Lassi Laitinen

Käyttäjien tietoisuus kyberturvallisuusuhista ja digitaalisten järjestelmien turvallisuus

Tieto- ja ohjelmistotekniikan kandidaatintutkielma

30. huhtikuuta 2024

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Lassi Laitinen

Yhteystiedot: lassi.k.laitinen@student.jyu.fi

Ohjaaja: Sanna Juutinen

Työn nimi: Käyttäjien tietoisuus kyberturvallisuusuhista ja digitaalisten järjestelmien turvallisuus

Title in English: User awareness about cyber security threats and safety of digital systems

Työ: Kandidaatintutkielma

Sivumäärä: 22+0

Tiivistelmä: Yhteiskunnan digitalisoituessa käyttäjien on osattava käyttää digitaalisia järjestelmiä turvallisesti. Tutkielmassa tutkittiin käyttäjien tietoisuutta ja suhtautumista digitaalisten järjestelmien kyberturvallisuusuhkiin ja pyrittiin etsimään keinoja turvallisemman kyberympäristön luomiseksi. Tavoitteena oli luoda kirjallisuuskatsauksella kokonaiskuva käyttäjien tietoudesta ja suhtautumisesta kyberturvallisuusuhkiin. Tarkasteltujen tutkimusten perusteella suurin osa käyttäjistä ei ole tietoisia kyberturvallisuusuhista tai siitä, miten niitä voi ehkäistä, ja lisäksi tietouden huomattiin vaikuttavan käyttäjän suhtautumiseen turvallisuusuhista. Näitä asioita voi parantaa esimerkiksi koulutuksella ja tiedon levittämisellä.

Avainsanat: tietoisuus, suhtautuminen, kyberturvallisuusuhat, digitaaliset järjestelmät

Abstract: As society digitalizes, users need to know how to use digital systems safely. This thesis explores users' awareness and attitudes towards security threats in digital systems and tries to find ways to create a safer cyber environment. The aim was to use a literature review to create an overall picture of users' awareness and attitudes towards cyber security threats. Based on the reviewed studies, most users are not aware of cybersecurity threats or how to prevent them, and awareness was found to influence the user's attitude towards cyber security threats. These can be improved through training and dissemination of information,for example.

Keywords: awareness, attitudes, cyber threats, digital systems

Sisällys

1 Johdanto

Informaatioteknologian kehityksen myötä maailma nojaa entistä enemmän digitaalisiin ratkaisuihin, ja samalla internetissä vietetään yhä enemmän aikaa. Samalla myös alustojen käyttäjistä kerätään enenevissä määrin erilaista tietoa, ja käyttäjän kannalta on tärkeää voida käyttää digitaalisia järjestelmiä turvallisesti. Käyttäjän virheitä kybrerympäristöissä on vaikeaa eliminoida täysin, minkä vuoksi on tärkeää tutkia käyttäjän toimintaa (T. Rahman ym. 2021) ja siihen vaikuttavia tekijöitä. Turvallisen kyber- ja informaatioympäristön eteen on tehty viime vuosina paljon työtä, mutta ainakin vielä näyttää siltä, että käyttäjä on edelleen heikoin lenkki (Alotaibi ja Alfehaid 2019) turvallisuuden kannalta. Mutta mitä käyttäjät tietävät näistä uhista ja miten niihin suhtaudutaan?

Tämän kandidaatintutkielman tavoitteena on tutkia miten käyttäjät suhtautuvat eri digitaalisten järjestelmien turvallisuusuhkiin ja mitä käyttäjät niistä tietävät. Aiheeseen liittyy paljon muitakin erilaisia tekijöitä, mutta tässä tutkielmassa on tarkoitus keskittyä nimenomaan käyttäjien turvallisuusuhkiin suhtautumiseen ja käyttäjien tietoisuuteen. Kyberturvallisuusuhkien osalta tämä tutkielma keskittyy vain kyberympäristön turvallisuusuhkiin, eikä esimerkiksi fyysisiin uhkiin, kuten laitteen katoamisia tai muita vastaavia uhkia. Tämä rajaus on syntynyt pitkälti saatavilla olevan tiedon perusteella, kun on huomattu tästä aihealueesta olevan suhteellisen kattavasti tietoa tarjolla. Tutkielma on toteutettu kirjallisuuskatsauksena.

Ensimmäiseksi käsitellään käyttäjän kannalta keskeisimpiä digitaalisten järjestelmien turvallisuusuhkia. Luvussa 3 taas käsitellään käyttäjien tietoisuutta ja suhtautumista edellisessä luvussa käsiteltyihin turvallisuusuhkiin. Tämän jälkeen tutkitaan tietoisuuden ja suhtautumisen vaikutuksia, ja viimeiseksi luvussa 5 sitä, miten voitaisiin luoda käyttäjille turvallisempi kyberympäristö.

2 Kyberympäristön turvallisuusuhat

Käyttäjiä eli järjestelmien loppukäyttäjiä uhkaavat digitaalisissa ympäristöissä monenlaiset turvallisuusuhat. Turvallisemman digitaalisen ympäristön ja kyberturvallisuuskulttuurin luomisessa oleellista on tietää keskeisimmät ja yleisimmät kyberturvallisuusuhat (T. Rahman ym. 2021). Kyberturvallisuusuhat voivat johtua suunnitteluvirheessä esimerkiksi ohjelmistossa tai internetsivussa, muusta virheestä tai toisaalta myös käyttäjän tekemästä virheestä tai huolimattomuudesta. Näiden uhkien tunnistamisen helpottamiseksi tässä kappaleessa käsiteltävät kyberympäristön turvallisuusuhat on jaettu järjestelmän heikkouksiin ja uhkiin, joiden toteutumiseen käyttäjät voivat omalla toiminnallaan vaikuttaa. Yleisimpiä kyberturvallisuusuhkia käyttäjille ovat esimerkiksi haittaohjelmat, tietojenkalasteluhyökkäykset sekä palvelunestohyökkäykset (Humayun, Niazi, Jhanjhi ym. 2020).

2.1 Käyttäjän toiminnasta mahdollistuvat turvallisuusuhat

Kyberturvallisuusuhkien konkretisoitumiseen vaikuttaa joissakin tapauksissa keskeisesti käyttäjän toiminta ja käyttäytyminen verkossa. Käytettävän järjestelmän tai ohjelmiston käyttämä teknologia saattaa mahdollistaa hyökkäyksen, mutta oleellisin asia hyökkäyksen onnistumisessa voi olla käyttäjän, eli hyökkäyksen kohteen, toiminta.

Aiemmin mainituista kyberturvallisuusuhista tietojenkalasteluhyökkäykset ovat kenties tunnetuimpia. Kalasteluhyökkäyksissä hyökkääjä voi esiintyä jonakin toisena henkilönä tai tärkeänä tahona esimerkiksi sosiaalisessa mediassa pyrkimyksenään tavalla tai toisella saada käyttäjä antamaan henkilökohtaisia tietojaan (Parmar 2012). Hyökkääjä saattaa vedota kiireeseen, asian tärkeyteen tai henkilön henkilökohtaisiin ominaisuuksiin. Humayun ym. (2020) mukaan kalasteluhyökkäyksissä hyödynnetään monia eri teknologioita, kuten internetsivuja, sähköposteja ja erilaisia kommunikaatiotapoja. Tietojenkalasteluhyökkäykset ovat melko yleisiä, sillä lähes kolmasosalla käyttäjistä on kokemusta kalasteluyrityksen kohteeksi joutumisesta (NortonLifeLock 2023).

Tietojenkalasteluhyökkäyksiä on mahdollista hyödyntää myös identiteettivarkauksien toteuttamiseen. Identiteettivarkaus on toisen henkilön henkilötietojen luvatonta käyttöä esimer-

kiksi rahan hankkimiseksi, ja internetissä tai muussa verkkoympäristössä identiteettivarkaus mielletään esiintymisenä toisena henkilönä luvatta sekä kohteen tietämättä ja tämän identiteetin hyväksikäyttöä (Irshad ja Soomro 2018). Onnistuneella tietojenkalasteluhyökkäyksellä henkilökohtaisten tietojen hankkimisessa on mahdollista onnistua, jolloin hyökkääjä voi mahdollisesti hyödyntää hankkimiaan tietoja, kuten toisen henkilön identiteettiä vakuuttavasti. Internetissä toisena henkilönä esiintyminen on helpompaa kuin internetin ulkopuolella, mikä voi osaltaan nostaa identiteettivarkauksien onnistumisprosenttia. Internet on toisaalta myös helpottanut tietojen hankintaa.

Tietojen hankintaan tietojenkalastelijat voivat käyttää myös haittaohjelmia. Näissä hyökkäyksissä hyökkääjä pyrkii levittämään järjestelmän heikkouksia hyödyntäviä haittaohjelmia, joilla pyritään saamaan pääsy tietokoneen järjestelmän kautta käyttäjän tietoihin (Dodge, Carver ja Ferguson 2007). Haittaohjelmia voidaan levittää harmittomilta näyttävien tiedostojen ja linkkien kautta, joita jaetaan esimerkiksi sähköpostin liitteinä, esimerkiksi PDF-tiedostojen ja .zip- tai .jar-muotoisten tiedostokansioiden kautta jaettavia haittaohjelmien osuus on suuri (Tsochev ym. 2020). Haittaohjelmat ovat yksi esimerkki siitä, kuinka kyberturvallisuusuhkia on vaikea jaotella pelkästään käyttäjän toiminnan mahdollistaviksi ja käytettävästä digitaalisesta järjestelmistä johtuviksi. Haittaohjelmien levittämisessä käyttäjillä on keskeinen rooli, vaikka haittaohjelma hyödyntääkin käytettävän järjestelmän heikkouksia.

2.2 Digitaalisten järjestelmien heikkoudet

Käyttäjän toiminnan mahdollistavien turvallisuusuhkien taustalla on kuitenkin osaltaan hyökkäyksen, esimerkiksi haittaohjelman tai tietojenkalasteluyrityksen mahdollistava digitaalinen järjestelmä. Käyttäjän turvallisuuden parantamisesta ja tietojen turvassa pitämisestä on tullut yksi tärkeimmistä vaatimuksista digitaalisille alustoille ja järjestelmille (Hossain ja Zhang 2015). Digitaalisten järjestelmien yleisimmät heikkoudet ovat järjestelmien laitteistoissa, ohjelmistoissa, verkkoinfrastruktuurissa ja protokollissa (Jang-Jaccard ja Nepal 2014).

Aiemmin mainituista kyberturvallisuusuhkista palveluestohyökkäykset ovat esimerkki hyökkäyksestä, joissa hyödynnetään digitaalisen järjestelmän heikkouksia ohjelmistossa, verk-

koinfrastrukstuurissa ja protokollissa. Palvelunestohyökkäyksissä pyritään estämään tietyn palvelun, kuten internetsivuston, käyttö tarkoituksena haitan aiheuttaminen käyttäjälle tai organisaatiolle (Kadena ja Gupi 2021). Humayunin ym. mukaan (2020) yksi syy, miksi esimerkiksi palvelunestohyökkäykset ovat suhteellisen yleisiä on se, että usein käytetään samankaltaisia teknologioita, joita hyökkääjät pystyvät hyödyntämään eri tahoihin kohdistuviin hyökkäyksiin.

Esimerkiksi useimpien sosiaalisen median alustojen arkkitehtuuri on keskitetty, joka altistaa alustan vakaville seurauksille, varsinkin jos hyökkääjä pääsee keskuspalvelimelle (Aswal ym. 2022). Käyttäjän kyberturvallisuuden kannalta tietojen turvassa pitäminen on erityisen tärkeää alustoilla, joissa käyttäjästä on paljon tietoa ja alusta käyttää teknologiaa joka on laajasti käytössä, kuten juuri sosiaalisen median alustoilla. Lisäksi on tärkeää, että järjestelmien suunnittelussa otetaan huomioon arkkitehtuurista tai muista teknologisista valinnoista mahdollisesti syntyvät turvallisuusuhat.

Kuten aiemmin todettiin, kybeturvallisuusuhkien jakaminen vain käyttäjän toiminnan mahdollistaviksi ja käytettävästä digitaalisesta järjestelmistä johtuviksi on vaikeaa, sillä usein sekä teknologialla että käyttäjän toiminnalla on vaikutusta uhkan konkretisoitumiseen. Haittaohjelmien lisäksi yksi esimerkki siitä, miten hyökkääjät voivat käyttää sekä käyttäjää että teknologiaa hyväkseen ovat avoimet Wi-Fi -verkot. Hyökkääjät voivat asettaa esimerkiksi kahvilaan tai muuhun julkiseen paikkaan julkisen langattoman verkon, jonka kautta hyökkääjä pääsee käsiksi kaikkeen verkon kautta lähetettävään informaatioon, kuten käyttäjän käyttäjätunnuksiin tai salasanoihin (Mhlanga, Maiti ja Hammer 2021). Teknologian kehittyessä myös järjestelmiin ja kyberympäristöön kohdistuvat hyökkäykset kehittyvät, mikä nostaa tarvetta kehittää myös suojausteknologioita ja -tapoja (Jang-Jaccard ja Nepal 2014). Paitsi järjestelmien salaus- ja suojausteknologioiden, myös käyttäjien taitojen ja tietojen kehittämiselle on edelleen jatkuvaa tarvetta.

3 Käyttäjien tietoisuus ja suhtautuminen kyberympäristön turvallisuusuhkiin

Tässä luvussa käsitellään käyttäjien tietoutta ja suhtautumista digitaalisten järjestelmien turvallisuusuhkiin. Tietoisuus on yksi merkittävimmistä tekijöistä, kun on tutkittu ihmisen vaikutusta kyberturvallisuuteen (Rohan ym. 2021). Käyttäjien tietoisuuteen sekä suhtautumiseen esimerkiksi internetin turvallisuusuhista vaikuttaa moni asia, joita tässä luvussa eritellään ja esitellään. Tieto käyttäjien tietoisuudesta ja suhtautumisesta kyberympäristön turvallisuusuhkiin on tärkeää esimerkiksi siksi, että voidaan tunnistaa vaikuttavimmat toimet, joilla etenkin käyttäjien turvallisuutta digitaalisissa järjestelmissä voidaan parantaa.

3.1 Käyttäjien tietoisuus kyberturvallisuusuhista

Käyttäjien voidaan olettaa olevan tietoisia termistä "kyberturvallisuus"(engl. *cyber security*) ja näin ollen käyttäjiä voi pitää tietoisina siitä, että toiminta digitaalisissa järjestelmissä voi altistaa heidät erinäisille turvallisuusuhille (Zwilling ym. 2022). Tietoisuutta erilaisten uhkien olemassaolosta voidaan pitää hyvänä lähtökohtana käyttäjien tietoisuuden tason selvittämiseksi.

Käyttäjän tietoisuus (engl. *awareness*) tarkoittaa sitä, että käyttäjä on tietoinen asiasta ja voi hyödyntää tietoa käyttäytymisessään (Alotaibi ja Alfehaid 2019). Tietoisuuteen mielletään usein vaikuttavan monet eri tekijät. Chandarmanin ja Van Niekerkin (2017) mukaan käyttäjän tietoisuuteen kyberturvallisuudesta vaikuttavat käyttäjän tiedot kyberturvallisuudesta, asenteet kyberturvallisuusuhkia kohtaan ja käsitykset omista taidoista, jotka muodostavat käyttäjän todelliset taidot ja käyttäytymisen sekä lopulta tietoisuuden.

Puutteellinen tieto ja tietämys kyberturvallisuudesta voi vaikuttaa esimerkiksi käyttäjän käyttämiin turvautumiskeinoihin tai keinojen käyttämättömyyteen. Turvallisuutta lisäävään käytökseen vaikuttaa lisäksi tietämyksen (engl. *knowledge*) taso (Quayyum, Cruzes ja Jaccheri 2021). Zwillingin ym. (2022) tutkimuksessa huomattiin, että usein käyttäjät käyttävät vain yksinkertaisia keinoja, kuten virustorjuntaohjelmiston asentamista ja vahvaa salasanasuo-

jausta, jotka eivät yksinään ole kovinkaan tehokkaita tai riittäviä. Vain yksinkertaisten keinojen käyttäminen voi kertoa esimerkiksi puutteellisista tiedosta siinä, mitkä toimet ovat tehokkaita käyttäjän kyberturvallisuuden lisäämiseksi, tai tietämyksestä käyttäjän tietojen käytöstä. Toisaalta tähän voi vaikuttaa myös käyttäjän suhtautuminen kyberturvallisuusuhkiin. Kuitenkin maailmanlaajuisesti 83 prosenttia käyttäjistä haluaisi tehdä enemmän oman yksityisyytensä eteen, mutta hieman yli puolet käyttäjistä ei tiedä miten (NortonLifeLock 2023). Tämä viittaa puutteelliseen tietoon juuri niistä keinoista, joilla käyttäjä voisi omaa turvallisuuttaan parantaa.

Puutteellinen tieto näkyy esimerkiksi siten, että online-alustojen, kuten sosiaalisen median alustojen ja sovellusten, käyttäjistä melkein puolella ei ole tarpeeksi tietoa alustojen yksityisyyskäytännöistä tai -mekanismeista (Hossain ja Zhang 2015). Eri alustoilla on käytössä monia eri teknologioita, joilla käyttäjistä kerätään dataa, jota hyödynnetään parempien palveluiden tarjonnassa esimerkiksi kohdentamalla markkinointia. Näitä teknologioita voidaan käyttää kuitenkin myös käyttäjää vastaan. Esimerkiksi internetsivustojen ja sosiaalisen median alustojen käyttämiin evästeisiin liittyy korkea riski tietomurroista ja datan varastamisesta. Tirumalan ym. (2019) mukaan käyttäjät eivät kuitenkaan pidä evästeiden käyttöä heidän turvallisuuteensa tai yksityisyyteensä vaikuttavana tekijänä, eikä myöskään tietous tietojen keräämisestä tai sen tavoista ole kovinkaan laajaa.

Toisaalta voidaan myös pohtia sitä, mikä vaikutus käyttäjän kokemuksella omista taidoistaan on. Vaikka käyttäjä luottaisi täysin omiin taitoihinsa, hän ei voi mennä takuuseen siitä, ettei joutuisi esimerkiksi kyberrikoksen uhriksi. Chandarmanin ja Van Niekerkin (2017) mukaan käyttäjän kokemuksella omista taidoista on kuitenkin suuri vaikutus käyttäjän todelliseen käytökseen, mutta käyttäjän luottamus omiin taitoihin on kuitenkin turhaa ilman oikeita tietoja ja asenteita sekä todenmukaista ymmärrystä omista taidoista tai käyttäytymisestä.

3.2 Käyttäjien suhtautuminen turvallisuuteensa digitaalisissa järjestelmissä

Tieto siitä, miten käyttäjät suhtautuvat omaan yksityisyyteensä, on tärkeää siksi, että heikko tietoturva tai turvaton järjestelmä voi olla itsessään turvallisuusuhka. Myös tietojen keräämi-

nen rikolliseen toimintaan on vakava uhka käyttäjien kyberturvallisuuden kannalta. Samaan aikaan internetin ja eri alustojen käyttö on lisääntynyt, mikä on samalla kasvattanut myös käyttäjistä kerättävien tietojen määrää. Internetin käyttäjiä on maailman reilusta 8 miljardista 66 prosenttia ja näistä käyttäjistä noin 30 prosenttia on huolissaan tietojensa väärinkäytöstä (DataReportal 2024). Kyseessä on kuitenkin lähes kolmannes käyttäjistä, joten huoli mahdollisesta tietojen väärinkäytöstä ei ole vähäistä. Hossainin ja Zhangin (2015) mukaan suhtautumiseen tietojen väärinkäytöstä voivat vaikuttaa esimerkiksi epäselvät tietoturva- ja yksityisyyskäytännöt, joita hieman yli puolet ei ole edes silmäillyt läpi.

Useimpien käyttäjien on huomattu olevan huolissaan paitsi tietojen väärinkäytöstä myös omien tietojensa yksityisyydestä sekä turvallisuudestaan digitaalisissa järjestelmissä. Tämä tuli esiin myös edellisessä kappaleessa 3.1, kun pohdittiin käyttäjien tietoutta kyberturvallisuusuhista. Hossainin ja Zhangin (2015) tutkimuksessa todetaan, että vähintään kaksi kolmesta on huolissaan tietojensa yksityisyydestä, mutta suurin osa käyttäjistä on tyytyväisiä alustojen yksityisyyskäytäntöjen oletusasetuksiin.

Kiinnostavaa onkin se, että tietoturvasta ja yksityisyydestään huolissaan olevia käyttäjiä on enemmän kuin niitä, jotka ovat lukeneet omien tietojensa käytöstä. Kuitenkin useimmiten käyttäjän tulee hyväksyä alustan tai sovelluksen tietoturva- ja yksityisyyskäytännöt ennen käyttöä. Mikäli suurin osa käyttäjistä ei syystä tai toisesta lue tai silmäile näitä käytäntöjä, voi käyttäjälle muodostua epärealistinen kuva tietojensa käytöstä ja tätä kautta turvallisuudestaan. Suhtautuminen digitaalisten järjestelmien tietoturva- ja yksityisyyskäytäntöihin on yllättävän välinpitämätöntä, sillä Aswalin ym. (2022) mukaan suurin osa erityisesti sosiaalisen median käyttäjistä haluaa turvaa erinäisiä turvallisuusuhkia vastaan.

Käyttäjät joutuvat punnitsemaan järjestelmän käytössä hyötyjen ja haittojen välillä. Vaikka suurin osa käyttäjistä kokee haluavansa turvallisuutta kyberympäristöissä, on kuitenkin aina myös käyttäjiä, joille tietoturvan ongelmat eivät ole niin merkittäviä. Baker-Evelethin ym. (2022) mukaan useimmiten ne käyttäjät, jotka arvostavat sosiaalisen median hyötyjä esimerkiksi näkyvyyden tai verkoston kasvattamisessa, suhtautuvat yksityisyyteen väljemmin ja esimerkiksi rajoittavat profiiliensa näkyvyyttä harvemmin.

Vaikka käyttäjä suhtautuisi tarvittavalla vakavuudella turvallisuuteensa digitaalisissa järjes-

telmissä, suhtautuminen yksittäisiin turvallisuutta heikentäviin tapoihin voi näin olla välinpitämätöntä tai käyttäjän kyberturvallisuutta heikentävää. Käyttäjän suhtautuminen kyberturvallisuusuhkiin voi olla ylenkatsovaa esimerkiksi siten, että käyttäjä luottaa siihen etteivät ystäviltä tulevat viestit tai tiedostot sisällä mitään vaarallista, vaikkei siitä olisi takuita (Chandarman ja Van Niekerk 2017). Haittaohjelmia tai muita tietojenkalastelulinkkejä voidaan hyvinkin levittää harmittomilta vaikuttavien tiedostojen kautta, eikä luotetulta henkilöltä tuleva tiedosto ole automaattinen takuu turvallisuudelle.

Chandarmanin ja Van Niekerkin (2017) tutkimuksessa tuodaan esille myös suhtautumisen negatiivinen korrelaatio tietämyksen, todellisten tietojen ja taitojen sekä omien taitojen käsityksen kanssa. Heidän mukaansa esimerkiksi huono tietämys kyberturvallisuusuhista johtaisi asenteeseen, joka voisi parantaa käyttäjän kyberturvallisuutta, tai toisinpäin. Tämän korrelaation kautta huomataan, ettei suhtautuminen kyberturvallisuusuhkiin ole yksiselitteistä. Suhtautuminen vaihteleekin paljon riippuen käyttäjästä, käyttäjän kiinnostuksesta ja kokemasta hyödystä. Hossainin ja Zhangin (2015) mukaan myös tietämättömyys keinoista tai uhista ylipäätään voi vaikuttaa käyttäjien suhtautumiseen.

4 Kyberturvallisuusuhkien ja tietoisuuden vaikutukset käyttäjään

Suurin osa käyttäjistä pitää kyberrikollisuutta maansa turvallisuuteen vaikuttavana tekijänä (Adebiaye, Alryalat ja Owusu 2016). Käyttäjän näkökulmasta kyberturvallisuusuhkien vaikutukset voivat näkyä, paitsi yhteiskunnan turvallisuuden kautta, myös monin eri tavoin, joita tässä luvussa eritellään. Samalla kun yhteiskunta digitalisoituu ja luottaa enenevissä määrin digitaalisiin ratkaisuihin, on järjestelmien kyberturvallisuusuhista ja erityisesti niiden vaikutuksista oltava tietoisia.

Vaikka kyberrikokset ja -hyökkäykset kohdistuvat useammin yrityksiin ja organisaatioihin kuin suoraan käyttäjään (Humayun, Niazi, Jhanjhi ym. 2020), on organisaatioilla usein juuri käyttäjien dataa, joka on vaarassa joutua hyökkääjän käsiin. Erityisesti kriittiseen infrastruktuuriin liittyvillä hyökkäyksillä voidaan aiheuttaa paljon haittaa sekä yhteiskunnalle että käyttäjille, jotka voivat vaikuttaa talouteen, yleiseen elämään sekä turvallisuuteen (Kadena ja Gupi 2021). Erityisesti näiden uhkien konkretisoituminen esimerkiksi kyberhyökkäyksenä vaikuttaa käyttäjään. Kyberrikoksen tai -terrorismin uhriksi joutuminen voi muuttaa käyttäjän suhtautumista säädöksiin sekä ohjeistuksiin, ja uhriksi joutuneet haluavat viranomaisilta kovempia toimia sekä enemmän tietoa heitä mahdollisesti uhkaavista uhista (Snider ym. 2021).

Lisäksi jatkuvat turvallisuusrikkomukset tai tietomurrot voivat vaikuttaa negatiivisesti käyttäjien luottamukseen digitaalisia järjestelmiä kohtaan (McCrohan, Engel ja Harvey 2010). Näin käyttäjälle voi aiheutua turvattomuuden tunnetta digitaalisissa järjestelmissä toimiessa ja täten myös vaikuttaa käyttäjän toimintaan sekä suhtautumiseen digitaalisia järjestelmiä kohtaan. Mikäli saman järjestelmän heikkoudet nousevat jatkuvasti esiin, on mahdollisesta ettei osa käyttäjistä halua jatkaa järjestelmän tai sovelluksen käyttämistä. Jos tähän yhdistetään käyttäjän tietoisuuden puute siitä, miten omaa turvallisuuttaan voi parantaa, käyttäjälle voi tulla vahva turvattomuuden tunne kyberympäristössä toimimisesta.

Myös tietoisuuden taso ja siinä tapahtuvat muutokset voivat näkyä sekä käyttäjän turvallisuutta lisäävinä, että heikentävinä vaikutuksina. Tietoisuuden vaikutukset voivat näkyä pait-

si käyttäjän suhtautumisessa, myös käyttäjän toiminnassa ja käyttäytymisessä. Zwillingin ym. (2022) mukaan mitä enemmän käyttäjä on tietoinen turvallisuusuhista, sitä enemmän käyttäjä pyrkii välttämään arkaluonteisten tietojensa, kuten kotiosoitteen, puhelinnumeron tai kirjautumisessa käytettävien käyttäjätunnusten jakamista tai paljastamista. Tästä johtuen tietoisuuden lisääntymistä voi seurata käyttäjän kyberturvallisuutta lisäävän käyttäytymisen yleistyminen. Parhaimmillaan turvallisuusuhkien vaikutukset ovat kuitenkin käyttäjien turvallisuuden näkökulmasta positiivisia esimerkiksi johtamalla järjestelmien turvallisuuden paranemiseen. Tässä parhaassa tapauksessa käyttäjä voi mahdollisesti myös tunnistaa oman virheensä ja tätä kautta parantaa omaa toimintaansa.

Samalla kun tietoisuus kyberturvallisuusuhista kasvaa, lisääntyy myös tietoisuus siitä mihin tietoja voidaan käyttää. Lisääntyvä tietoisuus näyttää johtavan kriittisempään suhtautumiseen digitaalisten järjestelmien turvallisuushuolia kohtaan ja parhaassa tapauksessa tämä näkyy käyttäjän toiminnassa. Täten on olennaista parantaa käyttäjien tietoisuutta niistä toimista, joilla käyttäjän kyberturvallisuutta ja yksityisyyttä voidaan parantaa (Tirumala, Valluri ja Babu 2019). Puutteellinen tarkempi tieto turvallisuusuhista näyttää taas vaikuttavan siihen, kuinka käyttäjät suhtautuvat tai voivat itse vaikuttaa omaan turvallisuuteensa digitaalisissa järjestelmissä. Tietoisuuden puute siitä, miten käyttäjä voi parantaa omaa turvallisuuttaan, näkyy vaatimuksena järjestelmille lisätä turvallisuutta.

5 Käyttäjälle turvallisemman kyberympäristön luominen

Niin kauan kuin digitaaliset järjestelmät ovat olemassa, on niillä myös jokin loppukäyttäjä, jonka tarpeita varten järjestelmiä kehitetään. Siksi on olennaista parantaa eri järjestelmien ja alustojen turvallisuutta juuri näitä käyttäjiä varten. Turvallisuutta voidaan parantaa paitsi turvallisuusuhat paremmin huomioon ottavilla järjestelmillä, myös koulutuksella kyberturvallisuudesta, kasvattamalla tietoisuutta ja harjoittelemalla (Shillair ym. 2022). Tässä kappaleessa esitellään erilaisia keinoja, joilla käyttäjän turvallisuutta kyberympäristöissä voitaisiin parantaa.

5.1 Koulutus

Ihmisille tuttujen tapojen ja heidän toimintansa muuttaminen ei ole yksinkertaista. Jotta ihmisten toimintaa digitaalisissa järjestelmissä voitaisiin muuttaa turvallisempaan suuntaan, on ihmisten, eli käyttäjien, kouluttaminen yksi keskeisimpiä keinoja. Hossainin ja Zhangin (2015) mukaan on runsaasti tarvetta kouluttaa käyttäjiä tietoturvasta, yksityisyyden suojaa koskevista käytännöistä sekä tavoista, joilla käyttäjä voi yksityisyyttään parantaa.

Koulutuksessa tulisi kuitenkin pyrkiä sitomaan turvallisuutta lisäävät toimet käyttäjien yksityiselämään, jotta koulutus olisi kiinnostavampaa ja kannustavampaa tapojen muuttamiseen (He ja Zhang 2019). Sitomalla koulutus käyttäjien yksityiselämään saadaan koulutettavat näkemään konkreettisesti se, miksi toimet ovat tärkeitä heidän itsensä kannalta. Ongelmaksi voi muodostua se, että vaikka koulutus olisi tehokasta ja hyödyllistä, kouluttautumiseen ja taitojen kehittämiseen ei haluta käyttää omaa rahaa tai aikaa (N. A. A. Rahman ym. 2020). Tällöin korostuu koulujen ja yritysten rooli käyttäjien tietoisuuden parantamisessa. On myös organisaatioiden ja yritysten intressien mukaista parantaa käyttäjien taitoja ja tietoja, sillä näiden paraneminen voi näkyä organisaation kohentuneena kyberturvallisuutena.

Esimerkiksi yrityksille tietoturva voi olla erittäin tärkeää, mutta pelkästään yrityksen näkökulmasta asian tarkasteleminen ei välttämättä ole yhtä tehokasta kuin käyttäjän näkökulmasta tarkasteleminen. Hen ja Zhangin (2019) mukaan toimivan koulutuksen tulisi lähteä siitä, mikä on käyttäjän kannalta tärkeää ja motivoivaa, sillä muuten on epätodennäköisempää että

koulutus muuttaa käyttäjien todellista käyttäytymistä.

5.2 Käyttäjien tietoisuuden kasvattaminen

Zwilling ym. (2022) mukaan kyberturvallisuudesta oppiminen formaalin, eli tutkintoon tähtäävän, koulutuksen kautta on positiivisesti yhteydessä tietoisuuden tasoon. Koulutuksen kokonaisuudessaan voidaan katsoa parantavan käyttäjän tietoutta kyberturvallisuudesta, mikä on yksi keskeisimpiä keinoja kyberturvallisuuden parantamiseksi. Chandarman ja Van Niekerk (2017) toteavat, että kyberrikosten uhrien määrää voidaan vähentää lisäämällä käyttäjien tietoisuuden tasoa. Käyttäjien tietoisuutta ja kyberturvallisuustaitoja voidaan kasvattaa edellisessä luvussa mainitun koulutuksen lisäksi harjoittelemalla ja tietoisuuteen liittyvillä ohjelmilla (Shillair ym. 2022). Harjoittelun ja ohjelmien tulisi kuitenkin olla relevantteja ja motivoivia koulutuksen tavoin, jotta käyttäjät voivat muuttaa käyttäytymistään kyberturvallisuutta kasvattavaan suuntaan (He ja Zhang 2019).

Tietoisuuden kasvattaminen tapahtuu paljolti oppimalla asioita ja hankkimalla tietoa kyberturvallisuudesta sekä keinoista, joilla käyttäjä voi omaa kyberturvallisuuttaan parantaa. Shillarin ym. (2022) mukaan myös muiden opettaminen ja yhdessä oppiminen voi mahdollisesti olla jopa hyödyllisempää kuin järjestetyt oppimistilaisuudet. He viittaavat Duttonin ja Shepherdin (2006) tutkimukseen, jonka mukaan esimerkiksi internetin käytössä tarvittavia taitoja opitaan syvemmin kokemuksen ja kokeilun kautta. Tämä tulisi huomioida myös koulutuksessa, harjoittelussa ja ohjelmissa, jotta käyttäjien tietoisuuden tasoa voitaisiin kasvattaa.

Koulutuksen ja oppimisen merkitys korostuu myös siinä, kuinka kyberturvallisuustaitojen oppiminen vähintään muun oppimisen sivussa vaikuttaa positiivisesti käyttäjän tietoisuuteen kyberturvallisuusuhista (Zwilling ym. 2022). Mikäli kaikessa koulutuksessa ja oppimisessa pyritään turvalliseen toimintaan kyberympäristöissä, voivat vaikutukset olla käyttäjän kyberturvallisuuden kannalta merkittävän positiivisia. Erilaisia digitaalisia laitteita ja järjestelmiä käytetään opetuksessa ja opiskelussa laajasti, joten jo laitteiden käyttöä opeteltaessa voitaisiin opettaa turvallisia tapoja toimia kyberympäristöissä.

5.3 Tiedon levittäminen

Aiemmin todettiin tietoisuuden lisäävän käyttäjän turvallisuutta digitaalisissa järjestelmissä. Tietoisuuden lisääntymiseen vaikuttaa läheisesti saatavilla olevan luotettavan tiedon määrä, joten myös tiedon levittämistä ja jakamista voidaan pitää keskeisenä keinona lisätä käyttäjän turvallisuutta kyberympäristöissä toimiessa. Tiedon levittämistä ei tule kuitenkaan sekoittaa tietoisuuden lisäämiseen, vaikka lopputavoite on sama. Tiedon levittäminen eli saatavilla olevan tiedon määrän kasvattaminen ei itsessään lisää tietoisuutta, vaan keskeisimpänä erona tietoisuuden lisäämiseen tiedon levittäminen on yksi keinoista lisätä tietoisuutta.

Turvallisuuden parantamiseksi erityisesti tiedon ja tätä kautta tietoisuuden kasvattaminen esimerkiksi internetsivustojen evästeistä, ohjeistuksista ja yleisistä kyberturvallisuutta lisäävistä asioista on erityisen tärkeää (Tirumala, Valluri ja Babu 2019). Kuten luvussa 3.1 todettiin, käyttäjien omaavan puutteellista tietoa juuri evästeistä, on tiedon levittäminen näistä aiheista ensiarvoisen tärkeää käyttäjien kyberturvallisuuden parantamiseksi. Tutkimuksissa on esitelty myös muita yksinkertaisia ja tehokkaita keinoja tapana lisätä käyttäjän turvallisuutta kyberympäristöissä. Näitä ovat esimerkiksi kaksivaiheinen tunnistautuminen ja salasanojen säännöllinen vaihtaminen (Aswal ym. 2022).

Tietoisuuden kasvattamisen lisäksi myös tiedon levittäminen näistä yksinkertaisista keinoista on tärkeää, jotta mahdollisimman moni käyttäjä pystyy hyödyntämään esimerkiksi kyseisiä keinoja toiminnassaan. Aswalin ym. (2022) mukaan välttääkseen tietojensa vuotamista, käyttäjällä tulisi olla perustiedot käyttämänsä alustan yksityisyyskäytänteistä, turvallisuusuhista sekä turvallisesta käytöstä. Käyttäjien kyberturvallisuuden kannalta tiedon levittäminen on erityisen tärkeää, jotta käyttäjillä on saatavilla tietoa ja keinoja kyberturvallisuutensa parantamiseksi.

Vaikeuksia tiedon levittämisessä saattaa kuitenkin aiheuttaa esimerkiksi se, että nuorilla luottamus yksipuolisen viestinnän tiedotusvälineitä kohtaan on pienempää. Tämän takia on tärkeää kehittää ja ideoida tapoja siitä, miten tiedon levittämisessä voidaan ottaa käyttöön saavutettavia, luotettavia ja tehokkaita tapoja (Norri-Sederholm ym. 2019). Toinen tärkeä asia tiedon levittämisessä on se, että käyttäjät osaavat sekä pystyvät erottamaan faktan ja disinformaation toisistaan (Zhang ja Gupta 2018).

5.4 Turvallisemmat järjestelmät

Organisaatioiden ja yritysten käyttämien järjestelmien tulisi olla niin turvallisia käyttäjälle, että käyttäjän oma toiminta vahvistaa järjestelmän tai organisaation turvallisuutta. Käyttäjän näkökulmasta olisi parasta, että käyttäjät olisivat kyberturvallisuuden ja -puolustuksen viimeinen lenkki, jolloin heidän oma toimintansa ei aiheuttaisi niin suuria riskejä järjestelmän kyberturvallisuudelle. Järjestelmien kehittämisessä on tarpeen ottaa huomioon kyberturvallisuusuhat sekä niiden torjuminen niin suunnittelussa, toteutuksessa kuin ylläpidossa (Humayun, Niazi, Jhanjhi ym. 2020).

Tätä kautta turvallisempien järjestelmien luomisessa avainasemassa ovat järjestelmien kehittäjät sekä heidän tietoisuutensa ja suhtautumisensa järjestelmän turvallisuuteen. Sovelluskehittäjät ja -insinöörit ovat osaltaan myös järjestelmien käyttäjiä, jolloin myös kehittäjien tietoisuutta voidaan parantaa käyttäjien tietoisuutta lisäävillä keinoilla, kuten koulutuksella, harjoittelulla ja tiedon levittämisellä. Kehittäjät voivat vaikuttaa myös luomiensa digitaalisten järjestelmien toiminnallisuuksiin ja ominaisuuksiin. Yksi keino turvallisempien järjestelmien luomiseksi on kehittää järjestelmiä siten, että ne ohjaavat käyttäjän toimimaan kyberturvallisuuden kannalta turvallisesti. Tirumalan ym. (2019) mukaan sääntöjen tiukentaminen, esimerkiksi tekemällä järjestelmään salasanan luontiin säännöt, joita salasanan tulee noudattaa tai kaksivaiheisen tunnistautumisen asettaminen pakolliseksi, ovat keinoja lisätä järjestelmien turvallisuutta. Turvallisemmat järjestelmät eivät kuitenkaan yksin luo täyttä suojaa kyberturvallisuusuhkia ja -hyökkäyksiä vastaan (Kadena ja Gupi 2021), vaan myös käyttäjien toiminnan kehittämiselle on tarvetta.

Kuten luvussa 4 todettiin, parhaiten käyttäjän kyberympäristön turvallisuus paranee, kun kasvanut tietous näkyy kyberturvallisuutta edistävänä käytöksenä. Voidaan kuitenkin huomata kaikkien tässä luvussa 5 esiteltyjen keinojen vaikuttavan toisiinsa. Esimerkiksi lisäämällä tietoa tavoista, joilla käyttäjä voi lisätä turvallisuuttaan kyberympäristöissä, voidaan asia ottaa paremmin huomioon esimerkiksi kouluissa digitaalisten järjestelmien käyttöä opeteltaessa. Toisaalta on tärkeää jokaisen tässä luvussa mainitun osa-alueen erillinen parantaminen. Tosin Shillairin ym. (2022) mukaan kokonaisuuden kehittäminen on vähintään yhtä tärkeää, mutta tässä luvussa esitellyt keinot vaativat kuitenkin lisäpanostuksia kyberturvallisuuden kasvattamiseksi.

6 Yhteenveto

Tässä tutkielmassa tutkittiin käyttäjien tietoisuutta ja suhtautumista digitaalisten järjestelmien turvallisuusuhkiin. Tutkielmassa käsiteltiin sekä yleisimpiä turvallisuusuhkia että keinoja, joilla toimimisesta digitaalisissa järjestelmissä voidaan tehdä käyttäjälle turvallisempaa. Tutkielmassa käsiteltiin myös kyberturvallisuusuhkien vaikutuksia käyttäjän näkökulmasta.

Tutkielmassa huomattiin enemmistön käyttäjistä haluavan lisää turvallisuutta erilaisia kyberturvallisuusuhkia vastaan. Samaan aikaan suurimmalla osalla käyttäjistä ei ole kuitenkaan tarpeeksi tietoa tai osaamista siitä, miten käyttäjä itse voi vaikuttaa turvallisuuteensa digitaalisissa järjestelmissä positiivisesti. Myös käyttäjien tiedoissa esimerkiksi tietojensa käytöstä on puutteita, jotka voivat vaikuttaa käyttäjän hyödyntämiin suojautumistyökaluihin tai -tapoihin. Käyttäjien suhtautumiseen vaikuttavat kuitenkin monet eri tekijät, kuten se, miten hyödyllisenä käyttäjä kokee käyttämiensä järjestelmien käytön.

Käyttäjän huomattiin suhtautuvan sitä kriittisemmin mahdollisiin kyberympäristön turvallisuusuhkiin mitä enemmän käyttäjä niistä tietää. Tietoisuuden kyberturvallisuusuhista voidaan nähdä jollakin tasolla vaikuttavan suhtautumiseen. Tämän tietoisuuden lisääntyminen voi parhaimmillaan johtaa käyttäjän käyttäytymisen muutokseen kyberturvallisuutta lisäävään suuntaan. Käyttäjällä voi olla esimerkiksi vähemmän halua jakaa henkilökohtaisia tietojaan. Myös uhkien konkretisoituminen voi vaikuttaa käyttäjän toimintaan ja suhtautumiseen.

Viimeisenä esiteltiin erilaisia keinoja, joilla käyttäjän tietoisuutta voitaisiin parantaa, kun todettiin tietoisuuden paranemisella olevan positiivisia vaikutuksia käyttäjän turvallisuuteen. Erityisesti koulutuksella sekä yksinkertaisilla sekä tehokkailla teoilla, kuten kaksivaiheisen tunnistautumisen käytöllä, on suuri merkitys. Paitsi koulutuksen, niin myös harjoittelun avulla esimerkiksi näitä yksinkertaisia keinoja voidaan opettaa ja niistä kertoa käyttäjille. Myös tiedon levittäminen yleisistä kyberturvallisuusuhista, kuten kalasteluyrityksistä tai järjestelmien heikkouksista, auttaa parantamaan käyttäjän turvallisuutta digitaalisissa järjestelmissä. Kaikkien näiden edellä mainittujen osa-alueiden todettiin vaikuttavan läheisesti toisiinsa.

Lähteet

Adebiaye, Richmond, Haroun Alryalat ja Theophilus Owusu. 2016. “Perspectives for cyber-deterrence: A quantitative analysis of cyber threats and attacks on consumers”. *International journal of innovative research in science, engineering and technology* 5 (7). https://doi.org/10.15680/IJIRSET.2016.0507157.

Alotaibi, Mutlaq ja Waleed Alfehaid. 2019. “Information Security Awareness: A Review of Methods, Challenges and Solutions” (maaliskuu). https://doi.org/10.2053/ICITST.WorldCIS.WCST.WCICSS.2018.0016.

Aswal, Narottam, Atharva Kale, Dhanamma Jagli ja Ramesh Solanki. 2022. “Security Hazards of Social Media And Their Resolutions”. Teoksessa *2022 Algorithms, Computing and Mathematics Conference (ACM),* 48–53. https://doi.org/10.1109/ACM57404.2022.00016.

Baker-Eveleth, Lori, Robert Stone ja Daniel Eveleth. 2022. “Understanding social media users’ privacy-protection behaviors”. *Information & Computer Security* 30 (3): 324–345. https://doi.org/10.1108/ICS-07-2021-0099.

Chandarman, Rajesh ja Brett Van Niekerk. 2017. “Students’ Cybersecurity Awareness at a Private Tertiary Educational Institution”. *The African Journal of Information and Communication (AJIC),* numero 20, https://doi.org/10.23962/10539/23572.

DataReportal. 2024. “Digital 2024: Global Overview Report”. Viitattu 29. huhtikuuta 2024. https://datareportal.com/reports/digital-2024-global-overview-report.

Dodge, Ronald C., Curtis Carver ja Aaron J. Ferguson. 2007. “Phishing for user security awareness”. *Computers & Security* 26 (1): 73–80. ISSN: 0167-4048. https://doi.org/https://doi.org/10.1016/j.cose.2006.10.009.

He, Wu ja Zuopeng (Justin) Zhang. 2019. “Enterprise cybersecurity training and awareness programs: Recommendations for success”. *Journal of Organizational Computing and Electronic Commerce* 29 (4): 249–257. https://doi.org/10.1080/10919392.2019.1611528.

Hossain, Al Amin ja Weining Zhang. 2015. “Privacy and security concern of online social networks from user perspective”. Teoksessa *2015 International Conference on Information Systems Security and Privacy (ICISSP),* 246–253.

Humayun, Muhammad, Muhammad Niazi, Noreen Jhanjhi ym. 2020. “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study”. *Arab J Sci Eng* 45:3171–3189. https://doi.org/10.1007/s13369-019-04319-2.

Irshad, Shareen ja Tariq Rahim Soomro. 2018. “Identity theft and social media”. *International Journal of Computer Science and Network Security* 18 (1): 43–55.

Jang-Jaccard, Julian ja Surya Nepal. 2014. “A survey of emerging threats in cybersecurity”. Special Issue on Dependable and Secure Computing, *Journal of Computer and System Sciences* 80 (5): 973–993. ISSN: 0022-0000. https://doi.org/https://doi.org/10.1016/j.jcss.2014.02.005.

Kadena, Esmeralda ja Marsidi Gupi. 2021. “Human factors in cybersecurity: Risks and impacts”. *Security science journal* 2 (2): 51–64. https://doi.org/10.37458/ssj.2.2.3.

McCrohan, Kevin F., Kathryn Engel ja James W. Harvey. 2010. “Influence of Awareness and Training on Cyber Security”. *Journal of Internet Commerce* 9 (1): 23–41. https://doi.org/10.1080/15332861.2010.487415.

Mhlanga, McKringle Xolani, Richard Rabin Maiti ja Bennet Hammer. 2021. “Privacy and Security Matters Related To Use Of Mobile Devices and Social Media”. Teoksessa *SoutheastCon 2021,* 1–6. https://doi.org/10.1109/SoutheastCon45413.2021.9401838.

Norri-Sederholm, Teija, Elisa Norvanto, Aki-Mauri Huhtinen ja Karoliina Talvitie-Lamberg. 2019. *Social media as the pulse of national security threats : A framework for studying how social media influences young people’s safety and security situation picture.* Toimittanut Wybe Popma, Stuart Francis, Informaatioteknologian tiedekunta, Faculty of Information Technology, Tietojärjestelmätiede ja Information Systems Science. Academic Conferences / Publishing International Limited. http://www.urn.fi/URN:NBN:fi:jyu-202110155252.

NortonLifeLock. 2023. “2023 NCSIR US-Global Report”. Viitattu 16. huhtikuuta 2024. https://www.gendigital.com/media/qcymrc1i/2023-ncsir-us-global-report_final.pdf.

Parmar, Bimal. 2012. “Protecting against spear-phishing”. *Computer Fraud & Security* 2012 (1): 8–11. ISSN: 1361-3723. https://doi.org/https://doi.org/10.1016/S1361-3723(12)70007-6.

Quayyum, Farzana, Daniela S Cruzes ja Letizia Jaccheri. 2021. “Cybersecurity awareness for children: A systematic literature review”. *International Journal of Child-Computer Interaction* 30:100343. https://doi.org/10.1016/j.ijcci.2021.100343.

Rahman, Nurul Amirah Abdul, Izzah Hanis Sairi, Nurul Akma M Zizi ja Fariza Khalid. 2020. “The importance of cybersecurity education in school”. *International Journal of Information and Education Technology* 10 (5): 378–382. https://api.semanticscholar.org/CorpusID:218824588.

Rahman, Tashfiq, Rohani Rohan, Debajyoti Pal ja Prasert Kanthamanon. 2021. “Human Factors in Cybersecurity: A Scoping Review”. IAIT ’21. New York, NY, USA: Association for Computing Machinery. ISBN: 9781450390125. https://doi.org/10.1145/3468784.3468789.

Rohan, Rohani, Suree Funilkul, Debajyoti Pal ja W. Chutimaskul. 2021. “Understanding of Human Factors in Cybersecurity: A Systematic Literature Review”, 133–140. Joulukuu. https://doi.org/10.1109/ComPE53109.2021.9752358.

Shillair, Ruth, Patricia Esteve-González, William H. Dutton, Sadie Creese, Eva Nagyfejeo ja Basie von Solms. 2022. “Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise”. *Computers & Security* 119:102756. ISSN: 0167-4048. https://doi.org/https://doi.org/10.1016/j.cose.2022.102756.

Snider, Keren LG, Ryan Shandler, Shay Zandani ja Daphna Canetti. 2021. “Cyberattacks, cyber threats, and attitudes toward cybersecurity policies”. *Journal of Cybersecurity* 7 (1): tyab019. https://doi.org/10.1093/cybsec/tyab019.

Tirumala, S S, Maheswara Rao Valluri ja GA Babu. 2019. “A survey on cybersecurity awareness concerns, practices and conceptual measures”. Teoksessa *2019 International Conference on Computer Communication and Informatics (ICCCI),* 1–6. https://doi.org/10.1109/ICCCI.2019.8821951.

Tsochev, Georgi, Roumen Trifonov, Ognian Nakov, Slavcho Manolov ja Galya Pavlova. 2020. “Cyber security: Threats and Challenges”. Teoksessa *2020 International Conference Automatics and Informatics (ICAI),* 1–6. https://doi.org/10.1109/ICAI50593.2020.9311369.

Zhang, Zhiyong ja Brij B. Gupta. 2018. “Social media security and trustworthiness: Overview and new direction”. *Future Generation Computer Systems* 86:914–925. ISSN: 0167-739X. https://doi.org/https://doi.org/10.1016/j.future.2016.10.007.

Zwilling, Moti, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin ja Hamdullah Nejat Basim. 2022. “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study”. *Journal of Computer Information Systems* 62 (1): 82–97. https://doi.org/10.1080/08874417.2020.1712269.