Tampereen yliopisto

Teemu Merisalo

TIETOTURVA SOSIAALISESSA MEDIASSA: UHAT JA VARAUTUMINEN

Diplomityö
Informaatioteknologian ja viestinnän tiedekunta
Tarkastaja: tutkija Tiina Schafeitel-Tähtinen
Tarkastaja: yliopistonlehtori Jukka Koskinen
Toukokuu 2022

TIIVISTELMÄ

Teemu Merisalo: Tietoturva sosiaalisessa mediassa: uhat ja varautuminen
Diplomityö
Tampereen yliopisto
Tietotekniikan DI-ohjelma
Toukokuu 2022

Sosiaalisen median käyttäjämäärät ovat huomattavassa kasvussa ja koskevat yhä useammin eri tietoteknisen taustan sekä iän omaavia henkilöitä. Sosiaalisen median tietoturvan edistymisen myötä, käyttäjien tietoturvan sekä tietoisuuden olisi aiheellista pysyä kehityksessä mukana. Palveluiden tulee ylläpitää sekä päivittää tarjoamiaan tietoturvaominaisuuksia ehkäisemällä käyttäjien tietoturvattomuutta alustoillaan.

Tutkimus käsitteli tietoturvaa peruskäyttäjän näkökulmasta, jolloin saatiin kartoitettua käyttäjän tietoturvan tasoa ottamatta kantaa henkilön tietotekniikan lähtötasoon. Tutkimuksessa kartoitettiin sosiaalisen median alustoilla esiintyviä tämänhetkisiä tietoturvauhkia sekä niiden yleisyyttä. Tutkimuksessa myös selvitettiin laaditun kyselyn avulla käyttäjien tietoturvakäytäntöjä, tietoisuutta sekä sitä, ovatko käyttäjät kohdanneet tutkimuksessa käsiteltyjä kirjallisuudesta esille nousseita tietoturvauhkia.

Tutkimuksessa päätavoitteena oli selvittää, miten käyttäjien sosiaalisen median tietoturvaa voitaisiin parantaa sekä lisätä heidän tietoisuuttaan. Tavoitteeseen pyrittiin vastaamaan analysoimalla käyttäjiltä saatuja vastauksia heidän tietoturvastaan. Tutkimuksessa selvitettiin disinformaation sekä valeuutisten vaikutusta sosiaalisessa mediassa ja sitä, koetaanko valeuutiset ongelmaksi sosiaalisen median alustoilla. Tutkimuksessa tarkasteltiin käyttäjien luottamusta sosiaalisen median sisältöihin.

Tutkimuksen kirjallisuuslähteinä hyödynnettiin vertaisarvioituja tutkimuksia sekä muita raportteja ja artikkeleita. Kirjallisuuslähteiden lisäksi tutkimuksessa käytettiin aineiston hankkimista varten laadittua kyselylomaketta, jossa tietoturvan opiskelijat haastattelivat tuttaviaan heidän sosiaalisen median tietoturvan kartoittamiskeksi.

Kyselyn vastausten perusteella käyttäjien tietoisuus tutkimuksessa käsitellyistä tietoturvauhista oli pääosin hyvällä tasolla. Käyttäjien vastausten perusteella tietoisuuden lisäämiseksi perinteisen median tulisi lisätä tietoturvan ja tietoturvauhkia koskevan informaation levittämistä. Hyvästä tietoisuudestaan huolimatta käyttäjät nostivat esille sen, että tietoturvaohjeissa harvoin ohjeistetaan, miten tulisi toimia joutuessaan kyberrikoksen uhriksi. Tutkimuksen perusteella käyttäjien tulisi kiinnittää enemmän huomiota omaan tietoturva-arkeen, ja toteuttaa säännöllisesti hyviä tietoturvakäytäntöjä, sillä käyttäjillä on siihen tietotaitoa heidän vastaustensa perusteella. Tutkimuksen tulosten mukaan käyttäjien omia tietoturvakäytäntöjä tulisi kehittää ja mahdollistaa niiden hyödyntäminen tietoturva-arjessa. Käyttäjien tulisi kiinnittää enemmän huomiota tiedon todenmukaisuuden varmistamiseen. Vastaajat toivovat ajankohtaista informaatiota tietoturvauhista ja tietoa tietoturvaohjeistuksista. Käyttäjiä tulisi ohjeistaa laajemmin valeuutisia sekä disinformaatiota varten erityisesti kriisien aikana.

Avainsanat: sosiaalinen media, tietoturva, valeuutiset, misinformaatio, disinformaatio, tietojenkalastelu, yksityisyys

ABSTRACT

Teemu Merisalo: Information security on social media: threats and preparedness
Master's thesis
Tampere University
Information Technology
May 2022

The number of users of social media is growing significantly, and it is increasingly affecting people from different IT backgrounds and ages. As social media security advances, user information security and awareness should keep pace with developments. The services must maintain and update the security features they provide so that the services can prevent users from being insecure on their platforms.

The study dealt with information security from the basic user's point of view, which made it possible to map the user's level of information security without taking a position on the person's initial level of information technology. The study mapped the current information security threats on social media platforms and their prevalence. The study also used the survey to find out users' information security practices, awareness, and whether users have encountered security threats from the literature.

The main objective of the study was to find out how users' social media information security could be improved, and their awareness increased. To achieve this, responses from users about their information security were analyzed. The study examined the impact of disinformation and fake news on social media and whether false news is perceived as a problem on social media platforms. The study looked at user confidence in social media content.

Peer-reviewed studies as well as other reports and articles were utilized as literature sources for the study. In addition to the literature, the study used a questionnaire designed to obtain data, in which information security students interviewed their acquaintances to map their social media information security.

Based on the responses to the survey, users' awareness of the security threats addressed in the survey was generally at a good level. Based on user responses, to raise awareness, traditional media should increase the dissemination of guidance about information security and its threats. Despite their good awareness, users pointed out that security guidelines rarely provide instructions on how to act when you become a victim of cybercrime. Based on the research, users should pay more attention to their own information security in everyday life, and regularly implement good information security practices, as users have the knowledge to do so based on their responses. According to the results of the study, users' own information security habits should be developed and enabled to be used in everyday information security. Users should pay more attention to ensuring the veracity of the information. Respondents want up-to-date information on security threats and information on security guidelines. Users should be instructed more widely on fake news and disinformation, especially during crises.

Keywords: social media, information security, fake news, misinformation, disinformation, phishing, privacy

SISÄLLYSLUETTELO

KUVALUETTELO

1. JOHDANTO

Sosiaalisella medialla tarkoitetaan tietoverkkojen avulla tapahtuvaa yhteisöllistä viestintää. Sosiaalisen median palveluissa voidaan jakaa sisältöä, päivityksiä sekä keskustella muiden ihmisten kanssa. Mätön (2015) mukaan Ylen vuonna 2015 teettämän kyselyn perusteella sosiaalisen median palvelu Facebookia käytti 56 % vastaajista ja WhatsAppia 37 % (Mättö, 2015). Sosiaalisen median käytön yleistyessä on hyvä myös tarkastella tietoturvaa peruskäyttäjän näkökulmasta, sillä sosiaalisen median käyttäjäkunta on laajentunut koskemaan kaiken ikäisiä sekä eri taustoista olevia henkilöitä. Sosiaalisessa mediassa on DataReportalin (2022) tammikuun 2022 raportin mukaan 4,62 miljardia käyttäjää ja käyttäjien lukumäärä on kasvanut 424 miljoonalla viimeisen 12 kuukauden aikana (DataReportal, 2022).

SOSIADMIN (2018) mukaan nettirikoksista on tullut arkipäiväistä internetin käytön yleistyttyä. Perinteiset tietoturvauhat ja uusien palveluiden yhdistelmät ovat nykyään iso osa sosiaalisessa mediassa esiintyviä tietoturvaongelmia. Keskeisimmät uhat perustuvat usein käyttäjän omaan toimintaan tai osaavaan ja harkittuun rikostoimintaan sosiaalisen median palveluiden keskuudessa. (SOSIADMIN, 2018)

Tutkimuksen tavoitteena on tutkia sosiaalisen median eri alustoilla esiintyviä tietoturvauhkia. Tutkimuksessa pyritään saamaan vastaus määriteltyihin tutkimuskysymyksiin, joita ovat:

- Mitkä ovat tavallisen käyttäjän tämän hetken tietoturvauhat sosiaalisessa mediassa ja kuinka tietoisia he ovat niistä?
- Ovatko valeuutiset ja väärä informaatio ongelma sosiaalisessa mediassa?
- Luottavatko käyttäjät helposti sosiaalisessa mediassa jaettuun tietoon?
- Miten käyttäjien sosiaalisen median tietoturvaa voitaisiin parantaa?

Tässä työssä käsitellään pääosin seitsemää ennalta valittua sosiaalisen median alustaa. Käsiteltyjen alustoiden osalta tarkastellaan niiden levinneisyyttä, omistussuhteita, käyttöehtoja sekä alustojen tietoturvaa koskevia tapauksia, esimerkiksi tietovuotoja. Alustoista selvitetyillä tiedoilla luodaan pohjatieto eri alustojen taustoista sekä tietoturvakäytännöistä, joita voidaan myöhemmin vertailla käyttäjien omiin kokemuksiin.

Tutkimuksessa kartoitetaan myös kyselyyn osallistuneiden tietoisuutta tietoturvauhkien osalta ja siitä, miten he ovat mahdollisesti kohdanneet ja tunnistaneet näitä kyseisiä uhkia. Tutkimuksessa painotetaan peruskäyttäjän näkökulmaa sosiaalisen median tietoturvan osalta. Peruskäyttäjällä tarkoitetaan tässä tutkimuksessa kaikkia sosiaalisen median käyttäjiä riippumatta heidän tietoteknisistä taustoistaan, jolloin saadaan kattava läpileikkaus koko käyttäjäkunnasta. Tutkimusmenetelmänä hyödynnetään kyselylomaketta, jonka avulla kerätään tietoa myös siitä, millä tavoin sosiaalisen median käyttäjät ovat varautuneet tietoturvauhkia varten. Kyselylomake koostuu sosiaalisen median tietoturvauhkiin liittyvistä kysymyksistä, joiden vastausten perusteella paneudutaan käyttäjien tietoturvaan liittyviin ongelmakohtiin ja arvioidaan tutkimuksen onnistuneisuutta aikaisempiin tutkimuksiin verrattaessa. Tutkimuksesta saatujen tulosten perusteella pyritään löytämään kehityskohteita käyttäjien jokapäiväiseen tietoturvaan liittyen. Aiempien tutkimusten ja saatujen vastausten avulla voidaan arvioida tutkimuksen luotettavuutta sekä muodostaa yhdessä tutkimustiedon kanssa kokonaiskuva merkittävistä tekijöistä ja kehityskohteista sosiaalisen median tietoturvauhista käyttäjien arjessa.

Tutkimus toteutetaan määrällisenä tutkimuksena, jonka avulla tulkitaan sosiaalisen median tietoturvaa ja käyttäjien käyttäytymistä erilaisten tilastojen ja numeroiden avulla. Jyväskylän yliopiston (2015) mukaan määrällisen tutkimuksen avulla on mahdollista tarkastella sosiaalisen median tietoturvaan liittyviä toimintaan yhteydessä olevia ilmiöitä sekä vertailla aiemmin tehtyjä tutkimuksia kyselystä saatuihin tuloksiin (Jyväskylän yliopisto, 2015). Määrällisen tutkimuksen avulla halutaan ymmärtää tutkittavan aiheen ilmiöitä sekä merkityksiä kokonaisvaltaisesti sosiaalisen median käyttäjien keskuudessa. Tutkimustuloksia käsitellään Jyväskylän yliopiston (2021) määrittelemän tilastollisesti kuvaavaa analyysin avulla (Jyväskylän yliopisto, 2021b). Tämän analyysimenetelmän avulla tutkimusaineistoa on mahdollista havainnollistaa graafisesti ja verrata analysoituja tuloksia teoriaan.

2. TIETOTURVAUHAT SOSIAALISESSA MEDIASSA

Sosiaalinen media käsitteenä sisältää internetissä olevat yhteisöpalvelut mahdollistaen vuorovaikutuksen muiden käyttäjien kanssa. Sosiaalisen median käyttäjämäärät ovat nopeassa kasvussa muokaten sosiaalisen median tietoturvaa. Tilastokeskuksen (2021) tutkimuksen perusteella 58 % vastaajista ovat seuranneet yhteisöpalveluita vähintään päivittäin (Tilastokeskus, 2021). Sosiaalisen median tietoturvauhissa hyödynnetään usein käyttäjien yhteisöllisyyttä ja ihmisten avuliaisuutta, jolloin hyökkäyksissä uhri luottaa enemmän hyökkääjään kuin esimerkiksi sähköpostien välityksellä tapahtuvassa huijauksessa.

Tietoturvauhat voivat olla seurausta tarkoituksellisista hyökkäyksistä tai käyttäjän huonoista tietoturvakäytännöistä sosiaalisessa mediassa. Seuraavassa alaluvussa pohjustetaan tässä tutkimuksessa käsiteltyjä tietoturvauhkia. Tutkimuksessa käsiteltävät tietoturvauhat ovat valikoituneet aiempia tutkimuksia tarkastelemalla sekä perustuen tutkimuksen tekijän omiin huomioihin sosiaalisen median alustoilla.

2.1 Sosiaalisen median yksityisyys

Sosiaalisen median yksityisyydellä tarkoitetaan sosiaalisessa mediassa jaetun sisällön sekä oman käyttäjäprofiilin yksityisyyttä. Monet sosiaalisen median palvelut sisältävät kattavat työkalut sekä ohjeistukset yksityisyysasetusten muokkaamiseen. Huonosti määritellyt yksityisyysasetukset voivat johtaa tietoturvauhkien realisoitumiseen kuten esimerkiksi identiteettivarkauteen.

Rikoslaki turvaa omalta osaltaan sosiaalisen median yksityisyyttä, jolloin väärinkäytöksistä voidaan tarvittaessa rankaista. Rikoslaissa on 24 luvun 8 §:n mukaan yksityiselämää loukkaava tiedon levittäminen on määritelty rangaistavaksi. Finlexin (2013) mukaan rikoslaissa määritellään seuraavasti: “joka oikeudettomasti esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, on tuomittava yksityiselämää loukkaavasta tiedon levittämisestä sakkoon” (Finlex, 2013).

2.2 Tietojenkalastelu

Tietojenkalastelulla tarkoitetaan hyökkäystä, jonka tavoitteena on saada uhrilta tietoja. Hyökkääjä voi kalastella esimerkiksi kohteen käyttäjätietoja tai henkilötietoja. Tietojenkalastelulla halutaan usein päästä käsiksi kohteen käyttäjätilille. F-Securen (2021) mukaan tietojenkalastelussa houkutellaan usein käyttäjää painamaan linkkiä ja siirtymään sivustolle, jossa tietoja kalastellaan (F-Secure, 2021).

Tietojenkalastelu on yleistynyt sosiaalisessa mediassa sen suosion kasvaessa. Tietojenkalastelu on tapahtunut aikaisemmin pääosin sähköpostitse roskapostien mukana. PhishLabsin (2021) mukaan, vuonna 2021 tietojenkalasteluhyökkäysten määrä on noussut n. 32 % vuoteen 2020 verrattuna (PhishLabs, 2021). Tietojenkalasteluviestien avulla voidaan saada houkuteltua uhri ulkoiselle sivustolle esimerkiksi sillä, että hän on voittanut jotain. Viestissä voidaan kertoa myös, että hänelle on tulossa lähetys ja uhrin pitää klikata linkkiä voiton tai lähetyksen lunastamiseksi.

Tietojenkalastelussa voidaan hyödyntää käyttäjien yhteisöjä sekä kaverisuhteita, jolloin uhria huijataan muodostamalla todenmukainen verkko huijauksen ympärille. Uhria voidaan lähestyä sosiaalisessa mediassa yksityisviestillä sekä tekaistulla profiililla, jolloin uhrilla voi olla enemmän luottamusta hyökkääjää kohtaan. PhishLabsin (2021) marraskuun 2021 raportin mukaan sosiaalisen median kautta tapahtuvat hyökkäykset ovat nousseet 82 % tammikuun ja syyskuun välillä vuonna 2021 (PhishLabs, 2021).

2.2.1 Käyttäjätilin kaappaukset

Käyttäjätilin kaappaukset voivat olla kohdistettuja hyökkäyksiä, jolloin hyökkääjä valitsee uhrin tarkoituksella ja lähestyy tätä esimerkiksi tietojenkalastelulla. Useimmiten käyttäjätilin kaappaukset tapahtuvat tietomurron jälkeen tai käyttäjän jouduttua tietojenkalastelun uhriksi. Tietomurtojen jälkeen verkossa on usein esillä listoja, jotka voivat sisältää käyttäjätunnuksen tai sähköpostin selvätekstinä. Tietojen avulla hyökkääjä voi yrittää murtautua tilille arvaamalla salasanan. Neskeyn (2022) mukaan MD5 tiivistealgoritmilla suojatun 8-merkkisen salasanan, joka sisältää numeroita, isoja sekä pieniä kirjaimia ja erikoismerkkejä voi pilvipalvelun laskentateholla murtaa 39 minuutissa (Neskey, 2022). Käyttäjätilin kaappaus voi tapahtua F-Securen (n.d.) mukaan myös haittaohjelman tai viruksen kautta, mikäli käyttäjän laite on saastunut (F-Secure, n.d.).

Kyberturvallisuuskeskus (2022) varoitti Facebook-käyttäjätilien tunnusten kalastelusta sekä tilien kaappaamisesta, joissa hyökkääjä lähettää uhrille viestin Facebook Messengerin kautta saadakseen hänen puhelinnumeronsa. Puhelinnumeron saamisen jälkeen

hyökkääjä kertoo käyttäjälle, että hän on osallistunut kilpailuun, jolloin käyttäjä vastaanottaa tekstiviestin arvontaan liittyen. Tekstiviesti sisältää koodin, jolla hyökkääjä ottaa käyttäjätilin haltuunsa ja vaihtaa salasanat sekä muut kirjautumistiedot, jolloin hyökkäystä voidaan jatkaa juuri kaapatulla tilillä. (Kyberturvallisuuskeskus, 2022)

2.2.2 Identiteettivarkaudet

Identiteettivarkaudella tarkoitetaan tilannetta, jossa esiinnytään toisen henkilön nimellä ja henkilöllisyydellä hyödyntäen yksilöivää tietoa. Rikosuhripäivystyksen (n.d.) mukaan toisen nimellä tehdyn tilauksen tai sopimuksen katsotaan täyttävän identiteettivarkaudelle asetetut kriteerit. Identiteettivarkaus on rangaistava teko, jos siitä on aiheutunut suurta haittaa tai taloudellista vahinkoa uhrille. Toisen identiteetillä esiintyminen ja sillä hyödyn hankkiminen tai haitan tekeminen voivat johtaa myös muihin rikosnimikkeisiin, kuten identiteettivarkaus, kunnianloukkaus, petos tai yksityiselämää loukkaavan tiedon levittäminen. (Rikosuhripäivystys, n.d.)

Tilastokeskuksen (2022) mukaan identiteettivarkaus lisättiin rikoslakiin vuonna 2015, jolloin siitä tehtiin 530 rikosilmoitusta. Vuonna 2021 identiteettivarkauksista tehtiin rikosilmoituksia 3300 kappaletta. (Tilastokeskus, 2022) Vakuutuspalvelu MySafetyn (2021) maaliskuussa 2021 suorittamassa haastattelussa Rikosuhripäivystyksen kehitysjohtaja Jaana Koivukangas kertoi, että kaikki uhrit eivät välttämättä tiedä identiteettivarkauden olevan rikos, eivätkä uhrit monesti ilmoita rikoksesta, ellei siitä ole tapahtunut taloudellista haittaa (MySafety, 2021).

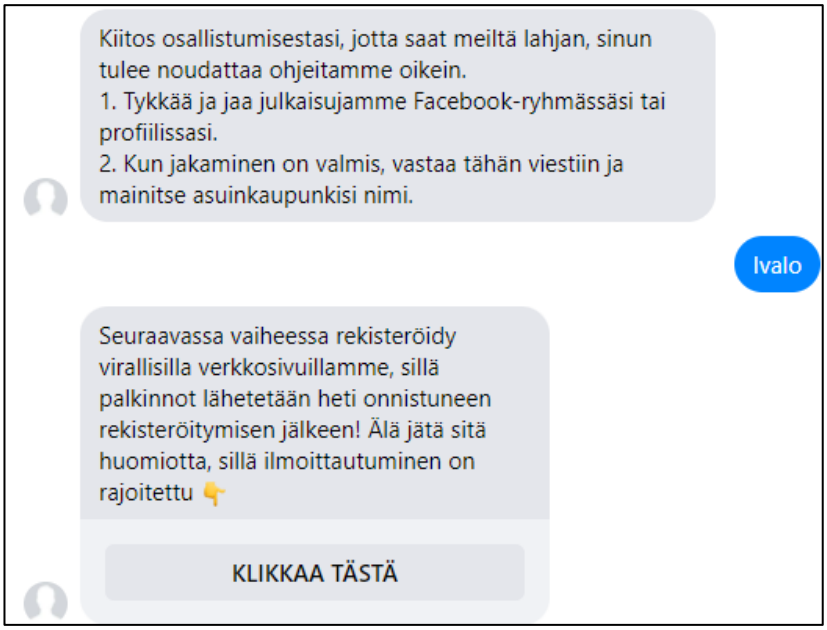
Identiteettivarkaudet eivät ole harvinaisia sosiaalisessa mediassa, sillä monella käyttäjällä on esillä paljon avointa tietoa itsestään ja käyttäjän profiili on helppo kopioida esiintyäkseen kyseisenä henkilönä. Rafterin (2020) mukaan identiteettivarkauksissa usein hyökkääjän motiivina toimii raha, jolloin toisen identiteetillä tehdään useasti tilauksia tai pyydetään rahaa uhrin sosiaalisen median verkoston kautta (Rafter, 2020).

2.3 Valearvonnat ja tilausansat

Valearvonnat ovat sosiaalisessa mediassa levitettäviä “arvontoja”, jotka johdattelevat käyttäjän luovuttamaan tietojaan tai asentamaan haittaohjelman laitteelle. Valearvontojen järjestäjät luovat sosiaaliseen mediaan väärennetyn sivuston tunnetun yrityksen tai brändin nimellä. Tunnetun yrityksen tai brändin nimellä järjestetty arvonta luo julkaisulle uskottavuutta, jolloin on helpompi saada käyttäjä osallistumaan valearvontaan.

Kuva 1 *Kuvakaappaus: R-Kioskin nimissä oleva valearvonta* (R-Kioski, 2021)

Kuvassa (Kuva 1) on esimerkki Facebook-palvelussa kiertävästä valearvonnasta, jossa tekeydytään R-Kioskiksi. Arvonnassa luvataan sadalle ensimmäiselle oikein arvanneelle 500 € palkinnoksi. Valearvonnoissa pyritään usein jäljittelemään yrityksen teemaa sekä lupaamaan suuria palkintoja käyttäjien kiinnostuksen lisäämiseksi.



Kuva 2 *Kuvakaappaus: valearvonnan yhteydenotto (Merisalo, 2021)*

R-Kioskin nimissä tehdyn valearvonnan julkaisuun kommentoijat saavat yhteydenoton Facebookin Messengerissä (Kuva 2), jossa käyttäjää pyydetään tykkäämään julkaisusta

sekä jakamaan sitä eteenpäin, jonka jälkeen pyydetään rekisteröitymään ulkoiselle sivustolle palkinnon lunastamiseksi. Sivustolla käyttäjältä voidaan kalastella tietoja tai sitoa käyttäjä tilausansaan.

Tilausansalla tarkoitetaan tilannetta, jossa käyttäjä sitoutuu tietämättään tilaamaan jonkin esineen tai palvelun, jota ei ole todellisuudessa halunnut. Kyberturvallisuuskeskus (2019) varoitti käyttäjiä eri kuluttajapalveluiden nimillä tehdyistä huijauksista, joissa viestit muotoillaan vastaamaan palvelun normaalia viestiä. Huijauksissa on käytetty hyväksi esimerkiksi Postin saapumisilmoitusta, jolloin käyttäjä voidaan tietämättään johdatella rekisteröitymään sivustolle jonkin palvelun tilaajaksi. (Kyberturvallisuuskeskus, 2019)

2.4 Disinformaatio, valeuutiset ja vaikuttaminen

Disinformaatio on Wigmoren (2013) mukaan valheellista tietoa, jota levitetään tarkoituksellisesti ja tietoa pyritään esittämään totuutena. Disinformaatiolla pyritään aiheuttamaan vahinkoa tai haittaa, sekä valheellisen tiedon avulla pyritään vaikuttamaan lukijan mielipiteeseen aiheesta. (Wigmore, 2013) Disinformaatio käsitettä ei tule kuitenkaan sekoittaa misinformaation kanssa, koska käsitteiden sisällön voi erottaa julkaisijan agendasta. Disinformaatio on tarkoituksellista ja misinformaatio tarkoituksetonta valheellisen informaation jakamista. Straussin (2018) mukaan misinformaatiota jakaessaan ihmiset itse uskovat usein tiedon sisällön olevan totta, jolloin valheellisen informaation jakaminen on tarkoituksetonta (Strauss, 2018). Misinformaatiota voidaan vähentää huomattavasti tarkistamalla jaetun sisällön lähteet sekä vertaamalla jaettua sisältöä muihin saman aiheisiin julkaisuihin. Käyttäjä voi vähentää valheellisen informaation kohteeksi joutumista tarkistamalla tiedon lähteet sekä vertaamalla sitä muihin aiheesta jaettuihin tietoihin.

Valeuutiset ovat yksi disinformaation muoto, jolloin valeuutisilla pyritään vääristelemään uutisessa käsiteltyä aihetta. Valeuutiset ovat internetissä levitettäviä uutisia, jotka sisältävät valheellista tai harhaanjohtavaa informaatiota. Valeuutisen tunnusmerkit täyttävät myös sellaiset uutiset, jonka henkilö tai sivusto on jakanut luulleen esitetyn asian olevan faktaa, mutta ei ole huolella tarkastanut lähteitään ja sisältö paljastuukin valheeksi. Sosiaalisen median käytön kasvaessa myös valeuutisten määrä on kasvanut, ja nykyään valeuutisia pystytään levittämään laaja-alaisesti sekä nopeasti sosiaalisen median verkostoissa. Valeuutisilla voidaan yrittää vaikuttaa ihmisten mielipiteisiin tietyistä asioista sekä harjoittaa myös niiden avulla tietojenkalastelua.

Tilastokeskuksen (2021) mukaan tutkimukseen vastaajista 63 % on nähnyt epätosia tai epäilyttävää sisältöä uutissivustoilla tai sosiaalisessa mediassa. Kuitenkin vain 31 % tutkimuksen vastaajista ovat tarkastaneet sisältöjen todenperäisyyden (Tilastokeskus,

2021). Tutkimus vahvistaa olettamusta siitä, että valeuutiset ovat yleinen ongelma sosiaalisessa mediassa. Huomioitavaa tutkimuksessa on kuitenkin se, että vain alle puolet vastaajista olivat tarkistaneet sisällön todenmukaisuuden.

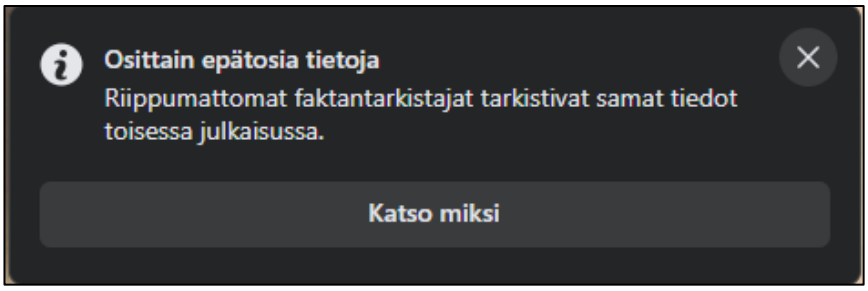
Valeuutiset on käsitteenä laaja ja se voidaan jakaa monen tyyppisiin uutisiin. Bothan ja Pietersen (2020) mukaan sosiaalisessa mediassa on useampaan eri kategoriaan kuuluvia valeuutisia. Yleisimpiä valeuutisten muotoja ovat “klikkiotsikot”, joissa lukija houkutellaan klikkaamaan uutinen auki houkuttelevalla otsikolla, joka ei juurikaan edes liity uutiseen. Tällä tavalla saadaan vierailijoita valheelliselle sivustolle. Mielipiteen muuttamiseen ja poliittisen agendan ajamiseen tarkoitetut valeuutiset voidaan luokitella “propagandaksi”. Tarkoituksella ja huumorimielessä tehtyjä valeuutisia voidaan kutsua “satiireiksi”, jotka ovat tarkoitettu olemaan harmittomia, mutta voivat silti olla harhaanjohtavia lukijalle. Huonolaatuiset uutiset sekä tarkistamattomista lähteistä kootut tiedot täyttävät valeuutisen vaatimukset. Huonolaatuiset uutiset eivät tarkoituksella levitä väärää tietoa, mutta tarkistamattomat faktat voivat johdattaa lukijan harhaan. (Botha & Pieterse, 2020)

Kaspersky (2021) varoittaa valeuutisten leviämisestä sosiaalisen median alustoilla bottien välityksellä. Bottien avulla voidaan sosiaaliseen mediaan luoda valetilejä, joille kerätään seuraajia ja näkyvyyttä, jonka myötä valheellisen tiedon levittäminen on helppoa isossa verkostossa. Usein sosiaalisen median alustat näyttävät ensin suosittuja julkaisuja sekä uutisia, jolloin esimerkiksi houkuttelevien klikkiotsikoiden levittäminen on helpompaa. (Kaspersky, 2021)

Valeuutisissa voidaan hyödyntää myös syväväärennöksiä (“deepfakes”), jolloin uutisesta saadaan uskottavampi ja houkuttelevampi. Bothan ja Pietersen (2020) mukaan syväväärennökset nousivat ihmisten tietoisuuteen internetin Reddit nimisen keskustelualustan kautta vuonna 2017, jossa käyttäjä u/deepfakes perusti sivustolle yhteisön nimeltä r/deepfakes. Yhteisössä luotiin algoritmeilla väärennettyjä videoita, jotka vaikuttavat aidoilta ja realistisilta, mutta videolla olevaa tapahtumaa ei ole koskaan oikeasti tapahtunut. (Botha & Pieterse, 2020)

Valeuutisilla vaikuttaminen on kasvava ongelma sosiaalisessa mediassa. Tämä ongelma on näkynyt esimerkiksi koronapandemian ja Ukrainan sodan aikana, jolloin liikkeellä on ollut paljon valheellista informaatiota. Kriiseihin liittyvää valheellista informaatiota on alettu suodattamaan sekä poistamaan sosiaalisen median palveluiden toimesta. Rosenin (2021) mukaan Facebook on poistanut valheellista informaatiota sisältävää sisältöä jo 20 miljoonan kappaleen verran koronapandemian alusta kesäkuuhun 2021

mennessä. Yli 3000 käyttäjätiliä tai sivustoa on poistettu palvelusta jatkuvien rikkomusten takia liittyen esimerkiksi koronavirusta koskevaan valheelliseen informaatioon (Rosen, 2021).



Kuva 3 *Facebook: valeuutisen varoitus (Facebook, 2021)*

Sosiaalisen median alustat ovat alkaneet tarkistamaan julkaisujen sekä sisältöjen todenmukaisuutta. Monilla alustoilla on käytössä valheellisesta informaatiosta varoittavat merkinnät, esimerkiksi kuvassa (Kuva 3) esitetään, kuinka Facebook varoittaa käyttäjää valheellista informaatiota sisältävän julkaisun sisällöstä.

Freiling et al. (2021) mukaan sosiaalisessa mediassa käyttäjät uskovat enemmän sellaisiin uutisiin, jotka ovat jonkin tunnetun henkilön jakamia, sekä uudelleenjakavat uutisia, mikäli ne tukevat omaa ideologiaa (Freiling et al., 2021). Uutisen todenmukaisuutta arvioitaessa käyttäjän mielipiteet voivat vaikuttaa negatiivisesti omaan arviointikykyyn, jolloin omaa ideologiaa tukevat uutiset voivat tuntua todenmukaisemmilta. Käyttäjän oma mielipide asiaan vaikuttaa uutisen todenperäisyyden arviointiin, jolloin voi tulla tilanne, että käyttäjä uskoo valheellista informaatiota uutisen tukiessa omaa ideologiaansa.

2.5 Kriisien vaikutus sosiaalisen median tietoturvaan

Hyökkääjät hyödyntävät usein uhrien inhimillisyyttä hyökkäyksissä sekä huijauksissa kriisien aikana. Hyökkääjän on helppo käyttää edukseen ihmisen perusominaisuuksia, esimerkiksi luottamusta, ihmisen avuliaisuutta sekä epätietoisuutta kriisin vallitessa.

Kriisit ovat lisänneet valheellisen informaation määrää sosiaalisessa mediassa, jolloin käyttäjien on vaikeampaa varmistaa tiedon todenmukaisuus. Kriisien avulla on tehty huijauksia sosiaalisessa mediassa sekä sähköpostitse, joissa usein vedotaan kiireeseen ja kriisin aiheuttamaan avun tarpeeseen.

2.5.1 Koronapandemia

Koronavirustauti COVID-19 on herkästi leviävä, mutta useimmiten lieviä oireita aiheuttava tauti. Useimmiten taudin oireisiin kuuluvat kuume, väsymys ja yskä, mutta virus voi

myös aiheuttaa maku- sekä hajuaistin tilapäisen katoamisen. WHO:n (n.d.) mukaan vaikeammissa tapauksissa oireisiin voi kuulua erinäiset kiputilat sekä hengitystievaikeudet. (WHO, n.d.).

Suomessa koronapandemian aikana varmistettuja tartuntoja on Terveyden ja hyvinvoinnin laitoksen THL (2022) maaliskuussa 2022 julkaiseman raportin mukaan hieman yli 713 000 (THL, 2022). Euroopan tautienehkäisy- ja valvontakeskuksen ECDC (2022) maaliskuussa 2022 julkaiseman raportin mukaan maailman laajuisesti varmistettuja tartuntoja on yli 446 miljoonaa ja viruksen aiheuttamia kuolemia on yli 6 miljoonaa (ECDC, 2022). Anttilan (2021) mukaan koronavirus COVID-19 lähti väitetysti liikkeelle Kiinasta Wuhanin kaupungista joulukuussa 2019, jonka jälkeen virus levisi maailmanlaajuiseksi epidemiaksi. Laajalti levinnyt virus julistettiin pandemiaksi 11.3.2020 terveysjärjestö WHO:n toimesta. (Anttila, 2021)

Trend Micron (2022) vuonna 2021 julkaisemassa raportissa kerrotaan pandemiarajoitusten myötä lisääntyneen etätyön vaikuttaneen voimakkaasti tietojenkalastelun määrään. Raportissa kerrotaan myös, että sähköpostitse leviävä tietojenkalastelu on kasvanut vuonna 2021 melkein seitsemänkertaiseksi vuoteen 2020 verrattuna. (Trend Micro, 2022)

Koronaviruspandemian varjolla on levitetty haittaohjelmia sekä harjoitettu tietojenkalastelua sähköpostitse. Tidyn (2020) mukaan käyttäjiä on johdateltu klikkaamaan tietojenkalastelusivustolle johtavaa linkkiä sekä joissain tapauksissa on pyydetty lataamaan haittaohjelman sisältävä sähköpostin liitetiedosto. Hyökkäyksissä on esiinnytty terveysviranomaisena ja tällä tavoin on pyritty saamaan uhrin luottamus. (Tidy, 2020) Kuluttajaliiton (n.d.) ohjeistuksessa kerrotaan maailmalla liikkuvan useita erilaisia huijausviestejä, joiden tarkoituksena on käyttää hyödyksi koronaviruksen aiheuttamaa pelkoa sekä siihen liittyvää epätietoisuutta. Käyttäjien on suotavaa ilmoittaa harhaanjohtavasta markkinoinnista ja kohtaamistaan huijauksista viranomaisille. (Kuluttajaliitto, n.d.)

Veerasamyn (2021) mukaan tietojenkalastelua on harjoitettu koronaviruspandemiaan liittyen ainakin sähköposteilla, tekstiviesteillä sekä sosiaalisessa mediassa. Käyttäjiä on johdateltu klikkaamaan linkkejä, jotka johtavat ulkoiselle sivustolle erityisesti vedoten tärkeään informaatioon koronaviruspandemiaa koskien. Hyökkäyksissä esitetään viestin tai julkaisun tulleen viranomaiselta, jotta käyttäjä luottaisi saamaansa viestiin ja luulee linkkiä tai sivustoa turvalliseksi. (Veerasamy, 2021)

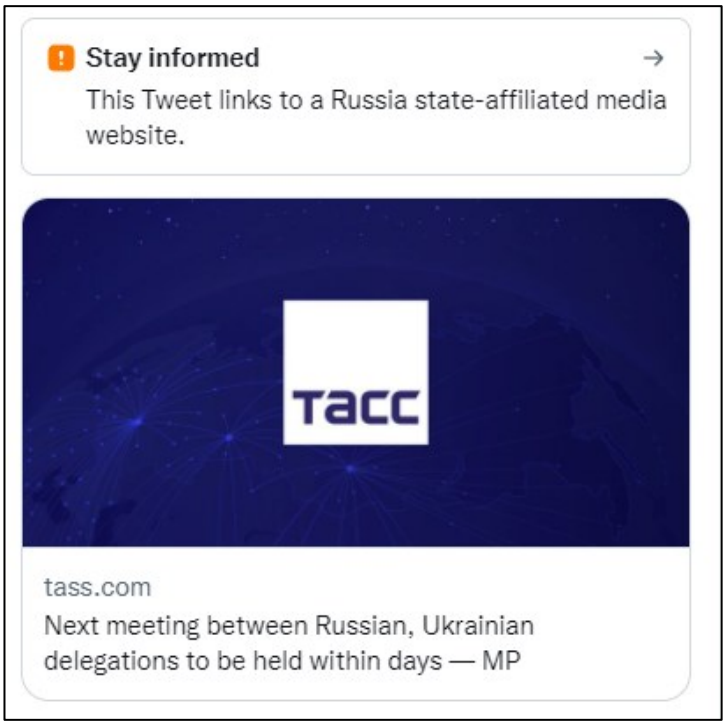
Viruksesta on saatavilla paljon informaatiota useista eri lähteistä, jolloin luotettavan tiedon löytäminen sekä tiedon oikeellisuuden tarkastaminen voi olla haasteellista. Monilla sosiaalisen median alustoilla on otettu käyttöön koronavirukseen liittyville sisällöille omat

ohjeistuksensa, jonka vuoksi palvelut poistavat sekä suodattavat valheellista sisältöä. Euroopan komission (n.d.) mukaan koronaviruksesta on levitetty paljon disinformaatiota, kuten esimerkiksi “valkaisuaineen juomisen parantava vaikutus koronaan sairastuessa” ja erilaiset teoriat koronaviruksen alkuperästä (Euroopan komissio, n.d.).

Sosiaalisen median alustat tekevät yhteistyötä Euroopan komission (n.d.) kanssa todenmukaisen tiedon välittämiseksi sekä valheellisen informaation karsimiseksi. Euroopan komissio on tiukentanut disinformaatiota koskevia käytännesääntöjä, jolloin esimerkiksi Google, Twitter, Microsoft ja Facebook ovat terveysviranomaisten avulla jakaneet tietoa aktiivisesti ja suodattaneet disinformaatiota. (Euroopan komissio, n.d.)

2.5.2 Venäjän hyökkäys Ukrainaan

Ukrainan kriisi alkoi Venäjän aloitettua hyökkäyksen Ukrainaan helmikuussa 2022, jolloin informaatiosodankäynti alkoi molempien osapuolten toimesta. Konfliktin osapuolet pyrkivät vaikuttamaan julkaistuilla sisällöillä yleiseen mielipiteeseen sekä omien- ja vihollisjoukkojen taistelutahtoon. Suurin osa Suomessa käytössä olevista sosiaalisen median palveluista ovat länsimaisia, jolloin luotettavampana pidetään Ukrainan näkökantaa asioista. Tietoturva-arjessa kaikkien osapuolten julkaisemaa sisältöä tulee tulkita kriittisesti, ja päätellä mikä tiedosta on totuudenmukaista sekä mikä sisältö ajaa jotakin agendaa. Molempien osapuolten julkaisut konfliktin uhriluvuista vaihtelevat huomattavasti, jolloin voidaan käyttää sanontaa “totuus on jossain siltä väliltä”. Valtiolliseen mediaan kytköksissä olevien tilien sisältöihin on alettu merkitsemään huomautuksia sosiaalisen median palveluiden toimesta. Kuvassa (Kuva 4) on esimerkkinä kuvakaappaus Twitterissä jaetusta sisällöstä, jossa huomautetaan linkin johtavan Venäjän valtioon kytkeytyvän median sivustolle.



Kuva 4 *Twitter: huomautus valtioon kytköksissä olevasta mediasta (FoxBat, 2022)*

Bîzgă (2022) kertoo Ukrainan konfliktin tuoneen esiin uusia hyökkäyksiä kohteenaan yritykset sekä yksityishenkilöt. Yksityishenkilöihin kohdistuvia huijauksia on toteutettu hyväntekeväisyyskeräysten muodossa lähestymällä uhria sähköpostitse vedoten humanitääriseen kriisiin. Keräyksissä on huijattu ihmisiltä ainakin Bitcoin-, Ethereum- ja Tether-kryptovaluuttaa, mutta myös muitakin kryptovaluuttoja on pyydetty huijausviesteissä. Ukrainan kriisiin vedoten moniin yrityksiin on kohdistunut hyökkäyksiä sähköpostin välityksellä, jolloin viestin liitetiedostona yritykselle on lähetetty haittaohjelmia. Viesteissä vedotaan Ukrainassa olevaan kriisiin ja pyydetään uhria avaamaan haittaohjelman sisältävä liitetiedosto. Haittaohjelma voi kerätä esimerkiksi käyttäjätietoja, leikepöydän sisältöä ja rekisteröidä näppäinpainalluksia, mutta haittaohjelman avulla voidaan ottaa myös koko uhrin laite hallintaan. (Bîzgă, 2022)

Verkossa on olemassa paljon keräyksiä Ukrainan väestön auttamiseksi, jolloin oikean keräyksen erottaminen huijauksesta on vaikeaa. Valekeräyksiä on Ukrainan kriisin varjolla lähes jokaisella verkossa toimivalla sosiaalisen median alustalla, joten keräykseen lahjoittaessa tulee aina varmistaa keräyksen pitäjän luotettavuus.

3. SOSIAALISEN MEDIAN ALUSTAT

Sosiaalisen verkostoitumisen alustat tarjoavat käyttäjilleen mahdollisuuden löytää yhteisöjä ja kavereita sekä jakaa sisältöä näiden kesken. Sosiaalisen median alustoja voidaan jaotella erilaisiin ryhmiin sen mukaan, minkälaista sisältöä käyttäjät voivat palvelussa jakaa.

Sosiaalisen median alustoilla käyttäjät voivat jakaa päivityksiä, medioita sekä blogijulkaisuja keskenään. Nykyiset pikaviestisovellukset tarjoavat yleisimpien sosiaalisten medioiden tavoin yhteisöjen välistä keskustelua sekä laajat mahdollisuudet median ja sisällön jakamiseen.

3.1 Facebook

Facebook on Mark Zuckerbergin vuonna 2004 perustama sosiaalisen verkostoitumisen palvelu. Phillipsin (2007) mukaan syyskuussa vuonna 2006 palvelu avattiin kaikille käyttäjille, jonka ainoana vaatimuksena palvelun käyttämiseen oli sähköpostiosoite. (Phillips, 2007).

Facebook on keskittynyt sosiaaliseen verkostoitumiseen, joten palvelun olennaisena osana on tarjota käyttäjilleen mahdollisuus tavata kavereita, pitää yhteyttä heihin ja seurata kiinnostavia yhteisöjä tai ryhmiä. Palvelussa käyttäjä voi keskustella muiden käyttäjien kesken, jakaa päivityksiä, pelata pelejä sekä jakaa kaikenlaista mediasisältöä. Facebook on ilmainen ja rahoittaa toimintaansa mainoksilla. Facebookin omistaa Meta Plaftforms Inc., jonka toimitusjohtajana toimii Facebookin perustaja Mark Zuckerberg.

DataReportalin (2021) lokakuussa 2021 laatiman analyysin perusteella palvelulla on 2,91 miljardia aktiivista käyttäjää ja se on käyttäjämäärältään maailman aktiivisin sosiaalisen median alusta (DataReportal, 2021).

Abramsin (2021) mukaan Facebook-palveluun on tehty tiedettävästi ainakin yksi suuri tietomurto, jossa vietiin 533 miljoonan käyttäjän tietoja. Tietomurrossa saadussa datassa on havaittu ainakin seuraavia käyttäjätietoa: puhelinnumero, nimi, sukupuoli, siviilisääty, ammatti, syntymäaika, sijainti sekä sähköposti. Varastettuja tietoja myytiin ensimmäisen kerran kesäkuussa vuonna 2020. Asiantuntijoiden mukaan tietomurto on kuitenkin tapahtunut jo vuonna 2019 Facebookin haavoittuvuuden kautta. Suomalaisia käyttäjiä on vuodetuissa tiedoissa n. 1,4 miljoonaa. (Abrams, 2021)

3.2 Twitter

Twitter on “microbloggaamiseen” tarkoitettu palvelu, joka on perustettu vuonna 2006. Kempin (2021) mukaan Twitterissä on 211 miljoonaa aktiivista käyttäjää (Kemp, 2021b). Twitterissä käyttäjät voivat julkaista päivityksiä, joiden maksimipituus on 280 merkkiä.

Twitterin (2021) mukaan palvelu taistelee aktiivisesti valeuutisia ja valheellista informaatiota vastaan varoittamalla käyttäjiään sekä poistamalla palvelusta haitallista sisältöä. Twitterin (2021) mukaan tammikuussa 2020 julkaistun koronaviruspandemiaa koskevan valheellisen informaation linjauksen jälkeen palvelu on poistanut yli 72 000 julkaisua, ja tämän lisäksi yli 4100 tiliä on jäädytetty (Twitter, 2021).

3.3 Instagram

Instagram on sosiaalisen median palvelu, joka tarjoaa käyttäjilleen mahdollisuuden jakaa kuvia ja videoita sekä kommentoida sisältöjä. Instagram tuottaa mainostuloilla voittoa palvelun ollessa käyttäjilleen ilmainen. Kempin (2021) mukaan Instagramilla on käyttäjiä n. 1,39 miljardia, joista 2,1 miljoonaa käyttäjää on Suomesta (Kemp, 2021c).

Mottolan (2016) mukaan Instagram-palvelu julkaistiin kuudes päivä lokakuuta vuonna 2010. Instagramia on syytetty kilpailevien sovellusten kopioimisesta, josta esimerkkinä toimii Snapchatista kopioitu “stories” ominaisuus, missä käyttäjä voi jakaa lyhyen videon seuraajilleen. Instagram kutsuu myös tätä ominaisuutta “stories” nimellä. (Mottola, 2016) Facebookin (2012) mukaan yhtiö osti Instagram-palvelun vuonna 2012 (Facebook, 2012). Palvelun omistaa nykyisin Meta Plaftforms Inc Facebookin tekemän nimenvaihdon jälkeen.

Instagram on ollut useasti esillä tietovuotojen ja tietomurtojen johdosta. Cobbsin (2017) mukaan vuonna 2017 palvelusta löytyi bugi, jonka avulla hyökkääjät saivat haltuunsa noin kuuden miljoonan käyttäjän puhelinnumeroita sekä sähköpostiosoitteita (Cobbs, 2017). Paulin (2019) mukaan Facebook ilmoitti maaliskuussa vuonna 2019, että yritys oli varastoinut yhteensä satojen miljoonien käyttäjien salasanoja salaamattomana Facebook- ja Instagram-alustoillaan. Facebook kertoi, että ainakin Instagram-palvelun salasanoja oli säilytetty luettavassa muodossa. (Paul, 2019) Whittaker (2019) kertoo vuonna 2019 tapahtuneesta Instagramin tietovuodosta, jossa käyttäjien tietoja levisi huonosti konfiguroidun Amazon Web Services -tietokannan kautta. Tietovuodon vuoksi noin 350 tuhannen Instagram-vaikuttajan käyttäjätietoja oli vapaasti saatavilla tietokannasta. Tietokannan omisti sosiaalisen median markkinointiyritys Chtrbox, joka otti verkkolehti TechCrunchin yhteydenoton jälkeen tietokannan kokonaan pois verkosta. (Whittaker, 2019).

3.4 WhatsApp

WhatsApp on pikaviestipalvelu, joka on saatavilla mobiililaitteille sekä tietokoneelle. WhatsAppin (2022) mukaan palvelulla on tällä hetkellä jo yli 2 miljardia käyttäjää (WhatsApp, 2022). Summersin (2020) mukaan Facebook osti palvelun helmikuussa vuonna 2014 (Summers, 2020).

WhatsApp on kehittänyt palvelun tietoturvaa aktiivisesti. WhatsAppin (2019) mukaan palveluun lisättiin vuonna 2016 päästä päähän salaus eli “end-to-end encryption”, sinä vuonna palvelussa oli jo miljardi käyttäjää kuukaudessa (WhatsApp, 2019).

Kyberturvallisuuskeskus (2020) varoitti sivuillaan WhatsApp-tilien kaappausyrityksistä, joissa käyttäjiä on lähestytty aktiivisesti viesteillä, joilla yritetään kalastella WhatsApp-viestisovelluksen vahvistuskoodia. Hyökkääjä kertoo uhrille lähettäneensä vahingossa uhrille tekstiviestin, jossa on kuusi numeroa ja uhrin tulee kertoa kyseinen numerosarja hyökkääjälle, jolloin hyökkääjä voi kaapata uhrin tilin. Vahvistuskoodia on yritetty kalastella myös tekeytymällä sovelluksen tukihenkilöksi sekä harvemmissa tapauksissa kalastelua on tapahtunut myös puhelinvastaajan avustuksella. (Kyberturvallisuuskeskus, 2020b)

Hernin (2021) mukaan WhatsApp menetti miljoonia käyttäjiä vuoden 2021 alussa, kun sovellus muutti käyttöehtojaan. Monet käyttäjät vaihtoivat kilpaileviin sovelluksiin kuten Telegram ja Signal. Sovelluksen uudet käyttöehdot ovat luovuttaneet lisää käyttäjädataa emoyhtiö Facebookin käytettäväksi. Käyttäjästä luovutettavia tietoja voivat olla esimerkiksi käyttäjän puhelinnumero, kontaktit, sekä WhatsApp-viestisovelluksen käyttötottumuksia koskevat tiedot. Sovellus siirsi uuden käyttöehtopäivityksen julkaisemista myöhemmäksi suunnitellusta tammikuusta saman vuoden toukokuuhun, jolloin uudet käyttöehdot astuivat voimaan toukokuun 15. päivä. (Hern, 2021) WhatsApp (n.d.) on ilmoittanut, että mikäli käyttäjä ei hyväksy uusia käyttöehtoja, ei käyttäjän tiliä kuitenkaan poisteta eikä toimintaa rajoiteta (WhatsApp, n.d.).

3.5 Telegram

Telegram on pikaviestisovellus, josta on Telegramin (n.d.) mukaan versiot iOS-, Android-, Windows-, Linux- ja macOS-käyttöjärjestelmille sekä web-selaimelle. Sovelluksen ensimmäinen versio julkaistiin elokuussa vuonna 2013. (Telegram, n.d.-b) Telegramin (2021) mukaan palvelu on tarjonnut “end-to-end” eli päästä päähän salausta keskusteluihin jo lokakuusta 2013 lähtien (Telegram, 2021). Telegramin (n.d.) mukaan sovelluksen nykyversioissa viestien salaukseen on käytetty AES-256 salausta (Telegram, n.d.-a).

Telegram tukee botteja, eli ohjelmia, jotka suorittavat automatisoituja sekä ennalta määritettyjä tehtäviä. Boteilla voidaan automatisoida toimintoja tai esimerkiksi viihdyttää sovelluksen käyttäjää. Telegramin suosion kasvaessa botteja on alettu käyttämään myös tietojenkalastelun apuvälineenä. O'Donnellin (2021) mukaan vuonna 2020 Telegram-bottien avulla käyttäjiltä huijattiin ainakin 6,5 miljoonaa dollaria. Botit kommunikoivat itsenäisesti käyttäjien kanssa ja voivat esimerkiksi jakaa linkkejä sivustoille, joissa kalastellaan tietoja. Esimerkkitapauksessa käyttäjää johdatellaan ansaan "myymällä" jotain tuotetta halvalla. Ostaakseen tuotteen käyttäjän tarvitsee ottaa yhteys myyjään Telegramin kautta, jolloin botti keskustelee käyttäjän kanssa ja ohjaa tämän saastuneelle sivustolle tietojen kalastelemiseksi. (O'Donnell, 2021)

3.6 TikTok

TikTok on kiinalaisen ByteDance-yrityksen kehittämä sovellus, joka julkaistiin syyskuussa vuonna 2016. Sovelluksessa käyttäjät voivat jakaa lyhyitä videoita, joiden kesto on 15–60 sekuntia. D'Souzan (2021) mukaan TikTokin kasvu alkoi vuonna 2018 kun TikTok sai paljon käyttäjiä ostaessaan kilpailevan sovelluksen nimeltä Musical.ly ja siirsi 200 miljoonaa käyttäjää omaan sovellukseensa (D'Souza, 2021). TikTok (2021) ilmoitti vuonna 2021, että sovelluksella on jo yli miljardi kuukausittaista käyttäjää (TikTok, 2021). Kempin (2021) raportin perusteella voidaan päätellä, että sovellus on erityisesti nuorten käyttäjien suosiossa, sillä käyttäjistä suurin osa (44,8 %) on 18–24-vuotiaita (Kemp, 2021a).

TikTok on saanut kritiikkiä misinformaation levittämisestä, sillä palvelussa on levinnyt koronaviruspandemiaa sekä Ukrainan kriisiä koskevaa misinformaatiota. Kaplanin (2020) mukaan palvelussa on esiintynyt paljon salaliittoteorioita sekä valheellista informaatiota, vaikka TikTok on kertonut taistelevansa aktiivisesti misinformaatiota vastaan (Kaplan, 2020). Hernin (2022) mukaan TikTokissa on mahdollista törmätä Ukrainan sodasta kertoviin valeuutisiin pelkästään selaamalla uutta sisältöä. Toimittajat loivat täysin uudet tilit palveluun ja selasivat ainoastaan palvelun syötettä, jolloin jo 45 minuutin kohdalla algoritmi ehdotti käyttäjilleen videoita, jotka sisälsivät valheellista informaatiota Ukrainan sodasta. (Hern, 2022) Huomioitavaa palvelun algoritmissa on myös se, että vaikka käyttäjä ei hae tai seuraa valheellista sisältöä, voi palvelu silti näyttää sellaista käyttäjilleen.

3.7 YouTube

YouTube on Googlen omistama videopalvelu ja sosiaalisen median alusta, jonka ensimmäinen versio on avattu vuonna 2005. YouTuben (2010) mukaan Google osti palvelun

lokakuussa vuonna 2006 (YouTube, 2010). YouTubella on DataReportalin (2022) mukaan 2,56 miljardia käyttäjää. YouTube on käyttäjämäärältään toiseksi suurin sosiaalisen median palvelu. (DataReportal, 2022).

YouTube (n.d.) mukaan palvelu suodattaa jatkuvasti alustalle lisättyä sisältöä ja tarvittaessa poistaa sieltä sisältöä, kanavia sekä kommentteja. Helmikuuhun 2022 mennessä YouTube on poistanut jo 3,85 miljoonaa kanavaa. Vuonna 2021 lokakuun ja joulukuun välisellä ajanjaksolla pelkästään poistettuja kanavia on ollut yli 77 000. Yhteisön sääntöjä rikkovia kommentteja YouTube on helmikuuhun 2022 mennessä poistanut jo 1,2 miljardia, joista suurin osa on poistettu automaattisesti ilman käyttäjien ilmoitusta. (YouTube, n.d.)

4. KÄYTTÄJIEN TIETOISUUS SEKÄ KÄYTTÄYTYMINEN

Tietoturvan kannalta tärkeässä osassa pidetään käyttäjän tietoturva-arkea, joka sisältää erilaisia käyttäytymismalleja sekä käyttäjien tietoisuuden ja varautumisen tietoturvariskejä kohtaan. Tietoturva-arki ohjaa käyttäjän jokapäiväistä käyttäytymistä verkossa.

Hyvän tietoturva-arjen omaava henkilö osaa ennakoida tietoturvauhkia sekä tarkastella kriittisesti verkossa esiintyvää sisältöä. Tietoturva-arjessa kokemuksen ja tietoisuuden tuomat käytännöt auttavat käyttäjää toimimaan turvallisemmin myös sosiaalisessa mediassa.

4.1 Tietoisuus ja yksityisyydensuoja

Hossainin sekä Zhangin (2015) tutkimuksessa 44 % sosiaalisen median käyttäjistä eivät olleet tietoisia käyttämänsä sosiaalisen median palvelun tietosuojakäytännöistä. Tutkimukseen vastanneista käyttäjistä 75 % ovat olleet vähintään jonkin verran huolissaan yksityisyydensuojastaan. (Hossain & Zhang, 2015) Tämä vaikuttaa huomattavasti käyttäjien sosiaalisen median tietoturvaan ja siihen, kuinka käyttäjät voivat suojata omaa yksityisyyttään sosiaalisessa mediassa. Sosiaalisen median palvelut panostavat yksityisyysasetuksien kehittämiseen ja tarjoavat käyttäjilleen helppokäyttöisempiä työkaluja omien yksityisyysasetuksien tarkastamiseksi.

Käyttäjän tulisi suunnitella minkälaista sisältöä haluaa julkaista sekä määritellä julkaisuiden yksityisyysasetukset, mikäli käyttäjä haluaa pitää huolta omasta yksityisyydestään. Julkaisuiden kanssa tulee huomioida yksi internetin kirjoittamattomista perussäännöistä: jos internettiin laittaa jotakin, sitä ei saa koskaan pois sieltä.

4.2 Käyttäytyminen ja tietoturva-asenteet

Baker-Eveleth et al. (2021) tekemässä tutkimuksessa selvisi, että yksityisyydensuojaa koskevat kokemukset vaikuttavat suoraan käyttäjän tietoturva-asenteisiin sekä käytäntöihin. Negatiivisen kokemuksen omaava käyttäjä ei luota käyttämäänsä palveluun. Käyttäjän huolestuneisuus omasta yksityisyydestään voi johtaa oman tietoturvan kehittymiseen. (Baker-Eveleth et al., 2021) Tutkimuksesta voidaan päätellä, että oma kokemus tietoturvasta ohjaa käyttäjän tietoturvakäytäntöjä, jolloin positiivisen kokemuksen omaava käyttäjä ei ole niin huolissaan omasta tietoturvan tasosta kuin negatiivisen kokemuksen omaava käyttäjä. Baker-Eveleth et al. (2021) mukaan yksityisyyden suojan

vahvistamiseksi käyttäjille tulisi jakaa muiden negatiivisia kokemuksia tai simuloida yksityisyyden suojaa koskevia skenaarioita, jolloin käyttäjät tarkastelevat yksityisyyden suojaa kriittisesti. (Baker-Eveleth et al., 2021)

Boshmaf et al. (2011) mukaan jopa 80 % käyttäjistä hyväksyvät Facebookissa myös tuntemattomia kavereiksi (Boshmaf et al., 2011). Tuntemattomien käyttäjien hyväksyminen kavereiksi tai seuraajiksi sosiaalisessa mediassa luo riskin tietojenkalastelulle sekä identiteettivarkaudelle. Sosiaalisessa mediassa tulisi tarkastaa oman profiilin sekä julkaisuiden yksityisyysasetukset aina tapauskohtaisesti. Rajoittamisen hyöty katoaa täysin, mikäli käyttäjä hyväksyy myös tuntemattomia käyttäjiä kavereikseen. Khan et al. (2021) mukaan käyttäjistä 70,77 % pitivät sosiaalisen median profiiliaan julkisena kaikkien nähtävillä ja 89,7 % käyttäjistä esiintyivät sosiaalisessa mediassa oikealla nimellään (Khan et al., 2021). Sosiaalisen median profiilin pitäminen julkisena lisää riskiä identiteettivarkaudelle, etenkin jos profiilissa on esillä paljon julkista tietoa sekä käyttäjän omia kuvia.

4.3 Tietoturvauhkien välttäminen

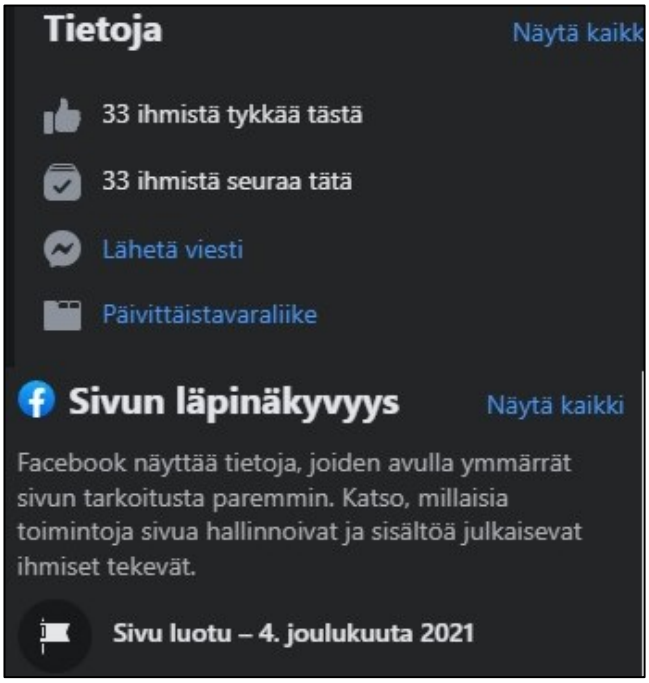
Sosiaalisen median käyttäjätilin yksityisyyttä ajatellen tulee pohtia minkälaista tietoa haluaisi itsestään jaettavan julkisesti tai ystävien kesken sekä mitä tietoja olisi hyvä pitää omana tietonaan. Profiilitietoja kannattaa muokata näiden ajatusten perusteella, jolloin käyttäjän tiedot eivät näy avoimesti. Asetukset tulisi myös tarkastaa julkaisuiden ja muun sisällön kanssa, sillä kaikki julkaisut ja kommentit eivät välttämättä ole tarkoitettu julkiseksi. Täysin julkisella paljon informaatiota sisältävällä profiililla voi olla monia riskejä, sillä esimerkiksi identiteettivarkautta on helppo yrittää, mikäli käyttäjästä on paljon avointa sekä yksilöivää tietoa julkisena. Paljon yksilöivää informaatiota sisältävä julkinen profiili voi johtaa identiteettivarkauden uhriksi, jolloin hyökkääjän on helppo käyttää saatua tietoa hyödykseen.

Microsoftin (n.d.) mukaan sähköpostilla tapahtuvan tietojenkalastelun voi usein tunnistaa kirjoitusvirheistä ja kalastelun yhteydessä saatetaan vedota myös asian kiireellisyyteen. Hyökkääjät yrittävät luoda uskottavuutta esiintymällä jonkin organisaation nimissä, mutta tämän voi tunnistaa tarkistamalla sähköpostiosoitteen, josta sähköposti on lähetetty. (Microsoft, n.d.)

Käyttäjätilin turvaamiseksi käyttäjiä ohjeistetaan valitsemaan vähintään 12-merkkinen salasana. Kaikissa palveluissa suositellaan käyttämään eri salasanaa, jolloin salasanan vuotaessa hyökkääjät eivät pääse kaikkiin palveluihin käsiksi samalla salasanalla. Palveluihin kannattaa ottaa käyttöön myös kaksivaiheinen tunnistautuminen, jolloin palveluun kirjautuessa syötetään kirjautumisen vahvistama koodi.

Sosiaalisessa mediassa identiteettivarkauden riskiä voidaan vähentää säätämällä sosiaalisen median yksityisyysasetuksia, jolloin esimerkiksi kuvat ja julkaisut on hyvä piilottaa julkisesta jakelusta ja jakaa niitä vain oman verkoston kesken. Sosiaalisen median profiilissa näkyvät tiedot kannattaa myös asettaa nähtäväksi vain rajatulle yleisölle. Rafterin (2020) mukaan identiteettivarkautta ajatellen on hyvä aika ajoin hakea tietoa itsestään sosiaalisen median palvelujen hakukoneilla sekä Googlesta, jolloin voi tarkistaa onko omasta profiilista tehty väärennettyjä profiileita (Rafter, 2020).

Valearvonnan tunnistamiseksi voidaan aluksi pohtia, olisiko kyseinen yritys valmis jakamaan näin suuren summan rahaa arvonnassa näkyvyyden vuoksi, eli voidaanko arvonnan palkinnon ajatella olevan realistinen. Tunnetun yrityksen nimissä tehdyn valearvonnan tunnistaa usein myös siitä, että julkaisijalla ei ole profiilissaan Facebookin “vahvistettu” merkkiä.



Kuva 5 *Kuvakaappaus: Väärennetty R-Kioskin Facebook-sivu (R-Kioski, 2021)*

Arvonnan julkaisijan luotettavuus on helppo tunnistaa tarkistamalla kokonaisuudessaan julkaisijan profiili. Kuvassa (Kuva 5) on esitetty kuvassa (Kuva 1) olevan valearvonnan julkaisijan Facebook-sivuston tiedot, josta voidaan nopeasti päätellä sivuston olevan väärennös. Tunnetun yrityksen sivulla olisi paljon enemmän seuraajia sekä tykkäyksiä, jolloin väärennetyn sivun paljastaa myös se, että sivusto on uusi. Esimerkiksi oikealla R-Kioskin Facebook-sivustolla on 99 000 tykkäystä ja sivulla on Facebookin “vahvistusmerkki”. Merkin avulla sivuston kerrotaan olevan vahvistettu ja se on todellinen yrityksen tai brändin sivu.

Misinformaation ja disinformaation vaikutusta pystyy vähentämään huomattavasti, jos käyttäjät tarkistavat jaetun sisällön lähteet sekä vertaavat jaettua sisältöä muuhun samasta aiheesta jaettuun tietoon. Valeuutisia varten kannattaa pohtia ajetaanko uutisella jotain agenda tai pyritäänkö sillä vaikuttamaan johonkin mielipiteeseen.

Bothan ja Pietersen (2020) mukaan syvävääreennetyn videon tai kuvan voi tunnistaa tarkastelemalla kuvaa tarkkaan, jolloin kuvan välkkyminen tai sumentuminen voivat olla merkki syvävääreennöksestä. Syvävääreennöksen voi myös tunnistaa, mikäli henkilön kasvoissa on eri värejä tai kasvon rajat ovat hämärät. (Botha & Pieterse, 2020)

Sosiaalisen median sisällön tarkistamiseksi verkossa on monia ohjeita sekä työkaluja, joista esimerkiksi Urbani (2019) on julkaissut First Draft sivustolla kattavan ohjeen verkossa olevan sisällön varmistamiseksi. Ohjeessa jaetaan sisällön tarkastaminen karkeasti viiteen osaan:

- Sisällön alkuperä
- Lähde
- Julkaisupäivämäärä
- Sijainti
- Motivaatio

Sosiaalisessa mediassa jaetusta sisällöstä kannattaa usein tarkastaa, onko katsomasi sisältö alkuperäinen ja kuka sen on alun perin tehnyt tai julkaissut. Sisällön julkaisupäivä sekä julkaisualusta tulee myös ottaa huomioon sisällön aitoutta tarkastellessa. Monesti sisällön luomisella sekä jakamisella on taustalla jokin motiivi, jolloin aiempien kohtien perusteella voit päätellä miksi sisältö on luotu ja yritetäänkö sillä vaikuttaa johonkin jollain tapaa. (Urbani, 2019)

Urbanin (2019) mukaan mediasisältöjä tarkastaessa kannattaa aluksi hakea kuvia käänteisellä kuvahaulla sekä videoita samoilla avainsanoilla kuin tarkastettavassa sisällössä, jolloin saadaan selville, onko mediasta olemassa muita versioita vai onko tarkastettava sisältö alkuperäinen. (Urbani, 2019)

5. TUTKIMUS SOSIAALISEN MEDIAN TIETOTURVASTA

Tutkimus toteutettiin määrällisenä tutkimuksena ja tutkimuksen aineistohankintamenetelmäksi valikoitui kysely, jonka avulla haluttiin myös haastaa käyttäjiä pohtimaan omaa tietoturvakäyttäytymistään. Kyselyä voidaan verrata Jyväskylän yliopiston (2021) mukaan strukturoituun haastatteluun (Jyväskylän yliopisto, 2021a). Strukturoidussa haastattelussa käyttäjät voivat vastata heille esitettyihin rajattuihin kysymyksiin omasta näkökulmastaan ja tulkita vastauksia muiden vastaajien kesken samalla tavalla. Vastaajille asetetut valmiit vastausvaihtoehdot mahdollistivat esimerkiksi tilastollisten kuvioiden muodostamisen tutkimuskysymysten analysoinnin avuksi.

Kyselyssä tarkasteltiin tavallisen käyttäjän näkökulmaa, joka voi tarkoittaa mitä vain käyttäjää sosiaalisen median alustoilla taustasta riippumatta. Kyselyllä kartoitettiin käyttäjien tietoisuutta tietoturvauhista, käyttäytymistä sekä tietoturvauhkiin varautumisesta.

5.1 Kyselyn toteutus

Kysely toteutettiin osana Kyberturvallisuus 1: perusteet kurssia, johon osallistuneet opiskelijat suorittivat kyselyn haastattelemalla muita osapuolia. Kysely toteutettiin Google Forms –alustalla, johon haastattelija tallensi kyselyn myötä saatuja vastauksia. Kyselylomakkeen (Liite A) kysymykset muodostuivat aiemmin esitettyjen tutkimuskysymysten pohjalta sekä aiempiin tutkimuksiin tutustumalla. Osa kysymyksistä toteutettiin myös avoimina kysymyksinä, jolloin vastaaja voi kertoa kysymykseen vapaamuotoisen vastauksensa. Ennalta asetettujen vastausvaihtojen lisäksi avoimet kysymykset antoivat vastaajille mahdollisuuden tuoda esiin omia näkökulmia ja kokemuksia tietoturva-arjen parantamisesta sekä kyselyn myötä heränneitä ajatuksia. Kyselyyn vastaaminen tapahtui täysin anonyymisti. Vastauksia käsiteltiin tutkijan toimesta täysin luottamuksellisesti eikä vastaajaa voitu yhdistää antamiinsa vastauksiin.

5.2 Kyselyn osiot ja rakenne

Sosiaalisen median tietoturvauhkien sekä käyttäjien tietoisuuden kartoittaminen kyselyn avulla pohjautuivat neljään tutkimuskysymykseen, joiden tehtävänä oli kohdentaa käyttäjille esitettävät kysymykset tiettyihin osa-alueisiin. Tällä tavoin mahdollistettiin myös käytännönläheisen tiedon hankkiminen sosiaalisen median käyttäjistä. Haastattelukysy-

mykset muodostuivat aiempien tutkimusten sekä mediassa esiintyneiden tietoturvauhkien pohjalta. Käyttäjien tietoisuus tietoturvauhkista määrittelee osaltaan käyttäjien toimintaa sosiaalisessa mediassa.

Tutkimuskysymyksiin pohjautuen kyselyssä esitettiin sosiaalisen median käyttäjille muutamaan eri osa-alueeseen kohdennettuja kysymyksiä, joiden myötä oli mahdollista tarkastella tietoturvauhkien esiintyvyyttä sosiaalisen median käyttäjien keskuudessa sekä lisätä heidän tietoisuuden tasoaan kyselystä saatujen tulosten perusteella. Tutkimuskysymyksiin pohjautuvat osa-alueet keskittyivät erityisesti tarkastelemaan tietoturvauhkiin sisältyviä kyberrikoksia, valeuutisia, tietojenkalastelua, valearvontoja, identiteettivarkauksia sekä sosiaalisen median käyttäjien yksityisyyttä. Kyberturvallisuuskeskuksen (2020a) mukaan vuonna 2020 tietoturvan suurimpia uhkia olivat, huijaukset, tietojenkalastelu, roskaposti, haittaohjelmat sekä tietomurrot (Kyberturvallisuuskeskus, 2020a). Kyselyssä selvitettiin, ovatko nämä uhat edelleen ajankohtaisia ja myös sitä, kuinka moni niistä ovat todellisia uhkia sosiaalisessa mediassa?

Kyselyn osa-alueiden myötä mahdollistui tutustuminen käyttäjän perustietoihin, kuten ikään, sukupuoleen, työssäkäyntiin sekä taustatietoihin sosiaalisen median käyttöön liittyen. Perustietojen ohella haluttiin kiinnittää huomiota myös käyttäjän tietoturvauhkien havainnointiin sekä huolestuneisuuteen kyberrikoksiin viitaten. Käyttäjän perustietoihin pohjautuvassa osa-alueessa pyrittiin selvittämään myös, olivatko kyselyyn vastanneet samaa mieltä Nortonin (2021) vuonna 2021 tekemän kyselyn vastaajien kanssa, jossa yli puolet vastaajista kertoivat, että verkossa nähtävän tiedon todenmukaisuus oli vaikeasti pääteltävissä (Norton, 2021). Kyselystä saatujen vastausten myötä kartoitettiin, olivatko vastaajat tietoisempia suojautumaan kyberrikoksilta kyselyyn vastaamisen jälkeen sekä sitä, kuinka huolestuneita vastaajat olivat ajatuksesta joutua kyberrikoksen uhriksi. Nortonin (2021) tekemässä kyselyssä vastaajista yli puolet kertoivat olevansa huolestuneita ajatuksesta joutua kyberrikoksen uhriksi, sekä yli puolet vastaajista kertoivat, etteivät tiedä miten suojautua kyberrikoksilta (Norton, 2021). Nortonin (2021) tekemää tutkimusta käytettiin pohjana vertailulle käyttäjien tietoturvakäyttäytymisestä sekä asenteista.

Käyttäjän perustietojen ohella käsiteltiin myös sosiaalisessa mediassa esiintyviä valeuutisia. Käyttäjille kerrottiin kysymyksen yhteydessä lyhyt tietoisku valeuutisen käsitteen vahvistamiseksi. Kyselyssä haluttiin kartoittaa käyttäjien luottamusta sosiaalisen median alustoilla jaettuihin uutisiin. Valeuutisiin liittyvien kysymysten avulla pyrittiin myös saamaan vahvistusta aikaisemmissa tutkimuksissa esitettyihin tuloksiin. Osiossa pyrittiin saamaan vastaus seuraaviin kysymyksiin, jotka pohjautuvat Alkawaz et al. (2021) tekemään tutkimukseen, jossa kartoitettiin 250 käyttäjän sosiaalisen median tietoturvaa (Al-

kawaz et al., 2021). Alkawaz et al. (2021) tutkimuksen tuloksia vertailtiin tämän tutkimuksen kanssa, sillä siinä on paljon samankaltaisia kysymyksiä valeuutisista ja disinformaatiosta sosiaalisen median alustoilla, jolloin voitiin tarkastella vahvistaako tämän tutkimuksen kyselystä saadut vastaukset aiemman tutkimuksen tuloksia ja päätelmiä.

- Alkawaz et al. (2021) mukaan vastaajista 64 % ovat kertoneet, että valeuutiset ovat ongelma sosiaalisessa mediassa sekä 24 % vastaajista ei osannut sanoa asiasta (Alkawaz et al., 2021). Pystyikö oma tutkimus vahvistamaan enemmistön näkökannan valeuutisten ongelmasta?
- Alkawaz et al. (2021) mukaan vastaajista noin 58 % ovat joutuneet valeuutisten uhriksi (Alkawaz et al., 2021). Olivatko oman tutkimuksen vastaajat myös kohdanneet valeuutisia?
- Alkawaz et al. (2021) mukaan vain pieni osa (16 %) vastaajista tarkistaa aina uutisen todenmukaisuuden. (Alkawaz et al., 2021). Tarkistivatko oman tutkimuksen kyselyyn vastanneet useammin sosiaalisessa mediassa jaetun uutisen todenmukaisuuden?

Kyselyssä käsiteltiin myös tietojenkalastelua ja siihen liittyen kartoitettiin, olivatko käyttäjät osanneet tunnistaa tietojenkalasteluyrityksen. Kyselystä saatujen vastausten myötä oli mahdollista tarkastella tietojenkalastelun esiintyvyyttä eli sitä, olivatko käyttäjät kohdanneet tietojenkalastelua tai ovatko käyttäjät joutuneet tietojenkalastelun uhriksi.

Valearvonnat ovat yleistyneet sosiaalisessa mediassa ja ne leviävät nopeasti sosiaalisen median verkostoissa. Kysymyksillä on haluttu kartoittaa myös, olivatko käyttäjät huomanneet valearvontoja ja olivatko he tietoisia siitä, mitä valearvonnat tarkoittavat. Valearvonnat toteutetaan yleensä jonkin tunnetun brändin nimissä, joten kyselyssä selvitettiin myös sitä, osasivatko käyttäjät tunnistaa valearvonnan oikeasta arvonnasta sekä tarkastivatko käyttäjät mihin he olivat osallistumassa, ja mihin heidän tietojaan aiottiin käyttää.

Käyttäjien tietoisuutta sekä havaintoja kartoitettiin identiteettivarkauksiin liittyen. Kysymysten avulla selvitettiin, olivatko käyttäjät kohdanneet sosiaalisessa mediassa jonkun esiintyvän toisen henkilön identiteetillä. Kyselyssä haluttiin myös kartoittaa käyttäjien omia kokemuksia mahdollisen identiteettivarkauden uhriksi joutumisesta. Vastaajilta kysyttiin myös, miten he olivat itse suojautuneet identiteettivarkauksia vastaan.

Käyttäjätilin suojausta ja käyttäjien yksityisyyttä haluttiin tarkastella sosiaalisen median alustoja käytettäessä. Sosiaalisen median tietoturvakäytäntöjä kartoitettiin käyttäjien yksityisyyden osalta ja siihen liittyen haluttiin myös selvittää, olivatko käyttäjät huolestuneet

omasta yksityisyydestään sosiaalisessa mediassa. Edellä mainittujen asioiden lisäksi kyselyssä haluttiin selvittää, miten käyttäjät suojautuivat käyttäjätilin kaappauksilta ja kuinka tietoisia käyttäjät olivat hakukoneilla löytyvistä heitä koskevista avoimista tiedoista.

Käyttäjien tietoturvauhkiin liittyvää tietoisuutta haluttiin kartoittaa selvittämällä, olivatko käyttäjät saaneet neuvoja välttääkseen tietoturvauhkien realisoitumista, ja mistä he olivat näitä neuvoja saaneet. Kyselyn lopuksi tutkittiin, aiheuttiko käyttäjän omat tietoturvakäytännöt pohdintaa sen suhteen, millaisia asioita käyttäjän tulisi parantaa omassa tietoturva-arjessaan.

6. TUTKIMUSTULOKSET

Tutkimuksen kyselyyn osallistuneista 69 vastaajasta 47,8 % oli naisia ja 46,4 % miehiä. Loput vastaajista eivät halunneet kertoa sukupuoltaan. Vastaajat olivat iältään 16–67-vuotiaita ja ikäjakauman mediaaniksi osoittautui 27 vuotta.

Tutkimustuloksia analysoitiin tilastollisesti kuvaamalla saatuja vastauksia kuvien ja diagrammien avulla. Tutkimustulosten analysoinnissa hyödynnetyt ympyrä- ja pylväsdiagrammit auttoivat havainnollistamaan erilaisten osuuksien suhdetta kokonaismäärään. Ympyrädiagrammit osoittavat osuuksien suhteita prosentuaalisessa muodossa, kun vastaavasti pylväsdiagrammin avulla määriä havainnollistetaan akseleille asetettujen arvojen mukaan.

6.1 Käyttäjien taustat

Kyselyn ensimmäisessä osiossa käsiteltiin käyttäjien taustatietoja sekä käyttäytymistä sosiaalisessa mediassa. Kysymyksillä haluttiin kartoittaa millaisissa tilanteissa ja millä tavoin käyttäjät olivat mahdollisesti kohdanneet tietoturvauhkia sosiaalisessa mediassa. Käyttäjien hyödyntämiä sosiaalisen median alustoja haluttiin myös kartoittaa kokonaisuudessaan.

Kyselyyn vastanneista suurin osa 62,3 % on työssäkäyviä, 44,9 % opiskelijoita ja loput ovat työelämän ulkopuolella tai eläkkeellä. Kuitenkin vastauksiin liittyen tuli huomioida se, että vastaaja voi käydä töissä sekä opiskella samaan aikaan, jolloin vastauksien prosentit eivät ole tasan 100 %.

***Kuva 6** Oletko havainnut tietoturvauhkia sosiaalisessa mediassa?*

Kuvasta (Kuva 6) käy ilmi jakauma kysymykseen, ovatko vastaajat kohdanneet tietoturvauhkia sosiaalisessa mediassa. Kuitenkin suuri osa vastaajista 40,6 % on havainnut tietoturvauhkia vähintäänkin joskus. Vastauksista käy ilmi, että valveutuneimmat käyttäjät ovat todennäköisesti osanneet tunnistaa uhkia paremmin ja kokevat kohdanneensa tietoturvauhkia “useasti”. Vastausta “en koskaan” voidaan tulkita pienellä varauksella, vaihtoehdon “en koskaan” valinneet 17,4 % ovat todennäköisesti kohdanneet tietoturvauhkia sosiaalisessa mediassa, mutta he eivät välttämättä ole huomanneet niitä.

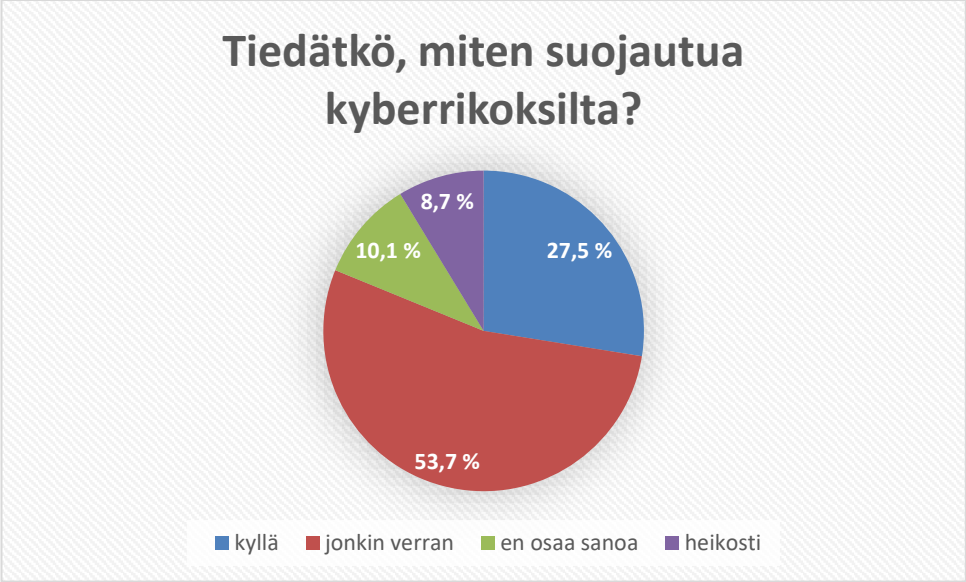
Jatkokysymykseen “jos olet havainnut uhkia sosiaalisessa mediassa, niin millaisia uhat ovat olleet?”, monet vastaajista kertoivat kohdanneensa sosiaalisessa mediassa paljon tietojenkalastelua sekä johdattelua saastuneille sivustoille. Vastaajat ovat havainneet myös disinformaatiota sekä valeuutisia.

***Kuva 7** Oletko huolestunut ajatuksesta joutua kyberrikoksen uhriksi?*

Kuvassa (Kuva 7) on kysymyksen ‘’oletko huolestunut ajatuksesta joutua kyberrikoksen uhriksi?’’ vastausten prosentuaalinen jakauma. Vastaajista 11,6 % kokevat olevansa huolissaan ja 39,1 % jonkin verran huolissaan ajatuksesta joutua kyberrikoksen uhriksi. Kyselyn antamat vastaukset vahvistavat Nortonin (2021) tekemän tutkimuksen tuloksia, jossa vastaajista yli puolet olivat vastanneet olevansa huolissaan ajatuksesta joutua kyberrikoksen uhriksi (Norton, 2021).

Jatkokysymykseen “Mistä huolesi koostuu?”, moni käyttäjä kertoi olevansa huolissaan identiteettivarkauden mahdollisuudesta. Vastaajat ovat huolissaan myös mahdollisista

taloudellisista vahingoista sekä tilien kaappaamisesta. Osa vastaajista ilmaisi myös huolensa oman sisällön käyttämisestä väärässä kontekstissa ja erityisesti tietoisuuden puutteesta.

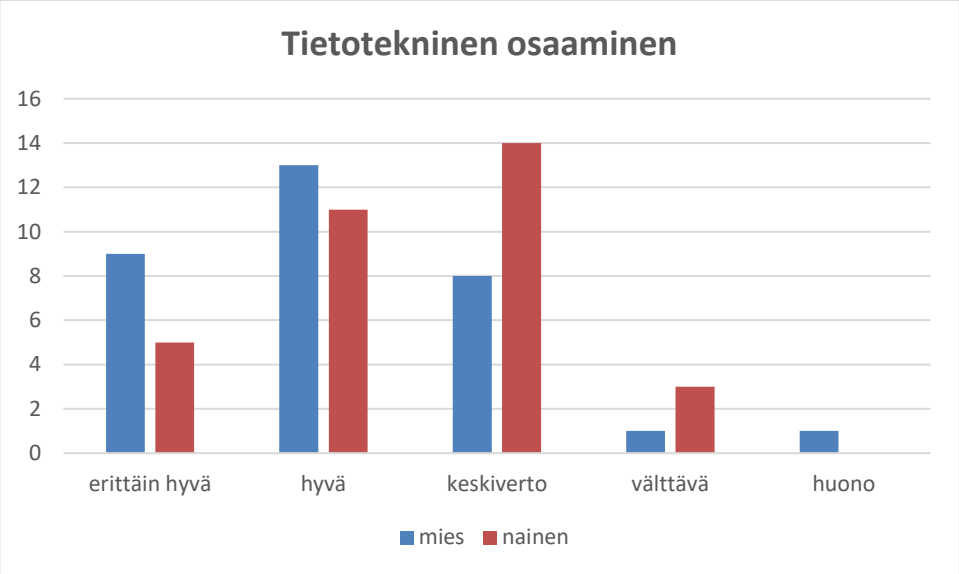


Kuva 8 *Tiedätkö, miten suojautua kyberrikoksilta?*

Kysymykseen (Kuva 8) “Tiedätkö, miten suojautua kyberrikoksilta?”, vastaajista suurin osa (81,2 %) osaa omasta mielestään vähintäänkin “jonkin verran” suojautua kyberrikoksilta. Kyselyssä huomattavaa on, että vain 8,7 % arvioi oman kykynsä suojautua kyberrikoksilta heikoksi.

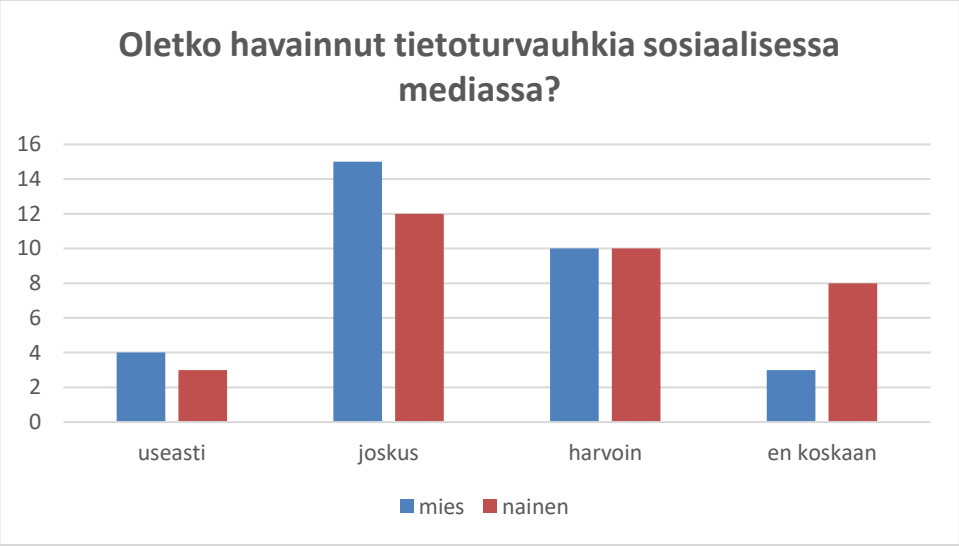
Kuva 9 *Verkossa jaetun tiedon todenmukaisuuden pääteltävyys*

Kysymykseen (Kuva 9) “onko heidän mielestään verkossa jaetun tiedon todenmukaisuus helposti pääteltävissä?”, suurin osa vastaajista (63,8 %) ovat sitä mieltä, että tiedon todenmukaisuus on vaikeasti pääteltävissä. Tämä vahvistaa myös Norton tietoturvayrityksen (2021) vuonna 2021 tekemän tutkimuksen tuloksia. Nortonin tekemässä tutkimuksessa 62 % vastaajista kertoivat, että verkossa jaetun tiedon todenmukaisuus on vaikeasti pääteltävissä (Norton, 2021).



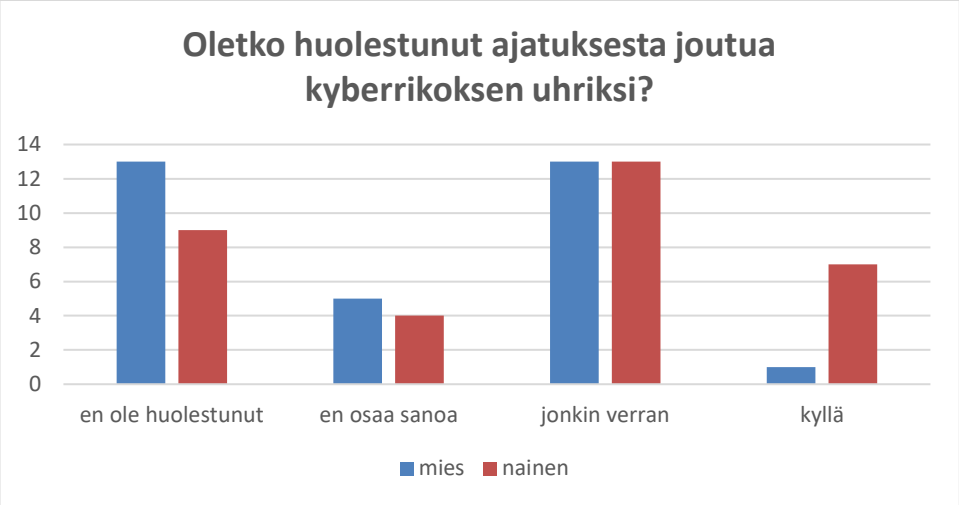
Kuva 10 *Tietotekninen osaaminen sukupuolittain*

Käyttäjiltä kysyttiin heidän omaa arviotaan tietoteknisestä osaamisesta, jolloin kysymys tarjoaa taustatietoa käyttäjästä ja hänen lähtökohdistaan tietoturvan pariin. Vastauksista huomataan (Kuva 10), että miehet arvioivat oman tietoteknisen osaamisen korkeammaksi kuin naiset.



Kuva 11 *Tietoturvauhkien havainnot sukupuolittain*

Kuvassa (Kuva 11) huomataan tietoturvauhkien jakautuminen sukupuolittain, josta voidaan päätellä, että vastaajista miehet ovat havainneet tietoturvauhkia enemmän kuin naiset.



Kuva 12 *Huolestuneisuus ajatuksesta joutua kyberrikoksen uhriksi sukupuolittain*

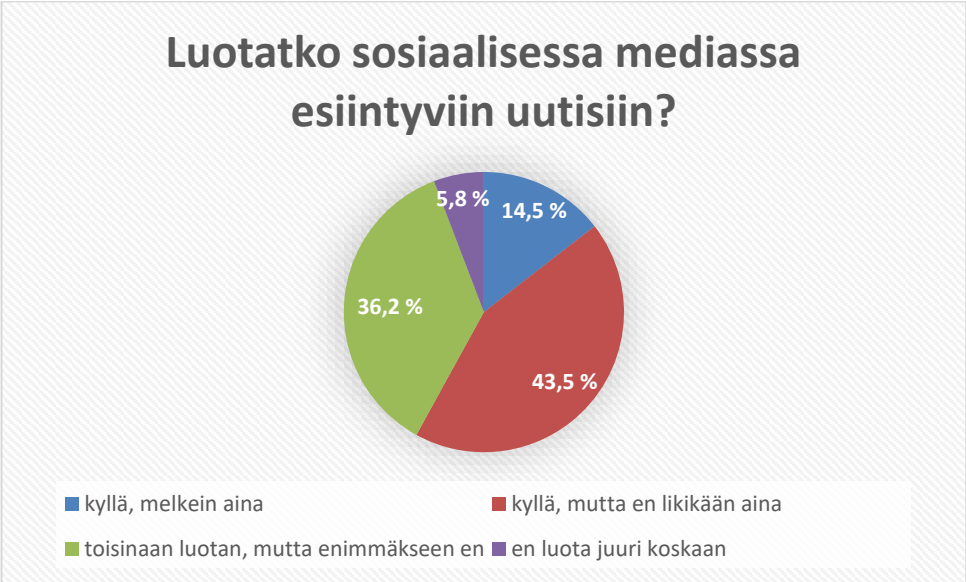
Kysymykseen “Oletko huolestunut ajatuksesta joutua kyberrikoksen uhriksi?” vastaajista naiset kertovat olevansa enemmän huolestuneita ajatuksesta joutua kyberrikoksen uhriksi. Kuvan (Kuva 12) mukaan miesvastaajista vain yksi kertoi olevansa tosissaan huolissaan kyberrikoksen uhriksi joutumisesta. Saatujen tulosten mukaan valtaosa miesvastaajista eivät kokeneet olevan huolissaan joutumisesta kyberrikoksen uhriksi.

6.2 Disinformaatio ja valeuutiset

Kyselyn vastaajista 98,6 % tietää mitä tarkoitetaan valeuutisen käsitteellä ja yksi vastaaja ei osaa sanoa asiasta. Kysymykseen “Mitä ymmärrät tarkoitettavan valeuutisilla?”, vastaajat kertovat valeuutisten olevan uutisia, joista puuttuu luotettavat lähteet tai uutisia, jotka ajavat jotain tiettyä agendaa. Vastauksissa painotetaan valeuutisilla vaikuttamista ja valheellisen tiedon jakamista tarkoituksella. Kyselyn vastaajista 73,9 % kertovat kohdanneensa valeuutisia sosiaalisessa mediassa, josta voidaan päätellä valeuutisten olevan suhteellisen yleisiä sosiaalisessa mediassa. Vastaajat kertovat monien valeuutisten sekä disinformaation liittyneen Ukrainan sotaan ja koronapandemiaan.

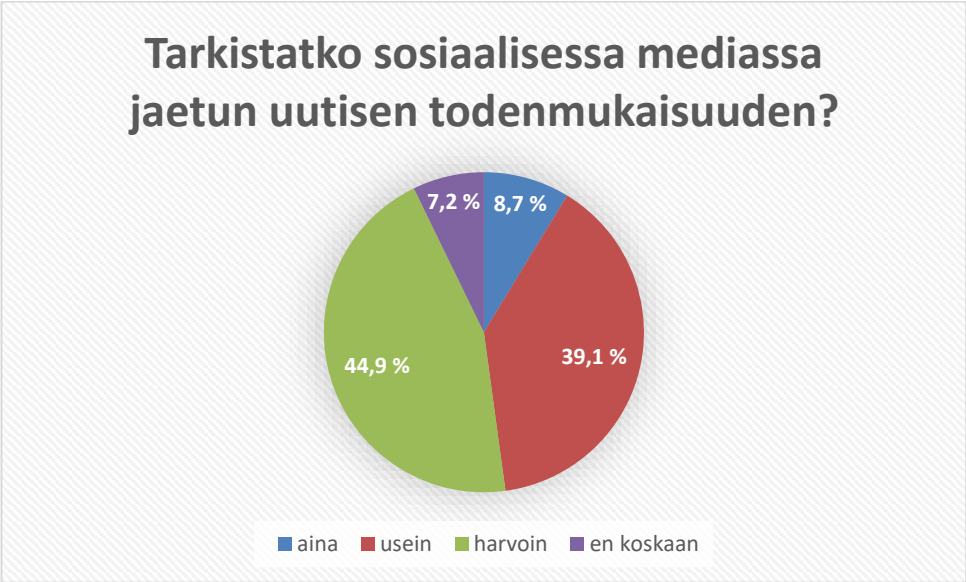
Kyselyn vastauksien mukaan käyttäjät ovat havainneet eniten valeuutisia Facebookissa, YouTubessa sekä Instagramissa. Kysymykseen “kuinka usein olet tavannut valeuutisia sosiaalisessa mediassa?”, vastaajista 15,4 % kertovat kohdanneensa valeuutisia päivittäin ja 38,5 % kerran viikossa, jolloin voidaan päätellä valeuutisten olevan suhteellisen yleisiä viikkotasolla tarkasteltuna. Kuitenkin vajaa kolmasosa (28,8 %) vastaajista kertoo

havainneensa valeuutisia kerran kuussa ja loput vastaajista (17,3 %) harvemmin kuin kerran kuussa.



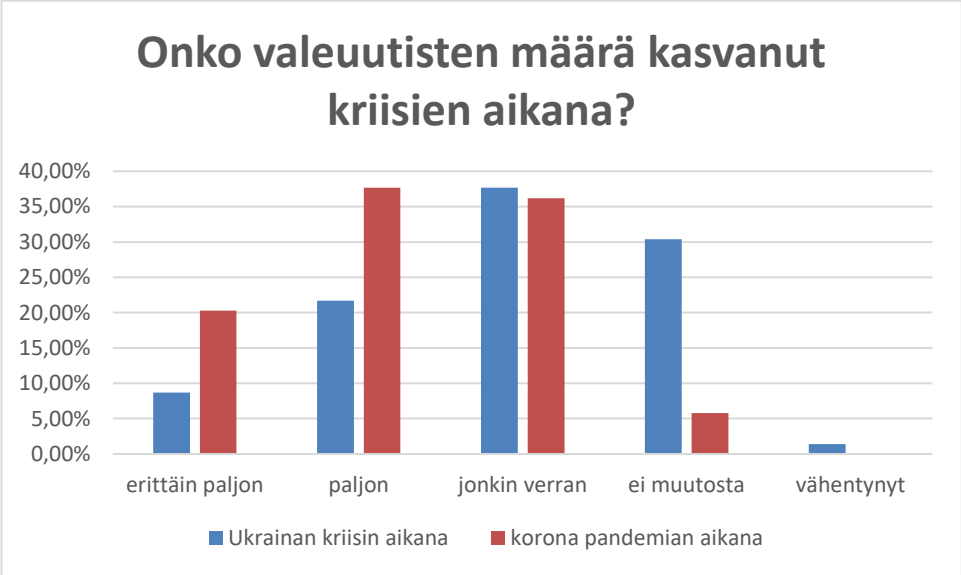
Kuva 13 *Luotatko sosiaalisessa mediassa esiintyviin uutisiin?*

Kysymykseen “Luotatko sosiaalisessa mediassa esiintyviin uutisiin?” (Kuva 13), vastaajista ainoastaan 14,5 % luottaa melkein aina näkemäänsä uutiseen sosiaalisessa mediassa. Vastauksista voidaan päätellä, että käyttäjät tarkastelevat sosiaalisessa mediassa jaettua tietoa pääosin kriittisesti ja vain pieni osa luottaa täysin sosiaalisessa mediassa jaettuun tietoon. Vastaukset jakautuivat pääosin kysymyksessä “kyllä, mutta en likikään aina” (43,5 %) ja “toisinaan luotan, mutta enimmäkseen en” (36,2 %).



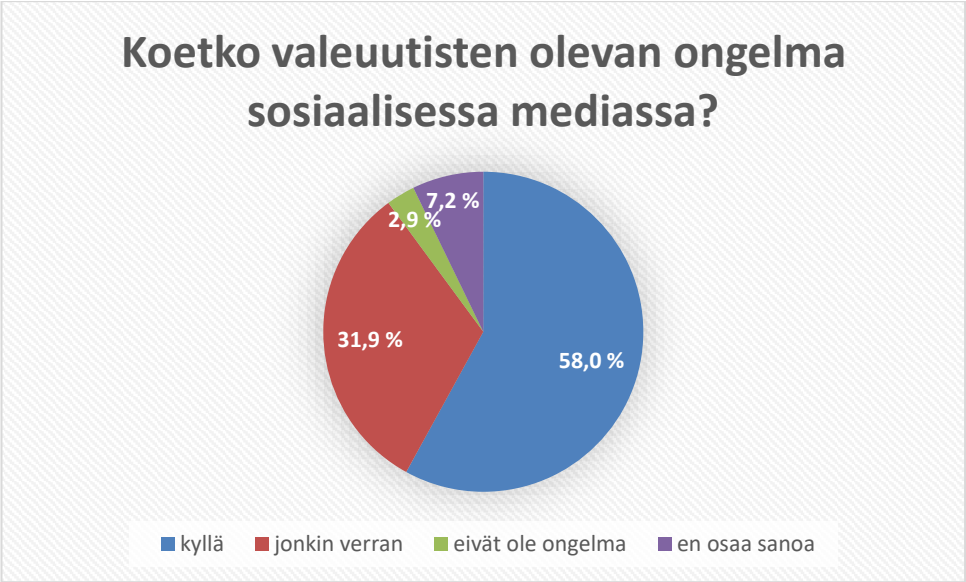
Kuva 14 *Tarkistatko sosiaalisessa mediassa jaetun uutisen todenmukaisuuden?*

Kysymyksen “tarkistatko sosiaalisessa mediassa jaetun uutisen todenmukaisuuden?” (Kuva 14), vastauksien perusteella voidaan päätellä, että vastaajista yli puolet eivät tarkasta uutisen todenmukaisuutta säännöllisesti, vaikka aiemmassa kysymyksessä käyttäjät ilmaisivat epäluottamuksensa sosiaalisessa mediassa jaettuihin uutisiin. Alkawaz et al. (2021) tekemässä tutkimuksessa 16 % vastaajista kertoi tarkistavansa aina uutisen todenmukaisuuden (Alkawaz et al., 2021). Aiempaan tutkimukseen verrattuna 8,7 % osuus käyttäjistä, jotka kertoivat tarkistavansa aina uutisen todenmukaisuuden, on todella huono. Vastausten perusteella käyttäjien tulisi lisätä uutisten todenmukaisuuden tarkistamista huomattavasti.



Kuva 15 *Valeuutisten määrän kehitys kriisien aikana*

Kysymyksen “onko valeuutisten määrä kasvanut kriisien aikana?”, vastausten perusteella kuvasta (Kuva 15) voidaan päätellä koronapandemian lisänneen valeuutisten määrää sosiaalisen median alustoilla huomattavasti. Ukrainan kriisin aiheuttama informaatiosota on vastaajien mielestä lisännyt jonkin verran valeuutisten määrää, mutta myös osa vastaajista ei ole huomannut muutosta aiempaan verrattuna. Jatkokysymykseen “Oletko huomannut pandemiaan liittyvän sosiaalisen median uutisoinnin muuttuneen viime aikoina Ukrainan sodan uutisten vallatessa alaa?”, suurin osa vastaajista (42 %) kertoi, että koronapandemiaan liittyvä uutisointi on vähentynyt. Vastaajista 33,3 % ei osannut sanoa onko koronapandemian uutisointi lisääntynyt tai vähentynyt, sillä he seuraavat aihetta vähemmän kuin aikaisemmin.



Kuva 16 *Koetko valeuutisten olevan ongelma sosiaalisessa mediassa?*

Kysymykseen (Kuva 16), “koetko valeuutisten olevan ongelma sosiaalisessa mediassa?”, vastaajista suurin osa (58 %) vastaa valeuutisten olevan selkeä ongelma. Vastaajista 31,9 % kertovat valeuutisten olevan “jonkin verran” ongelma, joten voidaan päätellä, että vahva enemmistö vastaajista kokee valeuutiset ongelmaksi sosiaalisessa mediassa. Vastaus vahvistaa Alkawaz et al. (2021) tekemän tutkimuksen vastauksia, tutkimuksessa 64 % vastaajista kertoi valeuutisten olevan ongelma (Alkawaz et al., 2021).

Kysymykseen “millä tavoin tunnistat valeuutisen?”, moni vastaaja kertoo tarkastavansa uutisen lähteet ja lähteiden luotettavuuden. Vastaajista osa myös kertoo vertaavansa nähtyä uutista muihin lähteisiin, jotka käsittelevät samaa uutisessa esiintyvää aihetta. Vastauksissa mainittiin myös uutisen taustojen tarkistus, ajetaanko uutisella jotain agendaa tai yritetäänkö aiheuttaa jotakin reaktiota lukijassa.

6.3 Tietojenkalastelu

Kyselyssä käsiteltiin yhdessä osiossa tietojenkalastelua ja sitä, ovatko käyttäjät kohdanneet tai havainneet tietojenkalastelua sosiaalisessa mediassa. Kyselyyn vastaajista 97,1 % tietää mitä tietojenkalastelu tarkoittaa ja loput kaksi vastaajaa ei osaa sanoa asiasta. Kyselyn vastaajista 59,4 % on kohdannut tietojenkalastelua sosiaalisessa mediassa, joten voidaan päätellä tietojenkalastelun olevan ajankohtainen sekä yleinen tietoturvauhka. Sähköpostitse tapahtuva tietojenkalastelu on edelleen yleistä sen helppouden vuoksi, vastaajista 78,3 % on tavannut tietojenkalastelua sähköpostitse.

Kyselyn vastaajista 78,3 % kertovat osaavansa tunnistaa tietojenkalasteluyrityksen ja vastaajista 20,3 % ei osaa sanoa, osaavatko he tunnistaa kyseisen uhan. Vastaajista

vain yksi kertoi, että hän ei osaa tunnistaa tietojenkalasteluyritystä. Luvuista voidaan päätellä käyttäjien tietoisuuden tietojenkalastelusta olevan yleisesti hyvällä tasolla ja käyttäjät osaavat todennäköisesti tunnistaa mahdollisen uhan. Kysymykseen “Oletko joutunut tai epäiletkö joutuneesi tietojenkalastelun uhriksi?”, suurin osa 68,1 % käyttäjistä vastasi, että he eivät ole joutuneet tietojenkalastelun uhriksi. Vastaajista 20,3 % kertoi joutuneensa tietojenkalastelun uhriksi ja loput vastaajista eivät osaa sanoa asiasta.

Vastauksia voidaan kuitenkin tulkita varauksella, sillä kaikkia tietojenkalasteluyrityksiä ei välttämättä ole huomattu, jolloin todellisuudessa suurempi osuus käyttäjistä on voinut joutua tietojenkalastelun uhriksi. Vastauksien prosentit kuitenkin tukevat aiempaa kysymystä tietojenkalasteluyrityksen tunnistamisesta, jolloin 20,3 % vastaajista, jotka eivät osanneet varmaksi sanoa tunnistavatko he tietojenkalasteluyrityksen, voivat sisältyä 20,3 % käyttäjistä, jotka ovat joutuneet tietojenkalastelun uhriksi.

Kysymykseen “ovatko käyttäjät avanneet epäluotettavia linkkejä sosiaalisesta mediasta?”, vastaajista suurin osa 65,2 % vastasi, etteivät he ole avanneet epäilyttäviä linkkejä. Kuitenkin 27,5 % vastaajista olivat avanneet epäilyttäviä linkkejä joskus ja kaksi vastaajaa kertoi avaavansa niitä melko usein.

6.4 Valearvonnat

Vastaajista 82,6 % tietää mikä on valearvonta, mutta 11,6 % eivät tiedä ollenkaan mitä tarkoitetaan valearvonnan käsitteellä. Vastaajista huomattava enemmistö 73,9 % oli huomannut valearvontoja sosiaalisessa mediassa, joten voidaan päätellä valearvontojen olevan ajankohtainen uhka sosiaalisen median alustoilla.

Kyselyyn vastaajista vain 30,4 % on osallistunut arvontoihin sosiaalisessa mediassa, mutta kuitenkin vain 38,1 % vastaajista lukee aina arvonnan säännöt sekä mihin osallistujan tietoja käytetään. Vastaajista 33,3 % lukee arvonnan säännöt silloin tällöin ja loput vastaajista eivät lue ollenkaan arvonnan sääntöjä. Vastauksista voidaan päätellä, että arvonnan sääntöjä ei lueta tarkkaan eikä säännöllisesti, joten arvontoihin osallistutaan usein tietämättä mitä tietoja arvonnan pitäjä kerää osallistujasta ja mihin tietoja käytetään. Kuitenkin vastaajista enemmistö 60,5 % tarkistaa arvonnan pitäjän olevan oikea yritys, joten suurin osa vastaajista osaa välttää valearvonnat. Käyttäjiltä kysyttiin “osaatko erottaa valearvonnan oikeasta arvonnasta?”, johon enemmistö 66,7 % vastasi osaavansa erottaa valearvonnan oikeasta arvonnasta. Vastaajista 33,3 % eivät joko osanneet erottaa arvontoja tai eivät osanneet sanoa asiasta.

6.5 Identiteettivarkaudet

Kyselyyn vastaajista lähes kaikki (98,6 %) kertovat tietävänsä mitä tarkoitetaan identiteettivarkauksilla. Vastaajista 60,9 %, kertovat huomanneensa jonkun esiintyvän toisen henkilön tai yrityksen nimellä, tämän perusteella voidaan pitää identiteettivarkauksia yleisenä ja huomattavana tietoturvauhkana. Vastaajista 27,5 % eivät ole havainneet toisen nimellä esiintyviä käyttäjiä ja loput vastaajista eivät osaa sanoa asiasta.

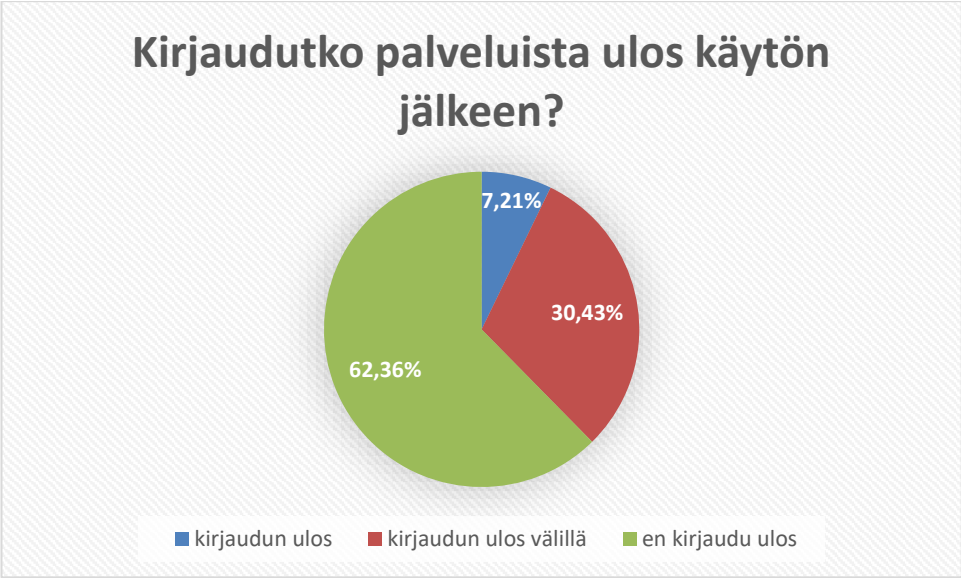
Vastaajista 40,6 % on joutunut tai tietää tuttavansa joutuneen identiteettivarkauden uhriksi, kuitenkin suurin osa 55,1 % kertovat, etteivät ole joutuneet identiteettivarkauden uhriksi. Vastauksissa tulee huomioida, että tässä kartoitetaan tietävätkö käyttäjät joutuneensa identiteettivarkauden uhriksi, sillä todellisuudessa kaikki uhrit eivät tiedä joutuneensa identiteettivarkauden kohteeksi.

Käyttäjiltä kysyttiin miten he suojautuvat identiteettivarkauksilta, johon monet käyttäjät vastasivat rajoittamalla tietojensa syöttämistä palveluihin sekä rajaamalla tietojensa julkisuutta sosiaalisessa mediassa. Käyttäjät myös kertoivat tarkastavansa palvelut missä tietoja kysytään sekä olemalla mahdollisimman “tuntematon henkilö” internetissä.

6.6 Käyttäjätilin suojaus ja yksityisyys

Kyselyssä kartoitettiin ovatko käyttäjät huolestuneita käyttäjätilin yksityisyydestä sosiaalisessa mediassa, johon 65,2 % vastasi, etteivät he ole huolestuneita käyttäjätilinsä yksityisyytensä puolesta. Käyttäjiltä kysyttiin ovatko he hyväksyneet kavereita tai seuraajia, joita he eivät tunne. Kysymykseen vastaajista 49,3 % vastasi hyväksyneensä kavereita, joita he eivät tunne ja 47,8 % käyttäjistä ei ole hyväksynyt tuntemattomia käyttäjiä kavereiksi. Sosiaalisen median profiilin yksityisyyttä on vaikea ylläpitää, mikäli suuri osa käyttäjistä hyväksyy jopa tuntemattomia kavereiksi, jolloin tuntemattomat kaverit voivat nähdä sinusta enemmän tietoa kuin heidän kuuluisi.

Kyselyyn vastaajista 79,7 % on rajoittanut sosiaalisessa mediassa julkaisuiden näkyvyyttä ja 14,5 % vastaajista ei ole rajoittanut näkyvyyttä ollenkaan. Vastauksista voidaan päätellä, että suurin osa käyttäjistä ei halua tietojansa näkyvän julkisesti, mutta edellisen kysymyksen antama tulos on ristiriidassa tämän kysymyksen tulosten kanssa. Mikäli vastaaja rajoittaa julkaisut esimerkiksi vain kavereiden nähtäväksi, mutta silti hyväksyy tuntemattomia kavereiksi, on tällöin julkaisuiden julkisuuden rajoitus vähemmän hyödyllinen.



Kuva 17 *Kirjaudutko palveluista ulos käytön jälkeen?*

Käyttäjätilien suojaamiseksi 69,6 % vastaajista on ottanut käyttöön kaksivaiheisen tunnistautumisen ja loput vastaajista eivät ole näin tehneet. Vaikka suurin osa vastaajista on ottanut kaksivaiheisen tunnistautumisen käyttöönsä, olisi hyvä, mikäli luku olisi vielä suurempi, sillä kyseessä on yksi helpoin ja tehokkain tapa vähentää tilin kaappaamisen riskiä. Kuvasta (Kuva 17) huomataan, että käyttäjistä vain 7,21 % kirjautuu ulos palveluista käytön jälkeen. Monesti pankkien palveluita ja viranomaispalveluita käytettäessä palveluissa on aikakatkaisu, jolloin palvelu kirjaa käyttäjän ulos tietyn ajan jälkeen. Kuitenkaan sosiaalisen median alustoilla automaattista aikakatkaisua ei ole, jolloin käyttäjätiliä on mahdollista väärinkäyttää. Käyttäjätilin turvaamiseksi tulisi käytön jälkeen tietokone vähintäänkin lukita, jolloin palvelua ei voida suoraan käyttää tietokoneelta.

Kyselyssä kartoitettiin myös ovatko käyttäjät tietoisia, kuinka paljon heistä löytää hakukoneiden avulla. Käyttäjistä 88,4 % ovat hakeneet itseään googlesta ja katsonut mitä tietoa heistä löytyy hakukoneen avulla. Käyttäjistä, jotka ovat haun suorittaneet 80,3 % löysivät jonkin verran tietoa itsestään ja 3,3 % löysivät huomattavia määriä tietoa itsestään haun avulla. Vastaajista 16,4 % eivät löytäneet ollenkaan tietoa itsestään. Käyttäjistä kuitenkin 80,3 % eivät ole ollenkaan huolestuneita löytämistään tiedoista hakukoneilla ja vain 3,3 % vastaajista kokevat olevansa todella huolestuneita löydöistä. Vastaajista 16,4 % ovat jonkin verran huolestuneita tiedoista, joita löysivät. Vastausten pohjalta kiinnitetään huomiota siihen, kuinka aktiivisesti vastaajat hakevat itseään hakukoneilla. Käyttäjien tulisi suorittaa hakuja säännöllisesti, jolloin voidaan ennakoivasti löytää itsestä sellaista tietoa, jonka ei kuuluisi olla julkisesti saatavilla.

6.7 Vastaajien tietoisuus

Kyselyssä kartoitettiin käyttäjien tietoisuutta käsitellyistä tietoturvauhista sekä siitä, ovatko käyttäjät saaneet tarpeeksi tietoa välttääkseen sosiaalisessa mediassa esiintyviä tietoturvauhkia. Kuvassa (Kuva 18) nähdään, kuinka tietoisia käyttäjät olivat käsitellyistä tietoturvauhista ennen kyselyä.

Kuva 18 *Käyttäjien tietoisuus tietoturvauhista ennen kyselyä*

Käyttäjistä 72,5 % ovat sitä mieltä, että he ovat saaneet tarpeeksi tietoa tietoturvauhista kyselyn avulla tunnistaakseen sekä välttääkseen kyselyssä käsiteltyjä tietoturvauhkia. Vastaajista 13 % eivät koe saaneensa tarpeeksi tietoa tietoturvauhkien välttämiseksi ja 14,5 % eivät osaa sanoa asiasta. Vastauksien perusteella kyselyssä olevat tietoiskut olivat hyviä ja informatiivisia auttamaan käyttäjää sosiaalisen median tietoturvassa. Tietoiskuissa pohjustettiin aluksi käsittelyssä olevaa tietoturvauhkaa sekä aiheen kysymysten jälkeen kerrottiin, kuinka kyseisiä uhkia tulisi välttää jatkossa.

Kuva 19 *Mistä olet saanut tietoa sosiaalisen median tietoturvasta?*

Kysymykseen “mistä olet saanut tietoa sosiaalisen median tietoturvasta?” (Kuva 19), suurin osa käyttäjistä on saanut tietoa tuttaviltaan sekä itse hakemalla tietoa verkosta. Vastausten pohjalta voidaan pitää huomion arvoisena perinteisen median kuten TV:n, radioiden sekä lehtien osuutta tietoturvaan liittyvän tiedon jakamisessa käyttäjille. Tuttavien vaikutus käyttäjien tietoturvaan näkyi myös jatkokysymyksessä “mitkä tiedonlähteistäsi ovat vaikuttaneet eniten tietoturvakäyttäytymiseesi tai tietoturvakäytäntöihisi sosiaalisessa mediassa?”. Kysymykseen 49,3 % kertovat tuttavien vaikuttaneen eniten heidän tietoturvakäyttäytymiseensä ja netistä itse hakeman tiedon vaikuttaneen toiseksi eniten (40,3 %).

Käyttäjistä monet kertovat, että he haluaisivat lisää käytännön läheistä tietoa tietoturvasta jostakin luotettavasta lähteestä. Käyttäjät myös painottavat, että uusien tietoturvauhkien tullessa niistä voisi tiedottaa ihmisiä median avulla. Monet vastaajista myös kaipaavat tietoa, mitä tulisi tehdä, jos joutuu kyberrikoksen uhriksi. Ohjeissa monesti opetetaan kuinka tulisi välttää tietoturvauhkia, mutta harvemmin kerrotaan mitä tulisi tehdä kyberrikoksen uhriksi joutuessa.

7. POHDINTA

Tutkimuksen lopuksi arvioidaan tulosten pohjalta muodostettuja kokonaisuuksia käyttäjien sosiaalisen median tietoturvaan liittyen. Tutkimuksen lopuksi pohditaan tutkimustyölle asetettujen tavoitteiden toteutumista sekä tutkimuksen tekemisen kulkua.

Pohdinnassa arvioidaan myös sitä, ovatko saadut tulokset vastanneet tutkimukselle asetettuihin tutkimuskysymyksiin. Kokonaiskuvaa muodostettaessa tarkastellaan ovatko tutkimuksessa esitetyt kysymykset tuottaneet aiempien tutkimusten rinnalla uutta tietoa tietoturva-arjen parantamiseksi sosiaalisen median käyttäjien perspektiivistä.

7.1 Tutkimusmenetelmä

Tutkimuksessa hyödynnetty tutkimusmenetelmä oli määrällinen. Tämän tutkimusmenetelmän avulla tutkimus toi esiin vastaajien kokemusten ja ajatusten pohjalta sellaisia huomioita, joita tutkimusta aloitettaessa ei tullut välttämättä otettua huomioon. Tutkimuksen myötä nousi esiin muutamia puutteita ja kehitysideoita, joihin vastaajat toivoivat muutosta turvallisemman ja monipuolisemman tietoisuuden varmistamiseksi. Johtopäätöksissä tuodaan paremmin esille vastaajien ajatuksia tietoturvan kehittämiseksi sekä tietoturvauhkien välttämiseksi.

Tutkimusmenetelmän, kyselyn sekä tilastollisesti kuvaavan analyysin hyödyntämisen myötä arvioidaan kokonaisuudessaan tutkimuksen luotettavuutta ja sitä, miten tutkimus on onnistunut. Määrällistä tutkimusmenetelmää käytettäessä tutkimuksen pätevyyttä ja luotettavuutta arvioidaan reliabiliteetin ja validiteetin käsitteitä hyödyntäen. KvantiMOTV (2008) mukaan validiteetin avulla arvioidaan sitä, onko valittu tutkimusmenetelmä mitannut juuri sitä, mitä on haluttu mitata. Reliabiliteetin avulla arvioidaan tutkimuksen johdonmukaisuutta ja sitä, että sillä mitataan kokonaisuudessaan aina samaa asiaa. (KvantiMOTV, 2008)

Tutkimuksen reliabiliteettia vahvistaa se, että vastaajat valikoituivat satunnaisesti haastattelijoiden tuttavapiiristä. Kyselyyn osallistumista varten vastaajille laadittiin hyvät vastausohjeet ja kysymykset esitettiin jokaiselle samassa järjestyksessä. Tutkimuksen kattava teoriatausta loi hyvän perustan tutkimukselle. Kyselyyn osallistuneet 69 vastaajaa mahdollistivat riittävän laajan tutkimusaineiston, jota analysoimalla tuotettiin uutta tietoa siitä, mitkä tekijät voivat vaikuttaa tietoturvauhkien ehkäisemiseen sekä edistää käyttäjien tietoturvatasoa. Tutkimusaineiston myötä saadut tulokset vastasivat hyvin todellisuutta, ja niitä voidaan yhdistää tutkimuksessa kohteena olleisiin ilmiöihin eli kriiseihin ja

tietoturvauhkiin. Tutkimuksen validiteettia lisää myös se, että valittujen tutkimusmenetelmien avulla vastauksia tavoiteltiin käyttäjien havaintojen, kokemusten sekä ajatusten pohjalta.

7.2 Kyselyn toteutuminen

Tutkimuksen kyselyn vastaajat valikoituivat haastattelijoiden tuttavapiiristä satunnaisesti, jolloin saatiin kattava katsaus vastaajien tietoturvaan liittyen vastaajan taustasta riippumatta. Vastaajat edustavat sosiaalisen median peruskäyttäjiä monella eri tietotekniikan lähtötasolla, iällä sekä koulutus ja työelämän taustoilla. Kyselyn toteuttaminen osana Kyberturvallisuus 1: perusteet kurssia vaikutti mahdollisesti siihen, että enemmistö vastaajista lukeutui nuorempaan ikäryhmään kyselyn vastauksista saadun mediaanin vuoksi. Kyselyn saavutettavuutta voidaan pitää hyvänä, sillä kyselyyn osallistumiseksi vastaajille tarjottiin web-lomakkeen lisäksi myös tulostettua lomaketta. Tutkimuksessa oli tärkeää kiinnittää huomiota johdonmukaisuuteen ja täsmälliseen kieleen kyselyä laadittaessa. Kyselyn rakenne pyrittiin pitämään yksinkertaisena ja sopivan mittaisena, jotta vastaajat keskittyvät vastaamaan kysymyksiin kattavasti. Kyselyyn vastaaminen tapahtui anonyymisti, joten voidaan olettaa vastaajien vastanneen kysymyksiin rehellisesti ja todenmukaisesti. Anonyymissä kyselytutkimuksessa yksittäisiä vastaajia ei voida tunnistaa, eikä tutkimuksessa ole käytetty vastaajiin liittyviä luokitteluja. Kyselyn myötä kerätyt aineistot poistetaan tutkijan toimesta heti tutkimuksen valmistuttua.

Tutkimuksen validiteettiin vaikuttaa erityisesti se, ymmärsivätkö vastaajat esitetyt kysymykset samalla tavalla kuin tutkija. Vastaajat pitivät kysymyksiä hyvinä ja ajankohtaisina, sillä niissä huomioitiin tämän hetken tietoturvauhat sekä kriisit. Vastaajat antoivat esitettyihin kysymyksiin kattavia vastauksia ja tämän perusteella haastattelua voidaan pitää laadukkaana. Käyttäjien vastaukset olivat pääosin kirjattu sanasta sanaan, joten myös vastauksia voidaan pitää todenmukaisina.

Haastattelijoiden mukaan kyselyä pidettiin selkeänä, eikä kysymyksiä tarvinnut haastattelun aikana tarkentaa. Haastattelijoiden mukaan käyttäjien tietoisuus tietoturvauhista oli pääosin hyvällä tasolla, mutta joitakin tietoturvakäytäntöjä tulisi parantaa. Kyselyä varten pidetyssä teematilaisuudessa nousi esiin, että kyselyn haastattelijoiden hyvästä tietoteknisestä tasosta ja tietoturvan osaamisestaan huolimatta, haastattelijat löysivät paljon parannettavaa omista tietoturva käytännöistään.

7.2.1 Käyttäjien tietoturva

Valeuutisten määrä on kasvussa uusien ajankohtaisten tapahtumien tai kriisien myötä, esimerkiksi koronapandemia, Ukrainan sota tai vaalit, jolloin valeuutisilla yritetään vaikuttaa ihmisten yleiseen mielipiteeseen. Suurin osa käyttäjistä luottavat sosiaalisessa mediassa jaettuihin uutisiin varauksella. Käyttäjien kriittinen näkökulma sekä omat kokemukset auttavat välttämään jaettuihin uutisiin liittyen myös valeuutisten vaikutusta. Vastausten perusteella käyttäjät tunnistavat pääsääntöisesti valeuutisen sekä osaavan arvioida uutisen todenperäisyyttä. Huomioitavaa vastauksissa ja käyttäjien tietoturvakäytännöissä oli se, että vaikka kyselyssä käyttäjät kertoivat, etteivät he luota pääosin sosiaalisessa mediassa esiintyviin uutisiin, eivät he kuitenkaan tarkista uutisten todenmukaisuutta säännöllisesti. Käyttäjien tulisi kehittää omaa tietoturvakäyttäytymistään ja kehittää säännöllinen tapa sisällön tarkastamiselle.

Suurin osa käyttäjistä kertoi kohdanneensa tietojenkalastelua sosiaalisessa mediassa. Käyttäjät osaavat pääosin tunnistaa tietojenkalasteluyrityksen, jonka myötä vain viidesosa käyttäjistä on joutunut tietojenkalastelun uhriksi.

Käyttäjistä suurin osa on tavannut valearvontoja sosiaalisessa mediassa, mutta valtaosa käyttäjistä ei kuitenkaan osallistu arvontoihin sosiaalisessa mediassa, joten valearvonnan uhriksi joutuminen on harvinaisempaa. Huomattavaa vastauksissa kuitenkin on se, että osallistuessaan arvontaan käyttäjistä vain n. 40 % lukee aina mihin heidän tietojansa käytetään. Tietojen luovuttaminen arvonnan pitäjälle lukematta arvonnan sääntöjä sekä ehtoja aiheuttaa tietoturvariskin ja voi johtaa tilausansaan tai tietojenkalasteluun. Kuitenkin suurin osa käyttäjistä tarkistaa aina arvonnan pitäjän olevan oikea yritys tai sivusto, jolloin voidaan huomattavasti pienentää riskiä joutua valearvonnan uhriksi.

Käyttäjät ovat kohdanneet sosiaalisessa mediassa henkilöitä, jotka esiintyvät jonkin toisen yrityksen tai henkilön nimellä. Käyttäjistä n. 40 % kertoivat itsensä tai tuttavan joutuneen identiteettivarkauden uhriksi. Käyttäjät kertoivat kuitenkin pääosin osaavansa pienentää identiteettivarkauden riskiä. Monet käyttäjät ovat rajanneet mitä tietoja he laittavat verkkoon, eivätkä he luovuta kriittisiä tietojaan kenellekään verkossa.

Käyttäjien yksityisyysasetukset sosiaalisessa mediassa ovat hyvin rajattu, eivätkä käyttäjät koe olevansa huolestuneita heidän yksityisyydestään sosiaalisen median alustoilla. Käyttäjistä suurin osa on ottanut kaksivaiheisen tunnistautumisen käyttöön käyttäjätileille. Käyttäjien tietoturvallisissa käytännöissä on kuitenkin parannettavaa, sillä lähes puolet käyttäjistä olivat hyväksyneet sosiaalisessa mediassa kavereiksi käyttäjiä, joita he eivät tunne. Käyttäjät kirjautuvat harvoin palveluista ulos, joten vain n. 7 % käyttäjistä

kirjautuu palveluista ulos aina käytön jälkeen. Käyttäjät ovat hakeneet aktiivisesti itseään hakukoneilla verkosta kartoittaakseen millaista tietoa itsestä on julkisesti saatavilla, jolloin voidaan tarvittaessa rajoittaa omien tietojen näkymistä. Vastausten perusteella voitiin päätellä, että valeuutiset, tietojen kalastelu, valearvonnat sekä identiteettivarkaudet ovat ajankohtaisia tietoturvauhkia sosiaalisessa mediassa.

7.2.2 Johtopäätökset

Kyselyn vastausten perusteella suurin osa käyttäjistä kertoivat tietävänsä käsiteltyjen uhkien määritelmän ja osaavansa tunnistaa uhan tarvittaessa. Näin ollen käyttäjien tietoisuutta voidaan pitää tämän tutkimuksen osalta käsitellyistä tietoturvauhista varsin hyvänä. Osalle vastaajista valearvonta oli kuitenkin uusi käsite. Käyttäjät kokivat kyselyssä olevien tietoiskujen antavan tietoa esillä olleiden uhkien varalle sekä jatkossa pystyvänsä välttämään uhkien realisoitumisen. Suurin osa käyttäjistä ovat saaneet tietoa sosiaalisen median tietoturvasta tuttaviltaan sekä itse hakemalla tietoa verkosta. Perinteisen median (tv, radio, lehdet) kautta käyttäjät ovat saaneet myös huomattavan määrän tietoa. Kyselyn vastausten perusteella paremman tietoteknisen taidon omaava käyttäjä huomaa todennäköisemmin tietoturvauhkia kuin heikomman tietoteknisen taustan omaava henkilö. Käyttäjät suhtautuivat pääosin verkossa jaetun tietoon kriittisesti, joka on tärkeä ominaisuus tietoturvauhilta suojautumisessa. Tarkastelemalla verkossa jaettua sisältöä kriittisesti, käyttäjä voi vähentää huomattavasti riskiä joutua hyökkäyksen uhriksi. Kaikkien käyttäjien tulisi ottaa käyttöönsä myös kaksivaiheinen tunnistautuminen tiliensä tietoturvan parantamiseksi. Käyttäjien tulisi myös sisällyttää palveluista ulos kirjautuminen omaan tietoturva-arkeensa.

Käyttäjät kertoivat, että tietoturvakoulutuksiin pitäisi saada mukaan myös “mitä tehdä uhriksi joutuessa?”. Monesti tietoturvaa koskevissa oppaissa kerrotaan, miten voidaan minimoida riskejä sekä välttää uhkia, mutta harvemmin käsitellään miten toimia uhriksi joutuessa. Käyttäjät myös toivoivat perinteisen median kertovan ajankohtaisista tietoturva uhista ja teemoista, jolloin useampi käyttäjä taustoista sekä iästä riippumatta saisi tietoa tietoturvauhista. Sosiaalisen median käyttäjämäärien kasvaessa myös vanhemmat ihmiset ovat alkaneet käyttämään sosiaalista media, eivätkä he välttämättä seuraa verkossa toimivaa uutisointia, jolloin perinteisen median kautta tapahtuva uutisointi ajankohtaisista tietoturvauhista olisi tärkeää.

7.3 Tutkimuksen kehittämiskohteet

Tutkimuksen perusteella käyttäjien sosiaalisen median tietoturvaan liittyen suurimpana ongelmana ovat käyttäjien omat tietoturvakäytännöt. Tutkimuksen mukaan käyttäjien olisi syytä keskittyä enemmän tiedon todenmukaisuuden varmentamiseen, jolloin voidaan välttyä disinformaation vaikutukselta.

Käyttäjien vastausten perusteella erilaisten medioiden tulisi tiedottaa näkyvämmin myös ajankohtaisista tietoturvauhista sekä tietoturvaan liittyvistä ohjeistuksista. Perinteisen median (tv, radio, lehdet) tulisi tiedottaa enemmän myös ajankohtaisista tietoturvauhista. Tietoturvaa koskevia tiedotteita tulisi lisätä, jolloin tiedolla voitaisiin tavoittaa myös ne käyttäjät, jotka eivät seuraa aktiivisesti verkossa tapahtuvaa uutisointia. Tietoturvaohjeistuksiin tulisi sisällyttää myös aihe “mitä tehdä kyberrikoksen uhriksi joutuessa?”.

Tutkimuksen perusteella jatkotutkimuksessa olisi ajankohtaista tarkastella valeuutisten ja disinformaation vaikutusta sekä esiintyvyyttä kriisien aikana. Erityisesti koronapandemian ja Ukrainan kriisin aikana tapahtunut valeuutisten lisääntyvyys vaikuttaa sosiaalisen median tietoturvaan huomattavasti. Aiheesta tulisi tehdä kattava tutkimus, minkälaisia vaikutuksia disinformaatiolla on ja miten sitä voidaan ehkäistä sosiaalisen median alustoilla. Jatkotutkimuksessa tulisi myös selvittää kriisien ja disinformaation yhteyttä, sekä miten kriisejä hyödynnetään disinformaation levittämisessä.

Tutkimus voidaan todeta onnistuneeksi, sillä tutkimuskysymyksiin saatiin runsaasti vastauksia. Tutkimuksesta saatujen vastausten perusteella oli mahdollista tehdä johtopäätöksiä. Tutkimuksen aiheena oleva sosiaalinen media ja siihen sisältyvät tietoturvauhat ovat hyvin ajankohtaisia aiheita. Tutkimuksen tuloksia tulee tulkita varauksella, sillä tutkimuksen aiheena oleva sosiaalinen media ja sen tietoturva ovat jatkuvassa muutoksessa.

LÄHTEET

Abrams, L. (2021, April 3). *533 million Facebook users' phone numbers leaked on hacker forum*. https://www.bleepingcomputer.com/news/security/533-million-facebook-users-phone-numbers-leaked-on-hacker-forum/

Alkawaz, M. H., Khan, S. A., & Abdullah, M. I. (2021). Plight of Social Media Users: The Problem of Fake News on Social Media. *2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 289–293. https://doi.org/10.1109/ISCAIE51753.2021.9431841

Anttila, V.-J. (2021). Koronavirus (SARS-CoV-2, COVID-19). In *Lääkärikirja Duodecim*. https://www.terveyskirjasto.fi/dlk01257

Baker-Eveleth, L., Stone, R., & Eveleth, D. (2021). Understanding social media users' privacy-protection behaviors [Article]. *Information & Computer Security*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ICS-07-2021-0099

Bîzgă, A. (2022, March 4). *Bitdefender Labs Sees Increased Malicious and Scam Activity Exploiting the War in Ukraine*. Bitdefender Labs. https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine/?cid=soc%7Cc%7Cfb%7CH4SUKR&fbclid=IwAR3POXcpaNxFT8-H0pXeOfV1Lkg36_OzUH4G6vs0fbTpAJaPSLWMbHMp1zE

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). The Socialbot Network: When Bots Socialize for Fame and Money. *Proceedings of the 27th Annual Computer Security Applications Conference*, 93–102. https://doi.org/10.1145/2076732.2076746

Botha, J., & Pieterse, H. (2020). Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security. In *International Conference on Cyber Warfare and Security* (pp. 57–66, XII). Academic Conferences International Limited. https://doi.org/http://dx.doi.org/10.34190/ICCWS.20.085

Cobbs, J. (2017, September 14). *DoxaGram: Instagram API used to Extract Millions of User Information*. UHWO Cyber Security. https://westoahu.hawaii.edu/cyber/vulnerability-research/vulnerabilities-weekly-summaries/doxagram-instagram-api-used-to-extract-millions-of-user-information/

DataReportal. (2021, November 5). *FACEBOOK STATS AND TRENDS*. https://datareportal.com/essential-facebook-stats

DataReportal. (2022, January). *DataReportal: GLOBAL SOCIAL MEDIA STATS*. https://datareportal.com/social-media-users

D'Souza, D. (2021, July 22). *What Is TikTok?* INvestopedia. https://www.investopedia.com/what-is-tiktok-4588933

ECDC. (2022, March 10). *COVID-19 situation update worldwide, as of week 8, updated 10 March 2022*. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

Euroopan komissio. (n.d.). *Koronavirukseen liittyvän disinformaation torjunta*. Retrieved April 7, 2022, from https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_fi#results-of-working-with-platforms

Facebook. (2012, April 9). *Facebook to Acquire Instagram*. https://about.fb.com/news/2012/04/facebook-to-acquire-instagram/

Finlex. (2013, December 13). *Rikoslaki 24 luku 8 § Yksityiselämää loukkaava tiedon levittäminen*. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L24P8

Freiling, I., Krause, N. M., Scheufele, D. A., & Brossard, D. (2021). Believing and sharing misinformation, fact-checks, and accurate information on social media: The role of anxiety during COVID-19 [Article]. *New Media & Society*. https://doi.org/10.1177/14614448211011451

F-Secure. (n.d.). *MITEN KÄYTTÄJÄTILIN KAAPPAUS TAPAHTUU?* Retrieved March 17, 2022, from https://www.f-secure.com/fi/home/articles/how-account-takeover-happens

F-Secure. (2021, December 14). *MITÄ ON TIETOJENKALASTELU?* https://www.f-secure.com/fi/home/articles/what-is-phishing

Hern, A. (2021, January 24). *WhatsApp loses millions of users after terms update*. The Guardian. https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update

Hern, A. (2022, March 21). *TikTok algorithm directs users to fake news about Ukraine war, study says*. https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says

Hossain, A. A., & Zhang, W. (2015). Privacy and security concern of online social networks from user perspective. *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, 246–253.

Jyväskylän yliopisto. (2015, April 23). *Määrällinen tutkimus*. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus

Jyväskylän yliopisto. (2021a, October 28). *Haastattelut*.

Jyväskylän yliopisto. (2021b, October 28). *Tilastollisesti kuvaava analyysi*. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/tilastollisesti-kuvaava-analyysi

Kaplan, A. (2020, January 28). *TikTok is hosting videos spreading misinformation about the coronavirus, despite the platform's new anti-misinformation policy*. https://www.mediamatters.org/fake-news/tiktok-hosting-videos-spreading-misinformation-about-coronavirus-despite-platforms-new

Kaspersky. (2021, December 14). *Kuinka tunnistat valeuutiset*. https://www.kaspersky.fi/resource-center/preemptive-safety/how-to-identify-fake-news

Kemp, S. (2021a, November 5). *TIKTOK STATS AND TRENDS*. https://datareportal.com/essential-tiktok-stats

Kemp, S. (2021b, November 5). *Essential Twitter stats for 2021*. TWITTER STATS AND TRENDS. https://datareportal.com/essential-twitter-stats

Kemp, S. (2021c, November 5). *INSTAGRAM STATS AND TRENDS*. Datareportal. https://datareportal.com/essential-instagram-stats

Khan, N. F., Ikram, N., Murtaza, H., & Asadi, M. A. (2021). Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach [Article]. *Kybernetes*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/K-05-2021-0377

Kuluttajaliitto. (n.d.). *Koronavirukseen liittyvät huijaukset*. Retrieved April 18, 2022, from https://www.kuluttajaliitto.fi/materiaalit/koronavirukseen-liittyvat-huijaukset/

KvantiMOTV. (2008, July 2). *Mittaaminen: Mittarin luotettavuus*. https://www.fsd.tuni.fi/menetelmaopetus/mittaaminen/luotettavuus.html

Kyberturvallisuuskeskus. (2019, September 20). *Tekstiviestihuijauksia liikkeellä runsaasti – lue tarkasti, mihin olet sitoutumassa*. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekstiviestihuijauksia-liikkeella-runsaasti-lue-tarkasti-mihin-olet-sitoutumassa

Kyberturvallisuuskeskus. (2020a). *Tietoturvan vuosi 2020*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf

Kyberturvallisuuskeskus. (2020b, May 13). *WhatsApp-tilien vahvistuskoodeja kalastellaan Suomessa*. TIETOTURVA NYT! https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/whatsapp-tilien-vahvistuskoodeja-kalastellaan-suomessa

Kyberturvallisuuskeskus. (2022, January 20). *Aktiivista Facebook-tunnusten kalastelua Facebook Messengerin kautta*. TIETOTURVA NYT!

Mättö, V. (2015, January 3). *Suomalaiset vahvasti Facebook-kansaa – WhatsApp toiseksi suosituin*. Yle Uutiset. https://yle.fi/uutiset/3-7707216

Mottola, I. (2016, October 8). *The history of Instagram*. Medium.Com. https://medium.com/@ignaziomottola/the-history-of-instagram-ff266eb75427

MySafety. (2021, March 26). *SUOMALAISET EIVÄT MIELLÄ IDENTITEETTIVARKAUTTA RIKOKSEKSI – TÄMÄ VAIKUTTAA AVUN HAKEMISEEN*. https://www.mysafety.fi/lehdistohuone/suomalaiset-eivat-miella-identiteettivarkautta-rikokseksi

Neskey, C. (2022, March 2). *Are Your Passwords in the Green?* Hive Systems. https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Norton. (2021). *2021 NORTON CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS*.

O'Donnell, L. (2021, January 14). *Telegram Bots at Heart of Classiscam Scam-as-a-Service*. Threatpost. https://threatpost.com/telegram-bots-classiscam-scam/163061/

Paul, K. (2019, April 18). *Facebook security lapse affects millions more Instagram users than first stated*. The Guardian. https://www.theguardian.com/technology/2019/apr/18/instagram-facebook-password-lapse-privacy-breach-data-exposed-

Phillips, S. (2007, July 25). *A brief history of Facebook*. https://www.theguardian.com/technology/2007/jul/25/media.newmedia

PhishLabs. (2021, November). *QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT NOVEMBER 2021*. https://info.phishlabs.com/quarterly-threat-trends-and-intelligence-november-2021

Rafter, D. (2020, October 22). *Social Media Identity Theft: How to Protect Yourself*. LifeLock. https://www.lifelock.com/learn/internet-security/social-media-behavior-leads-identity-theft

Rikosuhripäivystys. (n.d.). *IDENTITEETTIVARKAUDESSA ESIINNYTÄÄN TOISEN HENKILÖLLISYYDELLÄ*. Retrieved February 23, 2022, from https://www.riku.fi/erilaisia-rikoksia/identiteettivarkaus-2/

R-Kioski. (2021, December 4). *R-Kioski Facebook päivitys*. www.facebook.com

Rosen, G. (2021, August 18). *Meta: Community Standards Enforcement Report, Second Quarter 2021*. https://about.fb.com/news/2021/08/community-standards-enforcement-report-q2-2021/

SOSIADMIN. (2018, July 4). *Sosiaalisen median tietoturvariskit*. http://www.sosiaalinenmediaopetuksessa.com/sosiaalisen-median-tietoturvariskit/

Strauss, V. (2018, December 10). *Word of the year: misinformation. Here's why.* The Washington Post. https://www.washingtonpost.com/education/2018/12/10/word-year-misinformation-heres-why/

Summers, A. (2020, June 28). *A brief history of Whatsapp and where Whatsapp for Business is heading*. Chatwise. https://www.chatwise.io/post/a-brief-history-of-whatsapp-and-where-whatsapp-for-business-is-heading

Telegram. (n.d.-a). *End-to-End Encryption, Secret Chats*. Retrieved February 18, 2022, from https://core.telegram.org/api/end-to-end

Telegram. (n.d.-b). *Telegram FAQ*. Retrieved February 18, 2022, from https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here

Telegram. (2021). *The Evolution of Telegram*. https://telegram.org/evolution?setln=en

THL. (2022, March 10). *Koronatapaukset, sairaalahoidon tilanne ja kuolemat*. https://www.thl.fi/episeuranta/tautitapaukset/koronakartta.html

Tidy, J. (2020, March 13). *Coronavirus: How hackers are preying on fears of Covid-19*. https://www.bbc.com/news/technology-51838468?fbclid=IwAR1bOZ4L5v4vK__zgu7ogAkMpHs1Q5ntjEm5Gt27eOUkjAltuLddZXGZ0_A

TikTok. (2021, September 27). *Thanks a billion!* https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok

Tilastokeskus. (2021, November 30). *Verkkokauppa murroksessa*. https://www.tilastokeskus.fi/til/sutivi/2021/sutivi_2021_2021-11-30_fi.pdf

Tilastokeskus. (2022, January 19). *Tietoon tulleiden omaisuusrikosten määrä laski 13,6 prosenttia*. https://www.stat.fi/til/rpk/2021/04/rpk_2021_04_2022-01-19_tie_001_fi.html

Trend Micro. (2022). *Trend Micro 2021 Annual Cybersecurity Report*. https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

Twitter. (2021, July 14). *COVID-19 Misinformation*. https://transparency.twitter.com/en/reports/covid19.html#Content:2021-jan-jun:

Urbani, S. (2019, October). *Verifying Online Information*. First Draft. https://firstdraftnews.org/wp-content/uploads/2019/10/Verifying_Online_Information_Digital_AW.pdf

WhatsApp. (n.d.). *About the effective date for the January 2021 update*. Retrieved March 12, 2022, from https://faq.whatsapp.com/general/security-and-privacy/what-happens-when-our-terms-and-privacy-policy-updates-take-effect/?lang=en

WhatsApp. (2019, February 25). *Thank You for 10 Years*. https://blog.whatsapp.com/thank-you-for-10-years

WhatsApp. (2022). *Tietoja WhatsAppista*. https://www.whatsapp.com/about/

Whittaker, Z. (2019, May 20). *Millions of Instagram influencers had their contact data scraped and exposed*. TechCrunch. https://techcrunch.com/2019/05/20/instagram-influencer-celebrity-accounts-scraped/

WHO. (n.d.). *Coronavirus disease (COVID-19)*. Retrieved March 10, 2022, from https://www.who.int/health-topics/coronavirus

Wigmore, I. (2013, October). *disinformation*. Techtarget.Com. https://www.techtarget.com/whatis/definition/disinformation

YouTube. (n.d.). YouTuben yhteisön sääntöjen valvonta. *Avoimuusrapotti*. Retrieved February 26, 2022, from https://transparencyreport.google.com/youtube-policy/removals?total_channels_removed=period:2021Q4&lu=channels_by_reason&channels_by_reason=period:2021Q4

YouTube. (2010). *A Brief History of YouTube*. YouTube5Year. https://sites.google.com/a/pressatgoogle.com/youtube5year/home/short-story-of-youtube

LIITE A: TIETOTURVA-ARKI SOSIAALISESSA MEDIASSA KYSELY 1/2022

1. Esitiedot

a. Ikä
b. Sukupuoli
c. Olen?
d. Korkein suorittamasi koulutusaste?
e. Tietotekninen osaaminen
f. Mitä sosiaalisen median alustoja käytät?
g. Kuinka aktiivisesti kommentoit tai jaat uudelleen sosiaalisen median sisältöjä?
h. Oletko havainnut tietoturvauhkia sosiaalisessa mediassa?
i. Jos olet havainnut uhkia sosiaalisessa mediassa, niin millaisia uhat ovat olleet? (avoin kysymys)
j. Oletko huolestunut ajatuksesta joutua kyberrikoksen uhriksi?
k. Mistä huolesi koostuu? (avoin kysymys)
l. Tiedätkö, miten suojautua kyberrikoksilta?
m. Onko mielestäsi verkossa jaetun tiedon todenmukaisuus helposti pääteltävissä?

2. Valeuutiset

a. Tiedätkö, mitä ovat valeuutiset?
b. Mitä ymmärrät tarkoitettavan valeuutisilla? (avoin kysymys)
c. Luotatko sosiaalisessa mediassa esiintyviin uutisiin?
d. Kuinka suuren osuuden lukemistasi uutisista luet sosiaalisen median kautta?
e. Oletko kohdannut sosiaalisessa mediassa valeuutisia?
f. Minkälaisia valeuutisia olet kohdannut? (avoin kysymys)
g. Millä sosiaalisen median alustalla olet tavannut valeuutisia?
h. Kuinka usein olet tavannut valeuutisia sosiaalisessa mediassa?
i. Tarkistatko sosiaalisessa mediassa jaetun uutisen todenmukaisuuden?
j. Onko mielestäsi valeuutisten määrä kasvanut Ukrainan kriisin kärjistyessä?
k. Onko mielestäsi valeuutisten määrä kasvanut koronapandemian aikana?
l. Oletko huomannut pandemiaan liittyvän some-uutisoinnin muuttuneen viime aikoina Ukraina-aiheen vallatessa alaa?
m. Koetko valeuutisten olevan ongelma sosiaalisessa mediassa?
n. Millä tavoin tunnistat valeuutisen? (avoin kysymys)

3. Tietojenkalastelu (phishing)

a. Tiedätkö, mitä tarkoittaa tietojenkalastelu?
b. Oletko kohdannut tietojenkalastelua sosiaalisessa mediassa?
c. Oletko kohdannut tietojenkalastelua sähköpostitse?
d. Oletko avannut epäluotettavia linkkejä sosiaalisesta mediasta?
e. Oletko joutunut tai epäiletkö joutuneesi tietojenkalastelun uhriksi?
f. Osaatko tunnistaa tietojenkalasteluyrityksen?

4. Valearvonnat

a. Tiedätkö, mikä on valearvonta?
b. Oletko huomannut valearvontoja sosiaalisessa mediassa?
c. Oletko osallistunut arvontaan sosiaalisessa mediassa?
d. Kuinka usein luet arvonnan säännöt ja sen mihin tietojasi käytetään?
e. Kuinka usein olet tarkastanut arvonnan pitäjän olevan oikea yritys tai sivusto?
f. Osaatko erottaa valearvonnan oikeasta arvonnasta?

5. Identiteettivarkaudet

a. Tiedätkö, mitä ovat identiteettivarkaudet?
b. Oletko huomannut sosiaalisessa mediassa jonkun esiintyvän toisen henkilön tai yrityksen nimellä?
c. Oletko joutunut tai tiedätkö jonkun tuttavasi joutuneen identiteettivarkauden uhriksi?
d. Miten suojaudut identiteettivarkaudelta? (avoin kysymys)

6. Käyttäjätilin suojaus sekä yksityisyys

a. Oletko huolestunut käyttäjätilisi yksityisyydestä sosiaalisessa mediassa?
b. Oletko hyväksynyt kavereita tai seuraajia, joita et tunne?
c. Oletko rajannut sosiaalisen median julkaisujen yksityisyyttä?
d. Oletko ottanut käyttöön kaksivaiheisen tunnistautumisen käyttäjätileille?
e. Kirjaudutko palveluista ulos käytön jälkeen?
f. Oletko hakenut itseäsi googlesta ja katsonut, kuinka paljon tietoa sinusta löytyy haun avulla?
g. Jos olet hakenut itseäsi Googlesta, kuinka paljon tietoa löysit?
h. Kuinka huolestunut olet tiedoista, joita löysit itsestäsi hakukoneilla? (esim. Google)

7. Tietoisuus

a. Mistä sosiaalisen median tietoturvauhista olet ollut tietoinen ennen tätä kyselyä?
b. Oletko saanut kyselyn myötä tarpeeksi tietoa esillä olleista uhista ja keinoista uhkien välttämiseksi?
c. Mistä olet saanut tietoa sosiaalisen median tietoturvasta?
d. Mitkä tiedonlähteistäsi ovat lisänneet tietojasi sosiaalisen median tietoturvasta?
e. Mitkä tiedonlähteistäsi ovat vaikuttaneet eniten tietoturvakäyttäytymiseesi tai tietoturvakäytäntöihisi sosiaalisessa mediassa?
f. Millaista tietoa toivoisit saavasi tulevaisuudessa ja mistä? (avoin kysymys)
g. Herättikö kysely ajatuksia sosiaalisessa mediassa esiintyvistä uhista?
h. Mitä muita ajatuksia kysely herätti? (avoin kysymys)

8. Kysely

a. Kuinka kauan haastattelu kesti?
b. Miten kysely toteutettiin?
c. Oliko kysymyksiä, joita piti tarkentaa tai oliko haastateltavalla muita jatkokysymyksiä? (avoin kysymys)
d. Haastattelija: Kirjaa tähän ja seuraavaan omat huomiosi haastattelun perusteella. Mitä parannettavaa vastaajan tietoturva-arjessa tuli ilmi? (avoin kysymys)
e. Kuvittele itsesi vastaajan tilanteeseen. Mikä olisi paras tapa saada sinut tekemään tarvittavia tietoturva-arjen parannuksia - erityisesti sosiaalisessa mediassa. Jos parannettavaa ei tullut ilmi, mistä hyvä tilanne johtuu, tulkintasi mukaan? (avoin kysymys)