). The roles of phishing knowledge, cue utilization, and decision styles in phishing email detection. *Applied Ergonomics*, *119*, 104309–104309. https://doi.org/10.1016/j.apergo.2024.104309

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748–1774. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2023.3273282

Syahreen, M., Hafizah, N., Maarop, N., & Maslinan, M. (2024). A Systematic Review on Multi-Factor Authentication Framework. *International Journal of Advanced Computer Science and Applications*, *15*(5). https://doi.org/10.14569/IJACSA.2024.01505105

Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Systems with Applications*, *210*, 118401. https://doi.org/10.1016/j.eswa.2022.118401

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017). Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1421–1434. https://doi.org/10.1145/3133956.3134067

Umejiaku, A. P., Dhakal, P. & Sheng, V. S. (2023). Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation. *Electronics (Basel)*, *12*(10), 2159-. https://doi.org/10.3390/electronics12102159

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*, *238*, 122199. https://doi.org/10.1016/j.eswa.2023.122199

Vishwakarma, A. (2023). Assessing the Effectiveness of Communication and Awareness Strategies for Promoting Email Security Best Practices Among End-Users A Survey-Based Study (SSRN Scholarly Paper 4404134). *Social Science Research Network*. https://doi.org/10.2139/ssrn.4404134

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, *52*, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Wasfi, H., & Stone, R. (2023). Usability and Security of Knowledge-based Authentication Systems: A State-of-the-Art Review. *International Journal of Advanced Computer Science and Applications*, *14*(5), 16–25. https://doi.org/10.14569/IJACSA.2023.0140502

Yasin, A., Fatima, R., JiangBin, Z., Afzal, W. & Raza, S., (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in Information Security. *Information and Software Technology*, *170*, 107426. https://doi.org/10.1016/j.infsof.2024.107426

Yee, C. K., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT in Education*, *8*(2), Article 2. https://doi.org/10.37134/jictie.vol8.2.4.2021

Zeng, P., Lin, G., Pan, L., Tai, Y., & Zhang, J. (2020). Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey. *IEEE Access*, *8*, 197158–197172. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3034766

Zukarnain, Z. A., Muneer, A., & Ab Aziz, M. K. (2022). Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. *Symmetry-Basel*, *14*(4), 821. https://doi.org/10.3390/sym14040821