SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Isola Silja & Römpötti Saana

Tietoturva sosiaalisessa mediassa

Kyselytutkimus

Opinnäytetyö
Syksy 2023
Tradenomi (AMK), Liiketalous

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Tradenomi (AMK), Liiketalous

Tekijät: Isola, Silja & Römpötti, Saana

Työn nimi alaotsikoineen: Tietoturva sosiaalisessa mediassa: Kyselytutkimus

Ohjaaja: Kulmala, Mikko

Vuosi: 2023 Sivumäärä: 54 Liitteiden lukumäärä: 1

Tässä opinnäytetyössä käsitellään yksityishenkilön tietämystä sosiaalisen median tietoturvasta: mitä uhkia sosiaaliseen mediaan liittyy, ja kuinka niiltä pystyy suojautumaan. Opinnäytetyön teorian lisäksi suoritettiin kyselytutkimus tutkimuskysymyksiin vastaamiseksi.

Opinnäytetyön teoriaosuudessa käydään läpi tietoturvan ja tietosuojan merkitystä sekä niiden määritelmiä. Teoriaosassa tarkastellaan suosituimpia sosiaalisen median alustoja. Näiden tukena teoriassa on myös osio, jossa käsitellään hyviä salauskäytäntöjä sekä kuinka suojautua sosiaalisessa mediassa esiintyviltä tietoturvauhilta.

Opinnäytetyön empiirisessä osassa toteutettiin määrällinen kyselytutkimus. Kyselytutkimukseen osallistui 112 henkilöä. Kysely luotiin ja julkaistiin Webropol-kyselytyökalun avulla. Kyselyn vastaajat löytyivät tutkimuksen tekijöiden lähipiiristä. Toteutettu tutkimuskysely oli vastaajille anonyymi. Tutkimuskyselyyn oli mahdollista vastata syksyllä 2023 viikkojen 42 ja 43 aikana.

Tutkimuksen tuloksista ilmeni, että valtaosa vastaajista on huolissaan sosiaalisen median turvallisuudesta. Vastaajilla oli myös tulosten mukaan hyvä tietoturvauhkatietämys, sillä suuri osa vastaajista tunnisti, mitä erilaiset uhat tarkoittavat. Lähes kaikki vastaajat olivat myös törmänneet joko itse tai läheisen kautta johonkin tutkimuksessa esiintyvään tietoturvauhkaan. Tutkimuksen tuloksen mukaan, vaikka tietoturvauhkatietämys olisi hyvä ja olisi ottanut käyttöön monivaiheisen tunnistautumisen eikä jakaisi mitään sosiaaliseen mediaan, moni ei silti enää luota sosiaalisen median turvallisuuteen.

[1] Asiasanat: Tietoturva, sosiaalinen media, tietosuoja

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Degree programme: Bachelor of Business Administration, Business Management

Specialisation:

Author/s: Isola, Silja & Römpötti, Saana

Title of thesis: Information security in social media: Survey study

Supervisor: Kulmala, Mikko

Year: 2023 Number of pages: 54 Number of appendices: 1

The thesis deals with a private person's knowledge about cyber threats in social media: what kinds of threats exist, and how to protect oneself from them. A survey was conducted to answer these research questions. The aim of the survey was to learn about individuals' knowledge of cyberthreats.

The theory part of this thesis deals with information security and data protection: what they are, and how they differ from each other. It discusses different social media platforms, as well as the most common cyber threats in social media. To support this, good password practices and ways to avoid cyber threats in social media are discussed.

The empirical part of this thesis included a quantitative survey with 112 respondents. The survey was created using the Webropol query tool. The respondents were found among those close to the authors of the study. The survey was completely anonymous. The questionnaire was open for answering in the fall of 2023, during weeks 42 and 43.

The results of the study show that most of the respondents are worried about their safety in social media. The results show that the respondents are aware the threats in social media. Almost all the respondents have experienced cyber threats themselves, or someone close to them has. According to the study, even if a person's knowledge of information security threats was good, and the person had taken every precaution step, and did not share anything in social media, the respondents' trust in social media is still not at a good level.

[1] Keywords: Information security, social media, data privacy

SISÄLTÖ

Kuva-, kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

Some	Some on lyhenne sanoista sosiaalinen media. (Kotimaisten kielten keskus, 2023).
FYP	For you page
GDPR	General Data Protection Regulation (yleinen tietosuoja-asetus**)**
Meemi	Sosiaalisessa mediassa ilmestyvä, nopeasti leviävä tyypillisesti kuva, joka on tehty huumori mielellä (Kielitoimiston sanakirja, 2023).
LGBTIQA+	Akronyymi sanoista: lesbian, gay, bisexual, transgender, intersex, queer/questioning, asexual (La Trobe Univercity, i.a.). Suomeksi HLBTIQA+ eli homo, lesbo, biseksuaali, trans, intersukupuolinen, queer, aseksuaali, ja +. +-merkki on termin perässä viittaamassa, niihin mitkä jäävät mainitsematta (Väestöliitto, 2020).
Mikrobloggaus	Mikroblogin ajatuksena on kirjoittaa lyhyitä viestejä ja nopeaa. (Tepa-termipankki, 2010)

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena oli tutkia henkilöiden tietoisuutta sosiaalisen median tietoturvauhkista ja selvittää henkilöiden kokemuksia sosiaalisen median turvallisuudesta. Tutkimuksen aihe on ajankohtainen jatkuvan digitaalisen kasvun myötä. Yksityishenkilöt ovat siirtyneet käyttämään pääasiallisesti pelkästään eri sosiaalisen median alustoja ja luovuttavat omia henkilökohtaisia tietojaan internetiin. Opinnäytetyön tavoite oli saada vastaus päätutkimuskysymykseen ”Mikä on yksityishenkilön tietämys tietoturvasta sosiaalisessa mediassa”

Sosiaalinen median käyttäminen on osa jokapäiväistä arkea suurimmalle osalle väestöstä. Sosiaalisen median yleistyttyä myös erilaiset tietoturvariskit ovat lisääntyneet. Yksityishenkilöiden kohdistuu aiempaa enemmän hyökkäyksiä ja sosiaalisen median alustoilla rikolliset pääsevät entistä kätevämmin kohdistamaan huijauksia uhreihinsa. Tunnistaako yksityishenkilö sosiaalisen median alustoilla piilevät tietoturvauhkat? Onko sosiaalisen median alustat turvallisia?

Opinnäytetyö koostuu teoriaosuudesta missä käsittelemme laajasti tietoturvaa, suosituimpia sosiaalisen median alustoja sekä tyypillisiä sosiaalisessa mediassa esiintyviä uhkia. Teoriaosuus sisältää myös osuuden hyvistä suojauskäytänteistä. Kyselytutkimus oli jaettu useampaan eri aihealueeseen käytännöllisemmän kyselytutkimuspohjan toteuttamiseksi. Ensimmäinen osa-alue koostui vastaajan perustietojen kartoituksesta (ikäryhmä, koulutusaste, sosioekonominen asema ja tietämystietoteknistä osaamisesta). Toisen kyselylomakkeen osa-alueen tarkoitus oli selvittää mitä sosiaalisen median alustoja vastaajat käyttivät ja kuinka aktiivisesti. Kyselyn kolmannessa osa-alueessa kerättiin tietoa vastaajien näkemyksistä sosiaalisen median turvallisuudessa ja luottamuksesta. Vastaajien tietämystä ja kokemuksia tietoturvaan liittyen selvitettiin kolmannessa osiossa, myös esittämällä yksityiskohtaisesti kysymyksiä koskien tietoturvaa ja sosiaalisessa mediassa liikkuvia tietoturvauhkia. Neljännessä kyselyn osa-alueessa selvitimme vastaajien tuntemuksia käyttäjätilien turvallisuudesta ja suojauksesta. Neljännen kysymyssarjan tarkoitus oli selvittää,

kuinka paljon vastaajat tietämättään jakavat omia henkilökohtaisiaan tietojaan sosiaalisen median alustoilla.

Kyselytutkimuksen tulokset on käsitelty kirjallisesti sekä havainnollistamalla tutkimustuloksia. Kyselytutkimukseen vastasi yhteensä 112 henkilöä. Kyselytutkimus toteutettiin Webropol–kyselytyökalun avulla. Kysely oli avoinna syksyllä 2023 aikavälillä 16.10.–1.11.2023. Kyselyn tulokset purettiin osiin ja avattiin havainnollistamalla kaavioiden ja kuvioiden avulla.

Tutkimustulosten perusteella sosiaalista mediaa ei pidetä enää turvallisena ympäristönä. Tutkimuksen vastaajat olivat hyvin tietoisia mahdollisista sosiaalisen median tietoturvauhkista. Erinäisten huijauksien uhriksi olivat joutuneet niin vastaajat henkilökohtaisesti ja heidän läheisensä. Vastaajien omat kokemukset huijauksista heikentävät luottamusta sosiaalisen median alustoja kohtaan merkittävästi. Tutkimustulosten perusteella sosiaalisen median suosituimmat alustat ovat menettäneet asemansa turvallisena sekä luotettavana ympäristönä internetissä yksityishenkilöiden keskuudessa.

2 TIETOTURVA JA TIETOSUOJA

Tässä osiossa käydään läpi tietosuojan, tietoturvan ja GDPR:n eroja ja niiden merkitystä yhteiskunnassa. Osiossa käsitellään lisäksi, mikä niiden tarkoitus on yksilön henkilötietojen turvallisuuden ja käsittelyn kannalta.

2.1 Tietoturva

Tietosuojavaltuutetun toimiston (i.a.) nettisivuilla kerrotaan tietoturvan olevan yksi tietosuojan toteuttamisen keino. Tämä viittaa siihen, että tietoturva on tietosuojalaissa määritelty tärkeä osa henkilön tietojen turvaamisen kannalta. Tiedon turvaamiseen käytettäviä keinoja voivat olla fyysiset tai hallinnolliset tavat. Fyysisillä keinoilla tarkoitetaan toimia, miten fyysisesti tieto turvataan, esimerkiksi turvallinen asiakirjasäilytys ja asianmukainen vanhentuneen tiedon hävitys. Tietoja voidaan myös turvata varmistamalla käytettävien laitteiden ajantasaiset päivitykset sekä huolehtimalla voimassa olevasta virusturvatorjunnasta ja palomuurista. Tärkeää on myös, että tietojenkäsittelijät ovat luotettavia ja oikeaoppisesti koulutettuja käsittelemään henkilötietoja. Tietoja käsitellessä tulee myös varmistaa, että niitä käsitellään luottamuksellisesti ja varovaisesti.

Tietoturvalla tarkoitetaan toimia, joilla voidaan varmistaa tiedon luottamuksellisuus, eheys ja käytettävyys (Traficom, 2020). Nämä kolme takaavat tietojen turvallisen käsittelyn, luotettavuuden sekä tuovat rekisteröidylle oikeuden tarkistaa häntä koskevat tiedot. Tiedon luottamuksellisuudella tarkoitetaan, että tieto on vain siihen oikeutettujen henkilöiden saatavilla. Tiedon eheys takaa, että tietoja ei pääse muuttamaan kukaan ulkopuolinen. Käytettävyydellä varmistetaan, että tieto on siihen oikeutettujen henkilöiden ja järjestelmien hyödynnettävissä. Tämä tarkoittaa, että esimerkiksi sosiaalisessa mediassa alusta on rekisterinpitäjä, joka kerää henkilötietoja, joita rekisteröitynyt käyttäjä luovuttaa. Kukaan ulkopuolinen ei ole oikeutettu tarkastelemaan tai muuttamaan näitä henkilötietoja.

2.2 Tietosuoja

Tietosuojan tarkoituksena on suojata luonnollisen henkilön henkilökohtaisia tietoja ja taata niiden asianmukaisen käsittelyn (Tietosuojalaki 1050/2018). Henkilötietojen käsittely on perustuttava aina lakiin. Tietosuoja-asetuksessa on määritelty kansallisena valvontaviranomaisena toimiva tietosuojavaltuutettu, joka työskentelee oikeusministeriön yhteydessä. Tietosuojavaltuutettu on toiminnassaan itsenäinen ja riippumaton. Valtioneuvosto nimeää tietosuojavaltuutetun ja apulaistietosuojavaltuutetut viiden vuoden mittaisiksi toimikausiksi. Tämänhetkinen Suomen tietosuojavaltuutettu on Anu Talus, joka on ollut tehtävässä 1. marraskuuta 2020 lähtien.

Tietosuojavaltuutetun toimiston mukaan (i.a.) tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksia ja vapauksia hänen henkilötietojansa käsitellessä. Henkilötietoja ovat kaikki luonnollisen henkilön tunnistamisessa auttavia tietoja. Henkilön suoria tunnistetietoja ovat esimerkiksi nimi, puhelinnumero, kotiosoite tai henkilötunnus. Henkilön voi tunnistaa välillisten tunnistetietojen avulla, näitä voivat olla työpaikkasi, lemmikin eläinlääkäritiedot ja isovanhempien perinnöllisiä sairauksia koskevat tiedot. Tietosuojalaki myös takaa yksityishenkilön oikeuden tarkastella hänestä kerättävän tiedon oikeellisuuden, ja tarvittaessa henkilö voi vaatia tietojen korjaamista. Rekisteröidyllä yksityishenkilöllä on tietosuojalain nojalla myös oikeus pyytää unohtamista. Unohtamista pyytäessään kaikki hänestä kerätty tieto tulee tuhota.

2.3 GDPR

Yleisen tietosuoja-asetuksen tavoitteena on suojella luonnollisen henkilön perusoikeuksia ja -vapauksia suojella hänen henkilötietojansa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679). Asetuksella myös taataan henkilötietojen vapaa liikkuminen Euroopan Unionin alueella. Tämä tarkoittaa, että tietojen liikkuvuutta ei saa rajoittaa tai kieltää mikäli tieto liittyy henkilön suojelemiseen henkilötietojen käsittelyssä. Yleisen tietosuoja-asetuksen mukaan henkilötietoja on aina käsiteltävä lainmukaisesti, asianmukaisesti ja läpinäkyvästi. Henkilötietojen keräämiseen tulee aina olla laillinen syy, eikä kerättyä tietoa saa käyttää tai tarkastella tämän määritellyn syyn ulkopuolella. Kerätty tieto tulee myös rajata,

vain siihen mikä on tarpeen. Kerättyä henkilötietoa voi kuitenkin käyttää rekisterin ulkopuolella historialliseen tai tilastolliseen tutkimukseen, edellyttäen tutkimuksen teettäjän käsittelevän tietoja yleisen tietosuoja-asetuksen mukaisesti. Yleinen tietosuoja-asetus koskee kaikkia organisaatioita, jotka käsittelevät yksityishenkilöiden henkilötietoja ja toimivat Euroopan Unionin alueella, myös sosiaalista mediaa.

Alkukesästä 2023 Euroopan tietosuojalautakunta määräsi Metalle 1,2 miljardin euron sakon Euroopan tietosuoja asetuksen rikkomisesta (EDPB, 2023). Tämä sakko määrättiin, koska Meta ei ole onnistunut noudattamaan Euroopan tietosuojalakia, vaan on laittomasti siirtänyt eurooppalaisten yksityishenkilöiden henkilötietoja Yhdysvaltoihin. Sakko on suurin tietosuojalautakunnan määräämä, sakon lisäksi Meta on määrätty muuttamaan tiedonsiirtonsa vastaamaan EU:n tiedonsiirto lakeja. Meta on myös määrätty lopettamaan tietojen laiton käsittely, mukaan lukien varastointi kuuden kuukauden sisällä päätöksestä.

3 SOSIAALISEN MEDIAN ALUSTAT

Lutkevichin (2021) mukaan sosiaalinen media on kollektiivinen termi verkkosivustoille ja sovelluksille, jotka keskittyvät kommunikointiin, yhteisökeskeiseen panostukseen, vuorovaikutukseen, sisällöntuottamiseen ja yhteistyöhön. Sosiaalista mediaa käytetään yhteyden pitämiseen ihmisten välillä. Yhteisöt ja organisaatiot myös hyödyntävät sosiaalista mediaa tuoden itseään esille verkossa.

Tässä teoriaosiossa käydään läpi yleisimpiä sosiaalisen median alustoja, niiden taustoja ja käyttötarkoituksia. Tähän teoriaosuuteen valikoitui sosiaalisen median alustoja, mitkä ovat suosittuja, mutta myös interaktiivisia. Alustoilla käyttäjät voivat siis halutessaan viestiä muiden kanssa, tuottaa sisältöä ja reagoida muiden sisältöön. Lisäksi tarkastelemme pikaviestintäpalveluita, kuten WhatsAppia ja Snapchatia.

3.1 Facebook

Hallin (2023) kirjoittamassa artikkelissa määritellään, että Facebook on sosiaalisen median alusta, jonka perustivat vuonna 2004 Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz ja Chris Hughes. Facebook oli alun perin suunniteltu Harvardin yliopiston opiskelijoiden käyttöön, josta se levisi muihin arvovaltaisiin yliopistoihin Yhdysvalloissa. Vuonna 2005 Facebook avattiin julkiseksi opiskelijoille Yhdysvaltojen ulkopuolella, ja vuonna 2006 Facebookista tuli julkinen kaikille yli 13-vuotiaille. Vuonna 2023 Facebookilla on noin 3 miljardia aktiivista kuukausikäyttäjää (Kemp, 2023b). Suomessa Facebookia käyttää 2,4 miljoonaa käyttäjää.

Facebook tunnusten luominen ja käyttäminen on käyttäjälleen ilmaista (Facebook, 2023). Käyttäjät voivat luoda oman sivunsa, julkaista päivityksiä, kuvia tai videoita lisäämiensä ystävien nähtäviksi. Käyttäjät voivat myös liittyä olemassa oleviin ryhmiin tai perustaa oman ryhmän. Yksi keskeisimmistä osista tällä alustalla on aikajana, mistä näkee Facebook-ystävien päivityksiä ja tapahtumia. Käyttäjät voivat myös viestitellä ystäviensä ja erilaisten yritysten kanssa Facebookin omalla Messenger-alustalla. Facebook Messenger

viestialustalla on Suomessa 1,55 miljoonaa käyttäjää (Kemp, 2023a). Maailmanlaajuisesti viestialustaa käyttää noin miljardi käyttäjää.

Meta tiedotti syksyllä 2023 muuttavansa Facebookin ja Instagramin mainoskäytäntöjä EU:n, ETA:n ja Sveitsin alueella (Meta, 2023). Facebookin ja Instagramin käyttö on jatkossakin ilmaista käyttäjille, jos he hyväksyvät mainokset. Mikäli mainoksista kuitenkin haluaa eroon, Meta tarjoaa mahdollisuuden maksulliseen Facebookiin ja Instagramiin. Maksuton versio näistä maksaa kuukaudessa tietokoneversiona 9,99 € tai 12,99 € mobiiliversiona. Hinnasto on luotu oletuksella, että käyttäjän Facebook ja Instagram -tili on yhdistettynä toisiinsa Metakeskuksen kautta. Meta teki päätöksen maksullisista vaihtoehdoista vastauksena Euroopan Unionin yleiseen tietosuoja asetukseen. Metalle annettiin Euroopan Unionin tietosuojalautakunnan toimesta 1,2 miljardin euron arvoinen sakko Euroopan yleisen tietosuoja-asetuksen rikkomisesta (EDPB, 2023).

3.2 Instagram

Eldridgen (2023) mukaan Instagram on vuonna 2010 julkaistu kuvien ja videoiden jakamiseen tarkoitettu sosiaalisen median alusta. Instagramin on perustanut Kevin Krieger ja Kevin Systrom. Instagram oli alun perin suunniteltu ja optimoitu vain iPhonelle. Instagramin peruskäyttötarkoitus on hyvin suoraviivainen. Käyttäjätilin luomisen jälkeen, julkaiset sisältöä matkapuhelimellasi. Julkaisusi näkyvät joko kaikille Instagramin käyttäjille tai vain tietyille käyttäjille riippuen yksityisyysasetuksistasi. Instagramissa on kaksi päätoiminnallisuutta: Kuvasyöte (*feed*) ja tarina (*story*). Kuvasyötteessä julkaistut kuvat ja videot näkyvät kaikkien sallittujen henkilöiden kuvasyötteessä ja myöhemmin ne ovat löydettävissä omasta profiilistasi. Kuvasyötteessä julkaistuja kuvia voivat muut käyttäjät kommentoida tai tykätä. Tarinassa julkaistut kuvat poistuvat 24 tunnin päästä julkaisusta, ellei niitä erillisesti arkistoida. Instagramissa on myös mahdollista lähettää yksityisviestejä (eli *direct message* [DM]), kuvia tai videoita muille käyttäjille.

Instagramin julkaisun jälkeen sen suosio kasvoi räjähdysmäisesti, ja kiinnostuneita ostajia oli paljon (Eldridge, 2023). Vuonna 2012–18 kuukautta julkaisemisen jälkeen Facebook

osti Instagramin. Facebookin ostaessa Instagramin vuonna 2012 julkaistiin versio, mikä oli tuettu myös Android-laitteiden käyttöön. Alkuvuonna 2023 Instagramilla oli maailman laajuisesti 1,6 miljardia käyttäjää (Kemp, 2023c). Suomessa Instagramia käyttää 2,3 miljoonaa käyttäjää.

3.3 X (entinen Twitter)

Twitter on vuonna 2006 julkaistu mikrobloggaamisen suunniteltu verkkopalvelu. Kempin (2023d) mukaan Twitterillä on yli 372.9 miljoonaa aktiivista käyttäjää. Suomessa Twitteriä käyttää 1,5 miljoonaa käyttäjää. Twitter on tarkoitettu yli 13-vuotiaille yksityishenkilöille, yrityksille ja yhteisöille. Näiden lisäksi Twitterissä on tilejä myös julkisuuden henkilöille, ja niin kutsuttuja fanisivuja tietyille aiheille, esimerkiksi eläimille ja elokuville. Twitterissä julkaistavien lyhyiden tekstien eli twiittien maksimipituus on 280 merkkiä. Twitterissä julkaistut twiitit ovat kaikkien käyttäjien nähtävillä.

Kesällä 2023 Twitter muutti nimensä ja ulkoasunsa X:ksi (Lehtinen, 2023). Samalla Twitter poisti käytöstä sinisen linnun, joka on toiminut Twitterin ikonina alusta lähtien. Uudelleen brändäämisen tarkoituksena on muodostaa, Twitterin toimitusjohtaja Linda Yaccarino ja omistaja Elon Muskin mukaan, ”globaali ajatusten, tuotteiden, palveluiden ja mahdollisuuksien markkinapaikka”. Yaccarinon mukaan tulevaisuudessa X keskittyy enemmän audiosisältöön, videoihin, viestinvaihtoon ja maksuliikenteeseen.

3.4 TikTok

TikTok on vuonna 2017 julkaistu sosiaalisen median videopalvelu (Dolan, 2023). TikTok on kiinalaisen yksityisomisteisen ByteDancen kehittämä sovellus. ByteDance omistaa kiinassa suositun Douyinin, minkä kansainvälinen versio on TikTok. TikTokin suosio nousi kansainvälisesti, kun ByteDance osti 2018 silloisen Musical.ly palvelun, mikä koostui käyttäjien lyhyistä (noin 15 sekuntia) laulu ja tanssivideoista. Kuten Musical.ly myös TikTok koostuu lyhyistä videoista, jotka käyttäjät tuottavat yhteiseen *for you pageen* (FYP). Käyttäjät voivat tuottaa yhteiseen syötteeseen myös muita videoita esimerkiksi yleistä turinaa,

videoesseitä, kepposia, haasteita ja meemejä. Vuonna 2022 tulleen päivityksen myötä videoiden maksimipituus on 10 minuuttia (Meltwater, 2023a)

TikTokia on laajasti kritisoitu eri verkoissa sen tuomien vaarojen vuoksi ja lisääntyvän verkkokiusaamisen takia. TikTok piilottelee erilaisten ryhmien esimerkiksi ylipainoisten ja LGBTIQA+ henkilöiden sisältöä (Mäkipää, 2019). Osa käyttäjistä ja videoista TikTokissa myös kannustaa ja tukee syömishäiriötä (Aarnio, 2020). TikTokissa saattaa esiintyä myös häiritsevää sisältöä liittyen itsetuhoisuuteen ja itsemurhaan. Vuosittain saa lukea uutisista, miten TikTok livessä nuori ihminen on päättänyt henkensä ja video tapahtuneesta jää kiertämään somealustalle. Kemppi (2020) kirjoitti *Iltalehdessä*, että TikTokin moderoinnista huolimatta video saattaa jäädä alustalle liikkumaan naamioituneena muuksi. Toinen huolenaihe New York Timesin mukaan on TikTokin omistaman ByteDancen liitokset Kiinan hallitukseen (Maheshwari & Holpuch, 2023). Intia on kieltänyt koko alustan vuonna 2020. Muissa maissa ja hallinnoissa esimerkiksi Euroopassa, Kanadassa ja Australiassa on TikTokin sovellus kielletty hallituksen virallisissa laitteissa.

3.5 WhatsApp

WhatsApp julkaistiin vuonna 2009, Facebook osti WhatsAppin vuonna 2014 (Martin, 2023). WhatsApp on verkossa toimiva viestipalvelu, jonka toimimiseen tulee olla toimiva verkkoyhteys. Martinin mukaan WhatsAppissa käyttäjät pystyvät kommunikoimaan muiden käyttäjien kanssa viestien (kirjoitettu tai ääniviesti), WhatsAppilla pystyy myös soittamaan muille käyttäjille ääni- tai videopuheluita. Yksityisten viestikeskustelujen lisäksi, WhatsAppissa pystyy muodostamaan ryhmiä ja kommunikoida ryhmän kanssa. WhatsApp on pääosin mobiililaitteissa käytettävä sovellus, koska sen aktivointi vaatii puhelinnumeron. Aktivoinnin jälkeen sovellus on myös käytettävissä tietokoneella. WhatsApp on aluksi ollut tarkoitettuna yksityishenkilöille, mutta on sittemmin laajentunut myös yritysten käyttöön. Meta mahdollistaa yrityksille suoraa viestimisen heidän nettisivuiltaansa WhatsApp-napin kautta (Meta, 2022). Metan julkaiseman neljännesvuosi raportin mukaan WhatsApp-napin tuotto kasvoi yli 80 % vuodessa, saavuttaen 1,5 miljardin dollarin käyttöasteen.

Kempin (2023e) mukaan WhatsAppilla on yli 2 miljardia aktiivista käyttäjää päivittäin maailman laajuisesti, käyttäjät koostuvat pääosin yksityishenkilöistä ja yrityksistä. WhatsAppin kokonaiskäyttäjämäärän arvioidaan olevan suurempi, sillä kaikki käyttäjät eivät käytä sovellusta päivittäin. WhatsApp on kuitenkin maailman laajuisesti kolmanneksi käytetyin sosiaalisen median alusta. Clausnitzerin (2023) mukaan Suomessa 89 % aikuisväestöstä käyttää WhatsAppia, näistä lähes puolet avaavat sovelluksen useita kertoja päivässä. WhatsAppin tarkkaa käyttäjä kuntaa on haastava arvioida, sillä käyttöehtojen mukaan sovellus on tarkoitettu yli 13-vuotiaille henkilöille (WhatsApp, 2021). Euroopan alueella asuvien käyttäjien tulee olla vähintään 16-vuotiaita, elleivät he saa huoltajalta lupaa sovelluksen käyttöön.

3.6 Snapchat

Snapchat on vuonna 2011 julkaistu pikaviestisovellus (Jäntti, 2017). Snapchatissa käyttäjät keskustelevat toistensa kanssa kuvien välityksellä. Snapchatissa voi jutella kavereiden kanssa, jotka ovat lisätty käyttäjätunnuksen perusteella. Etenkin nuorten keskuudessa Snapchat on saanut suuren suosion, sen nopean kommunikointi mahdollisuuden vuoksi. Snapchatissa voi myös muokata kuvia ja videoita ottamisen jälkeen tai kuvatessa käyttää erilaisia filttereitä muun muassa sosiaalisessa mediassa levinnyt koirafiltteri on lähtöisin Snapchatista. Alun perin Snapchatissa lähetetyt kuvat ja videot näkyivät vastaanottajalle korkeintaan 10 sekuntia. Nykyään lähetettyjen kuvien ja videoiden näkyvyyttä voi lähettäjä muuttaa, että kuva tai video näkyy vastaanottajalla 10 sekuntia tai sen voi myös muuttaa näkymään niin kauan kunnes vastaaja painaa kuvan tai videon pois.

Kempin (2023f) mukaan Snapchatilla on 654,4 miljoonaa käyttäjää. Snapchatin kokonaiskäyttäjistä 1,85 miljoonaa on Suomalaisia. Eniten Snapchat-käyttäjiä maailmassa on Intiassa, missä on arviolta 182,4 miljoonaa aktiivista käyttäjää. Snapchat on nuorten aikuisten keskuudessa suosittu pikaviestintäsovellus. Tilastollisesti 38,6 % Snapchat-käyttäjistä on 18–24-vuotiaita, eli noin 243 miljoonaa käyttäjää.

4 TIETOTURVAUHAT SOSIAALISESSA MEDIASSA

Sosiaalisessa mediassa esiintyy päivittäin erilaisia tietoturvauhkia, mitkä ovat vaaraksi henkilötiedoillemme. Tietoturvarikokset aiheuttavat uhreilleen usein taloudellista haittaa tai muuta elämiseen liittyvää haittaa. Tässä teoriaosiossa käydään läpi yleisimpiä tietoturvauhkia.

4.1 Kalastelu (phishing)

National Cyber Security Center (NCSC, 2018), määrittelee *phishingin*, eli tietojenurkinnan olevan verkossa tapahtuvaa tietojenkalastelua. Tällöin hyökkääjä yrittää ohjastaa henkilön (uhrin) avaamaan linkin, mikä ohjaa hänet kyseenalaiselle web-sivustolle tai lataa haittaohjelman laitteelleen. Tietojenurkinta on yleisintä sähköpostitse, mutta sitä tapahtuu myös sosiaalisessa mediassa, tekstiviesteillä ja puhelimitse. F-Securen (2023a) mukaan tietojenkalastelulla on kolme eri muotoa, kohdennettu tietojenkalastelu (*spear phishing*), tekstiviestihuijaukset (*smishing*) ja huijauspuhelut (*vishing*).

F-Securen sivuilla (2023a) kerrotaan, että kohdennetussa tietojen kalastelussa kohteena voivat olla yksityishenkilöt ja yritykset. Kohdennettu kalastelu on enemmän yrityksiin kohdistuneempi tietojenkalastelumuoto. Tässä tietojenkalastelumuodossa viestit ovat räätälöity kohdetta ajatellen, ja näitä on tämän takia vaikeampi tunnistaa kalasteluyrityksiksi. Kohdennetun tietojenkalastelun tarkoituksena on saada haltuunsa esimerkiksi organisaation sisäistä tietoa, tai yksityishenkilön henkilötietoja.

Traficomin (2019) mukaan tekstiviestihuijauksissa lähettäjän tiedot ovat väärennettyjä. Viestit vaikuttavat tulevan luotettavalta lähettäjältä, mutta viestissä oleva linkki kuitenkin ohjaa sivustolle, millä ei ole mitään tekemistä oikean lähettäjän kanssa. Tyypillisiä viestien lähettäjiä ovat esimerkiksi Postin nimissä lähetetty viesti, missä kerrotaan esimerkiksi olevan paketin seurantakoodi tai saapuvasta lähetyksestä on tullimaksuja maksamatta. Viimeisen parin vuoden aikana tekstiviestihuijaukset ovat myös jalkautuneet pikaviestipalveluihin kuten WhatsAppiin. F-Securen (2023b) mukaan yksi yleinen huijaus WhatsAppissa

on ”Hei äiti”. Tällä huijauksella kerrotaan lapsen puhelimen hajonneen ja viesti lähetetään hänen uudesta puhelinnumerostansa. Tällä huijausmuodolla pyritään hyväksi käyttämään vanhempien tunteellista puolta, ja pyytää heitä lähettämään rahaa kiireelliseen laskuun tai uuden puhelimen ostamiseen. Viestissä painotetaan rahan siirtämisen kiireellisyyttä ja kuinka raha tulee siirtää toiselle tilille, sillä ”lapsi” ei pääse käsiksi omaan tiliinsä.

F-Securen (2023a) mukaan huijauspuheluissa kalastellaan usein pankki- ja henkilötunnuksia. Huijauspuheluita soittavat esiintyvät tyypillisesti pankin tai muun luotettavan tahon edustajana. Näissä huijauksissa pyritään saamaan uhri luovuttamaan puhelimitse henkilötietonsa, kuten verkkopankin salasana tai henkilötunnuksensa. Huijauspuheluita voi myös esiintyä IT-tuen nimissä, näiden puheluiden tarkoituksena on saada kohde asentamaan tietokoneelleen etähallintaohjelman. Laitteelle asennetun etäohjelman tarkoituksena on vakoilla laitteen käyttäjää ja potentiaalisesti saavuttaa tietoonsa arkaluontoisia salasanoja ja tietoja.

4.2 Romanssihuijaukset

Kuluttajaliiton (i.a) mukaan romanssihuijaukset esiintyvät yleensä seuranhakupalveluissa. Romanssihuijarit ottavat myös yhteyttä sosiaalisessa mediassa tai sähköpostitse. Tyypillisesti romanssihuijarit esittävät olevansa varakkaita ja korkeassa asemassa olevia henkilöitä. Romanssihuijauksissa pyritään luomaan luottamussuhde ensin, joten rahanpyyntöön voi mennä viikkojakin. Luottamuksen saavutettua rahaa pyritään pyytämään kaikilla mahdollisilla tekosyillä ja selityksillä.

Knuuttilan (2022) mukaan romanssihuijaukset ovat yleistyneet pandemian aikana ja sen jälkeen. Romanssihuijauksissa pyritään hyväksikäyttämään uhrin ihastuksen, kiintymyksen tai empatian tunnetta. Uhrille usein uskotellaan, että kiintymyksen kohde on pulassa ja tarvitsee rahaa tai kiintymyksen kohde tarvitsee rahaa lähettääkseen uhrille arvokkaan lahjan. Rahan pyytämisen jälkeen uhria pyritään pelottelemaan maksamaan nopeaa. Mikäli uhri ei siirrä rahaa kiintymyksen kohteelle tulee vakavia seurauksia, kuten vankila tai hänet irtisanotaan työstään. Näissä huijauksissa rahanpyyntö viesti voi tulla myös joltain toiselta

henkilöltä, kuin kiintymyksen kohteelta, esimerkiksi huijarin esimieheltä, armeijan kenraalilta tai lakimieheltä.

4.3 Identiteettivarkaudet

Rikosuhripäivystyksen (2021) mukaan identiteettivarkaudesta on kyse silloin, kun esiinnytään toisen henkilöllisyydellä. Identiteettivarkauden tarkoitus on erehdyttää henkilö antamaan henkilötietojaan rikoksen tekijälle. Identiteettivarkautta on myös tehdä verkkokaupassa ostoksia tai osamaksusopimuksia toisen henkilön tiedoilla. Identiteettivarkaus on rikoslaissa (rikoslaki 38 luku 9 a §) rangaistava teko, jos siitä koituu uhrille taloudellista vahinkoa tai vähäistä suurempaa haittaa.

Trejtnarin (i.a.) mukaan toisena ihmisenä esiintyminen sosiaalisessa mediassa voi myös olla identiteettivarkaus. Sillä toisena ihmisenä esiintyessä tavoitteena on tyypillisesti saada varastetun identiteetin läheisiä kertomaan henkilökohtaisia tietoja varkaalle. Valeprofiilin poistaminen sosiaalisesta mediasta voi olla hankalaa, josta voi tulla uhrille kuluja tilanteen selvittämisestä sekä vähäistä suurempaa haittaa tilanteen korjaamiseen vaadittavassa vaivannäössä. Tjetnar toteaa, että toisen henkilötietoja hyväksikäyttäessä saattaa syyllistyä petokseen (rikoslaki 36 luku 1§).

4.4 Verkkopetokset

Verkkopetos on Minilexin (i.a.) mukaan verkossa tapahtuva petoksen muoto. Verkkopetoksissa uhrille annetaan virheellistä tai harhaanjohtavaa tietoa, jotta uhri siirtää rahaa sähköisesti petoksen tekijälle. Verkkopetoksia esiintyy usein verkossa olevien ostospaikkojen ja huutokauppojen yhteydessä. Yleistä verkkopetoksissa on, että tavara jätetään toimittamatta tai sitä ei ole oikeasti olemassakaan. Sosiaalisessa mediassa esiintyviä verkkopetoksia tapahtuu usein Facebook Marketplacessa tai Torin kaltaisilla alustoilla.

Facebook Marketplace on Facebook käyttäjille tarkoitettu myyntialusta (Facebook, 2022). Alustalla Facebookin käyttäjät saavat myydä tuotteita ja tavaroitaan muille käyttäjille.

Facebook ei ole missään muodossa osallinen kaupankäynnissä, eikä näin ollen ole kaupoista vastuussa. Tutkimuksen tekijöiden huomioiden mukaan yleisimmät huijaukset Facebook marketplacessa ovat olemattoman tuotteen myynti. Näissä tapauksissa ostaja maksaa ostamansa tuotteen verkonvälityksellä myyjän tilille, ennen kuin saa ostamaansa tuotetta. Myyty tuote luvataan postittaa myyjän toimesta, mutta usein estyy erilaisilla tekosyillä postittamasta tuotetta ja lopulta estää ostajan sosiaalisessa mediassa. Toinen yleinen huijaus, mikä nousee esille etenkin talvi- ja kesäsesongin aikana, on vuokrahuijaukset. Facebook marketplacen kautta vuokrataan majoituspaikkaa. Vuokraajan saapuessa paikalle tilalla on, joko tyhjä tontti tai majoituspaikka on vuokrattu jo toiselle. Joissakin tapauksissa vuokratun tilan vuokra perutaan vuokraajan toimesta juuri ennen sovittua ajankohtaa, ja vuokraaja ei palauta rahoja.

Seuraavassa kappaleessa käydään läpi, kuinka käyttäjätilin voi suojata salasanan ja monivaiheisentunnistautumisen avulla. Seuraavassa kappaleessa kerrotaan kuinka tunnistaa paremmin sosiaalisessa mediassa esiintyviä uhkia ja kuinka toimia joutuessaan huijauksen uhriksi.

5 KÄYTTÄJÄTILIN SUOJAUS

Tässä teoriaosiossa käydään läpi, kuinka yksityishenkilö voi varmistaa paremman turvallisuuden omille sosiaalisen median käyttäjätileilleen. Tässä osassa selvitetään hyviä salasana käytäntöjä ja kuinka kaksi- tai moniosainen tunnistautuminen tukee hyvää salasanaa. Tässä osiossa myös tarkastellaan, kuinka yksityishenkilö voi paremmin suojata henkilötietonsa tietoturvauhilta ja kuinka toimia, jos epäilee tietoturvarikosta.

5.1 Salasana käytännöt

Traficom (2023b) kirjoittaa sivullaan hyvistä salasanakäytännöistä. Kirjautuessasi palveluun käyttäjätunnuksena usein toimii sähköpostiosoite eli hyvä ja turvallinen salasana on henkilötietojen kannalta oleellinen. Samaa salasanaa ei kannata käyttää joka paikassa, salasanasi vuotaessa yhdestä sivustosta, sillä pääsee kirjautumaan kaikkialle. Traficom muistuttaa, että hyvää salasanaa ei tarvitse olla vaihtamassa jatkuvasti. Hyvän salasanan tulisi olla pitkä ja sisältää erikoismerkkejä. Vaikka salasana on pitkä, sen tulee olla helposti muistettava ja myös vaikeasti arvattava. Kasvavissa määrin nykyään suositellaankin käyttämään salauslauseita. Suomen kieli on hakkereille ja boteille haastava, joten salasanassa olisi hyvä olla murresanoja, ääkkösiä ja mahdollisesti kirjoitusvirheitä. Hakkerit käyttävät botteja apunaan eli yleisimmät korvaukset eivät enää ole turvallisia, esimerkiksi 1 = I ja 3 = E.

Salasanoja kuitenkin pystyy hallitsemaan erilaisten ulkoisten ohjelmistojen avulla, mitkä tallentavat salasanan salattuun pilvipalveluun tai pääteasemalle (Traficom, 2023a). Ulkoista apuohjelmaa käyttäessä, tulee muistaa vaan apuohjelman salasana. Monet selaimet kuten Chrome ja Safarikin tarjoaa nykyään mahdollisuutta salasanojen hallintaan ja tallentamiseen. Salasanoja on myös mahdollista kirjoittaa ylös paperille, jos ei luota teknologiaan tai omaan muistiin. Paperille kirjoitetut salasanat kuitenkin tulee pitää piilossa, ja mahdollisesti kaukana tietokoneesta. Salasanan nollaaminen sen unohtuessa ei välttämättä ole yksinkertaista etenkin, jos unohtaa pääsalasanan salasanojen hallintaohjelmaan. Tällöin voi joutua hyppimään useammankin mutkan kautta saadakseen salasanan

vaihdettua. Pääsalasanaan kannattaa siis panostaa niin ettei sitä unohda. Salasanat ovat myös henkilökohtaisia, ja niitä ei tulisi koskaan kertoa kenellekään, ei edes virallisille tahoille. Monessa virastossa ja heidän nettisivuillaan muistutetaankin, että he eivät koskaan kysy salasanaasi.

Käyttäjätilin suojaamisen avuksi hyvän salasanan lisäksi kannattaa aktivoida sisäänkirjautumisilmoitukset ja monivaiheinen tunnistautuminen. Kirjautumisilmoituksen käyttöönotto auttaa sinua hallitsemaan laitteita, joilla kirjaudut käyttäjätilillesi. Kirjautuessa palveluun saat ilmoituksen, missä kerrotaan uudesta laitteesta tai sijainnista. Tämän ilmoituksen avulla voit vahvistaa olitko sinä asialla, vai oliko kyseessä ei luotettavan tahon kirjautumisyritys. Monivaiheinen tunnistautuminen auttaa luomaan ylimääräisen turvakerroksen käyttäjätilisi ympärille. Monivaiheisen tunnistautumisen idea on tukea hyvää salasanaa. Käyttäjätunnuksen ja salasanan lisäksi sisäänkirjautumiseen tulee käyttää vielä jotain toista lähdettä. Monivaiheinen tunnistautuminen voikin olla esimerkiksi ylimääräinen PIN-koodi, turvallisuuskysymys, puhelimeesi lähetettävä koodi tai sormenjälki. Monivaiheisen tunnistautumisen idea on turvata käyttäjätili paremmin, ja mikäli käyttäjätunnus ja salasana päätyisi vääriin käsiin, käyttäjätilille ei pääse kirjautumaan ilman tätä vaihetta. Käyttäjille kenellä on monivaiheinen tunnistautuminen käytössä, tulee sisäänkirjautumisvaiheessa ilmoitus vaadittavasta monivaiheisesta tunnistautumisesta. Mikäli käyttäjä ei pyri kirjautumaan itse tililleen voi hän jättää huomiotta tämän sisäänkirjautumisyrityksen.

5.2 Tietoturvauhkien välttäminen

Sosiaalinen media ja internet ovat täynnä vaaroja ja tietoturvauhkia. Rikolliset yrittävät saada käsiinsä yksityishenkilöiden henkilötietoja ja yritysten tietoja monilla eri keinoilla. Tietoturvarikolliset käyttävät hyväkseen psykologiaa ja käsityksiä (Europol, 2022). Verkossa suojautumisen kannalta on tärkeää olla tietoinen potentiaalisista vaaroista. Tietoturvauhkien huomaamiseksi ei tarvitse kuitenkaan olla tietotekniikan ammattilainen. Maalaisjärjellä pärjää hyvin pitkälle muistaessaan yleisen ohjeen, mikäli jokin vaikuttaa liian hyvälle ollakseen totta, se pitää yleensä paikkaansa.

Yleisellä tasolla tietojen turvallisuuden kannalta suositellaan tarkistamaan käyttäjätilit säännöllisesti (Europol, 2022). Sosiaalisessa mediassa tulee olla aina varovainen mitä henkilötietoja jakaa itsestään julkisesti. Omia henkilötietoja ei myöskään koskaan tulisi kertoa verkossa viestillä toiselle osapuolelle. Vaikka omalla kaverilistalla sosiaalisessa mediassa olisi vain ihmisiä ketkä tunnet todellisuudessa, valitettavasti verkossa toimivat rikolliset löytävät keinot saada käyttäjätilin hallintaansa, ja sitä kautta pyytävät muilta henkilötietoja. Verkossa pystyy luomaan väärän identiteetin pelkästään muutamalla tiedolla ja kuvalla. Sosiaalisen median lisäksi myös verkkoshoppailu on yleistynyt. Verkossa ostoksia tehdessä kannattaa suosia tunnettuja ja luotettuja verkkoalustoja. Ostoksia maksaessa varmista aina yhteyden turvallisuus verkkosivupalkista näkyvästä lukosta tai https-tunnuksesta. Verkkomaksamisessa kannattaa suosia turvallisia maksutapoja, ja mahdollisesti käyttää luottokorttia, minkä avulla huijauksen sattuessa rahojen takaisin saanti on helpompaa. Tarkista pankkitilisi väärinkäytösten estämiseksi säännöllisesti. Säännöllisesti tarkistaessa pankkitilin huomaa nopeammin, jos tilillä on epäilyttävää toimintaa ja aktiivisella tarkastamisella suuri rahallinen tappio on minimoitavissa ja rahojen saanti on aavistuksen helpompaa.

Identiteettivarkaudelta verkossa suojautuminen ei vaadi, kuin muutaman yksinkertaisen toimen (Europol, 2016). Europolin listauksen mukaan identiteettivarkaudelta suojautuessa tulee suhtautua epäilevästi kaikkiin viesteihin, missä pyydetään henkilökohtaisia tietoja. Erityisesti tapauksissa, joissa viestin lähettäjä on virallinen taho kuten pankki tai verovirasto. Viralliset tahot eivät koskaan pyydä henkilötietojasi verkossa sähköpostilla tai Facebook viestillä. Verkossa lähetetyissä viesteissä oleviin linkkeihin tulee suhtautua terveen epäilevästi, mikäli lähettäjästä ei ole varma. Identiteettivarkaudelta pystyy myös suojelemaan henkilötietojaan varmistamalla, että käyttämässään laitteessa on ajantasainen päivitys ja palomuuri. Laite on riskialttiimpi haittaohjelmille ja viruksille ellei sen päivitys ei ole ajan tasalla. Laitetta kannattaa myös suojata virustentorjuntaohjelmalla. Virusturvaohjelmaa ladatessa laitteelle kuitenkin tulee olla tarkka, että ohjelman lataa luotettavalta palveluntarjoajalta.

Tietojenkalastelu on yleisin käyttäjän manipulointihyökkäys, jonka kohteena on pankkitiedot (Europol, 2022). Tietojenkalasteluviesteissä hyväksikäytetään kiireen tunnetta ja uhrin herkkäuskoisuutta. Jos viestissä puhutaan kiireestä, tai sakosta, ja asetetaan vastaanottajalle aikarajoite toimimiseen tietyssä ajassa, kyseessä on tyypillisesti tietojenkalastelu yritys. Epäilyttävän viestin vastaanottaessasi, missä pyydetään kertomaan pankkitietojasi tai henkilötietojasi kuten sosiaaliturvatunnustasi, tarkastele viestiä ja sen lähettäjää tarkemmin. Tietoturvarikolliset käyttävät luotettavan ja aidon näköisiä sähköposteja tai puhelinnumeroita, näiden olematta turvallisia. Älä koskaan avaa linkkiä tai lataa liitetiedostoa, mikä tulee tällaisista lähteistä. Viestin lähettäjä saattaa vaikuttaa luotettavalle ja aidolle, mutta esimerkiksi sähköpostiosoitteessa on saatettu muuttaa o-kirjain nollaksi (0). Saadessasi viestin mikä vaikuttaa epäilyttävälle, tarkista viesti myös kirjoitusvirheiden varalta.

Mikäli koet joutuneesi tietoturvarikoksen tai huijauksen uhriksi, älä jää yksin (RIKU, 2021). Rikosuhripäivystys tarjoaa apua ja neuvoja tilanteessa, jossa uhri kokee henkilötietojensa päätyneen vääriin käsiin. Tärkeintä uhrina on pysyä rauhassa ja ottaa yhteyttä vaadittaviin viranomaisiin. Esimerkiksi pankkitunnusten päätyessä vääriin käsiin, ota yhteyttä pankkiisi mahdollisimman pian sulkeaksesi pankkitunnuksesi ja välttääksesi mahdollisen tietojen kopioinnin. Henkilötunnuksen, passin, ajokorini tai muun henkilökohtaisen tunnistautumisvälineen päätyessä rikollisille, tulee Poliisiin ottaa yhteyttä ja tehdä tapahtuneesta rikosilmoitus.

6 KYSELYTUTKIMUS MENETELMÄNÄ

Kyselytutkimus on yksinkertainen ja selkeä tapa saada kerättyä vastaustuloksia asetettuun hypoteesiin. Tutkimuksen aloittamisessa on tärkeää asianmukainen kysymysasettelu, että mahdollistetaan oikeanlaisten vastauksien saaminen tutkimuksen tavoitteiden toteutumiseksi.

Määrällinen tutkimus on hyvä valinta valitsemaamme aiheeseen, koska tutkimuksen tavoitteenamme oli selvittää yleisemmällä tasolla eri elämänvaiheissa olevilta henkilöiltä tietämystä ja kokemuksia kyseiseen aihealueeseen ja määrällisen tutkimuksen avulla saamme laajemman vastausmäärän mukaisesti tutkimukseen.

Hirsjärvi ym. (2009) kertovat yleisemmin käytettyjä perinteisiä tutkimusstrategioita olevan kolmea eri tyylistä.

1. Kokeellinen tutkimus. Hyvä mittari mikäli tutkimuksessa tarkastellaan yhden tekijän vaikutusta eri muuttujaan.
2. Survey-tutkimus. Tämän tutkimuksen käytön tarkoituksena on mahdollistaa konkreettisesti muutoksen tekemisen tutkimuksen pohjalta.
3. Tapaustutkimus (*case study*). Kyseinen tutkimusstrategia on kaikista yksityiskohtaisin ja tavoitteena on saada yksityiskohtaista tietoja yksittäisistä asioista tai todella pienestä ryhmästä.

Tutkimusstrategian valitseminen ennen virallisen tutkimuksen aloittamista on hyvin tärkeää tutkimuksen tavoitteiden onnistumisen näkökulmasta. Tämän tutkimuksen tarkoituksena on tuottaa lisäinformaatiota yksityisten henkilöiden tiedon määrästä sosiaalisen median tietoturvasta ja sen mahdollisista uhista. Tutkimustulokset antavat informaatiota henkilöiden tietoisuudesta sosiaalisen median alustan tietoturvasta ja siellä piilevistä tietoturvauhkista.

Hirsjärvi ym. (2009) toteavat kyselytutkimuksen olevan yksi Survey-tutkimuksen tärkeimmistä työskentelymenetelmistä, koska kyselytutkimuksen avulla saadaan sovittujen yhteisen toimintatapojen mukaan kerättyä tarvittava aineisto kasaan.

Metodina kyselytutkimus mahdollistaa suuren vastausmäärän saamisen useilta henkilöiltä, ja tutkimustulokset ovat laadukkaita suuren otannan avulla. Hirsjärvi ym. (2009) huomauttaakin tutkimusmetodiin liittyvän kuitenkin heikentäviä ominaisuuksia.

Määrällisessä kyselytutkimuksessa on omat heikkoutensa ja nämä voivat haastaa tutkimusprosessia ja sen etenemistä. Yksi isoin mahdollinen heikentävä tekijä tässä tutkimuksessa on, saavuttaako tutkimus tarpeeksi kattavan vastausprosentin tai jääkö avoimet vastaukset liian suppeaksi. Määrällinen tutkimus sopii kuitenkin hyvin tähän tutkimukseen aiheen ollessa sellainen, että vastaajia löytyy tarvittavissa määrin kattavan vastausprosentin saamiseksi tutkimukseen.

7 TUTKIMUS SOSIAALISEN MEDIAN TIETOTURVASTA

Tässä osiossa käydään läpi kyselytutkimuksen toteutusta ja sen etenemistä. Tässä osiossa myös tarkastellaan kyselyn eri osioita ja rakennetta yleisesti. Tutkimuskysymyksenämme oli selvittää yksityishenkilön tietämystä sosiaalisessa mediassa esiintyvistä tietoturvariskeistä. Kyselyn tarkoituksena oli myös herättää vastaajissa mietteitä omasta käyttäytymisestä sosiaalisessa mediassa ja heidän tietoturvatietämyksestään. Aihetta on aikaisemmin tarkastellut Merisalo (2022).

7.1 Kyselyn toteutus

Kysely rakennettiin teoriaan liittyen sosiaalisen median tietoturvauhista. Kyselyn tarkoituksena oli selvittää yksityishenkilöiden tietämystä sosiaaliseen mediaan liittyvistä tietoturva uhista. Kysely toteutettiin hyödyntäen Webropol-kyselytyökalua, missä kysely tehtiin ja julkaistiin. Webropol-kyselytyökalu oli hyvä valinta, sillä se tarjosi kattavan raportin kyselyn lopuksi. Työkalulla pystyi myös hallinnoimaan, milloin kysely on auki ja millä tavalla siihen pääsee vastaamaan. Tutkimukseen liittyvien kysymysten lisäksi kyselyssä pyydettiin lopuksi avointa palautetta kyselystä. Kokonaisuudessaan tutkimuksessa oli yhteensä 28 kysymystä. Kysymyksissä on pääosin ennalta määrätyt vastaukset, jotka mahdollistavat tulosten analysoinnin. Kyselyssä oli myös muutama avoin kysymys, joihin vastaajat saivat jättää avoimen vastauksen liittyen edeltävään kysymykseen.

Kysely toteutettiin syksyllä 2023. Tavoitteenamme oli saada 100 vastaajaa kyselyyn noin kahden viikon aikajaksolla. Kyselyn sulkeutuessa vastauksia olimme saavuttaneet 112. Tutkimuksen kysely toteutui tavoitteen mukaisesti saavuttaen hyvän vastaajamäärän opinnäytetyötä varten. Tutkimuksen vastaajiksi valikoitui yksityishenkilöitä tutkimuksen tekijöiden ympäriltä, monesta eri asemasta ja ikäluokasta. Tutkimus suoritettiin täysin anonyymisti, jotta tuloksia voidaan tulkita luottamuksellisesti paljastamatta vastaajien henkilötietoja.

7.2 Kyselyn osiot ja rakenne.

Tutkimuksen kysymykset ovat liitteenä lopussa. Kysely on rakennettu neljässä osassa. Kyselyn alussa kartoitetaan vastaajan perustietoja. Perustiedoilla kyselyssä tarkoitetaan vastaajien ikäryhmää, koulutusastetta, sosioekonomista asemaa ja vastaajien tietämystä tietoteknisistä laitteista. Kyselyssä tietotekniset laitteet rajattiin älypuhelimeen, älykelloon, kannettavaan-, tabletti- ja pöytätietokoneeseen.

Toinen osa kyselystä keskittyi sosiaaliseen mediaan. Tässä osassa selvitettiin mitä sosiaalisen median alustoja vastaajilla on käytössä, ja mitkä ovat vastaajien keskuudessa yleisimmät alustat. Vastaajien suosituimpien alustojen lisäksi kyselyssä selvitettiin, kuinka aktiivisia vastaajat ovat sosiaalisessa mediassa. Aktiivisuutta mitataan sillä, kuinka paljon vastaaja julkaisee jotain, reagoi, tykkää tai kommentoi toisen käyttäjän julkaisua. Osiossa myös selvitetään kuinka turvallisena ja luotettavana vastaajat pitävät sosiaalista mediaa, sekä siellä jaettavaa informaatiota.

Kyselyn kolmannessa osiossa käydään läpi sosiaalisessa mediassa ja internetissä esiintyviä yleisiä tietoturvauhkia. Tämän tarkoituksena on selvittää kuinka moneen eri turvallisuusuhkaan vastaajat ovat törmänneet, joko henkilökohtaisesti tai läheisen kautta. Tähän liittyen tutkimukseen osallistuneet saivat kertoa vapaasti, missä muodossa ovat törmänneet näihin uhkiin. Osiossa käytiin läpi yksitellen turvallisuusuhat ja selvitettiin, kuinka hyvin vastaajat tuntevat termit yleisistä huijauksista. Kyselyn vastauksia läpi käydessä tutkimuksen tekijät huomasivat, että osion kysymykset olisi voitu muotoilla toisella tavalla tai antaa enemmän mahdollisuuksia vastata vapaasti tietoturvauhkiin liittyen. Vastausvaihtoehdot ovat hieman mustavalkoiset, eivätkä jätä paljoa tulkitsemisen varaan.

Neljännessä osassa kyselyä käydään läpi vastaajien tuntemuksia käyttäjätilien turvallisuudesta ja suojauksesta. Osion keskeiset kysymykset olivat ovatko vastaajat huolissaan henkilötiedoistaan sosiaalisessa mediassa ja käyttäjätiliensä suojauksesta. Osion tarkoituksena oli myös selvittää, kuinka paljon vastaajat tahattomasti tai tahallisesti tuovat ilmi sosiaalisessa mediassa omia henkilötietoja. Liittyen henkilötietojen turvallisuuteen vastaajille annettiin mahdollisuus kertoa avoimesti omia mietteitä, jos he eivät koe henkilötietojensa

olevan turvassa sosiaalisessa mediassa. Osio tarjoaa myös mahdollisuuden vastaajille pohtia omia salauskäytäntöjään, liittyen kaksiosaiseen tunnistautumiseen ja salasanoihin.

Tutkimuksen lopussa esitettiin muutama kysymys liittyen sosiaalisen median tietosuojaselosteisiin. Kysymysten muotoilu oli yksinkertainen. Kysymysten avulla selvitettiin, kuinka moni vastaaja on lukenut tietosuoja selosteen sanasta sanaan ja kuinka moni tietää mistä tarvittaessa löytää sosiaalisenmedian tietosuojaselosteen. Kysymykset liittyen tietosuojaselosteisiin oli muotoiltu suorasti. Tällä pyrittiin saamaan selvä vastaus vastaajalta liittyen tietosuojaselosteisiin. Kysymysten vastausvaihtoehdot olisi voinut muotoilla laajemmin tai lisätä vaihtoehtoja, sillä toteutuneessa kyselyssä vastaukset olivat joko-tai-vastauksia.

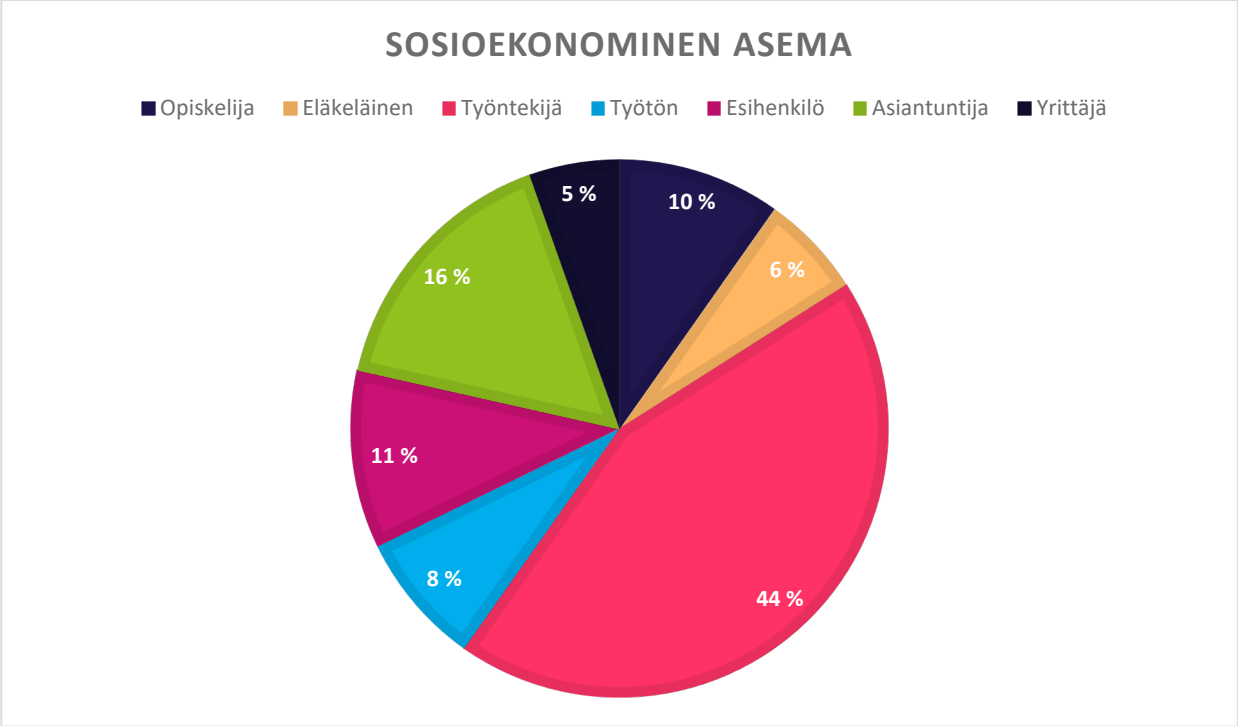
8 TUTKIMUKSEN TULOKSET

Tutkimukseen osallistui 112 henkilöä. 98,2 % vastaajista on täysi-ikäisiä, ja 1,2 % on alaikäisiä. Vastaajien tarkat iät eivät ole saatavilla, mutta suurin osa vastaajista tutkimuksessa on iältään 36–45-vuotiaita, heitä on 24,1 %. Seuraavaksi suurin vastaajaryhmä on yli 55-vuotiaita, heitä on 21,4 %. Lähes 80 % vastaajista on työelämässä tällä hetkellä.

Tässä luvussa käydään läpi tarkemmin tutkimuksen tuloksia. Tutkimustulosten havainnollistamisen apuna käytämme pylväs- ja ympyräkaavioita. Tutkimuksesta saatuja tuloksia verrataan analysoinnin yhteydessä aikaisemmin aiheesta tehtyihin tutkimuksiin ja niistä kerättyyn dataan.

8.1 Vastaajien perustiedot

Tutkimuksen alussa kysyttiin vastaajien perustietoja, jotta saadaan selvitettyä ovatko he missä sosioekonomisessa asemassa, mitkä ovat vastaajien koulutustaustat ja minkälaisiksi vastaajat kokevat itse tietotekniset taitonsa. Näiden tietojen lisäksi selvitettiin, onko vastaajilla käytössä sosiaalista mediaa ja ovatko he siellä törmänneet turvallisuusuhkiin, joita teoriaosassa käsiteltiin. Sosiaalisen median tilien olemassaolon lisäksi tutkimuksessa selvitettiin vastaajien aktiivisuutta sosiaalisessa mediassa. Alapuolella olevassa kuviossa (kuvio 1) näkyy tarkempi tilasto vastaajien tämänhetkisestä työllisyystilanteesta.



Kuvio 1. Vastaajien sosioekonominen asema (n=112).

Yläpuolella olevasta ympyräkaaviosta (kuvio1) näkyy vastaajien hajauman kysyttäessä mikä on heidän tämänhetkinen työllisyystilanteensa. Valtaosa tutkimukseen osallistuneista vastaajista on tällä hetkellä työelämässä. Heidän työasemansa vaihtelee, mutta lähes puolet kaikista vastaajista on työelämässä työntekijöinä. Työelämässä olevista vastaajista toiseksi suurin luokka koostuu asiantuntijoista. Muut työelämässä olevat vastaajat työskentelevät joko esimiehinä tai yrittäjinä. Lähes neljäsosa vastaajista on tällä hetkellä työvoimien ulkopuolella olevia opiskelijoita, eläkeläisiä tai työttömiä. Tilastokeskuksen (2023) mukaan Suomessa 20–64-vuotiaiden työllisyysaste on 77,8 %. Tämä tilasto ei erittele, ovatko henkilöt minkälaisessa työasemassa. Tutkimukseemme osallistuneista henkilöistä 76 % on tällä hetkellä työelämässä, tämä on hyvin lähellä koko Suomen tilastollista tasoa. Tutkimusten vertaaminen on mahdollista ainoastaan työntekijöiden ja työttömien suhteen, sillä Tilastokeskuksen tilastotieto ei erottele tarkemmin, ovatko työelämässä olevat missä asemassa, tai ovatko työvoiman ulkopuolella olevat eläkeläisiä tai opiskelijoita.

Tutkimukseen osallistuneilta vastaajilta kysyttiin, mikä on heidän korkein tällä hetkellä suoritettu koulutusaste. Tuloksissa on hyvä huomioida, että vastaajista 10 % on tällä hetkellä opiskelijoita, joten heidän tällä hetkellä suoritettavana oleva koulutus ei näy vastauksissa. Vastaajista yli puolet (58,9 %) on suorittanut vähintään jonkin toisen asteen koulutuksen, tarkoittaen lukiota tai ammatillista perustutkintoa. Lähes kolmannes (27,7 %) vastaajista on suorittanut alemman korkeakoulututkinnon. Ylemmän korkeakoulututkinnon on suorittanut 4,5 % vastanneista ja yliopiston käyneitä oli 2,7 %. Tutkimukseen osallistuneista vastaajista 6,2 % on suorittanut korkeimpana koulutusasteenansa kansakoulun tai peruskoulun. Kansakouluista on siirrytty peruskoulujärjestelmään 70-luvulla (Arkistojen Portti, i.a.). Osa tutkimuksen vastaajista on eläkkeellä, mistä voidaan päätellä heidän koulutustasostaan, että he ovat saattaneet käydä ainoastaan kansakoulun ja tehneet pitkän työuran. Kaksi vastaajista on myös alaikäisiä, joten he eivät ole vielä voineet suorittaa peruskoulua korkeampaa tutkintoa ikänsä vuoksi.

Kysyttäessä vastaajien tietoteknistä osaamista, vastaajista suurin osa 98,2 % kokee hallitsevansa tietotekniset laitteet vähintään hyvin. Viidesosa kaikista vastaajista kokee olevansa asiantuntijoita tietotekniikan parissa. Alle kaksi prosenttia vastaajista kokee olevansa aloittelija teknologian kanssa ja tarvitsevansa paljon apua sen kanssa. Vastaajien iästä voidaan olettaa, että he ovat olleet aikuisia tai lapsia internetin ja älypuhelimien yleistyessä. Älypuhelimien aikakauden alkua on vaikea arvioida, sillä jokainen määrittelee älykkään puhelimen eri tavalla. Ensimmäinen älypuhelin julkaistiin markkinoille 1994 (Chantel, 2023). Tämä oli SPC eli Simon Personal Communicator. Tällä laitteella pystyi hallinnoimaan sähköpostia ja faxia. Laitteessa oli myös kalenteri, osoitekirja ja muistio. SPC oli myös maailman ensimmäinen kosketusnäytöllinen puhelin.

Melkein 10 vuotta myöhemmin 2001 ensimmäinen puhelin liitettiin 3G verkkoon, jonka jälkeen älypuhelimien valmistus lähti uudelle tasolle. Vasta vuonna 2007 julkaistiin ensimmäinen iPhone, joka muistuttaa eniten nykyaikaista älypuhelinta. Modernin pöytätietokoneet tavallisilla yksityishenkilöillä alkoivat yleistyä 70-luvulla (Olito, 2019). Vastaajista nuorimmat ovat alle 18-vuotiaita ja he ovat eläneet koko ikänsä älylaitteiden ympäröiminä. Vanhimmat vastaajista ovat nuorimmillaan 55-vuotiaita eli he ovat syntyneet 60-luvun

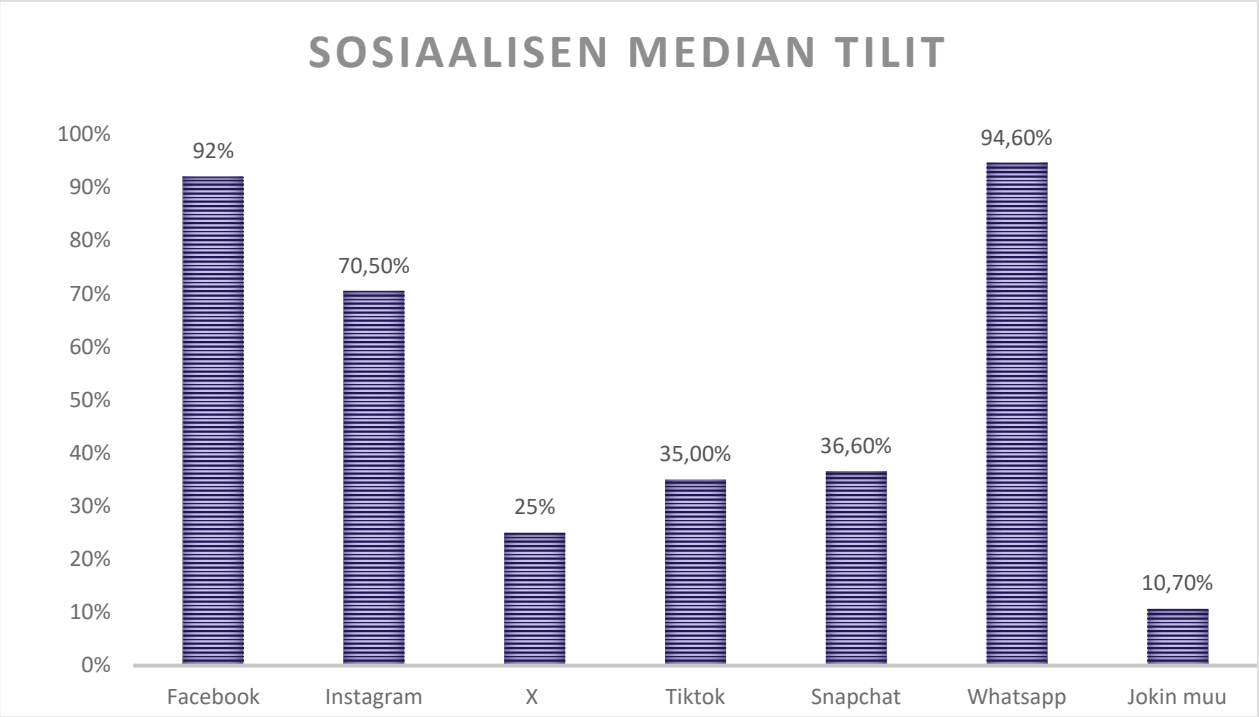
loppupuolella. Vanhimmatkin vastaajat ovat olleet ensimmäisen älypuhelimen aikana nuoria parikymppisiä ja osa vastaajista vastasyntyneitä 90-luvun alussa tietokoneiden yleistyessä kotitalouksissa. Teknologian kehittymisen seuraaminen on yksilöllistä, osa henkilöistä lähtevät heti mukaan suosittelijoina ja testaajina, toisilla henkilöillä menee taas pidempään lämmetä teknologialle. Nykyään teknologiaa tarvitsee lähes kaikessa ja maailma muuttuu eli sen mukaan on täytynyt kehittyä jatkuvasti. On loogista tulosten perusteella, että lähes kaikki vastaajista kokee olevansa teknologian kanssa vähintään hyviä, sillä vastaajat ovat tekemisissä päivittäin teknologian kanssa. Osa vastaajista koko ikänsä ja toiset nuoresta aikuisuudesta lähtien.

Tutkimukseen osallistuneista vastaajista lähes kaikilla on jokin sosiaalisen median tili käytössä, ainoastaan kahdella tutkimukseen osallistuneella ei ole sosiaalisen median tiliä käytössä. Tätä lukua voi tarkastella hieman varauksella, sillä tässä kysymyksessä ei ollut määritelty tarkasti sosiaalisen median tiliä käsitteenä. Jokaisen ihmisen käsitys sosiaalisesta mediasta voi olla erilainen, moni ei esimerkiksi laske välttämättä pikaviestipalveluita kuten WhatsAppia tai Signalia sosiaaliseksi mediaksi. Seuraavassa kappaleessa tutkitaan tarkemmin sosiaaliseen mediaan liittyviä kysymyksiä, kuten mitä sosiaalisen median alustoja vastaajat käyttävät. Tutkimuksen vastaajista 16 % kokee olevansa erittäin aktiivisia sosiaalisessa mediassa, jakaen jotain ja reagoiden muiden ihmisten päivityksiin päivittäin. Suurin osa vastaajista kuitenkin kokee olevansa jossain määrin aktiivisia sosiaalisessa mediassa. 12,5 % vastaajista kokee, ettei ole yhtään aktiivinen sosiaalisessa mediassa. Nämä vastaajat voivat omistaa sosiaalisen median tilin, mutta eivät ikinä avaa sovellusta tarkoituksenaan kommentoida, reagoida tai julkaista jotain siellä.

8.2 Sosiaalisen median käyttö

Kysyimme tutkimuksessamme mitä sosiaalisen median tilejä vastaajilla on käytössä. Vastausvaihtoehdoista vastaajat saivat valita useamman käytössä olevan sovelluksen. Vertailemme saamaamme dataa Datareportalin tutkimukseen vuodelta 2023 (Kemp, 2023e). Tutkimuksessa on käytetty käyttäjätilastoissa hyödyksi sosiaalisen median alustojen tarjoamaa mainostyökalua, ja kuinka paljon nämä mainokset saavuttavat käyttäjiä.

Tutkimustuloksissa on myös hyvä muistaa, että suuri osa some-alustoista on sallittuja yli 13-vuotiaille, mutta niissä voi olla silti nuorempia käyttäjiä. Alapuolella olevassa kuvaajassa (kuvio 2) on vastaajien tarkempi hajonta liittyen sosiaalisen median tileihin.



Kuvio 2. Vastaajien käyttämät sosiaalisen median tilit (n=112).

Yläpuolella olevasta pylväskaaviosta (kuvio 2) näkee tarkan hajonnan ja prosentit vastaajien kesken eri sosiaalisen median alustoissa. Vastaajien kesken suosituimmat sosiaalisen median alustat ovat selvästi Metan omistamat Facebook, Instagram ja WhatsApp. Tuloksemme poikkeavat Facebookin osalta suuresti koko Suomen tilastosta, sillä Suomen laajuisesti Facebookia käyttää vain hieman yli 40 % yksityishenkilöistä (Kemp, 2023b). Instagramia käyttää lähes yhtä moni yksityishenkilö, mitä Facebookia Suomen laajuisesti.

Tähän tutkimukseen osallistuneista vastaajista Facebookia käyttää yli 90 % ja Instagramia yli 70 %. Clausnitzerin (2023) mukaan vuonna 2022 teetetyn kyselyn mukaan 89 % suomalaisista käyttää WhatsAppia. WhatsAppin käyttäjien kohdalla eroa on vain muutama prosenttiyksikkö verrattuna koko Suomeen tilastoon. Tällä hetkellä WhatsAppin käyttö on

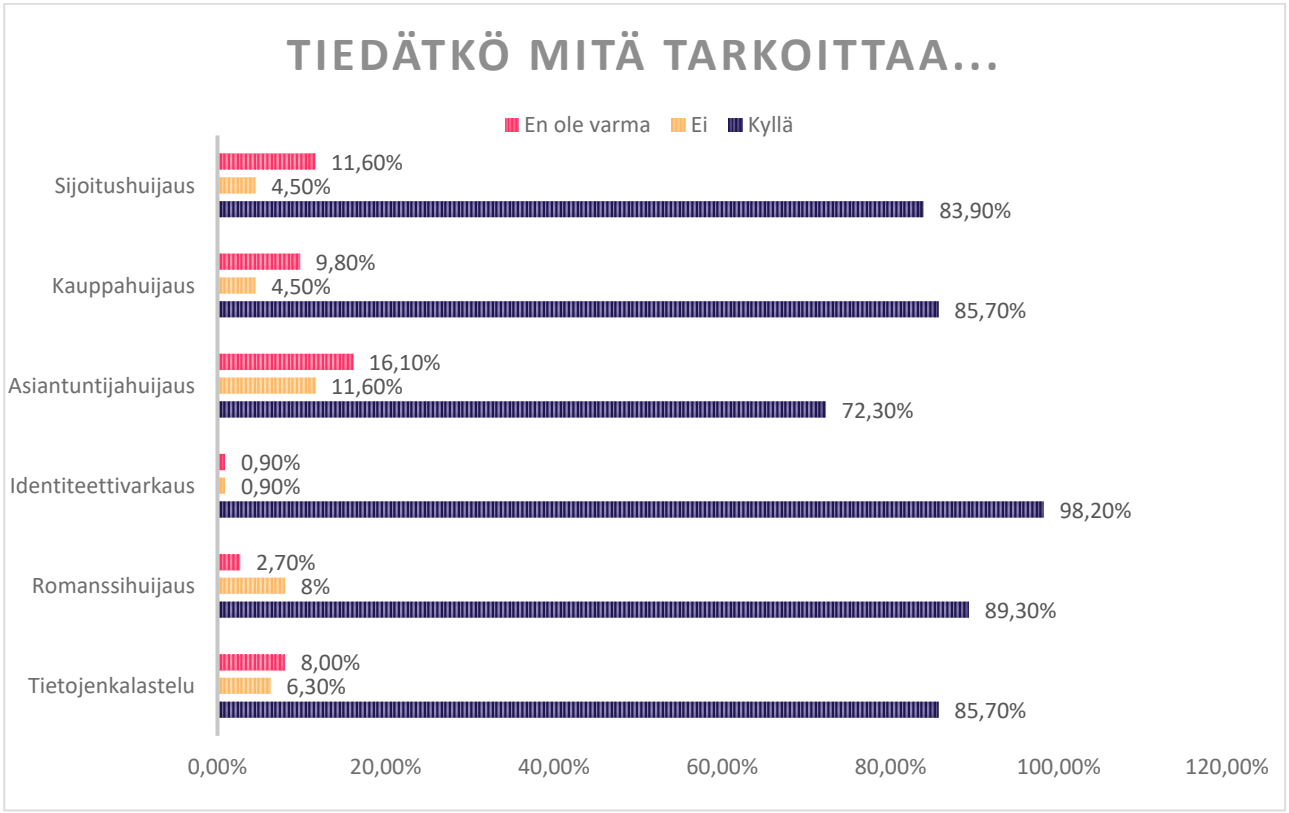
yleistä, sillä alustalle ei ole kilpailevaa pikaviestipalvelua. Muutama kyselyn vastaajista kertoi käyttävänsä Signalia. Signal on Yhdysvalloista lähtenyt avoimeen lähdekoodiin perustuva pikaviestipalvelu (Signal, 2018). Signalin on toiminta periaatteeltaan hyvin samankaltainen mitä WhatsApp. Signal ei kuitenkaan ole vielä saavuttanut yhtä suurta suosiota toisin kuin WhatsApp. Google Play-kaupan mukaan Signal on ladattu yli 100 miljoonaa kertaa. WhatsApp on ladattu yli 5 miljardia kertaa, mikä vahvistaa alustan olevan suosituin pikaviestipalvelu.

Muita suosittuja sosiaalisen median alustoja vastaajien keskuudessa ovat Tiktok ja Snapchat, jotka ovat etenkin nuorten aikuisten suosimia sovelluksia. Kempin (2023e) mukaan TikTokia käyttää suomessa 1,42 miljoonaa täysi-ikäistä, mikä on jopa 31,4 % Suomen aikuisväestöstä. Tiktok on sallittu kaikille yli 13-vuotiaille, mutta sovelluksen omistama ByteDancen käyttäjätyökalu näyttää tilastoissa ainoastaan kaikki täysi-ikäiset. Kyselyn vastaajista 35 % kertoi käyttävänsä TikTokia, mikä on hyvin lähellä ByteDancen julkaisemaa tilastoa. Kempin (2023e) mukaan Snapchatia käyttää noin 38 % yli 13-vuotiaista Suomalaisista. Tutkimukseen osallistuneista vastaajista 36,6 % käyttää Snapchatia. Tulos on hyvin lähellä Snapchatin omaa tulosta, eroten alle kahdella prosentilla toisistaan.

Vähiten vastaajista käytti X:ää, mikä tunnetaan paremmin entisellä nimellään Twitterinä. X:ää käyttää vastaajista neljännesosa. Kempin (2023d) mukaan Twitteriä käyttää 31 % kaikista yli 13-vuotiaista suomalaisista. Kemp huomauttaa, että mainosten saavuttavat käyttäjät eivät ole sama asia mitä aktiiviset käyttäjät kuukaudessa. Tässä opinnäytetyössä teetetyn tutkimuksen tulos on jonkin verran alhaisempi verrattuna Suomen tilastoon. Vastaajat saivat myös kertoa halutessaan muun vaihtoehdon listauksen ulkopuolelta ja siellä muutamia kertoja nostettiin esille Discord. Se on maailmanlaajuinen puhe-, viesti- ja videopalvelu (Discord i.a.). Palvelun avulla voi pitää yhteyttä yhteisöihin ympäri maailmaa. Palvelu on kehitetty pääosin online-peliyhteisöjä ajatellen.

8.3 Sosiaalisen median huijaukset

Sosiaalisessa mediassa liikkuu paljon erilaisia tietoturvauhkia huijausten muodossa. Tutkimuksessa selvitettiin tietävätkö vastaajat mitä mikäkin mahdollinen huijaus tarkoittaa. Vastausten perusteella vastaajat ovat hyvin tietoisia mitä eri huijausmuotoja on, ja mitä ne tarkoittavat. Lähes jokainen vastaajista 98,2 % vastasi tietävänsä mitä identiteettivarkaus tarkoittaa. Tulos vahvistaa onnistumisen tietoisuuden lisäämisestä identiteettivarkausten osalta eri tahoilta. Vähiten tiedetty huijausmuoto oli asiantuntijahuijaus. Vastaajista vain 72,3 % vastasi tietävänsä mitä asiantuntijahuijaus tarkoittaa. Asiantuntijahuijaukset on naamioitu niin hyvin tänä päivänä sosiaalisen median alustoille, mutta valitettavasti kyseisen huijauksen tietoisuus lisääntyy vasta uhriksi jouduttuaan. Alapuolella olevassa kuvaajassa (kuvio 3) näkyy vastaajien vastaukset kysyttäessä tietävätkö he mitä tarkoittavat yleisistä huijauksista käytettävät termit.



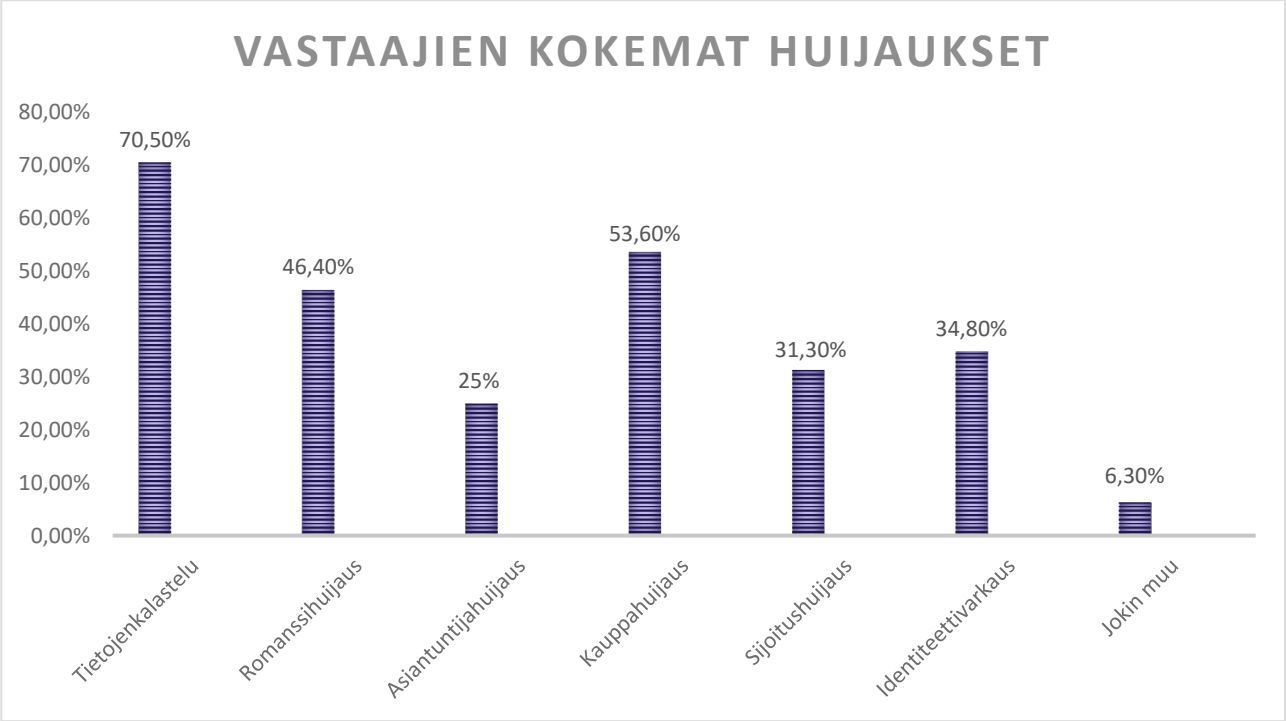
Kuvio 3. Vastaajien tietous huijauksista (n=112).

8.4 Sosiaalisen median uhat

Tutkimuksessa selvitettiin, olivatko vastaajat törmänneet erilaisiin sosiaalisen median uhkiin alustoilla. Tutkimuksessa oli valmiita vastausvaihtoehtoja yleisimpien huijausten osalta. Vastaajan oli mahdollisuus myös tarkentaa avoimen kommentin kautta tiedon siitä, oliko kyseinen uhka kohdistunut itseensä tai toiseen henkilöön. Vastaajista melkein jokainen oli kokenut huijausyrityksen omalla kohdallaan tai huijausyritys oli kohdistunut vastaajan läheiseen. Avoimin kommenttien mukaan huijausyritykset olivat jääneet yritysasteelle osalla, mutta yhdessä vastauksessa todettiin kokemuksesta tarkemmin.

”Muutamien tuttujen kuvia käytetty ja luotu uusi käyttäjäprofiili niiden avulla.”

Alapuolella olevasta pylväskaaviosta (kuvio 4) näkee vastaajien tarkan hajonnan erilaisten huijausten suhteen. Vastaajista jokainen oli törmännyt jollain tapaa ainakin yhteen sosiaalisessa mediassa liikkuvaan huijaukseen. Eniten kyselyyn vastanneista henkilöistä olivat törmänneet tietojenkalasteluun 71 %.



Kuvio 4. Vastaajien kokemat tietoturvauhat (n=112).

Tietojenkalasteluun oli avoimien kommenttien selvityksen mukaan jouduttu pääosin Facebookin välityksellä. Yksi vastaajista kertoi avoimessa kommentissaan:

> ”Kavereilta on kaapattu Facebookissa ja Instagramissa tilejä. Tietojenkalastelua on yritetty työpaikan sähköpostin kautta”

Vastauksien perusteella kuitenkin sähköpostin kautta tapahtuva tietojenkalastelu on vähenevässä suunnassa sosiaalisen median kasvun myötä. Tietojenkalastelu onkin yleisin huijausmuoto sosiaalisessa mediassa ja omakohtaisten kokemusten mukaan päivittäin törmätäänkin esimerkiksi valearvontoihin ja epämääräisiin linkkeihin missä pyydetään syöttämään omia henkilötietoja. Tietojenkalastelu on kehittynyt viime vuosina niin hyvin, että ei ole itsestään selvää tiedostaa kyseessä olevan huijaus. Yritykset järjestävät arvontoja Facebookissa päivittäin ja suurimpaan osaan arvonnoista kommentoi botit osallistujien viesteihin. Botit yrittävät kalastella tietoja ilmoittamalla arvontavoitosta, mutta käyttäjät tunnistavat kyseessä olevan tietojenkalastelua eivätkä mene kyseiseen huijaukseen.

Yli puolet vastaajista 54 % oli törmännyt myös kauppahuijauksiin. Sosiaalisessa mediassa voi törmätä kauppahuijauksiin varsinkin Facebookin Marketplacessa, siellä kauppahuijauksia tapahtuu päivittäin, mutta suomalaiset ovatkin perustaneet Facebook-ryhmiä parantaakseen tietoisuutta kauppahuijauksista ja niiden välttämisestä.

> ”Olen itse saanut phishing -viestejä ja **joutunut netin kirpparipalstalla huijauksen uhreiksi**. Läheisiltäni löytyy identiteettivarkauksia, some -tilien kaappauksia sekä whatsapp -viestien kautta tehtävää tilisiirtohuijausta, jossa huijari on tekeytynyt uhrin lapseksi”

Vastaajista vain 35 % olivat törmänneet identiteettivarkauksiin. Identiteettivarkauksien tietoisuutta on lisätty viime vuosina mahdollistamalla jopa itsensä vakuuttaminen identiteettivarkauden varalta. Viranomaiset sekä vakuutusyhtiöt ovat tietoisesti panostaneet informaation lisäämistä henkilöille identiteettiturvan varmistamiseksi. Sosiaalisessa mediassa tuodaan tietoiskuja niin nuorille kuin iäkkäämmillekin. Tutkimustuloksen perusteella tietoisuus identiteettivarkauksista on lisääntynyt ja mahdollisesti vähentänyt yritysten määrää

sosiaalisen median alustoilla, sillä onnistumisprosentti on pienentynyt identiteettivarkausten osalta.

Vähiten vastaajat olivat törmänneet asiantuntijahuijauksiin 25 % sekä sijoitushuijauksiin 31 %. Asiantuntija ja sijoitushuijauksia liikkuu paljon eri sosiaalisen median alustoilla. Kyseiset huijausten muodot on naamioitu tänä päivänä niin hyvin, että niiden havaitseminen ennen uhrisiksi joutumisesta on vähäistä.

8.5 Käyttäjätilien suojaus

Tutkimuksessa kysyttiin, kuinka huolissaan vastaajat ovat sosiaalisen median tiliensä suojauksesta. Kysymys toteutettiin asteikolla 1–10, 1 tarkoittaen, että vastaaja on erittäin huolissaan ja 10 tarkoittaa, että ei ole ollenkaan huolissaan. Vastauksia tarkastellaan hieman varovaisesti. Käytetty mitta-asteikko on laaja ja vastaajat jakautuivatkin laajasti koko asteikolle, ilman selviä piikkejä. Vastaajista 17 % kokevat, että eivät ole huolissaan käyttäjätiliensä suojauksesta. Vastaajista 36,6 % olivat huolissaan käyttäjätiliensä suojauksesta. Lähes puolet vastaajista sijoittui arviointiasteikon keskivaiheelle, ollen jossain määrin huolissaan käyttäjätiliensä suojauksesta. Vastaajista kuitenkin 77,7 % eli reilusti yli puolet ovat ottaneet käyttöönsä kaksiosaisen tunnistautumisen suojatakseen tiliä paremmin. Kaksiosaisessa tunnistautumisessa käyttäjä kirjautuu sosiaalisen median tiliin käyttäen ulkoista lähdettä, käyttäjätunnuksen ja salasanan lisäksi (F-Secure, i.a.-b.). Tämä ulkoinen lähde voi esimerkiksi olla puhelimeen lähetettävä tekstiviesti, sormenjälki tai mobiilisovellus.

Kaksiosaisen tunnistautumisen käyttöönoton pitäisi lisätä käyttäjätilin turvallisuutta, minimoida hakkerien tai muiden väärinkäyttäjien mahdollisuutta päästä sisälle käyttäjätiliin. Vastausten perusteella voi päätellä, että vaikka kaksivaiheinen tunnistautuminen on monella jo käytössä, silti moni epäilee tilinsä turvallisuutta. Tämä turvattomuuden tunne voi johtua lisääntyvistä tietomurtoyrityksistä ja tietovuodoista. Myöhemmin tutkimuksessa kysyttiin vastaajien omaa mielipidettä siitä, kuinka he kokevat henkilötietojensa olevan turvassa ja moni oli sitä mieltä, että ne eivät ole. Annoimme myös mahdollisuuden kommentoida vapaasti asiaa, ja näitä vastauksia käymme läpi seuraavassa osiossa tarkemmin.

Kaksiosaiseen tunnistautumiseen liittyen kuitenkin nostetaan yksi vastaajan kommentti esille.

> ”Nykyisin myös kaksivaiheisesta suojauksesta huolimatta some tilejä on joutunut kolmannen osapuolen haltuun.”

Tämä kommentti nostaa hyvin esille sen, kuinka kaikesta varautumisesta huolimatta sosiaalisen median tilit eivät silti ole täysin turvassa. Sosiaalisen median tilejä uhkaa ulkopuoliset riskit ja inhimilliset virheet ovat mahdollisia.

8.5.1 Vastaajien salasana käytännöt

Salasanat ovat nykyään tärkeässä roolissa sosiaalisessa mediassa ja oman käyttäjätilin suojaamista. Monella eri alustalla toimii käyttäjätunnuksena usein sähköpostiosoite, joten on erittäin tärkeää panostaa hyvään salasanaan, mitä käytetään mieluiten eri salasanaa jokaisella alustalla. Hyvää salasanaa ei kuitenkaan tarvitse vaihtaa alituiseen. Teoriaosuudessa käytiin läpi tarkemmin hyviä salasanakäytäntöjä. Osana tutkimusta selvitettiin vastaajien salasanakäytäntöjä. Vastaajilta kysyttiin käyttävätkö he samaa salasanaa joka paikassa. Vastaajista lähes kaikki 92,9 % vastasi, että eivät käytä samaa salasanaa kaikkialla. Seuraavalla sivulla olevassa kuviossa (kuvio 5) näkyy vastaajien salasanojen vaihtotiheys.

Kuvio 5. Vastaajien salasanojen vaihtotiheys (n=112).

Yläpuolella olevassa ympyräkaaviossa (kuvio 5) on kuvattuna tarkemmin vastaajien vastaukset salasanojen vaihtamiseen liittyen. Vastausvaihtoehdoista yleisin oli ”epäsäännöllisen säännöllisesti”, vastaajista yli puolet valitsivat tämän. Tämän vaihtoehdon kuvaukseksi olimme määritelleet, että vastaaja vaihtaa salasanansa säännöllisesti esimerkiksi kolme kertaa vuodessa. Vastaajalla ei ole tarkkaa aikataulua tai kuukausi väliä salasanan vaihtamiseen. Vastaajista viidesosa kertoi vaihtavansa salasanan silloin, kun sattuvat muistavat. Säännöllisesti kaksi kertaa vuodessa salasanan vaihtaa 12 % vastaajista ja kerran vuodessa 5 %. Loput vastaajista (7 %) vastasi, että eivät vaihda salasanaansa koskaan. Tätä viimeistä lukua tarkastelemme hieman varauksella. Vastaajan kokiessa ettei vaihda salasanaansa koskaan, on mahdollista salasanan unohtuneen joskus ja se tulee siinä yhteydessä vaihtaa.

Vastaajien salasanan vaihtojen yleisyydestä voidaan päätellä vastaajien olevan tietoisia salasanojen heikkouksista ja niiden potentiaalisesta päätymisestä rikollisten tietoihin. Vastaajien salasanajoen vaihtotiheydestä voidaan olettaa, että vastaajien salasanat

noudattelevat hyvien salauskäytäntöjen periaatteita ollen riittävän pitkiä ja monimutkaisia. Salasanaansa samana pitävät vastaajat todennäköisesti luottavat oman salasanansa olevan riittävän monimutkainen, etteivät hakkerit tai botit pystyisi murtamaan välittömästi. Näillä vastaajilla on myös todennäköisesti käytössä kaksiosainen tunnistautuminen, sillä se luo lisäturvaa käyttäjätilille hyvän salasanan lisäksi.

8.6 Henkilötiedot sosiaalisessa mediassa

Sosiaalista mediaa yleensä pidetään alustana, mihin voidaan jakaa hetkiä omasta elämästä ystäville ja muille ihmisille. Tällaisia hetkiä voivat olla syntymäpäivät, lapsen jalkapallopeli, isovanhempien muutto tai oma lomamatka. Nämä kaikki voivat olla väärissä käsissä vaarallisia tietoja, mikä voi johtaa tietomurtoihin tai henkilötietojen väärinkäyttöön. Tutkimukseen osallistuneista vastaajista 36,6 % myönsi jakaneensa henkilötietojaan sosiaalisen median tilillään. Loput yli 60 % vastaajista vastasi, että eivät ole jakaneet henkilötietojaan sosiaalisessa mediassa. Tähän tilastoon voi suhtautua hieman varauksella, koska moni saattaa jakaa henkilötietojaan vahingossa tai tietämättään. Tutkimuksessa selvitettiin ovatko vastaajien mielestä heidän henkilötietonsa turvassa sosiaalisessa mediassa, ja vastaukset olivat lähes samat mitä aikaisemmin esitetyssä kysymyksessä ovatko vastaajat jakaneet tietojaan. 43,7 % vastaajista kokee henkilötietojensa olevan turvassa sosiaalisessa mediassa ja vastaajista 56,3 % eivät koe henkilötietojen olevan turvassa.

Vastaajille annettiin mahdollisuus perustella, miksi heidän mielestänsä henkilötiedot eivät ole sosiaalisessa mediassa turvassa. 14 vastaajaa kertoi kokevansa hakkeroinnin yhdeksi syyksi minkä vuoksi eivät luota sosiaalisen median turvallisuuteen. Muutama vastaaja nosti esille myös huolensa henkilötietojen myymisestä tai vuotamisesta ulkopuolisille ison yrityksen toimesta. Vastaajat myös nostivat esille huolen siitä, vaikka he olisivat turvanneet käyttäjätilinsä, on aina potentiaalinen mahdollisuus, että he itse tekevät vahingossa virheen. Inhimillisen virheen seurauksena heidän henkilötietonsa voivat päätyä vääriin käsiin. Vastaajat kertoivat avoimissa kysymyksissä seuraavasti omista mielipiteistään sosiaalisen median turvallisuudesta.

> “Uskon, että sosiaalisen median alustojen suojaus on tarpeeksi tietotaitoa ja tahtoa osaavalle hakkerille helppo murrettava kohde. Henkilötietoja myydään eteenpäin laittomasti ympäri maailman erinäistä markkinointia ja bisnestä varten.”

> ”Laajan käyttäjäkunnan alustat ovat haluttuja tietomurron kohteina, nopeasti saatavissa paljon henkilökohtaista dataa yhdellä yrityksellä. Todennäköisyys tietojen päätymiseen ulkopuolisten haltuun on suuri. Vaikka en jaa kriittisiä tunnistettavia tietoja, nimi ja profiilikuva esimerkiksi ovat yleensä helposti saatavilla ja niitä voidaan käyttää toisaalla valeprofiilien yhteydessä.”

Näissä kommenteissa nousee esille hyvin yleisimmät kohdat, joista tutkimukseen osallistuneet vastaajat olivat huolissaan eli hakkereista ja tietojen myymisestä eteenpäin. Näistä ollaan edelleen huolissaan, vaikka käytössä olisikin hyvin turvattu käyttäjätili ja henkilötietoja ei jaeta sosiaalisen median tilillä.

Tutkimuksen tuloksista voidaan päätellä, että vastaajat ovat suurimmaksi osaksi varovaisia sosiaaliseen mediaan liittyen ja asioista mitä jakavat mediassa. Vastaajat osoittavat selvää epäluottamusta sosiaalisen median tietoturvaan ja myöntävät avoimesti pelkäävänsä tietomurtoja. Sosiaalisessa mediassa esiintyviä hakkereita ja muita tietoturvarikollisia pidetään todellisena uhkana myös vastaajien keskuudessa.

9 TUTKIMUKSEN YHTEENVETO

Tämä opinnäytetyö sai alkunsa ideasta alkaa selvittää, kuinka hyvin tutkijoiden lähipiirissä tunnetaan ja tunnistetaan tietoturvariskit. Ajatuksen pyörittelemisen jälkeen päätutkimuskysymykseksi nousi ”Mikä on yksityishenkilön tietämys tietoturvasta sosiaalisessa mediassa?”. Tämän tutkimuskysymyksen ympärille rakennettiin teoriaosuus. Tutkimus toteutettiin kyselytutkimuksena, mihin kysymykset ovat rakennettu teoriaosuudesta opittuihin asioihin. Teoriaosuudessa on hyödynnetty kirjallisuutta tietoturvasta ja sosiaalisesta mediasta sekä aiheesta löytyvää tutkimustietoa verkosta. Kyselytutkimus toteutettiin syksyllä 2023 ja siihen hyödynnettiin Webropol-kyselytyökalua. Webropol tarjosi mahdollisuuden luoda verkkokyselyn anonyymisti ja loi raportin kyselystä saadun datan analysoinnin avuksi.

Tutkimukseen osallistui 112 vastaajaa monesta ikäryhmästä ja sosiaalisesta asemasta. Tutkimukseen osallistuneista 110 vastaajalla on käytössä jokin sosiaalisen median tili. Tutkimuksen analysoinnin yhteydessä selvisi, kysymysten olevan osittain huonosti suunniteltuja tai vastaukset ovat mustavalkoiset. Osassa kysymyksistä ei annettu vastaajille riittävästi vaihtoehtoja tai tilaa vastata avoimesti, jotta he saisivat tuoda esille kokonaisen tietämyksensä, mikä olisi voinut auttaa kattavamman datan muodostamisessa.

Tutkimuksessa selvisi, että vastaajista 56 % kokee sosiaalisen median käytön turvalliseksi. Sosiaalinen media koetaan turvalliseksi huolimatta, siitä että vastaajista noin 70 % on törmännyt sosiaalisessa mediassa tietojenkalastelua. Sosiaalisessa mediassa esiintyvät tietoturvariskit ovat vastausten perusteella yleisiä ja niihin törmääminen ei vähennä sosiaalisen median turvallisuuden tunnetta. Vastaajien kokiessa sosiaalinen median koetaan turvalliseksi voi johtua vastaajien tietämyksestä siellä olevista vaaroista ja suurin osa vastaajista osaa tunnistaa hyvin yleisimmät tietoturvauhat ja osaa välttää niitä. Vastaajista lähes 80 % on ottanut käyttöönsä kaksiosaisen tunnistautumisen sosiaalisessa mediassa, mikä omalta osaltaan vähentää riskiä joutua tietomurron tai identiteettivarkauden uhriksi.

Vaikka valtaosa vastaajista kokee sosiaalisen median olevan turvallinen, vastauksista ilmeni kuitenkin, että hieman yli puolet vastaajista kokee henkilötietojensa olevan vaarassa sosiaalisessa mediassa. Henkilötietojen koetaan olevan vaarassa sosiaalisessa mediassa,

sillä tietovuotoja on ollut esillä digitaalisessa mediassa paljon. Avoimessa vastauksessa vastaajat paljastivat olevansa huolissaan myös hakkereista ja itseaiheutetusta tietovuodosta.

Tutkimuksen lopuksi vastaajat saivat antaa kyselytutkimuksesta avointa palautetta. Palautteen perusteella osaa kysymyksistä olisi voinut muotoilla tarkemmin koskemaan tiettyjä sosiaalisen median alustoja ennemmin kuin yleisellä tasolla. Tietosuojaan liittyvissä kysymyksissä etenkin olisi voinut olla enemmän vastausvaihtoehtoja. Toteutuneessa kyselyssä kysyttiin lukevatko vastaajat koko tietosuojaselosteen, kyllä tai ei. Tämän kysymyksen olisi voinut muotoilla toiseen muotoon, tai antaa vastaajille vaihtoehtoisesti mahdollisuuden avoimeen vastaukseen. Vastaajat toivat kyselyn lopussa avoimessa palautteessa ilmi, että eivät välttämättä lue tietosuojaselostetta sanasta sanaan, mutta silmäilevät usein pääkohdat läpi.

Tutkimuksesta voisi toteuttaa jatkotutkimus saadun palautteen avulla ja tarkentaa joitakin kysymyksiä. Tutkimuksen kysymyksiä uudelleen toteutettaessa voisi rajata tarkemmin, sillä toteutunut kysely oli hyvin laaja ja osa kysymyksistä oli hyvin yleisiä. Tutkimus kuitenkin koetaan onnistuneeksi. Vastaajia oli runsaasti ja vastausten koetaan olevan aitoja. Tutkimuksesta kerätystä datasta pystyy päättelemään, millaiseksi tutkimusryhmä kokee tietämyksensä sosiaalisessa mediassa olevista tietoturvauhista. Tutkimusaihe koetaan olevan ajankohtainen, sillä sosiaalinen media on iso osa arkea monelle ja tietoturvauhat lisääntyvät siellä jatkuvasti.

LÄHTEET

Aarnio, M. (8.8.2020). Hittisovelluksen varjopuoli – nuoret kertovat, miten haitallisia videoita TikTokista löytyy: "Ei se ole sen arvoista". *MTV Uutiset.* https://www.mtvuutiset.fi/artikkeli/hittisovelluksen-varjopuoli-nuoret-kertovat-miten-haitallisia-videoita-tiktokista-loytyy-ei-se-ole-sen-arvoista/7876734#gs.7nvhca

Andreasson, A., Riikonen, J., & Ylipartanen, A. (2019). *Osaava tietosuojavastaava ja EU: N yleinen tietosuoja-asetus.* Tietosanoma.

Arkistojen Portti. (i.a.). *Kansakoulut*. https://portti.kansallisarkisto.fi/fi/aineisto-oppaat/kansakoulut

Chantel, J. (25.4.2023). *Smartphone History:* The timeline of a Modern Marvel. *Textedly.* https://blog.textedly.com/smartphone-history-when-were-smartphones-invented

Choi, T. R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and informatics*, *35*(8), 2289-2298.

Clausnitzer, J. (9.3.2023). How often do you use WhatsApp? *Statista.* https://www.statista.com/statistics/560848/share-of-whatsapp-users-in-finland-by-usage-frequency/

Davies, M.B. (2007) *Doing successful research project: using qualitative or quantitative methods.* Palgrave Macmillan.

Discord. (i.a.). *Company*. https://discord.com/company

Dolan, B. (2023). What is TikTok? *Investopedia*. https://www.investopedia.com/what-is-tiktok-6826240

Eldridge, A. (3.10.2023). Instagram: Social networking service. *Britannica.* https://www.britannica.com/topic/Instagram

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

European Data Protection Board (EDPB). (22.5.2023). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Europol. (16.11.2016). Tips and Advice to prevent Identity Theft happening to you. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-and-advice-to-prevent-identity-theft-happening-to-you

Europol. (12.5.2022). Take control of your digital life. Don't be a victim of cyber scams! https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%E2%80%99t-be-victim-of-cyber-scams

Facebook. (28.5.2022). Miten Facebookin ja Instagramin kaupalliset tuotteet toimivat? https://www.facebook.com/legal/EEA_Commerce_Products_Disclosure

Facebook. (24.8.2023). Käyttöehdot. https://www.facebook.com/legal/terms

F-Secure. (2023a). Mitä on tietojenkalastelu? https://www.f-secure.com/fi/articles/what-is-phishing

F-Secure. (2023b). Vältä näitä 5 tietojenkalasteluhuijausta vuonna 2023. https://www.f-secure.com/fi/articles/5-phishing-scams-to-avoid-in-2023

Hakala, M., Vuorinen, O. & Vaino. (2006) *Tietoturvallisuuden käsikirja.* Docendo.

Hall, M. (3.10.2023). Facebook: Social network. *Britannica.* https://www.britannica.com/topic/Facebook

Hanninen, M., Laine, E., Rantala,K., Rusi,M. & Varhela, M. (2017). *Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset.* Kauppakamari.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.

Hyppönen, M. (2021). *Internet*. WSOY.

Juusola, E., Halonen, A., Bergius, H., & Metsola, A. (2018). *Sydän saaliina: Romanssihuijarit verkossa*. Docendo.

Jäntti, E. (2017). Mitä Snapchatissa tapahtuu? Pikaopas vanhemmille. Elisa. https://elisa.fi/ideat/mita-snapchatissa-tapahtuu/

Järvinen, P. (2002). *Tietoturva & yksityisyys*. Docendo.

Järvinen, P. (2022) *Digiajan tietosuoja: turvaa henkilötietosi, torju identiteettivarkaudet, suojaudu urkinnalta.* Tammi (2022). https://seamk.finna.fi/Record/seamk.991300514805969?sid=3125775465

Keller, M. (2023). *Mitä on tietosuoja?* Alma Talent.

Kemp, S. (2023a). Facebook messenger users, stats, data & trends. Datareportal. https://datareportal.com/essential-facebook-messenger-stats

Kemp, S. (2023b). Facebook users, stats, data & trands. Datareportal. https://datareportal.com/essential-facebook-stats?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Finland&utm_content=Facebook_Stats_Link

Kemp, S. (2023c). Instagram users, stats, data & trends. Datareportal. https://datareportal.com/essential-instagram-stats

Kemp, S. (2023d). Twitter users, stats, data & trends: Essential Twitter statistics and trends for 2023. DataReportal. https://datareportal.com/essential-twitter-stats

Kemp, S. (2023e). Digital 2023: Finland. Datareportal. https://datareportal.com/reports/digital-2023-finland

Kemp, S. (2023f). Snapchat users, stats, data & trends. Datareportal. https://datareportal.com/essential-snapchat-stats?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Finland&utm_content=Facebook_Stats_Link

Kemppi, J. (8.9.2020). Lasten suosimassa Tiktok-sovelluksessa leviää brutaali video – Nuoret käyttäjät vetoavat toisiinsa: ”Lopeta katsominen heti”. *Iltalehti.* https://www.iltalehti.fi/digiuutiset/a/5bd6cc4f-fedb-4d96-9f82-1f61b30cda7d

Knuuttila, T. (20.5.2022. Rakkaushuijaukset paljastuvat usein liian myöhään – älä jää yksin huijauksen kanssa. Pop Pankki. https://www.poppankki.fi/blogi/rakkaushuijaukset-paljastuvat-usein-liian-myohaan

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. (2022). *Tietosuoja*. Alma Talent.

Kotimaisten kielten keskus (Kotus). (2023). Some. Teoksessa Kielitoimiston sanakirja. https://www.kielitoimistonsanakirja.fi/#/some?searchMode=all

Kuluttajaliitto. (i.a.) Nettihuijaukset ja muut huijaukset. https://www.kuluttajaliitto.fi/materiaalit/huijaukset/

La Trobe Univercity. (i.a.) What does LGBTIA+ mean? https://www.latrobe.edu.au/students/support/wellbeing/resource-hub/lgbtiqa/what-lgbtiqa-means

Lehtinen, D. (24.7.2023). Twitterin lintulogo vaihtui X:ksi. *Helsingin sanomat.* https://www.hs.fi/talous/art-2000009737685.html

Lutkevich, B. (2021). Social Media. Tech Target. https://www.techtarget.com/whatis/definition/social-media

Maheshwari, S & Holpuch, A. (10.10.2023). Why Countries Are Trying to Ban TikTok? *The New York Times*. https://www.nytimes.com/article/tiktok-ban.html

Martin, R. (2.10.2023). WhatsApp: Messaging application. *Britannica*. https://www.britannica.com/topic/WhatsApp

Meltwater. (2023a). Kattava opas sosiaalisen median videokokoihin vuonna 2023. https://www.meltwater.com/fi/blog/sosiaalisen-median-videokoot

Meltwater. (2023b). 2023 Global Digital Report. https://www.meltwater.com/en/global-digital-trends

Merisalo, T. (2022). *Tietoturva sosiaalisessa mediassa: Uhat ja varautuminen* [diplomityö, Tampereen yliopisto]. Trepo. https://trepo.tuni.fi/bitstream/handle/10024/140482/MerisaloTeemu.pdf?sequence=2&isAllowed=y

Meta. (i.a.). Our Story. https://about.meta.com/company-info/

Meta. (30.10.2023). Facebook and Instagram to offer subscription for no ads in Europe. https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

Minilex (i.a). Verkkopetos. https://www.minilex.fi/a/verkkopetos

Mäkipää, S. (5.12.2019). Lasten suosikkisome Tiktok piilotti lihavien, homojen ja transihmisten tekemän sisällön sovelluksessaan. *Helsingin Sanomat.* https://www.hs.fi/nyt/art-2000006332409.html

Olito, F. (13.9.2019). Computers actually date back to the 1930s. Here's how they've changed. *Business Insider.* https://www.insider.com/how-computers-evolved-history-2019-9

Rikoslaki 39/1889 28. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

Rikosuhripäivystys (RIKU). (i.a.) Identiteettivarkaudessa esiinnytään toisen henkilöllisyydellä. https://www.riku.fi/erilaisia-rikoksia/identiteettivarkaus-2/

Rikosuhripäivystys (RIKU). (28.1.2021). Tietomurto – Neuvoja tietomurron tai tietovuodon uhriksi joutuneille. https://www.riku.fi/toimi-nain-jos-tietojasi-on-vuodettu-verkkoon/

Signal. (i.a.). Viestinnän vapautta. https://signal.org/fi/

Termipankki. (12.10.2010.) Mikroblogi. Teoksessa *TEPA-Termipankki.* Haettu 31.10.2023. https://termipankki.fi/tepa/fi/haku/mikroblogi

Termipankki (TEPA). (2018). Tietoturva. Teoksessa Erikoisalojen sanastojen ja sanakirjojen kokoelma - Sanastokeskus. Haettu 25.10.2023. https://termipankki.fi/tepa/fi/haku/tietoturva

Tietoarkisto. (i.-a.) Kvantitatiivisen tutkimuksen verkkokäsikirja. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/

Tietosuojalaki 1050/2018. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=tietosuoja

Tietosuojavaltuutetun toimisto. (i.a.) Mikä on henkilötieto? https://tietosuoja.fi/mika-on-henkilotieto

Tilastokeskus. (24.10.2023). Työvoimatutkimus. https://www.stat.fi/tilasto/tyti

Traficom. (20.9.2019). Tekstiviestihuijauksia liikkeellä runsaasti – lue tarkasti, mihin olet sitoutumassa. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekstiviestihuijauksia-liikkeella-runsaasti-lue-tarkasti-mihin-olet-sitoutumassa

Traficom. (9.7.2020). Tietoturva. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Traficom. (2023a). Pidempi parempi - Näin teet hyvän salasanan. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Traficom. (2023b). Salasanat haltuun - Kuka käyttää tiliäsi? https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun

Tranberg, P., Heuer, S., & Laukkanen, M. (2013). *Älä kerro kaikkea: Itsepuolustusopas verkkoon*. Talentum.

Trejtnar, E. (i.a.) Juristi vastaa: Mikä on identiteettivarkaus ja milloin se tulee rangaistavaksi? Rikosuhripäivystys. https://www.riku.fi/rikosuhripaivystys/riku-lehti/riku-lehti-1-2019/juristi-vastaa-mika-on-identiteettivarkaus-ja-milloin-se-tulee-rangaistavaksi/?gclid=CjwKCAjwnOipBhBQEiwACyGLuoxyr4axac-zzYi5Z-VFxz9Nmqr_bc0IIIBBxnbhF66k8djNDQlzexoC7nwQAvD_BwE

Vuorinen, T. (2013). *Strategiakirja: 20 työkalua*. Talentum.

Väestöliitto. (10.11.2020). Mitä tarkoittaa HLBTIQA+? *Hyvä kysymys.* https://www.hyvakysymys.fi/artikkeli/mita-tarkoittaa-hlbtiqa/

WhatsApp. (14.1.2021). WhatsAppin Käyttöehdot. https://www.whatsapp.com/legal/terms-of-service-eea

LIITTEET

Liite 1. Tutkimuksen kyselylomake

1. Kyselyyn vastaajan ikä.
2. Mikä on korkein suorittamasi koulutusaste?
    a. Peruskoulu, kansankoulu
    b. Ammatillinen perustutkinto, ylioppilastutkinto, lukion kokonaisoppimäärä
    c. Alempi korkeakoulututkinto
    d. Ylempi korkeakoulututkinto
    e. Yliopistotutkinto
3. Mikä on tämänhetkinen työasemasi?
    a. Työtön
    b. Opiskelija
    c. Eläkeläinen
    d. Työntekijä
    e. Esihenkilö
    f. Asiantuntija
    g. Yrittäjä
4. Millaiseksi koet tämänhetkisen tietoteknisen osaamisesi?
    a. perusteet, mutta tarvitsen usein apua.
    b. Olen keskiverto, hallitsen yleisimmät tietotekniset laitteet kohtalaisen hyvin, mutta tarvitsen apua joskus.
    c. Olen hyvä tietotekniikan kanssa ja osaan käyttää hyvin erilaisia laitteita.
    d. Olen asiantuntija tietotekniikan kanssa. Käytän sujuvasti erilaisia laitteita, sekä niiden ohjelmistoja.
5. Onko sinulla käytössäsi jokin sosiaalisen median tili?
6. Mitä sosiaalisen median tilejä käytät?
    a. Facebook
    b. Instagram
    c. X (entinen Twitter)

   d. TikTok
   e. Snapchat
   f. WhatsApp
   g. Jokin muu
7. Kuinka aktiivinen olet sosiaalisessa mediassa? Asteikolla 1–10.
8. Koetko sosiaalisen median käytön turvalliseksi?
9. Jos vastasit edelliseen kysymykseen kieltävästi, niin kerro miksi?
10. Kuinka luotettavana pidät sosiaalisessa mediassa jaettavan informaation? Asteikolla 1–10.
11. Sosiaalisessa mediassa on päivä päivältä enemmän uhkia henkilötiedoillemme. Oletko törmännyt johonkin seuraavista? (Voit valita useamman.)
    a. Tietojenkalastelu
    b. Romanssihuijaus
    c. Asiantuntijahuijaus
    d. Kauppahuijaus
    e. Sijoitushuijaus
    f. Identiteettivarkaus
    g. Jokin muu.
12. Jos olet törmännyt edellisiin uhkiin sosiaalisessa mediassa, oletko ollut itse uhrina, vai läheinen?
13. Tiedätkö mitä tarkoitetaan tietojenkalastelulla (Phishing)
14. Tiedätkö mitä tarkoitetaan romanssihuijauksella?
15. Tiedätkö mitä tarkoitetaan identiteetti varkaudella?
16. Tiedätkö mitä tarkoitetaan asiantuntijahuijauksella?
17. Tiedätkö mitä tarkoitetaan kauppahuijauksella?
18. Tiedätkö mitä tarkoitetaan sijoitushuijauksella?
19. Kuinka huolissasi olet käyttäjätilisi suojauksesta? Asteikolla 1-10
20. Oletko ottanut käyttöösi kaksiosaisen tunnistautumisen?
21. Oletko jakanut sosiaalisessa mediassa henkilötietojasi?
22. Koetko henkilötietojesi olevan turvassa sosiaalisessa mediassa?
23. Jos et koe henkilötietojesi olevan turvassa, niin miksi?

24. Käytätkö samaa salasanaa, joka paikassa?
25. Kuinka usein vaihdat salasanasi?
    a. Kerran vuodessa
    b. Pari kertaa vuodessa
    c. Silloin, kun satun muistamaan
    d. Epäsäännöllisen säännöllisesti
    e. En ikinä
26. Uuden käyttäjätilin luonnin yhteydessä tulee lukea kyseiseen mediaan liittyvä tietosuojaselosta. Luetko kyseisen tekstin?
27. Tiedätkö mistä löydät tarvittaessa tietosuojaselosteen?
28. Tähän voit jättää palautetta kyselystä, tai lisätietoja/kommentteja, jos haluat avata vastauksiasi enemmän.