Riikka Puhakka

TIETOMURTOJEN VAIKUTUS INTERNETIN KÄYTTÄJIEN TUNTEISIIN JA KÄYTÖKSEEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Puhakka, Riikka
Tietomurtojen vaikutus internetin käyttäjien tunteisiin ja käytökseen
Jyväskylä: Jyväskylän yliopisto, 2021, 64 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaajat: Rousi, Rebekah; Seppänen, Ville

Informaatioteknologian kehittymisen myötä tietojen kerääminen, säilyttäminen ja käsitteleminen tapahtuu erilaisissa tietojärjestelmissä. Vaikka tietoturvallisuuteen panostetaan ja tietoja pystytään turvaamaan kehittyneen teknologian avulla, myös tietoturvariskit lisääntyvät ja muuttuvat jatkuvasti. Yritysten ja muiden organisaatioiden joutuessa tietomurron kohteeksi seuraukset kohdistuvat myös niihin ihmisiin, joiden tietoja murretuissa järjestelmissä on säilytetty. Tällaiset hyökkäykset saavat paljon huomiota mediassa.

Tässä tutkimuksessa haluttiin selvittää, minkälaisia tunteita tietomurrot ja niistä seuraavat tietovuodot herättävät ihmisissä ja miten tieto mahdollisista tietoturvauhkista vaikuttaa internetin käyttäjien luottamukseen ja käytökseen.

Tutkimuksen empiirinen osuus toteutettiin määrällisenä kyselytutkimuksena. Olemassa olevaa teoriaa aiheesta kartoitettiin kirjallisuuskatsauksella ennen kyselylomakkeen luomista. Kirjallisuuskatsauksessa esiin nousseita tietoturvahuolien mittaamiseen tarkoitettuja IUIPC- ja CFIP-mittareita käytettiin pohjana kyselylomakkeen tunteita mittaavassa osassa. Suurin osa tutkimusaineistosta analysoitiin tilastollisin menetelmin. Avoimet vastaukset käytiin läpi ja luokiteltiin teemoittain.

Tutkimuksen tuloksista kävi ilmi, että tietomurrot herättävät yli 18-vuotiaissa internetin käyttäjissä ärsyyntymistä, vihaa ja ahdistusta. Varsinkin tietojen luvaton käyttö ja luvaton pääsy tietoihin herättivät negatiivisia tunteita suurimassa osassa vastaajista. Tiedolla havaittiin olevan tilastollisesti merkitsevä yhteys internetin käyttäjien varovaiseen käytökseen ja harkintaan tietojen luovuttamisessa. Erityisesti henkilökohtainen kiinnostus tietoturva-asioita kohtaan ja omaaloitteisesti hankittu tieto lisäsivät varovaista käytöstä. Tutkimuksessa todettiin myös, että tiedon ja käytöksen välisen yhteyden vahvistamiseksi vaaditaan vielä lisätutkimuksia.

Asiasanat: tietomurto, tietovuoto, tietoturvahuolet, tunteet, käytös

ABSTRACT

Puhakka, Riikka
The effect of data breaches to Internet users' emotions and behavior
Jyväskylä: University of Jyväskylä, 2021, 64 pp.
Information Systems Science, Master's Thesis
Supervisors: Rousi, Rebekah; Seppänen, Ville

With the development of information technology, the collection, storage, and processing of data takes place in various information systems. Although information security is being invested in and data can be secured with the help of advanced technology, security risks are also constantly increasing and changing. When companies and other organizations are compromised, the consequences also apply to the people whose data has been stored in the compromised systems. These kinds of attacks are getting a lot of attention in the media. The aim of this study was to find out what kind of feelings data breaches and the resulting data leaks evoke in people, and how knowledge of potential security threats affects the trust and behavior of Internet users.
The empirical part of the study was conducted as a quantitative survey. The existing theory on the topic was studied with a literature review before the questionnaire was created. The IUIPC and CFIP scales for measuring information security concerns emerged in the literature review and were used as the basis for the measuring emotions part of the questionnaire. Most of the research material was analyzed using statistical methods. Open responses were reviewed and categorized by theme.
The results of the study show that data breaches cause irritation, anger and anxiety among internet users over the age of 18. In particular, unauthorized use of data and unauthorized access to data aroused negative feelings in the majority of respondents. The information security knowledge was found to have a statistically significant connection to the cautious behavior and trust of Internet users in disclosing information. Especially, personal interest in information security issues and voluntary studying of the topic increased cautious behavior. The study also concluded that further research is needed to strengthen the connection between information security knowledge and behavior.

Keywords: data breach, data leak, information security concerns, emotions, behavior

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Informaatioteknologia on osa arkeamme ja yhä useampi käyttämistämme palveluista toimii nyt verkossa. Tietoja säilytetään erilaisissa tietojärjestelmissä ja joskus voi olla vaikeaa hahmottaa, kuinka paljon henkilökohtaisia tietoja yritykset ja muut organisaatiot meistä säilyttävät. Vaikka tietoturvallisuuteen panostetaan ja tietoja pystytään turvaamaan kehittyneen teknologian avulla, myös tietoturvariskit lisääntyvät ja muuttuvat jatkuvasti.

Mediassa uutisoidaan jatkuvasti suurista tietomurroista, joiden seurauksena käyttäjien tietoja on vuotanut suosituilta verkkosivustoilta ja sosiaalisen median palveluista. Suomessa tapahtuneista tietomurroista tunnetuimpia lienee vuonna 2020 paljastunut Psykoterapiakeskus Vastaamon tietomurto. Vastaamon tapauksessa varastetut tiedot olivat arkaluontoisia ja henkilökohtaisia terveystietoja. Tapaus sai paljon julkisuutta, ja se on yksi suurimmista inspiraation lähteistä tähän tutkimukseen. Vastaamon tietomurron uhrit ovat kuvailleet kokeneensa tapahtuneen vuoksi esimerkiksi stressiä ja ahdistusta (Tikkala & Torkki, 2020) sekä pelkoa ja vihaa (Mattila, 2021).

Tässä tutkimuksessa halutaan selvittää, miten lisääntynyt tieto tietoturvauhkien olemassaolosta vaikuttaa internetin käyttäjien käytökseen ja minkälaisia tunnereaktioita nämä tietoturvauhat herättävät. Tutkimus rajataan tietoturvauhkien osalta erityisesti tietomurtoihin ja niistä seuraaviin tietovuotoihin. Tutkimuksen tavoitteet voidaan tiivistää kahteen tutkimuskysymykseen:

1. Millaisia tunteita tietomurrot ja niistä aiheutuneet tietovuodot herättävät tietomurtojen uhreissa ja yleisesti kaikissa internetiä käyttävissä ihmisissä?
2. Miten tieto tietoturvariskeistä vaikuttaa ihmisten käytökseen ja haluk-kuuteen luovuttaa tietojaan yrityksille tai muille organisaatioille verkossa?

Tutkimuksen keskeisimpiä termejä ovat tietoturva, tietomurto ja tietovuoto. Kyberturvallisuuskeskuksen (2020a) määritelmän mukaan tietoturvalla pyritään varmistamaan tiedon eheys, luotettavuus ja saatavuus. Tietomurrot ja niistä

seuraavat tietovuodot ovat uhkia tietoturvan toteutumiselle. Tietomurrolla tarkoitetaan luvatonta tunkeutumista tietojärjestelmään tai sen osaan (Rikoslaki 38:8.1 §). Jos tietomurron yhteydessä tietoja päätyy ulkopuolisen haltuun, on kyseessä tietovuoto (Kyberturvallisuuskeskus, 2020b).

Ennen tutkimuksen empiiristä osiota tehtiin kirjallisuuskatsaus, jossa perehdyttiin aiempaan tutkimuskirjallisuuteen. Kirjallisuuskatsaukseen etsittiin artikkeleja Google Scholarista sekä Jyväskylän yliopiston kirjaston kautta eri tietokannoista. Haussa käytettyjä hakusanoja ja sanojen yhdistelmiä ovat esimerkiksi ”impact of cybercrime”, ”cybercrime impact on victims” ”data breach victims”, ”data leakage”, ”information security”, ”data security”, ”security breach”, ”information breach”, “technostress” + “internet vulnerabilities”, “information privacy concerns”, “privacy concerns online”, “IUIPC” ja “CFIP”. Hakutuloksista valikoitiin otsikoiden ja abstraktien perusteella aiheen kannalta olennaisilta vaikuttavat artikkelit lähempään tarkasteluun. Myös kirjallisuuskatsaukseen valittujen artikkelien lähdeluetteloista löydettiin lisää tutkimukseen soveltuvia lähteitä.

Kirjallisuuskatsaukseen hyväksyttiin ainoastaan vertaisarvioituja artikkeleita. Artikkeleita arvioitiin myös niiden julkaisukanavan, julkaisuvuoden ja käytettyjen lähteiden perusteella. Artikkelien haussa ei asetettu aikarajoitusta, mutta julkaisuaikaan kiinnitettiin erityistä huomiota, mikäli samasta teoriasta tai näkökulmasta on tehty useita artikkeleita, koska kirjallisuuskatsaukseen pyrittiin valitsemaan mahdollisimman tuoretta ja luotettavaa lähdemateriaalia.

Kirjallisuuskatsauksessa nousi esiin kaksi keskeistä tietoturvahuolien mittaamisessa käytettyä mallia, Internet Users' Information Privacy Concerns (IUIPC) ja Concern for Information Privacy (CFIP). Näiden mallien sisältämiä mittaristoja käytettiin pohjana tutkimuksen empiirisessä osiossa, jotta tietoturvahuolien kaikki ulottuvuudet tulisivat huomioiduksi aineistossa. Tässä tutkimuksessa jaettiin tietoturvahuolet neljään ulottuvuuteen CFIP-mallin mukaan: tietojen kerääminen, virheet tiedoissa, luvaton pääsy tietoihin ja tietojen luvaton käyttö (Smith ym., 1996). IUIPC-mallissa ulottuvuuksia on vain kolme ja ne ovat osittain samoja kuin CFIP-mallissa: tietojen kerääminen, tietojen hallinta ja tietoisuus kerättyjen tietojen käytöstä (Malhotra ym., 2004).

Empiirisen osion tutkimusotteeksi valittiin kvantitatiivinen eli määrällinen tutkimus ja aineisto kerättiin verkkokyselyllä. Tutkimuksen kohderyhmäksi valittiin yli 18-vuotiaat internetin käyttäjät, ja kohderyhmän tavoittamiseksi kyselylinkkiä jaettiin verkossa sosiaalisen median palveluissa sekä työ- ja harrastusryhmien keskusteluryhmissä. Kyselylomakkeella mitattiin vastaajien tietoa, tunteita, luottamusta, käsitystä yrityksen vastuusta tietomurtotilanteessa ja käytöstä. Saatua aineistoa analysoitiin tilastollisin menetelmin. Tuloksista löydettiin vastauksia tutkimuskysymyksiin, mutta havaittiin myös tarpeita lisätutkimukselle.

Tämä tutkielma jakautuu seitsemään lukuun. Johdantoluvun jälkeen toisessa ja kolmannessa luvussa esitellään tarkemmin tutkimuksen kannalta olennaiset käsitteet ja aiempi tutkimuskirjallisuus. Neljännessä luvussa käydään läpi empiirisen tutkimuksen toteutukseen valittu menetelmä ja tutkimuksen käytännön toteutus. Viidennessä luvussa esitellään empiirisen tutkimuksen tulokset.

Tutkimustulokset analysoidaan tarkemmin kuudennessa luvussa, jossa vastataan myös alussa määritettyihin tutkimuskysymyksiin. Lisäksi arvioidaan tutkimuksen rajoitteita ja esitetään mahdollisia aiheita jatkotutkimukselle. Tutkielman lopussa on yhteenvetoluku, jossa käydään tiivistetysti läpi tutkielman tarkoitus, tausta ja tulokset.

2 TIETOMURROT JA TIETOVUODOT

Tässä luvussa tarkastellaan tietoturvan käsitettä yleisesti ja esitellään yleisimpiä siihen liittyviä rikoksia sekä määritellään tutkimuksen kannalta keskeisimmät käsitteet. Tietoturvaan liittyvistä uhkista tietomurrot ja niistä aiheutuvat tietovuodot esitellään tarkemmin omissa alaluvuissaan.

2.1 Tietoturva ja tietojen yksityisyys

Tietoturvalla (engl. information security) tarkoitetaan toimia, joilla varmistetaan tiedon eheys, luottamuksellisuus ja käytettävyys (Kyberturvallisuuskeskus, 2020a). Raggadin (2010, s. 20) mukaan tiedon eheydellä tarkoitetaan pyrkimystä säilyttää tiedon paikkansapitävyys. Tiedon eheys on uhattuna, mikäli ihminen tai muu toimija pääsee muokkaamaan tietoa luvatta. Luottamuksellisuus takaa, että tietoa pääsevät tarkastelemaan ja käsittelemään vain siihen oikeutetut henkilöt. Tiedon luottamuksellisuus voi vaarantua tilanteissa, joissa luottamuksellisia tietoja sisältäviä dokumentteja luovutetaan tai hävitetään huolimattomasti. Tiedon käytettävyys varmistaa, että tiedot ovat saatavissa niihin oikeutetuille henkilöille, eivätkä tietojärjestelmien tekniset ongelmat tai puuttuvat käyttöoikeudet estä tietojen käyttöä. (Raggad, 2010, s. 20.)

Tietoturvalla varmistetaan myös tietojen yksityisyys (engl. information privacy). Belangerin ja Crosslerin (2011) mukaan tietojen yksityisyydestä on olemassa monia eri määritelmiä. Monissa tutkimuksissa tietojen yksityisyys määritellään usein yksilön mahdollisuudeksi hallita itseään koskevien tietojen käyttöä ja jakamista muille (Belanger & Crossler, 2011; Belanger ym., 2002; Liang & Xue, 2009). Malhotran ym. (2004) mukaan käytännöt ja käsitys tietojen yksityisyydestä vaihtelevat myös kulttuurin, lainsäädännön ja toimialan mukaan. Erityisesti moderneissa länsimaisissa yhteiskunnissa yksityisyyden arvostus näkyy lainsäädännössä ja sosiaalisissa järjestelmissä (Zhang ym., 2013).

Tietojen yksityisyyttä on käsitelty monen eri alan tutkimuksissa ja lukuisista eri näkökulmista. Tietojen yksityisyyteen liittyvää tutkimusta on tehty

esimerkiksi markkinoinnin, johtamisen, psykologian ja oikeustieteen aloilla. Tietojärjestelmätieteen tutkimuksessa eniten tutkittuja teemoja ovat käyttäjien tietoturvahuolet, tietojen yksityisyyden vaikutus verkkokauppaliiketoiminnassa ja tietojen yksityisyyteen liittyvät asenteet ja toimintatavat. (Belanger & Crossler, 2011.)

2.2 Kyberrikokset

Internetin käytön yleistyminen on tarjonnut mahdollisuuksia myös uudenlaiselle rikollisuudelle. Reep-van den Berghin ja Jungerin (2018) mukaan niin sanotun kyberrikollisuuden uhrien todellisesta määrästä ei ole tarkkaa tietoa. Suuri osa kyberrikoksen uhreista ei välttämättä huomaa itse joutuneensa rikoksen kohteeksi (De Kimpe ym., 2020).

Reep-van den Bergh ja Junger (2018) jakavat kyberrikokset kolmeen kategoriaan: tietokoneisiin kohdistuviin rikoksiin, tietokoneen mahdollistamiin rikoksiin ja sisältöön liittyviin rikoksiin. Tietokoneisiin kohdistuvat rikokset liittyvät luvattomaan pääsyyn laitteisiin ja niiden sisältämiin tietoihin. Esimerkiksi hakkerointi, haittaohjelmat ja palvelunestohyökkäykset kuuluvat tähän kategoriaan. (Reep-van den Bergh & Junger, 2018.) Tietokoneisiin kohdistuvissa rikoksissa kohteeksi ei yleensä valita tiettyä yksilöä vaan kuka tahansa voi joutua hyökkäyksen kohteeksi, mikäli hyökkääjän onnistuu tunkeutua laitteeseen (De Kimpe ym., 2020).

Tietokoneen mahdollistamia rikoksia ovat esimerkiksi identiteettivarkaudet, tietojenkalastelu ja erilaiset petokset (Reep-van den Bergh & Junger, 2018). Näissä rikoksissa tietokone on apuväline uhrin tavoittamiseen ja rikoksen suorittamiseen, mutta itse laitteelle ei tehdä vahinkoa. Sisältöön liittyvissä rikoksissa uhrit ovat yleensä passiivisemmassa asemassa ja voivat törmätä haitalliseen sisältöön vahingossa (De Kimpe ym., 2020). Sisältöön liittyviä kyberrikoksia ovat esimerkiksi pornografia, terrorismi ja vihapuhe verkossa (Reep-van den Bergh & Junger, 2018).

Myös yritykset ja muut organisaatiot joutuvat usein kyberrikosten kohteeksi. Suurin osa organisaatioiden kohtaamista kyberhyökkäyksistä tähtää tietojen varastamiseen (Iovan & Iovan, 2016). Yritykset säilyttävät usein paljon tietoja asiakkaistaan. Hyökkäys, joka vaarantaa näiden tietojen yksityisyyden, voi vaikuttaa itse yrityksen lisäksi myös asiakkaisiin. Tietomurrot ja tietovuodot aiheuttavat monenlaisia haittoja yrityksille. Khanin ym. (2021) mukaan tietomurroista voi seurata esimerkiksi taloudellisia tappioita, kilpailuedun menetys sekä yritystoiminnan kannalta kriittisen datan vuotaminen tai tuhoutuminen.

2.3 Tietomurto

Suomen rikoslaissa (38:8.1 §) tietomurto määritellään teoksi, jossa tunkeudutaan oikeudettomasti tietojärjestelmään tai sen osaan. Luvattomaan tunkeutumiseen voidaan käyttää jonkun toisen henkilön käyttäjätunnusta tai teknisiä keinoja, joilla järjestelmän suojaus on murrettavissa (Rikoslaki 38:8.1 §). Khanin ym. (2021) mukaan tietomurrossa (engl. data breach) luvattomasti kopioidaan, siirretään, tarkastellaan, varastetaan tai käytetään arkaluontoista, suojattua tai luottamuksellista tietoa.

Chatterjeen ym. (2019) määritelmän mukaan tietomurrossa ulkopuolinen taho pääsee luvatta käsiksi luottamukselliseen tietoon tai tietoa paljastuu ulkopuolisille. Tässä määritelmässä tiedon paljastumisen voisi tulkita viittaavan myös tietojen mahdolliseen vuotamiseen. Tietomurron ja tietovuodon eroja ei ole tutkimuskirjallisuudessa käsitelty, ja monissa artikkeleissa käytetään termiä data breach (tietomurto), kun käsitellään sekä tietomurtoa että siitä seurannutta tietovuotoa.

Kyberturvallisuuskeskuksen (2020b) määritelmässä tietovuoto on mainittu erillään tietomurrosta, sillä tietomurroilla voi olla muitakin tavoitteita kuin tietojen varastaminen ja vuotaminen ulkopuolisille. Murrettua järjestelmää voidaan käyttää haitallisen materiaalin jakamiseen tai järjestelmän toimintaa voidaan häiritä tai estää sisältä käsin (Kyberturvallisuuskeskus, 2020b).

2.4 Tietovuoto

Tietovuoto (engl. data leakage) tarkoittaa tilannetta, jossa tietomurron seurauksena luottamuksellisia tietoja on päätynyt murtautujan käsiin (Kyberturvallisuuskeskus, 2020b). Tietoja varastanut taho voi pahimmassa tapauksessa vuotaa tiedot verkkoon kaikkien nähtäville tai kiristää niillä rahaa. Avila ym. (2021) määrittelevät tietovuodon tietojen luvattomaksi siirroksi organisaation ulkopuolelle. Heidän mukaansa kaikki tietovuodot eivät ole tahallisia, eivätkä ne aina tapahdu teknologian välityksellä. Tietovuoto voi siis olla esimerkiksi paperille kirjoitettua tietoa, joka päätyy organisaation ulkopuolelle vahingossa.

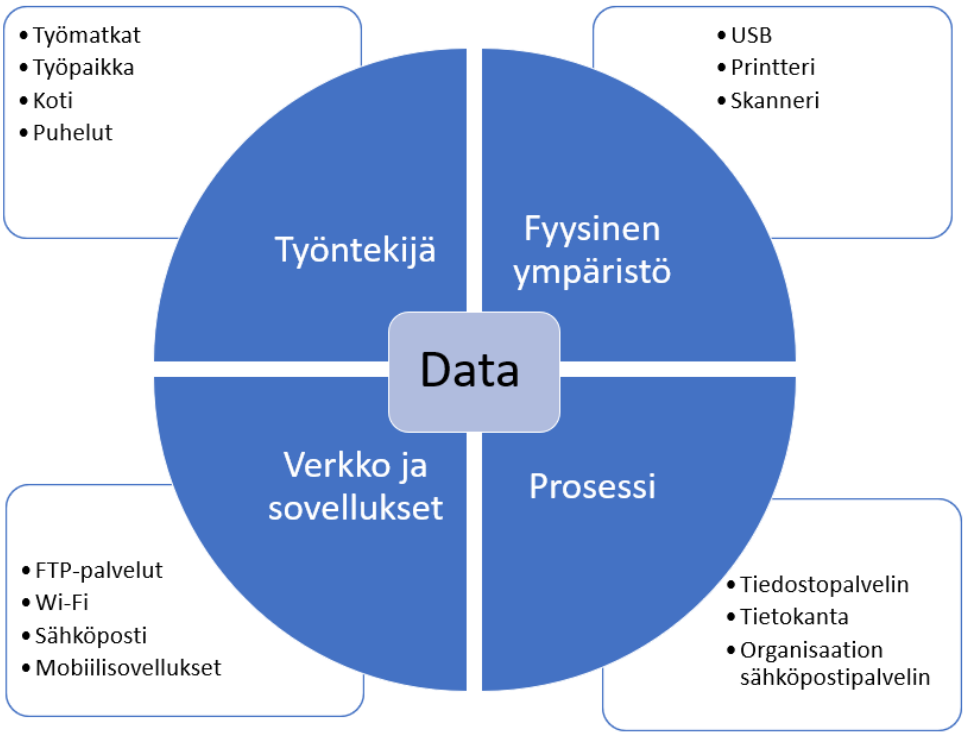
Avila ym. (2021) ovat tutkineet tietovuotoja ja jakaneet niiden kohteena olevat luottamukselliset tiedot neljään eri tyyppiin. Ensimmäinen tyyppi on ihmisten henkilökohtaiset tiedot, kuten henkilötiedot, terveys- tai taloustiedot tai tiedot henkilön internetin käytöstä. Toinen tyyppi on yritysten luottamukselliset tiedot, kuten sisäiset viestit, päivittäiseen toimintaan liittyvä data ja tiedot yrityksen strategiasta. Henkilötietojen ja yrityksen tietojen välillä saattaa olla päällekkäisyyksiä, sillä myös yritykset säilyttävät asiakkaidensa henkilötietoja. Kolmas tietotyyppi on liikesalaisuudet, joihin lukeutuvat esimerkiksi suunnitelmat, tuotekehitystiedot ja sopimustiedot. Neljänteen tietotyyppiin kuuluvat analyyttiset tiedot, eli suuri määrä dataa, jota yrityksessä käytetään päätöksenteon tukena.

Tällaisia tietoja voivat olla esimerkiksi asiakkaista tai koko liiketoimintaympäristöstä kerätyt demografiset tai käyttäytymiseen liittyvät tiedot. (Avila ym., 2021.)

Koti ym. (2017) jaottelevat tietovuodon mahdollistavat väylät neljään eri osaan: työntekijä, fyysinen ympäristö, verkko ja sovellukset sekä prosessi. Kuviossa 1 on listattu näihin osiin jaoteltuna esimerkkejä tietovuodon mahdollistavista väylistä. Organisaation työntekijät voivat aiheuttaa tietovuodon vahingossa käsittelemällä tietoja tai laitteitaan huolimattomasti kotona, työpaikalla tai työmatkoilla. Myös luottamuksellisia tietoja sisältävät puhelinkeskustelut voivat olla tietoturvariski, mikäli niitä käydään tiloissa, joissa ulkopuolinen voi kuulla keskustelun.

Fyysinen ympäristö mahdollistaa tietovuodon eri laitteiden kautta (Koti ym., 2017). Laitteiden fyysiseksi suojaamiseksi voidaan asettaa kulkurajoituksia ja valvontaa tiloihin, joissa laitteita säilytetään. Myös käytöstä poistettu laite voi olla riski tietoturvalle, mikäli sen sisältämiä tietoja ei ole poistettu asianmukaisesti. Organisaation sisäisesti yhteisessä käytössä olevat printterit ja skannerit mahdollistavat tietojen vuotamisen sellaisille työntekijöille, joilla ei pitäisi olla pääsyä tietoihin.

Koti ym. (2017) listaavat FTP-palvelut, Wi-Fin, sähköpostin ja mobiilisovellukset verkkoon ja sovelluksiin liittyviksi väyliksi tietovuodoille. Tietovuotoja voi tapahtua myös tietojen säilyttämisen, siirtämisen ja käyttämisen prosesseissa. Fyysisten ja käyttäjäperäisten uhkien lisäksi organisaation tulee suojautua teknisiltä uhilta.



KUVIO 1 Mahdollisia väyliä tietovuodoille (Koti ym., 2017, s. 627 mukaan)

2.5 Tietomurtojen paljastuminen ja niistä tiedottaminen

Uusia tietomurtoja ja tietovuotoja paljastuu jatkuvasti, ja ne ovat yhä enemmän esillä myös mediassa. Organisaatioilla on kuitenkin vaikeuksia havaita tietomurtoja ja puolustautua niitä vastaan (Rosati ym., 2019). Janakiramanin ym. (2018) mukaan tietomurron sattuessa organisaation tulisi pyrkiä aktiivisesti minimoimaan syntyviä vahinkoja ja tiedottaa tapahtuneesta asiakkailleen. Yritysten tulisi myös varautua etukäteen tietoturvariskeihin, tunnistaa haavoittuvuudet ja riskit sekä suunnitella, miten tietomurron sattuessa toimitaan (Khan ym., 2021).

Tietomurron kohteeksi joutuneet yritykset eivät usein halua paljastaa julkisuuteen tietomurron laajuutta, koska ne pelkäävät siitä seuraavaa negatiivista julkisuutta. Yritysnäkökulmasta tietomurtojen ja tietovuotojen vaikutusten tutkimiseen luokin haastetta se, että yritykset pyrkivät tiukentamaan turvallisuustoimenpiteitään ja ovat haluttomia jakamaan tietoa tietomurron yksityiskohdista ja vaikutuksista. (Janakiraman ym., 2018.) Khan ym. (2021) suosittelevat yrityksiä käyttämään tietoturvauhkien havaitsemiseen ja estämiseen tarkoitettua järjestelmää (engl. Incident Detection and Prevention System), jonka avulla hyökkäykset voidaan havaita nopeasti ja niistä voidaan kerätä todisteita jälkiselvitystä varten.

Tietomurron tapahduttua yrityksen täytyy tiedottaa asiasta sekä sisäisesti henkilöstölleen että julkisesti asiakkaille ja muille sidosryhmille. Tietovuodosta ilmoittamiseen liittyy myös sääntöjä ja lakeja riippuen toimialasta ja valtiosta, jossa yritys toimii. (Khan ym., 2021.) Usein yritykset tiedottavat ensin julkisesti tapahtuneesta tietomurrosta ja sen jälkeen ilmoittavat henkilökohtaisesti niille asiakkaille, joiden tietoja on mahdollisesti vuotanut murron yhteydessä. Näiden ilmoitusten yhteydessä kerrotaan yrityksen jatkotoimenpiteistä asian suhteen ja informoidaan asiakasta toimenpiteistä, joilla hän voi itse ehkäistä tietomurron aiheuttamia vahinkoja. (Janakiraman, 2018.)

3 TIETOMURTOJEN VAIKUTUS INTERNETIN KÄYTTÄJIEN TUNTEISIIN JA KÄYTÖKSEEN

Tässä luvussa käsitellään tarkemmin tietomurtojen ja tietovuotojen seurauksia uhrien näkökulmasta ja niiden ihmisissä herättämiä tunteita. Lisäksi käydään läpi, miten tietoisuus mahdollisista tietovuodoista ja muista tietoturvariskeistä vaikuttaa internetin käyttäjien käytökseen ja luottamukseen eri verkkopalveluja kohtaan. Lopuksi esitellään tietoturvahuolien mittaamiseen käytetyt IUIPC- ja CFIP-viitekehykset ja vertaillaan niitä keskenään.

3.1 Tietomurtojen seuraukset

Tietovuotojen seurauksia yrityksille ja organisaatioille on käsitelty useissa tutkimuksissa. Janakiramanin ym. (2018) mukaan yritykset ovat usein huonosti varautuneita tietomurtoihin eivätkä osaa arvioida niiden vaikutuksia. Tietomurrolla on kuitenkin negatiivinen vaikutus yrityksen asiakas- ja sidosryhmäsuhteisiin (Janakiraman ym., 2018; Khan ym. 2021). Valtion organisaatiot joutuvat usein vakoiluhyökkäysten kohteeksi, mutta myös yrityksiä kohtaan voidaan tehdä tällaisia hyökkäyksiä kilpailijoiden toimesta. Yleisin motiivi tahallisille tietomurroille on luottamuksellisten tietojen varastaminen. (Iovan & Iovan, 2016.)

Yritykset ja muut organisaatiot voivat kärsiä pitkään tietomurtojen taloudellisista vaikutuksista ja mainehaitoista. Myös asiakkaat, joiden tiedot ovat päätyneet ulkopuolisen haltuun, voivat joutua kärsimään monista negatiivisista seurauksista. Khan ym. (2021) luokittelevat tietomurtojen vaikutukset kolmeen luokkaan riippuen siitä, mihin tietoturvan osa-alueeseen murto kohdistuu. Tietojen luottamuksellisuuteen kohdistuva tietomurto syntyy, kun tietoihin pääsee käsiksi joku, jolla ei ole siihen oikeutta. Vaikka tilanne aiheutuisi vahingossa ilman tarkoitusta murtautua tietoihin, sitä pidetään silti tietojen hallinnan menettämisenä. Luottamuksellisuuteen kohdistuva tietomurto voi aiheuttaa yrityksille sakkoja, oikeusjuttuja ja kilpailuedun menettämisen. Yksittäisille ihmisille, kuten

asiakkaille ja työntekijöille, tällaisesta tietomurrosta voi seurata identiteettivarkauden kohteeksi joutuminen. (Khan ym., 2021.)

Mikäli tietojen käyttö tai saatavuus estyy tietomurron vuoksi, on kyseessä tietojen käytettävyyteen liittyvä tietomurto. Tämäntyyppisestä tietomurrosta voi seurata käyttökatko palveluissa, tietojen varkaus tai niiden katoaminen kokonaan järjestelmästä. Tahallisten käytettävyyteen liittyvien hyökkäysten motiivina on usein estää palvelun käyttö tai estää pääsy tietoihin ja kiristää tietojen omistajalta lunnaita vastineeksi tietojen vapauttamisesta. (Khan ym., 2021.)

Kolmas Khanin ym. (2021) esittämistä luokista on tietojen eheyteen liittyvä tietomurto. Tietojen eheys on uhattuna, mikäli joku vahingossa tai tahallaan muokkaa tietoja virheellisiksi. Tästä voi aiheutua yrityksille kilpailuedun menettämistä ja tietojen tuhoutumista ja vääristymistä. Virheet tiedoissa ja tietojen katoaminen vaikuttavat myös asiakkaisiin, joista yritys säilyttää tietoja. (Khan ym., 2021.) Esimerkiksi terveydenhuollossa potilastietojen luvaton muokkaaminen tai poistaminen voi pahimmillaan olla uhka potilaan hengelle.

De Kimpe ym. (2020) ovat tutkineet kyberrikoksia uhrien näkökulmasta ja käsitelleet uhrien kokemia taloudellisia, psyykkisiä ja emotionaalisia seurauksia. Tietomurrosta voi aiheutua suoria taloudellisia tappioita ja luottamuksen menetys esimerkiksi verkossa ostamiseen tai pankkiasiointiin. Uhrit menettävät myös paljon aikaa rikoksen jälkiseuraamusten vuoksi. He voivat joutua tekemään erilaisia toimenpiteitä suojatakseen tietojaan uudelleen ja estääkseen niiden leviämisen. Myös kyberrikoksen aiheuttamat negatiiviset tunteet, kuten ahdistus ja pelko, vievät uhrin aikaa ja voimavaroja. Kyberrikoksen uhrit ovat kertoneet kokeneensa myös fyysisiä oireita, kuten pahoinvointia, unettomuutta ja painon putoamista. (De Kimpe ym., 2020.)

3.2 Tietomurtojen herättämät tunteet

Tutkimusten mukaan tietomurrot aiheuttavat internetin käyttäjissä paljon erilaisia negatiivisiksi koettuja tunteita. Chatterjee ym. (2019) ovat tutkineet erityisesti pelon ja vihan ilmenemistä tietomurtotilanteissa. Sekä pelko että viha ovat yleisiä reaktioita tietomurtouutisiin ja ne ovat monin tavoin samanlaisia tunteita. Molemmat tunteet ovat synnynnäisiä puolustusmekanismeja, jotka aktivoituvat, kun ihminen joutuu uhkaavaan tilanteeseen. Molemmat aiheuttavat vaistomaisen reaktion uhkaan. Pelko herättää ihmisessä pakoreaktion ja viha hyökkäysreaktion. (Chatterjee ym., 2019.)

Chatterjeen ym. (2019) mukaan ihmiset käyttäytyvät eri tavalla kuullessaan tietomurrosta riippuen siitä, kokevatko he tilanteessa enemmän pelkoa vai vihaa. Pelkoa kokevat henkilöt keskittyvät enemmän itseensä ja saattavat esimerkiksi syyttää itseään siitä, etteivät ole suojanneet omia tietojaan tarpeeksi hyvin. He myös tuntevat usein, että tilanne ei ole heidän hallinnassaan. De Kimpen ym. (2020) mukaan erityisesti petosten ja huijausten uhrien on havaittu syyttävän itseään tapahtuneesta ja tuntevansa olonsa tyhmäksi. Tällaisten kyberrikosten uhrien luottamus itseensä ja muihin ihmisiin vähenee rikoksen seurauksena. Vihaa

kokevat ihmiset puolestaan syyttävät muita tietomurrosta, ja kokevat, että heille ei voisi käydä samoin. Tietomurtouutisen kuultuaan he syyttävät murron kohteeksi joutunutta yritystä ja kohdistavat vihansa siihen. (Chatterjee ym., 2019.)

Tietoturvaan kohdistuvat kyberrikokset herättävät uhreissa pelon ja vihan tunteiden lisäksi myös surua, masentuneisuutta, stressiä, ahdistusta ja häpeää. Ahdistus ja häpeä liittyvät uhrin itsesyytöksiin, ja voivat vaikeuttaa avun hakemista ja oman kokemuksen jakamista muille. (De Kimpe ym., 2020.) Bergströmin (2015) tutkimuksessa todettiin, että ihmiset, jotka ovat yleisesti ahdistuneempia, ovat tarkempia henkilökohtaisten tietojensa suojaamisesta. Saman tutkimuksen mukaan tietoturvahuolien voimakkuuteen vaikuttaa myös kyseessä olevien asioiden henkilökohtaisuus. Esimerkiksi verkossa maksamisen ja sosiaalisen median käytön havaittiin herättävän enemmän huolta henkilökohtaisten tietojen turvallisuudesta kuin sähköpostin tai hakukoneen käytön.

Demografisten tekijöiden vaikutusta tietoturvahuoliin on käsitelty useissa tutkimuksissa, mutta tulokset ovat osittain ristiriitaisia. Zhang ym. (2013) havaitsivat iän ja koulutustason vaikuttavan tietoturvahuoliin mobiilikaupan (engl. m-commerce) kontekstissa. Nuoret ovat avoimempia omaksumaan uutta teknologiaa ja halukkaampia mobiilikaupankäyntiin. Korkealla koulutustasolla havaittiin olevan yhteys suurempiin tietoturvahuoliin. (Zhang ym., 2013.) Hwangin ym. (2012) mukaan koulutustaso korreloi positiivisesti tietoturvahuolien määrän kanssa terveydenhuollon kontekstissa. Sukupuolten välisissä vertailuissa naisten on todettu huolehtivan tietojensa yksityisyydestä ja turvallisuudesta enemmän kuin miesten (Hoy & Milne, 2010; Janda & Fair, 2004), mutta korrelaatiota sukupuolen ja tietoturvahuolien välillä ei ole yksiselitteisesti vahvistettu. Esimerkiksi Zhang ym. (2013) ja Hwang ym. (2012) eivät löytäneet tilastollista merkitsevyyttä sukupuolen ja tietoturvahuolien välillä.

3.3 Tietoturvariskien vaikutus käyttäjän luottamukseen ja käytökseen

Bansal ja Zahedi (2015, s. 62) määrittelevät luottamuksen ”psykologiseksi tilaksi, jossa hyväksytään haavoittuvuuden mahdollisuus perustuen positiivisiin odotuksiin luottamuksen kohteen aikeista tai käytöksestä luottamusta osoittavalle osapuolelle tärkeitä asioita kohtaan”. Luottamus vaikuttaa internetin käyttäjien halukkuuteen tehdä ostoksia verkossa (Zorotheos & Kafeza, 2009) ja jakaa tietojaan palveluntarjoajille (Kusyanti ym., 2017). Metzger (2004) pitää luottamusta jopa tärkeimpänä vaikuttavana tekijänä tietojen luovuttamisessa. Bergströmin (2015) mukaan henkilön yleinen luottamus muita ihmisiä kohtaan vaikuttaa myös siihen, kuinka vakavina hän kokee erilaiset tietoturvauhat.

Kuluttajien luottamus yrityksiä kohtaan vähenee tietomurron tapahduttua (Janakiraman ym., 2018; Khan ym., 2021). Tämä voi näkyä negatiivisesti liikevaihdossa ja lisätä kilpailevien yritysten asiakasmääriä. Kyberrikoksen uhriksi itse joutuneet menettävät myös yleistä luottamustaan muihin ihmisiin ja omaan

itseensä (De Kimpe ym., 2020). Tietoisuus ja aiemmat kokemukset erilaisista tietoturvariskeistä lisäävät internetin käyttäjien pyrkimyksiä suojautua uhkilta omalla käytöksellään (Ortiz ym., 2018). Mahdollisia suojautumistoimenpiteitä ovat esimerkiksi väärien tietojen luovuttaminen, vaatimus poistaa palveluntarjoajan keräämät tiedot tai kieltäytyminen tietojen luovuttamisesta (Yang & Wang, 2009). Tietoturvahuolet vähentävät käyttäjien halukkuutta osallistua keskusteluun ja jakaa tietojaan internetin yhteisöpalveluissa. Tämä aiheuttaa niin sanottua lurkkausta (engl. lurking). Lurkkaamisella tarkoitetaan muiden käyttäjien keskustelun aktiivista seuraamista osallistumatta siihen itse. (Ortiz ym., 2018.)

Budak ym. (2021) nostavat yksilön resilienssin eli palautumiskyvyn yhtenä vaikuttavana tekijänä tietomurrosta aiheutuvasta stressistä toipumiseen. He esittelevät ehdotuksen mallista, jossa toipuminen riippuu ihmisen resilienssin voimakkuudesta. Kuviossa 2 esitetään Budakin ym. (2021) tutkimuksen malli kuluttajan käytökseen vaikuttavista tekijöistä. Stressitekijä on tapahtuma, jossa kuluttajan yksityisyyttä loukataan verkossa. Kuluttajan yksilöllinen resilienssi vaikuttaa siihen, miten voimakkaasti ja pitkäkestoisesti stressitekijä vaikuttaa kuluttajan käytökseen yksityisyysloukkauksen jälkeen. (Budak ym., 2021.)

KUVIO 2 Malli kuluttajan käytökseen vaikuttavista tekijöistä (Budakin ym., 2021, s. 5 mukaan)

Mitä korkeampi resilienssi yksilöllä on, sitä paremmin hän pystyy käsittelemään tietoturvauhkia ja toipumaan niiden aiheuttamasta stressistä. Resilienssiin vaikuttavia tekijöitä ovat psykologiset tekijät, asenteet internetin käyttöä kohtaan, demografiset tekijät ja ympäristötekijät. (Budak ym., 2021.) Taulukossa 1 on listattu tarkemmin näihin kategorioihin kuuluvia tekijöitä.

TAULUKKO 1 Resilienssiin vaikuttavat tekijät

Psykologiset tekijät
• Minäpystyvyys • Stressinsietokyky • Positiiviset emootiot • Ekstroverttiys • Hengellisyys • Itsetunto • Positiivinen affekti • Hallintakäsitys • Aktiiviset coping-keinot
Internetin käyttöön liittyvät asenteet
• Tietoturvatietoisuus • Internetin käytön koettu hyöty • Yksityisyyden tarve • Tietokoneen käyttöön liittyvä ahdistus ja pelko • Tietoturvahuolet • Omien tietojen hallinta • Halukkuus jakaa tietoja • Omien tietojen suojaamiseen tähtäävä käytös
Demografiset tekijät ja digitaidot
• Sukupuoli • Ikä • Koulutustaso • Ammatti • Asuinpaikka • Digitaidot
Mikroympäristötekijät

• Sosiaalinen tukiverkko
  ○ Perhe
  ○ Ystävät
  ○ Vertaistuki
  ○ Organisaatiot

Makroympäristötekijät
• Lait • Tavat • Kulttuuriin liittyvät käytänteet

3.4 Tietoturvahuolien mittaaminen

Tietojärjestelmätieteen tutkimuksessa yleisimmin käytettyjä tietoturvahuolien mittareita ovat Malhotran ym. (2004) kehittämä IUIPC (Internet Users' Information Privacy Concerns) ja Smithin ym. (1996) CFIP-malli (Concern for Information Privacy). Näistä malleista CFIP on luotu ensin ja sitä on käytetty lukuisissa tutkimuksissa. CFIP-mallin aktiivinen käyttäminen on jatkunut vaihtoehtoisen IUIPC-mallin syntymisestä huolimatta. Molempia malleja on kuitenkin käytetty, arvioitu ja vertailtu useissa tutkimuksissa. (Belanger & Crossler, 2011.)

3.4.1 CFIP

Smithin ym. (1996) kehittämä CFIP on teoreettinen viitekehys internetin käyttäjien tietoturvahuolien eri ulottuvuuksista. CFIP-malli tarkastelee tietoturvahuolia organisaationäkökulmasta. Malliin kuuluu neljä ulottuvuutta, jotka sisältävät yhteensä 15 väittämää tietoturvaan liittyen. Väittämät on esitetty liitteessä 1. Stewart ja Segars (2002) testasivat myöhemmin CFIP-mallia ja totesivat sen 15 kohdan mittariston päteväksi tavaksi mitata tietoturvaan liittyviä huolia.

CFIP-mallin neljä ulottuvuutta ovat tietojen kerääminen (engl. collection), virheet tiedoissa (engl. errors), tietojen luvaton käyttö (engl. unauthorized secondary use) ja luvaton pääsy tietoihin (engl. improper access) (Smith ym., 1996). CFIP-mallissa ensimmäinen ulottuvuus on tietojen kerääminen, jossa mitataan yksilön kokemusta siitä, kuinka huolestuttavana hän kokee kerätyn tiedon määrän ja tietojensa luovuttamisen yrityksille (Stewart & Segars, 2002).

Toinen CFIP-mallin ulottuvuus on virheet, joita ulkopuoliselle taholle luovutettuihin tietoihin voi tulla. Tietojen luovuttaja voi kokea huolta tietojensa oikeellisuudesta ja epäillä, että yritysten toimenpiteet tiedoissa esiintyvien virheiden etsimiseksi ja välttämiseksi eivät ole riittäviä. Useimmiten virheet ovat tahattomia, mutta on myös mahdollista, että joku, jolla on pääsy tietoihin, muokkaa niitä tahallaan virheellisiksi. (Stewart & Segars, 2002.)

Kolmas ulottuvuus, tietojen luvaton käyttö, voidaan jakaa kahteen osaan: tietojen sisäiseen ja ulkoiseen käyttöön. Sisäisellä käytöllä tarkoitetaan tietojen käyttöä sisäisesti siinä yrityksessä, jolle tiedot on luovutettu vapaaehtoisesti. Luvaton käyttö aiheuttaa tietoturvahuolia, sillä siinä tietoja käytetään johonkin muuhun tarkoitukseen kuin mihin tiedot on alun perin luovutettu. Tällaista luvatonta tietojen käyttöä on esimerkiksi kerättyjen asiakastietojen käyttö markkinointitarkoituksiin, vaikka tietoja olisi alun perin pyydetty muista syistä. Ulkoinen tietojen luvaton käyttö tarkoittaa tietojen päätymistä niitä keränneen yrityksen ulkopuoliselle taholle ja eri käyttötarkoitukseen, johon ne on luovutettu. (Stewart & Segars, 2002.)

Neljäs ulottuvuus CFIP-mallissa on luvaton pääsy tietoihin. CFIP-malli käsittelee tietoturvahuolia tietoja luovuttavan yksilön ja tietoja keräävän yrityksen vuorovaikutuksessa. Luvattoman pääsyn ulottuvuus viittaa siis yrityksen sisäisiin käytäntöihin siitä, kenellä on oikeus käsitellä tietoja. Tietoja luovuttavalla yksilöllä ei välttämättä ole tietoa siitä, kenelle organisaatiossa hänen tietonsa ovat

saatavilla. Tällainen epätietoisuus voi lisätä tietoturvahuolia. (Stewart & Segars, 2002.)

3.4.2 IUIPC

Toinen yleisesti tietoturvahuoliin liittyvässä tutkimuksessa käytetty malli on Malhotran ym. (2004) kehittämä IUIPC-malli. Se pohjautuu sosiaalisen sopimuksen teoriaan ja lähestyy internetin käyttäjien yksityisyyshuolia oikeudenmukaisuuden näkökulmasta. IUIPC-malliin sisältyy 10 kohdan mittaristo tietoturvahuolien mittaamiseksi. (Malhotra ym., 2004.) Mittaristo on esitetty liitteessä 2.

IUIPC-mallin kolme ulottuvuutta ovat tietojen kerääminen (engl. collection), tietojen hallinta (engl. control) ja tietoisuus kerättyjen tietojen käytöstä (engl. awareness). Tietojen keräämisen suhteen mahdolliset tietoturvahuolet liittyvät siihen, kuinka reiluna ja hyödyllisenä tietojaan luovuttava henkilö kokee näiden tietojen luovuttamisen. Kun kuluttaja antaa tietojaan esimerkiksi verkkokaupalle, hän arvioi tästä saamansa hyödyn suhdetta mahdollisiin riskeihin. Tietojen luovuttamisen suhteen ollaan sitä vastahakoisempia mitä suuremmaksi mahdolliset haitat tietojen luovuttamisesta koetaan. (Malhotra ym., 2004.)

Toinen IUIPC-mallin ulottuvuus on tietojen hallinta, jolla viitataan tietoturvan kontekstissa tietojaan luovuttaneen henkilön mahdollisuuteen vaikuttaa henkilökohtaisten tietojensa käyttöön ja halutessaan saada tietonsa poistettua toisen osapuolen hallusta. Hallinnan tunteen puuttuminen omien tietojen suhteen lisää tietoturvaan liittyviä huolia. (Malhotra ym., 2004.)

IUIPC:n kolmas ulottuvuus on tietoisuus siitä, mihin tarkoituksiin kerättyjä tietoja käytetään. Tietojen luovuttaja antaa tietojaan aina johonkin tarkoitukseen. Tiedot luovuttanut henkilö voi kokea epäoikeudenmukaisena tietojensa käyttämisen muihin kuin hänen ennalta tietämiinsä ja hyväksymiinsä tarkoituksiin. Tietoisuuden ulottuvuuteen kuuluu myös tieto siitä, miten tietojen haltija suojaa säilyttämiään tietoja. Tietoturvahuolia lisää epävarmuus siitä, miten hyvin tietoja säilyttävä osapuoli huolehtii tietojen turvallisesta säilyttämisestä ja käsittelystä. (Malhotra ym., 2004.)

3.4.3 IUIPC- ja CFIP-mallien vertailu

Tietoturvahuolien jako eri ulottuvuuksiin on yksi selkeimmistä eroista IUIPC- ja CFIP-mallien välillä. CFIP koostuu neljästä ulottuvuudesta, kun IUIPC-mallissa ulottuvuuksia on vain kolme. Ainoastaan tietojen keräämisen ulottuvuus on sisällytetty molempiin malleihin. Tietojen keräämistä lähestytään kuitenkin hieman eri näkökulmista. IUIPC-malli pohjautuu voimakkaasti ihmisten kokemuksiin oikeudenmukaisuudesta, ja sen mukaan tietojen luovuttamiseen ollaan suostuvaisempia, jos siitä koituvien riskien koetaan olevan kohtuullisia suhteessa saatuun hyötyyn (Malhotra ym., 2004). CFIP-mallissa huoli tietojen keräämisestä liittyy kerätyn tiedon määrään ja yksilön kokemukseen siitä, kuinka huolestuttavana hän kokee tietojensa luovuttamisen yrityksille (Stewart & Segars, 2002).

CFIP-mallin tietojen luvaton käyttö vastaa osittain IUIPC:n tietoisuuden ulottuvuutta, sillä molemmissa yksilön huoli tietojensa turvallisuudesta kasvaa,

mikäli tietoja käytetään muihin kuin hänelle ennalta ilmoitettuihin tarkoituksiin. Myös IUIPC:n tietojen hallinnan ulottuvuus sisältää elementtejä CFIP-mallin tietojen luvattoman käytön ulottuvuudesta: Molempiin ulottuvuuksiin liittyy esimerkiksi yritysten tekemät päätökset tietojen käytöstä ja luovuttamisesta kolmansille osapuolille. IUIPC-mallissa korostetaan yksilön oikeutta hallita omia tietojaan, joten yrityksellä ei koeta olevan oikeutta tehdä päätöksiä tietoihin liittyen (Malhotra ym., 2004).

Useissa tutkimuksissa on hyödynnetty sekä IUIPC- että CFIP-mallia ja verrattu niitä keskenään (Belanger & Crossler, 2011; Clouse ym., 2010; Fodor & Brem, 2015; Yang & Wang, 2009). Belanger ja Crossler (2011) nostavat artikkelissaan esille, että CFIP-mallia on käytetty tutkimuksissa huomattavasti enemmän kuin IUIPC-mallia. He kannustavat tutkijoita tekemään vertailua näiden mallien välillä ja selvittämään, ovatko molemmat mallit valideja käytettäväksi tulevassa tietoturvahuolien tutkimuksessa.

Sipior ym. (2013) käyttivät IUIPC-mallia ja sen mittareita tutkimuksessaan, ja saivat osittain mallia tukevia tuloksia. Myös heidän näkemyksensä kuitenkin oli, että mallia on vielä testattava ja arvioitava vertaamalla sitä esimerkiksi CFIP-malliin. Fodor ja Brem (2015) hyödynsivät molempia malleja tutkiessaan millenniaalien tietoturvahuolien vaikutusta halukkuuteen käyttää sijaintitietoja keräämiä sovelluksia. CFIP-mallin mittaristoa käyttämällä tutkimuksessa selvisi, että käyttäjien kokema luottamus palvelua kohtaan vaikuttaa halukkuuteen luovuttaa tietoja sovellukselle. IUIPC-mallin osalta luottamuksen merkitysestä ei saatu vahvistusta tutkimuksessa. Fodor ja Brem (2015) pitävät tästä huolimatta IUIPC-mallia parempana vaihtoehtona sen yksinkertaisuuden vuoksi.

Harborth ja Pape (2020) käyttivät IUIPC-viitekehystä tutkiessaan tietoturvahuolien vaikutusta aikomukseen käyttää yksityisyyttä parantavia teknologioita. Tässä kontekstissa IUIPC-mallia jouduttiin käyttämään eri näkökulmasta, sillä tutkimuksen kohteena oli turvallisuuden parantamiseen tarkoitettu palvelu. Myös tässä tutkimuksessa saatiin kuitenkin tuloksia, jotka viittasivat luottamuksen vaikuttavan ihmisten halukkuuteen käyttää palvelua.

IUIPC on suunniteltu erityisesti internetin kontekstiin (Malhotra ym., 2004). CFIP on puolestaan luotu mittaamaan kuluttajien organisaatioiden tietoturvakäytäntöihin liittyviä tietoturvahuolia (Stewart & Segars, 2002), mutta sitä on myöhemmin sovellettu lukuisissa internetin käyttäjien tietoturvahuoliin liittyvissä tutkimuksissa (Belanger & Crossler, 2011). Taulukkoon 2 on koottu CFIP:n ja IUIPC:n keskeisiä eroavaisuuksia ja tutkimusartikkeleja, joissa mittaristoja on testattu.

Belanger ja Crossler (2011) huomauttavat, että tietoturvan kontekstissa aikomus käyttäytyä tietyllä tavalla ei automaattisesti johda aiotun kaltaiseen käytökseen. Myös Fodor ja Brem (2015) nostavat tutkimuksensa päätelmissä esiin sen, että IUIPC- ja CFIP-mallien avulla selvitetään vain tutkittavien käyttäytymisaikomuksia ja varsinaisen käytöksen tutkimiseen tarvitaan muita menetelmiä. Tietoturvahuolien mittaamisessa ja käytösaikomusten selvittämisessä nämä mallit ovat kuitenkin vakiintuneet tutkijoiden käyttöön ja niitä on sovellettu useassa eri kontekstissa.

TAULUKKO 2 CFIP- ja IUIPC-mallien vertailu

	CFIP	**IUIPC**
Ulottuvuudet	Tietojen kerääminen, virheet tiedoissa, tietojen luvaton käyttö, luvaton pääsy tietoihin	Tietojen kerääminen, tietojen hallinta, tietoisuus kerättyjen tietojen käytöstä
Mittaristo	15 kohtaa (liite 1)	10 kohtaa (liite 2)
Tausta/motivaatio	Tietoturvahuolien mittaamiseen tarkoitettujen validoitujen mittarien puute	Sosiaalisen sopimuksen teoria ja tarve erityisesti internetin kontekstiin sopiville tietoturvahuolien mittareille
Näkökulma	Organisaationäkökulma	Oikeudenmukaisuuden näkökulma
Kritiikki	CFIP ei sovellu internetin kontekstiin yhtä hyvin kuin IUIPC (Malhotra ym., 2004). CFIP ei ennusta käytösaikomusta yhtä hyvin kuin IUIPC (Clouse ym., 2010)	IUIPC-mittaristoa ei voitu kokonaisuutena todeta validiksi, vaikka tutkimustulokset tukivat mallia osittain (Sipior ym., 2013). IUIPC:n avulla ei pystytty havaitsemaan merkittäviä yhteyksiä luottamuksen ja tietoturvahuolien välillä (Fodor & Brem, 2015). Alkuperäisten IUIPC-10-mittarien sijasta on ehdotettu korvaavia IUIPC-8-mittareita, joiden todettiin mittaavan tietoturvahuolia tarkemmin (Gross, 2021).
Validointi	Smith ym. (1996), Stewart & Segars (2002), Hwang ym. (2012), Osatuyi (2015)	Malhotra ym. (2004), Yang & Wang (2009), Clouse ym. (2010)

4 TUTKIMUSMENETELMÄ

Tässä luvussa tarkastellaan empiirisen tutkimuksen tutkimusmenetelmän valintaa, tutkimuksen toteutusta ja kerätyn aineiston analysointimenetelmiä. Aluksi esitellään tutkimuksen tavoite, tutkimuskysymykset sekä valittu tutkimusmenetelmä. Sen jälkeen käydään läpi tutkimuksen toteutus. Lopuksi esitellään tutkimusaineiston analysointiprosessi.

4.1 Tutkimuksen tavoite

Tutkimuksen tavoitteena oli selvittää, mitä tunteita tietomurrot ja niistä seuraavat tietovuodot herättävät yli 18-vuotiaissa internetin käyttäjissä. Kirjallisuuskatsauksen perusteella oletettiin, että tietomurtojen herättämät tunteet ovat pääosin negatiivisia, joten tutkimuksessa keskityttiin kartoittamaan yleisesti negatiivisina pidettyjä tunteita. Lisäksi tutkimuksessa haluttiin selvittää, miten internetin käyttäjien tietämys tietomurtojen mahdollisuudesta vaikuttaa heidän käytökseensä ja halukkuuteen luovuttaa tietojaan internetissä. Empiirisen osion tutkimusotteeksi valittiin määrällinen tutkimus. Aineisto kerättiin verkkokyselylomakkeella.

4.1.1 Tutkimuskysymykset

Tutkimusongelma tiivistettiin kahteen päätutkimuskysymykseen ja neljään niitä tarkentavaan kysymykseen:

1. Millaisia tunteita tietomurrot ja niistä aiheutuneet tietovuodot herättävät tietomurtojen uhreissa ja yleisesti kaikissa internetiä käyttävissä ihmisissä?
   1.1. Onko tunteissa eroja tietomurron uhreiksi joutuneiden ja muiden internetin käyttäjien välillä?
   1.2. Mitkä tietoturvahuolien ulottuvuudet herättävät eniten ja voimakkaimmin tunteita internetin käyttäjissä?

2. Miten tieto tietoturvariskeistä vaikuttaa ihmisten käytökseen ja halukkuuteen luovuttaa tietojaan yrityksille tai muille organisaatioille verkossa?
   2.1. Onko tiedolla vaikutusta käyttäjän luottamukseen ja siihen, millaisena käyttäjä kokee yrityksen vastuun tietomurtotilanteessa?
   2.2. Miten käyttäjät perustelevat tietomurron kohteeksi joutuneen palvelun käytön jatkamista?

Ensimmäisen tutkimuskysymyksen keskeisimpänä tarkoituksena on nimetä keskeisimmät tunteet, joita tietomurrot herättävät internetin käyttäjissä. Tutkimuksessa pyrittiin selvittämään eroavaisuuksia tunteissa eri vastaajaryhmien ja tietoturvahuolien ulottuvuuksien välillä. Toisessa tutkimuskysymyksessä tarkastellaan tiedon vaikutusta käytökseen, luottamukseen ja käsitykseen yrityksen vastuusta. Tässä tutkimuksessa tiedolla tarkoitetaan ensisijaisesti tietoa tietomurtojen olemassaolosta. Vastaajien syvällisempää ymmärrystä esimerkiksi tietomurtojen syntymisestä ei testattu kyselyssä eikä ennakkotietoja aiheesta vaadittu.

4.1.2 Tutkimusote

Tutkimusotteeksi valittiin kvantitatiivinen eli määrällinen tutkimus, koska tutkimuksessa haluttiin tutkia laajaa joukkoa internetin käyttäjiä ja saada tuloksia, jotka voidaan yleistää koskemaan koko kohderyhmää. Kvantitatiivisessa tutkimuksessa tutkittavaa ilmiötä ja siihen liittyviä tekijöitä pyritään muuttamaan lukuina mitattavaan muotoon. Aineistolle suoritettavilla tilastollisilla analyyseillä pyritään saamaan koko populaatioon yleistettäviä tuloksia. (Kananen, 2011, s. 17-18).

Aiemmilla teorioilla, tarkalla käsitteiden määrittelyllä ja hypoteesien esittämisellä on keskeinen rooli kvantitatiivisessa tutkimuksessa (Hirsjärvi ym., 2004, s. 131). Tietoturvauhkien ja tietoturvahuolien vaikutuksesta internetin käyttäjien käytökseen on olemassa kohtuullinen määrä aiempaa tutkimustietoa. Käytöstä on aiemmissa tutkimuksissa pyritty selittämään tietoturvahuolilla eikä tiedolla, kuten tässä tutkimuksessa. Internetin käyttäjien tietoturvauhkiin liittyvien tunteiden kohdalla aiempi tutkimus on vähäistä, ja usein keskittynyt vain muutamaan eri tunteeseen, kuten Chatterjeen ym. (2019) pelon ja vihan tunteita käsittelevä tutkimus.

Aiempaa tutkimustietoa ja tietoturvahuolien mittaamiseen tarkoitettuja malleja käytettiin tässä tutkimuksessa apuna kyselylomakkeen suunnittelussa. Vaikka kvantitatiivisessa tutkimuksessa asetetaan usein hypoteesit, tutkimuksen tavoitteen voi esittää myös kysymyksen muodossa, mikäli tutkimuskohteena ovat ennalta tutkitut muuttujat, joita ei ole aiemmassa tutkimuksessa tutkittu yhdessä (Metsämuuronen, 2005, s. 47). Tästä syystä tässä tutkimuksessa päädyttiin hypoteesien sijaan kysymysmuotoiseen tavoitteen määrittelyyn.

4.1.3 Tutkimusmenetelmä

Tutkimus toteutettiin survey- eli kyselytutkimuksena. Jokivuoren ja Hietalan (2015) mukaan kyselytutkimusta käytetään, kun halutaan tutkia laajoja ihmisjoukkoja. Verkkokyselyn koettiin olevan sopivin tapa saada tarpeeksi suuri aineisto ja tavoittaa tutkimuksen kohderyhmä. Koska tutkimuksen kohderyhmää ovat aikuiset, jotka käyttävät internetiä vähintään satunnaisesti, verkkokysely arvioitiin parhaaksi keinoksi toteuttaa aineistonkeruu. Survey-tutkimuksen tyypillinen piirre on tietojen kerääminen strukturoidussa muodossa jokaiselta yksilöltä samalla tavalla (Hirsjärvi ym., 2004, s. 125). Myös tässä tutkimuksessa kaikki vastaajat vastasivat tismalleen samoihin kysymyksiin.

Verkkokyselyn etuja ovat nopeus sekä aineiston keruussa että aineiston käsittelyssä. Tiedot voidaan siirtää suoraan ohjelmasta toiseen, joten litteroinnista ja tietojen manuaalisesta syöttämisestä aiheutuvat virheet jäävät pois. Sosiaalisen median kautta levitetyssä verkkokyselyssä on kuitenkin huomioitava, että tutkijalla ei ole mahdollisuutta noudattaa todennäköisyysotannan periaatteita ja valikoida tai rajata vastaajia. Näin ollen aineistossa on kyse otannan sijaan näytteestä. (Valli & Perkkilä, 2015.) Valitun levitystavan hyvänä puolena oli runsas vastaajamäärä lyhyessä ajassa. Sosiaalisessa mediassa levitetyssä verkkokyselyssä ei kuitenkaan voida varmuudella tietää, onko vastaukset annettu rehellisesti ja onko vastaaja tutkimuksen kohderyhmää. Tämä seikka tulee huomioida aineiston luotettavuutta arvioitaessa.

4.2 Tutkimuksen toteutus

Tutkimuksen aineisto kerättiin suomenkielisellä verkkokyselylomakkeella, joka oli avoinna aikavälillä 16.9.-26.9.2021. Kyselyvastauksia tuli tänä aikana 262 kappaletta. Kyselylomake luotiin Webropol-ohjelmalla, joka on ilmaiseksi saatavilla Jyväskylän yliopiston kautta. Saatavuuden lisäksi ohjelmiston valintaan vaikutti sen helppokäyttöisyys ja tutkimuksen tekijän aiempi kokemus ohjelman käytöstä.

Hirsjärvi ym. (2004, s. 193) sekä Holopainen ja Pulkkinen (2002, s. 40) kehottavat testaamaan kyselylomaketta koevastaajilla, jotta mahdolliset ongelmat ja puutteet voidaan havaita ja korjata ennen varsinaisen aineistonkeruun aloittamista. Kyselylomaketta testattiin useilla vastaajilla ennen valmiin lomakkeen julkaisemista ja aineistonkeruun aloittamista. Kaikki koevastaajat kuuluivat kyselyn kohderyhmään ja heiltä pyydettiin palautetta kyselyn ymmärrettävyydestä, vaihtoehtojen yksiselitteisyydestä ja kyselylomakkeen kieliasusta. Saadun palautteen perusteella kyselyn vastausvaihtoehtoihin tehtiin pieniä muutoksia.

Kyselylinkkiä levitettiin sosiaalisen median palveluissa (Facebook ja LinkedIn) ja suljetuissa keskusteluryhmissä (työ- ja harrastusyhteisöjen omat WhatsApp- ja Slack-keskusteluryhmät). Tällaisen sosiaalisen median kautta tehdyn aineistonkeruun haasteena on Vallin ja Perkkilän (2015) mukaan se, ettei vastaajia voi juurikaan rajata ja aineisto voi painottua johonkin tiettyyn ihmisryhmään. Aineistonkeruun aikana tarkkailtiin tavoitettujen vastaajien ikä-, koulutus- ja

sukupuolijakaumaa Webropolin seurannan kautta ja hyödynnettiin näitä havaintoja kyselyn jakelukanavien valinnassa. Kyselylinkin jakamisella LinkedInissa haluttiin tavoittaa myös yli 30-vuotiaita korkeakoulutettuja internetin käyttäjiä, koska Facebookin kautta saadut vastaajat olivat pääosin 18-30-vuotiaita toisen asteen tutkinnon suorittaneita.

Metsämuurosen (2005, s. 585) mukaan tutkimuksen teossa on huomioitava aineiston mahdollinen kato. Mikäli vastaamatta jättäneet painottuvat johonkin tiettyyn ryhmään, tutkimuksen tuloksia ei voida yleistää koskemaan kyseistä ryhmää. Tässä tutkimuksessa katoa esiintyi vanhempien vastaajien kohdalla, joten tuloksista ei voitu tehdä luotettavia päätelmiä yli 40-vuotiaiden internetin käyttäjien tunteista ja käytöksestä.

4.2.1 Kyselylomake

Kyselylomakkeessa (liite 3) on 18 kysymystä, joista suurin osa on monivalintakysymyksiä. Aluksi vastaajilta kysyttiin yleisiä taustatietoja, kuten sukupuolta, ikää ja koulutustasoa. Vastaajilta kysyttiin myös erityisesti tutkimuksen aihealueeseen liittyviä taustakysymyksiä. Näillä kysymyksillä haluttiin kartoittaa vastaajien internetin käytön määrää, internetin käytön tarkoitusta ja sitä, ovatko he joskus joutuneet tietomurron uhriksi.

Seuraavassa kyselyn osassa oli vastaajien tietoa mittaavia kysymyksiä, joilla selvitettiin vastaajien tietomurtoihin liittyviä ennakkotietoja. Kysymyksien laadinnassa pyrittiin huomioimaan mahdollisimman monipuolisesti eri keinot saada tietoa aiheesta. Työt, opiskelu, media, oma kiinnostus ja harrastuneisuus arvioitiin todennäköisimmiksi kanaviksi kerryttää tietoturvatietoisuutta ja oppia tietomurroista, joten ne sisällytettiin tietoa mittaaviin kysymyksiin. Vastausvaihtoehtoina tietoa mittaavissa kysymyksissä käytettiin kysymyksestä riippuen 5-portaista Likert-asteikkoa tai ”kyllä”, ”ei” ja ”en osaa sanoa” -vaihtoehtoja.

Tutkimuksen keskeisimpänä tavoitteena oli kartoittaa tietomurtojen internetin käyttäjissä herättämiä tunteita. Tunteiden mittaamista varten vastaajille esitettiin väittämiä ja lista eri tunteista. Vastaajia pyydettiin valitsemaan kunkin väittämän kohdalla tunne tai tunteet, joita kyseinen tilanne tai väittämä heissä herättää. Kyselyyn valittiin tunteita, jotka ovat nousseet esille aiemmissa tutkimuksissa. Lisäksi vaihtoehdoksi lisättiin ärsyyntymisen tunne, jota ei mainittu aiemmassa tutkimuskirjallisuudessa, koska vihalle kaivattiin lievempää vaihtoehtoa. Vastausvaihtoehtona oli myös ”ei mitään näistä”, mikäli vastaaja ei kokenut minkään annetuista tunteista sopivan esitettyyn väittämään.

Tunteiden mittaamiseen tarkoitetut väittämät perustuivat tutkimuksen teoreettiseen viitekehykseen. Väittämät voidaan jakaa CFIP-mallin neljään ulottuvuuteen: tietojen keräämiseen, virheisiin, luvattomaan käyttöön ja luvattomaan pääsyyn (Smith ym., 1996). Väittämien laadinnassa hyödynnettiin sekä CFIP- että IUIPC-malliin kuuluvia tietoturvahuolia mittaavia väittämiä ja CFIP-mallin eri ulottuvuuksia. Aiemmissa tutkimuksissa CFIP- ja IUIPC-mittareita on käytetty tietoturvahuolien määrän mittaamiseen Likert-asteikollisilla vastausvaihtoehdoilla. Tässä tutkimuksessa näitä väittämiä käyttämällä haluttiin varmistaa, että tutkimus kattaa kaikki tietoturvahuolien eri ulottuvuudet.

Luottamusta ja käsitystä yritysten vastuusta mitattiin neljällä kysymyksellä, joihin vastausvaihtoehtoina oli 5-portainen Likert-asteikko. Luottamusta mitattiin kysymällä suoraan, uskovatko vastaajat henkilötietojensa olevan turvassa, ja kuinka tarkoin he harkitsevat tietojensa luovuttamista verkossa. Yrityksen vastuuta käsittelevät väittämät perustuvat Chatterjeen ym. (2019) tutkimukseen, jossa tutkittiin pelon ja vihan tunteiden aiheuttamia eroja kuluttajien käytökseen tietomurtojen jälkeen.

Kyselylomakkeen laadinnassa pyrittiin pitämään kysymysten määrä kohtuullisena ja samalla kuitenkin kattavasti kerätä aineistoa tutkimuskysymyksiin vastaamiseksi. Holopaisen ja Pulkkisen (2002, s. 39) mukaan liian pitkä kyselylomake vaikuttaa negatiivisesti vastausten laatuun. Lomakkeen täyttämiseen arvioitiin kuluvan noin 5-10 minuuttia.

4.2.2 Tutkimusaineiston analysointi

Aineiston analysointi aloitettiin viemällä tutkimusaineisto Webropolista exceltiedostoksi ja silmäilemällä aineisto läpi. Aineistosta pyrittiin löytämään selkeästi epäasiallisesti täytetyt lomakkeet. Kaikki saadut vastaukset hyväksyttiin mukaan tutkimukseen, joten saadun aineiston lopullinen koko oli 262 vastausta.

Aineisto analysoitiin IBM SPSS -ohjelmalla. Aluksi aineistosta tarkasteltiin demografisia tietoja ja arvioitiin, kuinka hyvin aineisto edustaa valittua kohderyhmää. Taustakysymysten vastauksia analysoitiin laskemalla eri havaintojen frekvenssit. Frekvenssit ovat yksinkertainen tapa kuvailla aineistoa ja havaita eri suuruisten havaintojen lukumääriä (Nummenmaa, 2009, s. 60).

Kyselylomakkeella suurin osa kysymyksistä oli asetettu pakollisiksi. Ainoastaan avoimet kysymykset ja monivalintakysymys ”7. Työ- tai opiskelupaikallani on käytössä tietoturvaan liittyvä ohjeistus” oli jätetty vapaaehtoiseksi siltä varalta, että vastaaja ei opiskele tai käy töissä. Kuitenkin vain yksi vastaaja oli jättänyt vastaamatta tähän kysymykseen. Metsämuuronen (2005, s. 469) esittelee puuttuvien arvojen korvaamiseen vaihtoehdoiksi keskiarvon ja verrokkiarvon. Keskiarvolla korvaamisen ei katsottu sopivan tilanteeseen, koska kyseessä on nominaali- eli luokitteluasteikollinen muuttuja. Verrokkiarvo valitaan toiselta vastaajalta, joka on vastannut muihin kysymyksiin mahdollisimman samalla tavalla (Metsämuuronen, 2005, s. 469). Verrokkiarvon käyttämisen sijaan oletettiin, että vastaaja on jättänyt vastaamatta siksi, ettei opiskele tai käy töissä. Näin ollen puuttuva arvo korvattiin arvolla 2 (ei).

Luottamusta mittaava muuttuja L2 (”Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.”) ja käytöstä mittaava muuttuja K4 (”Käytän palveluita, vaikka niihin olisi aiemmin kohdistunut tietomurto.”) käännettiin päinvastaisiksi, jotta niiden skaalat vastaisivat muita luottamusta ja käytöstä mittaavia muuttujia. Kääntämisen jälkeen luottamusta mittaavien muuttujien suuri arvo kertoo voimakkaasta luottamuksesta. Käytöstä mittaavien muuttujien suuri arvo viittaa varovaiseen käytökseen ja vähäiseen halukkuuteen luovuttaa omia tietoja internetissä.

Muuttujien välisiä riippuvuuksia analysoitiin aluksi kahdella eri menetelmällä riippuen muuttujien tyypistä. Osa käytetyistä muuttujista on

luokitteluasteikollisia, eli eri arvot voidaan erottaa toisistaan vain laadullisesti, eikä niillä ole keskinäistä järjestystä (Karjalainen, 2010, s. 20). Näille muuttujille tehtiin Metsämuurosen (2005, s. 991) suosittelema ristiintaulukointi, jonka yhteydessä laskettiin Khiin neliö -testi ja kontingenssikerroin. Khiin neliö -testi testaa muuttujien keskinäistä riippuvuutta. Testin oletuksena on, ettei yksikään ristiintaulukon solun frekvenssi ole 0 ja korkeintaan 20 % niistä on alle 5. (Metsämuuronen, 2005, s. 992-993.) Järjestysasteikollisille muuttujille laskettiin Spearmanin järjestyskorrelaatiokerroin, jota sekä Metsämuuronen (2005, s. 1091) että Karjalainen (2010, s.122) ehdottavat järjestysasteikollisten muuttujien riippuvuuden mittariksi. Tulosten merkitsevyyttä arvioitiin p-arvon avulla.

Käytöstä selittäviä tekijöitä etsittiin monimuuttujamenetelmiin kuuluvan regressioanalyysin avulla. Monimuuttujamenetelmillä on paljon taustaoletuksia ja -vaatimuksia aineistolle, joten niiden sopivuus aineiston analyysiin on arvioitava huolella. Monimuuttujamenetelmiä käytettäessä muuttujien tulisi olla vähintään välimatka-asteikollisia. (Metsämuuronen, 2005, s. 866.) Tässä tutkimuksessa aineiston muuttujat eivät täytä tätä vaatimusta. Metsämuuronen kuitenkin huomauttaa (2005, s. 62), että Likert-asteikolla mitatuille muuttujille voi käyttää välimatka-asteikollisille muuttujille tarkoitettuja analyysimenetelmiä, sillä Likert-asteikollista muuttujaa voidaan pitää ”hyvänä järjestysasteikollisena”. Laatueroasteikolliset muuttujat saatiin mukaan regressioanalyysiin, kun niille suoritettiin dummy-koodaus Nummenmaan (2009, s. 325-326) ohjeen mukaan.

Lopuksi kyselyn avoimet vastaukset käsiteltiin lukemalla ne läpi ja etsimällä niistä yhtäläisyyksiä ja toistuvia teemoja. Vastaukset luokiteltiin näiden teemojen mukaan ja vastauksista laskettiin frekvenssit jokaiselle luokalle.

5 TUTKIMUKSEN TULOKSET

Tässä luvussa esitellään tutkimuksen tulokset. Ensin käydään läpi vastaajien demografisia tietoja ja taustatietoja internetin käytöstä sekä mahdollisesta tietomurtojen uhriksi joutumisesta. Seuraavaksi esitellään tietomurtojen herättämät tunteet ja tulokset tiedon vaikutuksesta luottamukseen, käytökseen ja käsitykseen yrityksen vastuusta. Lopuksi käytöstä ja luottamusta selittämään luodaan regressiomallit, joilla pyrittiin löytämään kutakin muuttujaa parhaiten selittäviä tekijöitä.

5.1 Vastaajien taustatiedot

Kyselyyn tuli yhteensä 262 vastausta, jotka kaikki hyväksyttiin mukaan analyysivaiheeseen. Kyselyyn vastanneiden demografiset tiedot on esitetty tiivistettynä taulukossa 3. Vastaajista 55,3 % oli naisia ja 43,9 % miehiä. ”Muu / En halua kertoa” -vaihtoehdon valitsi kaksi vastaajaa. Sekä naisten että miesten osuutta vastaajista voidaan pitää riittävänä, sillä molempia oli vastaajissa yli 100 kappaletta eivätkä vastaajat painottuneet huomattavasti yhteen sukupuoleen.

Ikäjakauman osalta vastaajat eivät jakautuneet normaalijakauman mukaan, vaan suurin osa vastaajista (63 %) ilmoitti olevansa 18-30-vuotias. Toisiksi suurin ikäryhmä oli 31-40-vuotiaat (24 %). Yli 60-vuotiaiden osuus vastaajista jäi odotetusti pienimmäksi (1,5 %). Vastaajien ikäjakaumaa voidaan selittää kyselyn levittämisellä sosiaalisessa mediassa ja nuorten aikuisten harrastusyhteisöjen keskusteluryhmissä. Yli 40-vuotiaiden vastaajien vähäisen määrän vuoksi eri ikäryhmien välisiä tuloksia ei voida luotettavasti vertailla, joten iän vaikutus vastaajien tunteisiin ja mielipiteisiin jätetään analyysin ulkopuolelle.

Koulutustasoltaan suurin osa vastaajista (45,8 %) on suorittanut toisen asteen tutkinnon (ammattikoulu tai lukio). Koulutustason jakaumaa voi selittää ainakin osittain vastaajien ikäjakaumalla. 18-30-vuotiaat vastaajat voivat mahdollisesti olla vielä opiskelemassa korkeakoulututkintoa. Vastausvaihtoehdoissa korkeakoulututkinnot oli jaettu alempaan ja ylempään korkeakoulututkintoon.

Yhteensä alemman (32,1 %) tai ylemmän (17,9 %) korkeakoulututkinnon suorittaneita oli 50 % vastaajista. Voidaan siis todeta, että sekä toisen asteen tutkinnon suorittaneet että korkeakoulutetut ovat tasaisesti edustettuna vastaajissa.

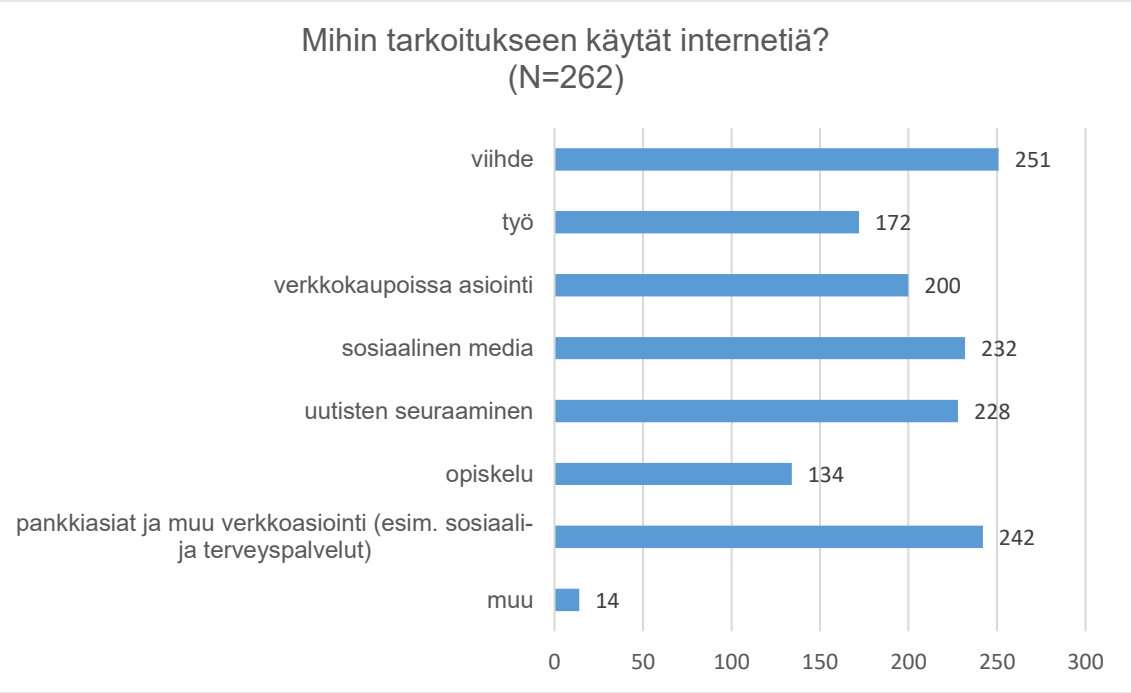
Vastaajilta kysyttiin taustatietona myös keskimääräistä internetin käytön määrää. 45,8 % vastaajista ilmoitti käyttävänsä internetiä keskimäärin 4-8 tuntia päivässä. Alle tunnin päivässä internetiä käyttävien osuus oli vain kolme vastaajaa (1,1 %). 30,2 % vastaajista ilmoitti käyttävänsä internetiä yli 8 tuntia päivässä.

TAULUKKO 3 Vastaajien demografiset tiedot

Vastaajien demografiset tiedot		**f**	**f %**
Sukupuoli (N=262)	Nainen	145	55,3 %
	Mies	115	43,9 %
	Muu / En halua kertoa	2	0,8 %
Ikä (N=262)	18-30 v	165	63,0 %
	31-40 v	63	24,0 %
	41-50 v	18	6,9 %
	51-60 v	12	4,6 %
	yli 60 v	4	1,5 %
Koulutustaso (N=262)	Peruskoulu	11	4,2 %
	Ammattikoulu / lukio	120	45,8 %
	Alempi korkeakoulututkinto	84	32,1 %
	Ylempi korkeakoulututkinto	47	17,9 %
Internetin käytön määrä keskimäärin (N=262)	alle 1 h/päivä	3	1,1 %
	1-4 h/päivä	60	22,9 %
	4-8 h/päivä	120	45,8 %
	yli 8 h/päivä	79	30,2 %

Internetin käytön määrän lisäksi vastaajia pyydettiin valitsemaan eri vaihtoehdoista, mihin tarkoitukseen he yleensä käyttävät internetiä. Kuviossa 3 esitetään kaikki annetut vastausvaihtoehdot ja kunkin vaihtoehdon kohdalla sen valinneiden vastaajien määrä. Eniten valittuja vaihtoehtoja olivat viihde, pankkiasiat ja muu verkkoasiointi sekä sosiaalinen media.

Muu-vaihtoehdon kohdalla lomakkeella oli avoin vastaustila, johon vastaajat pystyivät tarkentamaan vastaustaan. Avoimia vastauksia tähän kohtaan tuli 13 kappaletta. Näistä 5 oli sellaisia, jotka voidaan lukea kuuluvaksi viihteeseen (4 vastaajaa mainitsi erikseen pelaamisen, 1 vastaaja pornon kuluttamisen). Kolmessa vastauksessa mainittiin internetin käyttö viestintään. Muita mainittuja käyttötarkoituksia olivat karttapalvelut, dokumentointi, tiedonhaku, sijoittaminen ja harrastukseen liittyvien tekniikoiden opettelu.



KUVIO 3 Vastaajien syyt käyttää internetiä

Vastaajilta kysyttiin taustatietona, ovatko he joutuneet tietomurron uhriksi, koska tutkimuksessa haluttiin vertailla tietomurron uhrien ja muiden internetin käyttäjien kokemuksia keskenään. Taulukossa 4 on esitetty frekvenssit vastaajien kokemuksista tietomurron uhriksi joutumisesta. Suurin osa vastaajista (67,2 %) ilmoitti, ettei ole koskaan joutunut tietomurron uhriksi internetissä. Tietomurron uhriksi oli joutunut 43 vastaajaa (16,4 %). Saman verran vastaajia (16,4 %) ei osannut varmasti sanoa, ovatko he joutuneet tietomurron uhriksi.

TAULUKKO 4 Vastaajien kokemukset tietomurron uhriksi joutumisesta

		f	f %
Olen joutunut tietomurron uhriksi internetissä. (N=262)	kyllä	43	16,4 %
	ei	176	67,2 %
	en ole varma	43	16,4 %

5.2 Tietoturvauhkien herättämät tunteet

Tunteita mitattiin 10 väittämän avulla. Väittämät liittyvät CFIP-mallin neljään eri tietoturvahuolien ulottuvuuteen. Tietojen keräämiseen (TK) liittyviä väittämiä oli yhteensä kolme, ja niiden vastaajissa herättämät tunteet on esitetty taulukossa 5. Ärsyyntyminen, ahdistus ja stressi olivat tietojen keräämiseen liittyvistä tunteista yleisimpiä. Ensimmäisen väittämän TK1 kohdalla vaihtoehto ”ei mitään näistä” oli eniten valittu (n=119). Myös väittämissä TK2 ja TK3 tämä vaihtoehto oli yksi valituimmista (n=76 ja n=53).

TAULUKKO 5 Tietojen keräämisen (TK) herättämät tunteet

	suru	ahdistus	viha	stressi	häpeä	ärsyyntyminen	pelko	ei mitään näistä
TK1 (N=262)	1	31	8	20	1	115	18	119
TK2 (N=262)	1	56	10	35	1	133	38	76
TK3 (N=262)	5	57	2	37	2	154	31	53

TK1. Yritys pyytää minulta henkilötietojani.
TK2. Joudun luovuttamaan henkilötietojani usealle yritykselle.
TK3. Yritykset keräävät paljon henkilökohtaisia tietoja kuluttajista.

Tiedoissa esiintyvien virheiden (VT) herättämiä tunteita mitattiin yhdellä väittämällä VT. Virheisiin tiedoissa liittyvien tunteiden frekvenssit on esitetty taulukossa 6. Yli puolet vastaajista (n=150) ilmoitti virheiden herättävän ärsyyntymistä. Toisiksi valituin tunne oli viha (n=27). Myös tässä väittämässä ”ei mitään näistä” -vaihtoehdon valitsi merkittävä osa vastaajista (n=73).

TAULUKKO 6 Tiedoissa esiintyvien virheiden (VT) herättämät tunteet

	suru	ahdistus	viha	stressi	häpeä	ärsyyntyminen	pelko	ei mitään näistä
VT (N=262)	2	23	27	21	4	150	14	73

VT. Yrityksen säilyttämissä henkilötiedoissa on virheitä.

Tietojen luvattoman käytön (LK) herättämiä tunteita mitattiin neljällä väittämällä ja näihin väittämiin annetut vastaukset on koottu taulukkoon 7. Ärsyyntyminen, viha ja ahdistus olivat eniten valittuja tunnereaktioita tietojen luvattomaan käyttöön liittyen. Luvattoman käytön ulottuvuuden väittämissä ”ei mitään näistä” -vaihtoehtoa valittiin huomattavasti vähemmän kuin tietojen keräämisen ja virheiden ulottuvuuksien väittämissä.

TAULUKKO 7 Tietojen luvattoman käytön (LK) herättämät tunteet

	suru	ahdistus	viha	stressi	häpeä	ärsyyntyminen	pelko	ei mitään näistä
LK1 (N=262)	6	64	165	48	3	189	53	7
LK2 (N=262)	6	48	129	33	1	184	40	17
LK3 (N=262)	15	52	155	36	10	184	44	11
LK4 (N=262)	2	53	48	35	3	180	33	32

LK1. Yritys käyttää tietojani johonkin muuhun tarkoitukseen kuin mihin olen ne alun perin luovuttanut.
LK2. Yritys luovuttaa kuluttajista keräämiään tietoja muille yrityksille.
LK3. Yritys myy kuluttajista keräämiään tietoja muille yrityksille.
LK4. Yritys ilmaisee epäselvästi, mihin tarkoitukseen henkilötietoja kerätään.

Luvattoman pääsyn (LP) herättämiä tunteita mitattiin kahdella väittämällä. Vaihtoehtojen frekvenssit on esitetty taulukossa 8. Luvaton pääsy tietoihin herätti vastaajissa eniten ahdistuksen, ärsyyntymisen, stressin ja pelon tunteita. Tässä ulottuvuudessa väittämät herättivät monipuolisimmin eri tunteita. Surun ja häpeän tunteita heräsi selkeästi vähiten kaikkiin tietoturvahuolien ulottuvuuksiin liittyen, mutta luvattoman pääsyn ulottuvuuden väittämissä

vastaajat valitsivat myös näitä tunteita. Varsinkin väittämä LP2 herätti vastaajissa myös surua (n=54) ja häpeää (n=74).

TAULUKKO 8 Luvattoman pääsyn tietoihin (LP) herättämät tunteet

	suru	ahdistus	viha	stressi	häpeä	ärsyyntyminen	pelko	ei mitään näistä
LP1 (N=262)	18	140	58	112	19	129	114	14
LP2 (N=262)	54	162	134	136	74	159	132	10

LP1. Käyttämäni palvelu joutuu tietomurron kohteeksi.
LP2. Henkilökohtaiset tietoni päätyvät tietovuodon seurauksena kaikkien nähtäville.

Kokonaisuutena tietoturvariskit herättivät vastaajissa eniten ärsyyntymistä, vihaa ja ahdistusta. Eri ulottuvuuksien välillä on kuitenkin havaittavissa eroja siinä, mitä tunteita vastaajat valitsivat ja kuinka monipuolisesti ja voimakkaasti eri tunnereaktiot näkyivät vastauksissa. Tietojen luvaton käyttö ja luvaton pääsy tietoihin herättivät enemmän tunteita kuin tietojen kerääminen ja mahdolliset virheet tiedoissa. Ärsyyntyminen oli yleisin tunne ulottuvuuksiin tietojen kerääminen, virheet tiedoissa ja luvaton käyttö liittyen, mutta luvattoman pääsyn ulottuvuuden väittämät herättivät vastaajissa eniten ahdistusta. Luvattoman käytön ulottuvuuden väittämissä vihan tunne nousi voimakkaammin esiin kuin muissa tietoturvahuolien ulottuvuuksissa.

Vastaajat jaettiin ryhmiin sen mukaan, ovatko he koskaan joutuneet tietomurron uhriksi. Tunteiden frekvenssit eri ryhmillä on esitetty ulottuvuuksittain liitteissä 4-7. Eroavaisuuksia ryhmien välillä selvitettiin tekemällä niille ristiintaulukointi ja Khiin neliö -testi. Tulosten tilastollista merkitsevyyttä testattiin p-arvon avulla.

Tilastollisesti merkittäviä eroavaisuuksia näiden ryhmien välillä näkyi tietojen keräämisen ja luvattoman käytön ulottuvuuksissa. Tietojen keräämiseen liittyvistä väittämistä TK1 herätti enemmän ahdistusta tietomurron uhreissa kuin muissa ryhmissä (χ^2 (2) = 9,561; p = 0,008). Väittämän TK2 kohdalla tietomurron uhrit ilmaisivat muita enemmän ärsyyntymistä (χ^2 (2) = 11,675; p = 0,003). Muilla ryhmillä havaittiin tässä väittämässä merkitsevä riippuvuus ”ei mitään näistä” -vaihtoehtoon (χ^2 (2) = 6,954; p = 0,031). Väittämän TK3 kohdalla tietomurron uhriksi joutuneet kokivat enemmän pelon (χ^2 (2) = 13,573; p = 0,001) ja vihan (χ^2 (2) = 11,862; p = 0,003) tunteita kuin muut ryhmät.

Luvattoman käytön ulottuvuuden väittämässä LK2 tietomurron uhrit ilmaisivat muita ryhmiä enemmän pelkoa (χ^2 (2) = 9,015; p = 0,011). Myös väittämässä LK3 havaittiin merkitsevä riippuvuus näiden ryhmien välillä (χ^2 (2) = 15,395; p < 0,001). Väittämässä LK4 tietomurron uhriksi joutuneet kokivat muita enemmän ahdistuksen (χ^2 (2) = 6,849; p = 0,033) ja vihan (χ^2 (2) = 8,173; p = 0,017) tunteita.

5.3 Tietoturvariskien vaikutus luottamukseen ja käytökseen

Tietoa mittaavista luokitteluasteikollisista muuttujista T1, T2 ja T3 tehtiin ristiintaulukoinnit luottamusta, vastuuta ja käytöstä mittaavien muuttujien kanssa. Ristiintaulukoinnin yhteydessä laskettiin Khiin neliö -testi ja kontingenssikerroin C. Tulosten merkitsevyyttä arvioitiin p-arvon avulla. Tietoa mittaavien järjestysasteikollisten muuttujien T4 ja T5 yhteyttä luottamukseen, vastuuseen ja käytökseen tutkittiin Spearmanin järjestyskorrelaatiokertoimen ρ avulla. Tietomurron uhriksi joutumisen vaikutusta luottamukseen (muuttujat L1 ja L2) tai käsitykseen yrityksen vastuusta (muuttujat V1 ja V2) ei voitu luotettavasti tarkastella ristiintaulukoinnin avulla, sillä taulukoihin syntyi suuri määrä soluja, joiden frekvenssit jäivät alle viiden. Näin ollen tietomurron uhriksi joutumisen vaikutus jätettiin tulosten ulkopuolelle.

5.3.1 Tiedon vaikutus luottamukseen ja käsitykseen yrityksen vastuusta

Muuttujien T1, T2 ja T3 vaikutuksesta luottamukseen ja käsitykseen yrityksen vastuusta saadut ristiintaulukoinnin tulokset on esitelty taulukossa 9. Taulukkoon on merkitty ne muuttujat, joilla taulukon solun frekvenssi on alle 5 yli 20 prosentilla soluista. Näiden muuttujien osalta tuloksia ei pidetä luotettavina, ja luvuista ei voida tehdä päätelmiä muuttujien välisestä yhteydestä.

Internetin käyttäjän oma perehtyminen ja kiinnostus tietoturva-asioita kohtaan (T3) on tilastollisesti merkittävästi ($p < 0{,}001$) yhteydessä siihen, kuinka tarkasti käyttäjä harkitsee ennen tietojensa luovuttamista (L2). Näiden muuttujien välinen yhteys on kuitenkin melko heikko ($C = 0{,}261$). Muiden muuttujien välillä ei havaittu tilastollisesti merkittäviä yhteyksiä.

TAULUKKO 9 Muuttujien T1, T2 ja T3 vaikutus luottamukseen ja käsitykseen yrityksen vastuusta

	khiin neliö χ^2	**df**	**kontingenssikerroin C**	**p-arvo**
T1*L1**	4,147	8	0,125	0,844
T2*L1	1,538	4	0,076	0,820
T3*L1	9,213	4	0,184	0,056
T1*L2**	8,758	8	0,180	0,363
T2*L2	0,329	4	0,035	0,988
T3*L2	19,125	4	0,261	< 0,001
T1*V1	2,379	8	0,095	0,967
T2*V1	3,569	4	0,116	0,467
T3*V1	9,020	4	0,182	0,061
T1*V2**	13,216	8	0,219	0,105
T2*V2**	9,895	4	0,191	0,042
T3*V2**	8,356	4	0,176	0,079

** Yli 20 % soluista frekvenssi alle 5.
T1. Työ- tai opiskelupaikallani on käytössä tietoturvaan liittyvä ohjeistus.
T2. Olen käynyt tietoturvaan liittyvän kurssin tai koulutuksen töideni tai opintojeni kautta.
T3. Olen perehtynyt tietoturva-asioihin harrastuksen tai oman mielenkiinnon vuoksi.
L1. Uskon henkilötietojeni olevan turvassa.
L2. Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.
V1.Tietomurron kohteeksi joutuminen kertoo yrityksen liian vähäisistä turvatoimista.
V2.Yritys on vastuussa säilyttämistään henkilötiedoista ja sitä tulisi rangaista tietovuodon sattuessa.

Tietoa mittaavien muuttujien T4 ja T5 osalta vaikutusta luottamukseen ja käsitykseen yrityksen vastuusta testattiin laskemalla Spearmanin järjestyskorrelaatiokerroin ρ. Saadut tulokset on koottu taulukkoon 10. Tietomurtoihin liittyvän uutisoinnin seuraaminen (T4) korreloi positiivisesti (ρ = 0,391) internetin käyttäjän pyrkimykseen huolehtia laitteidensa tietoturvasta (T5). Tietojen luovuttamiseen liittyvän harkinnan (L2) ja tietomurtouutisoinnin seuraamisen välillä havaittiin tilastollisesti merkittävä negatiivinen korrelaatio (ρ = -0,236). Muuttuja L2 käännettiin päinvastaiseksi aineiston käsittelyn alussa, joten negatiivinen korrelaatio kertoo tietomurtouutisten aktiivisen seuraamisen lisäävän harkintaa tietojen luovuttamisessa. Tietomurtoihin liittyvän uutisoinnin seuraaminen ja yrityksen ansaitsema rangaistus tietomurron tapahtuessa (V2) korreloivat myös positiivisesti (ρ = 0,153).

Käyttäjän pyrkimys huolehtia laitteidensa tietoturvasta (T5) korreloi negatiivisesti (ρ = -0,321) tietojen luovuttamisen harkinnan (L2) kanssa. Laitteidensa tietoturvasta tarkemmin huolehtivat ovat siis myös harkitsevampia tietojen luovuttamisessa internetissä. Myös toinen luottamusta mittaava muuttuja L1 (ρ = 0,137) ja yrityksen vastuuta mittaava V2 (ρ = 0,139) korreloivat tilastollisesti merkitsevästi käyttäjän pyrkimykseen huolehtia tietoturvasta henkilökohtaisilla laitteillaan.

TAULUKKO 10 Muuttujien T4 ja T5 vaikutus luottamukseen ja käsitykseen yrityksen vastuusta

		T4	T5	L1	L2	V1	V2
T4	ρ	1,000	,391**	-,038	-,236**	,063	,153*
	p-arvo	.	<,001	,540	<,001	,309	,013
T5	ρ	,391**	1,000	,137*	-,321**	,100	,139*
	p-arvo	<,001	.	,026	<,001	,106	,024
L1	ρ	-,038	,137*	1,000	-,162**	,057	-,031
	p-arvo	,540	,026	.	,008	,360	,612
L2	ρ	-,236**	-,321**	-,162**	1,000	-,203**	-,235**
	p-arvo	<,001	<,001	,008	.	<,001	<,001
V1	ρ	,063	,100	,057	-,203**	1,000	,499**
	p-arvo	,309	,106	,360	<,001	.	<,001
V2	ρ	,153*	,139*	-,031	-,235**	,499**	1,000
	p-arvo	,013	,024	,612	<,001	<,001	.

** Merkittävä korrelaatio (p < 0,01)
* Merkittävä korrelaatio (p < 0,05)
T4. Seuraan tietomurtoihin liittyvää uutisointia.
T5. Pyrin toiminnallani ylläpitämään henkilökohtaisten laitteideni (esim. älypuhelin, tietokone) tietoturvaa esimerkiksi käyttämällä tietoturvallisia salasanoja, ja huolehtimalla, että laitteen virustorjuntaohjelma on päivitetty.
L1. Uskon henkilötietojeni olevan turvassa.
L2. Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.
V1.Tietomurron kohteeksi joutuminen kertoo yrityksen liian vähäisistä turvatoimista.
V2.Yritys on vastuussa säilyttämistään henkilötiedoista ja sitä tulisi rangaista tietovuodon sattuessa.

5.3.2 Tiedon vaikutus käytökseen

Muuttujille T1, T2 ja T3 tehtiin ristiintaulukointi käytöstä mittaavien muuttujien K1, K2, K3 ja K4 kanssa. Muuttujille T4 ja T5 tehtiin ristiintaulukointi vain

muuttujan K1 kanssa, koska K1 on luokitteluasteikollinen muuttuja. Saadut tulokset on esitetty taulukossa 11.

Vastaajien harrastuneisuudella ja mielenkiinnolla tietoturva-asioita kohtaan (T3) havaittiin yhteys siihen, kuinka paljon heidän käsityksensä palvelun tietoturvasta vaikuttaa valintaan käyttää palvelua (K3) ja kuinka paljon he kiinnittävät huomiota palvelujen tietosuojakäytäntöihin (K2). Tietoturvaan liittyvän koulutuksen tai kurssin käymisellä (T2) oli heikko (C=0,198) yhteys tietosuojakäytäntöjen huomioimiseen internetissä. Työ- tai opiskelupaikalla olevalla tietoturvaohjeistuksella (T1, C = 0,170), tietomurtoihin liittyvän uutisoinnin seuraamisella (T4, C = 0,255) ja pyrkimyksellä huolehtia omien laitteiden tietoturvasta (T5, C = 0,246) havaittiin myös heikot yhteydet maksullisen virusturvaohjelman käyttöön.

TAULUKKO 11 Ristiintaulukoimalla saadut tulokset tiedon vaikutuksesta käytökseen

	khiin neliö χ^2	**df**	**kontingenssikerroin C**	**p-arvo**
T1*K1	7,781	2	0,170	0,020
T2*K1	0,422	1	0,516	0,516
T3*K1	0,317	1	0,035	0,573
T1*K2**	37,865	8	0,355	< 0,001
T2*K2	10,679	4	0,198	0,030
T3*K2	44,556	4	0,381	< 0,001
T1*K3	14,554	8	0,229	0,068
T2*K3	3,994	4	0,123	0,407
T3*K3	46,897	4	0,390	<0,001
T1*K4**	8,293	8	0,175	0,405
T2*K4	4,749	4	0,133	0,314
T3*K4	5,141	4	0,139	0,273
T4*K1	18,207	4	0,255	0,001
T5*K1	16,807	4	0,246	0,002

** Yli 20 % soluista frekvenssi alle 5.
T1. Työ- tai opiskelupaikallani on käytössä tietoturvaan liittyvä ohjeistus.
T2. Olen käynyt tietoturvaan liittyvän kurssin tai koulutuksen töideni tai opintojeni kautta.
T3. Olen perehtynyt tietoturva-asioihin harrastuksen tai oman mielenkiinnon vuoksi.
T4. Seuraan tietomurtoihin liittyvää uutisointia.
T5. Pyrin toiminnallani ylläpitämään henkilökohtaisten laitteideni (esim. älypuhelin, tietokone) tietoturvaa esimerkiksi käyttämällä tietoturvallisia salasanoja, ja huolehtimalla, että laitteen virustorjuntaohjelma on päivitetty.
K1.Minulla on käytössäni maksullinen virustorjuntaohjelma.
K2. Kiinnitän huomiota internetissä käyttämieni palvelujen tietosuojakäytäntöihin.
K3. Käsitykseni palvelun tietoturvasta vaikuttaa valintaani käyttää palvelua.
K4. Käytän palveluita, vaikka niihin olisi aiemmin kohdistunut tietomurto.

Likert-asteikolla mitattujen muuttujien yhteyttä mitattiin Spearmanin järjestyskorrelaatiokertoimen ρ avulla. Tulokset esitetään taulukossa 12. Tietoa mittaavat muuttujat T4 ja T5 korreloivat keskenään (ρ = 0.391) ja muuttujien K2 ja K3 kanssa. Tietomurtoihin liittyvän uutisoinnin seuraamisella (T4) havaittiin yhteys siihen, kuinka paljon käyttäjät huomioivat palvelujen tietosuojakäytäntöjä (K2, ρ = 0.401) ja kuinka paljon heidän käsityksensä palvelun tietoturvasta vaikuttaa päätökseen käyttää palvelua (K3, ρ = 0.373). Pyrkimyksellä huolehtia omien laitteiden tietoturvasta oli hieman voimakkaampi korrelaatio muuttujien K2 ja K3 kanssa (ρ = 0.507 ja ρ = 0.474). Palveluiden tietosuojakäytäntöjen huomioimisella (K2) ja palvelun tietoturvan tason vaikutuksella palvelun käyttämispäätökseen (K3) havaittiin myös tilastollisesti merkittävä korrelaatio (ρ = 0.679).

TAULUKKO 12 Spearmanin järjestyskorrelaatiokertoimella saadut tulokset tiedon vaikutuksesta käytökseen

		T4	T5	K2	K3	K4
T4	ρ	1,000	,391**	,401**	,373**	-,108
	p-arvo	.	<,001	<,001	<,001	,081
T5	ρ	,391**	1,000	,507**	,474**	-,030
	p-arvo	<,001	.	<,001	<,001	,634
K2	ρ	,401**	,507**	1,000	,679**	-,026
	p-arvo	<,001	<,001	.	<,001	,680
K3	ρ	,373**	,474**	,679**	1,000	,037
	p-arvo	<,001	<,001	<,001	.	,551
K4	ρ	-,108	-,030	-,026	,037	1,000
	p-arvo	,081	,634	,680	,551	.

** Merkittävä korrelaatio (p < 0,01)
T4. Seuraan tietomurtoihin liittyvää uutisointia.
T5. Pyrin toiminnallani ylläpitämään henkilökohtaisten laitteideni (esim. älypuhelin, tietokone) tietoturvaa esimerkiksi käyttämällä tietoturvallisia salasanoja, ja huolehtimalla, että laitteen virustorjuntaohjelma on päivitetty.
K2. Kiinnitän huomiota internetissä käyttämieni palvelujen tietosuojakäytäntöihin.
K3. Käsitykseni palvelun tietoturvasta vaikuttaa valintaani käyttää palvelua.
K4. Käytän palveluita, vaikka niihin olisi aiemmin kohdistunut tietomurto.

5.3.3 Regressioanalyysi

Regressioanalyysissä yhtä muuttujaa selitetään useammalla selittävällä muuttujalla (Metsämuuronen, 2005, s. 660). Tässä tutkimuksessa regressioanalyysillä haluttiin selvittää ne tekijät, jotka selittävät parhaiten internetin käyttäjien luottamusta ja käytöstä. Tietoa mittaavien muuttujien T1, T2, T3, T4 ja T5 lisäksi mukaan analyysiin otettiin muuttuja TM, joka kertoo, onko vastaaja joutunut tietomurron uhriksi. Kuten aiemmin on todettu, osa muuttujista on luokitteluasteikollisia. Regressioanalyysi on tarkoitettu vähintään välimatka-asteikollisille muuttujille (Nummenmaa, 2015, s. 329), joten luokitteluasteikollisille muuttujille tehtiin dummy-koodaus. Tästä syntyvä dummy-muuttuja saa arvokseen joko 1 tai 0, ja sillä voidaan erottaa kaksi havaintoryhmää toisistaan regressiomallissa (Karjalainen, 2010, s. 139).

Metsämuurosen (2005, s. 662) mukaan liian suuri korrelaatio selittävien muuttujien välillä voi aiheuttaa multikollineaarisuutta, jossa turhia muuttujia päätyy mukaan malliin, koska ne korreloivat voimakkaasti jonkin selittävän muuttujan kanssa. Multikollineriaarisuuden välttämiseksi regressioanalyysi tehtiin askeltavalla menettelyllä (Stepwise order). Askeltavassa menettelyssä jokaista muuttujaa testataan erikseen poistamalla se mallista ja seuraamalla poiston vaikutusta mallin selitysasteeseen (Metsämuuronen, 2005, s.667).

Jokaiselle selitettävälle muuttujalle luotiin malli, jolla selitysaste on mahdollisimman korkea. Mallin selitysasteella tarkoitetaan multippelikorrelaation neliötä, joka kertoo kuinka suuren osan selitettävän muuttujan vaihtelusta malli selittää. Tässä tutkimuksessa selitysastetta arvioitiin korjatulla selitysasteella R^2, sillä se ottaa huomioon myös muuttujien lukumäärän ja antaa todenmukaisemman kuvan mallin sopimisesta populaatioon. (Nummenmaa, 2015, s. 321.)

Regressioanalyysin tuloksista voidaan havaita, että monen selitettävän muuttujan kohdalla mallin selitysaste R^2 jää alhaiseksi. Suurimmat selitysasteet

ovat muuttujilla K2 (R^2 = 0,330) ja K3 (R^2 = 0,286). β-kerrointen arvoja testattiin t-arvon avulla. Metsämuurosen (2005, s. 666) mukaan t-arvon tulisi olla korkeampi kuin 2 ja siihen liittyvän p-arvon pienempi kuin 0,05, jotta β-kerrointa voidaan pitää luotettavana. Muuttujia K2 ja K3 selittävät mallit täyttivät myös nämä vaatimukset.

Internetissä käytettävien palvelujen tietosuojakäytäntöjen huomioimiseen (K2) vaikuttavia tekijöitä ovat T5, T4, T3_k, T1_k ja T1_e. Huomionarvoista on, että sekä työ- tai opiskelupaikalla oleva tietoturvaohjeistus että sen puuttuminen päätyivät molemmat malliin mukaan. Kysymyksessä T1 annettiin myös kolmas vastausvaihtoehto ”en ole varma”. Tulosta voi mahdollisesti selittää se, että ne, jotka varmasti tietävät ohjeistuksen olemassaolosta tai sen puuttumisesta, ovat myös kiinnostuneempia tietoturvaan liittyvän ohjeistuksen lukemisesta, ja näin ollen lukevat tietosuojakäytännöt myös internetin palveluita käyttäessään. Voimakkaimmin vaikuttava tekijä muuttujaa K2 selittävässä mallissa on käyttäjän oma pyrkimys laitteidensa tietoturvasta huolehtimiseen (T5).

Muuttujaa K3 selittäviä tekijöitä ovat T5, T3_k ja T4, jotka nousivat esiin jo edellä mainitun K2-muuttujan selittäjinä. Tietomurtoihin liittyvien uutisten seuraaminen (T4), oma-aloitteinen tietoturva-asioihin perehtyminen (T3_k) ja pyrkimys tietoturvan ylläpitämiseen omalla toiminnalla (T5) liittyvät kaikki internetin käyttäjän omaan kiinnostukseen ja vapaaehtoiseen toimintaan. Työn tai opiskelun kautta saatu tieto ei vaikuta käytökseen yhtä voimakkaasti. Esimerkiksi töissä tai opinnoissa tietoturvaan liittyvän kurssin tai koulutuksen käyminen (T2) ei ole selittävänä tekijänä millään selitettävistä muuttujista. Regressioanalyysistä saadut tulokset on esitetty taulukossa 13.

TAULUKKO 13 Regressioanalyysin tulokset

	R^2	vaikuttavat tekijät	β	t	p-arvo
L1	0,059	TM_e	0,220	3,659	< 0,001
		T5	0,152	2,528	0,012
L2	0,112	T5	-0,275	-4,313	< 0,001
		T4	-0,126	-1,979	0,049
K1_k	0,090	T5	0,207	3,142	0,002
		T4	0,226	3,253	0,001
		T3_k	-0,145	-2,124	0,035
K2	0,330	T5	0,320	5,483	< 0,001
		T4	0,158	2,607	0,010
		T3_k	0,160	2,715	0,007
		T1_k	0,290	4,299	< 0,001
		T1_e	0,230	3,497	< 0,001
K3	0,286	T5	0,313	5,357	< 0,001
		T3_k	0,197	3,255	0,001
		T4	0,183	2,975	0,003
K4	0,086	TM_e	0,275	4,649	< 0,001
		T1_k	-0,127	-2,143	0,033

TM_k. Olen joutunut tietomurron uhriksi: kyllä
TM_e. Olen joutunut tietomurron uhriksi: ei
T1_k. Työ- tai opiskelupaikallani on käytössä tietoturvaan liittyvä ohjeistus: kyllä
T1_e. Työ- tai opiskelupaikallani on käytössä tietoturvaan liittyvä ohjeistus: ei
T3_k. Olen perehtynyt tietoturva-asioihin harrastuksen tai oman mielenkiinnon vuoksi: kyllä
T4. Seuraan tietomurtoihin liittyvää uutisointia.
T5. Pyrin toiminnallani ylläpitämään henkilökohtaisten laitteideni (esim. älypuhelin, tietokone) tietoturvaa esimerkiksi käyttämällä tietoturvallisia salasanoja, ja huolehtimalla, että laitteen virustorjuntaohjelma on päivitetty.

L1. Uskon henkilötietojeni olevan turvassa.
L2. Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.
K1_k. Minulla on käytössäni maksullinen virustorjuntaohjelma: kyllä
K2. Kiinnitän huomiota internetissä käyttämieni palvelujen tietosuojakäytäntöihin.
K3. Käsitykseni palvelun tietoturvasta vaikuttaa valintaani käyttää palvelua.
K4. Käytän palveluita, vaikka niihin olisi aiemmin kohdistunut tietomurto.

5.3.4 Avoimet vastaukset

Monivalintakysymysten lisäksi vastaajia pyydettiin omin sanoin kertomaan, mikäli he ovat tietomurrosta huolimatta jatkaneet jonkin palvelun käyttöä, ja mitä syitä heillä on ollut käytön jatkamiselle. Kysymys ei ollut pakollinen ja siihen vastasi 61 henkilöä. Osa vastaajista vastasi vain joko mainitsemalla jonkin käyttämänsä palvelun ilman perusteluita tai pelkät perustelut tietomurron kohteeksi joutuneen palvelun käytön jatkamiselle. Vastausten joukossa oli myös muita aiheeseen ja kyselyyn liittyviä kommentteja. Vastaajien mainitsemia palveluita ryhmiteltiin eri tyyppeihin ja vastauksista laskettiin maininnat näille palveluille. Ryhmittelyn tulokset on koottu taulukkoon 14.

TAULUKKO 14 Vastaajien käyttämät palvelut, joihin on kohdistunut tietomurto

palvelun tyyppi	esimerkkipalveluja	mainittu vastauksissa	mainittu vastauksissa %
sosiaalinen media	LinkedIn, Facebook, Twitter	19	31,1 %
pelit ja pelaamiseen liittyvät sivustot	WoT, Playstation Network	5	8,2 %
suoratoistopalvelut	Spotify, Netflix	1	1,6 %
viestintäpalvelut	WhatsApp, Zoom	3	4,9 %
verkkopankki	Nordea	3	4,9 %
verkkokauppa	Foodora, Hotels.com	3	4,9 %
pilvitallennuspalvelu	Dropbox	3	4,9 %
muu	Työpaikan sisäiset järjestelmät, Canva, F-Secure, Garmin Connect	8	13,1 %

Sosiaalisen median palvelut mainittiin 19 vastauksessa. Tunnettuja sosiaalisen median palveluita on paljon ja niiden käyttö on yleistä, joten niihin kohdistuvat tietomurrot saavat paljon julkisuutta. Lisäksi suuresta käyttäjämäärästä ja palvelujen tietojen jakamiseen perustuvasta luonteesta johtuen ne voivat olla houkuttelevia tietomurron kohteita. Seuraavaksi eniten mainintoja saivat pelit ja niihin liittyvät sivustot. Aktiiviset pelaajat voivat olla hyvin sitoutuneita johonkin tiettyyn peliin, joten kynnys pelaamisen lopettamiselle tietomurron jälkeen voi olla suuri.

Vastaajien perustelut jatkaa tietomurron kohteeksi joutuneen palvelun käyttöä jaettiin luokkiin, jotka on esitelty taulukossa 15. Sosiaaliseen mediaan liittyviä perusteluja olivat erityisesti koettu hyöty, varovaisuus omien tietojen luovutuksessa, tietomurtojen suuri määrä, vähäiseksi koettu uhka ja sosiaalinen paine. Peleihin liittyvissä vastauksissa yleisimmät perustelut olivat koettu hyöty,

varovaisuus omien tietojen luovutuksessa, vähäiseksi koettu uhka sekä luottamus ja palveluntarjoajan suhtautuminen tietomurtoon.

TAULUKKO 15 Vastaajien perustelut palvelujen käytön jatkamiselle

perustelu	**esimerkkejä vastauksista**	**mainittu vastauksissa**	**mainittu vastauksissa %**
pakko	”Joitan pakko käyttää työn takia, esim zoom” ”Kaikki rahaliikenne on pankkien takana niin pankkipalveluita ei voi lopettaa vaikka haluaisikin”	3	4,9 %
koettu hyöty	”koska ei ole parempaa vaihtoehtoa” ”Käyttö jatkunut, jotta saisin ajankohtaisesti tietoa työmahdollisuuksista” ”palvelu on niin houkutteleva, että tietoturvariskit ei pelota tarpeeksi”	16	26,2 %
varovaisuus omien tietojen luovutuksessa	”vaihdan salasanoja säännöllisesti, vähintään kerran kuussa ja käytän kaksivaiheista tunnistautumista” ”palvelulla ei ole esimerkiksi henkilötunnusta tai kotiosoitetta” ”olen siistinyt omia tietoja, ettei mitään tärkeää vuoda”	10	16,4 %
luottamus ja palveluntarjoajan suhtautuminen tietomurtoon	”Tällaista sattuu ja palvelut parantavat suojiaan” ”Sillä on vaikutusta kuinka tietovuoto informoidaan käyttäjille” ”Murron jälkeen osattaneen korjata järjestelmät ettei murreta uudestaan ainakaan yhtä helposti.”	8	13,1 %
tietomurtojen suuri määrä	”Jos en käyttäisi mitään palveluita, joihin olisi kohdistunut tietomurto, jäisi palvelut aika vähään” ”Suureen osaan palveluista on kohdistunut tietomurto jossain vaiheessa”	6	9,8 %
palvelu on sidoksissa johonkin toiseen palveluun	”Käytän edelleen harvakseltaan näitä palveluita, koska ne voivat olla sidoksissa toiseen palveluun jota tarvitsen”	5	8,2 %
vähäiseksi koettu uhka	”henkilötietoni eivät ole kovin arkaluontoisia kyseisessä palvelussa” ”en pitänyt tapahtunutta tietomurtoa niin oleellisena, että se olisi vaikuttanut käyttöön”	12	19,7 %
sosiaalinen paine	”Facebook, ei siitä eroon pääse jos haluaa pysyä maailman menossa” ”Facebook... Siellä on melko moni ystäväni”	6	9,8 %

6 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa analysoidaan tutkimuksen tuloksia ja verrataan niitä aiempaan tutkimuskirjallisuuteen, arvioidaan tutkimuksen rajoitteita ja luotettavuutta sekä esitellään mahdollisia jatkotutkimusaiheita.

6.1 Tietomurtojen vaikutus internetin käyttäjien tunteisiin

Tämän tutkimuksen ensimmäisenä pääongelmana oli selvittää, millaisia tunteita tietomurrot ja niistä aiheutuneet tietovuodot herättävät näiden rikosten uhreissa ja yleisesti kaikissa internetiä käyttävissä ihmisissä. Tutkimus toteutettiin määrällisenä kyselytutkimuksena. Tuloksista selvisi, että tietomurrot herättävät internetin käyttäjissä eniten ärsyyntymistä, vihaa ja ahdistusta. Tietomurtojen herättämien tunteiden mittaaminen monipuolisesti ja kattavasti varmistettiin hyödyntämällä Malhotran ym. (2004) kehittämää IUIPC-mittaristoa ja Smithin ym. (1996) kehittämää CFIP-mittaristoa. Tässä tutkimuksessa kysymykset jaettiin neljään eri tietoturvahuolien ulottuvuuteen CFIP-mallin mukaan: tietojen kerääminen, virheet tiedoissa, tietojen luvaton käyttö ja luvaton pääsy tietoihin. Näistä ulottuvuuksista varsinkin tietojen luvaton käyttö ja luvaton pääsy tietoihin herättivät negatiivisia tunteita suurimassa osassa vastaajista.

Ärsyyntyminen oli eniten valittu tunnereaktio tarkasteltaessa kaikkia neljää ulottuvuutta kokonaisuutena. Ärsyyntyminen oli tutkimukseen valituista tunteista ainoa, jota ei mainittu aiemmassa tutkimuskirjallisuudessa. Kyselylomakkeen laatimisvaiheessa vihan tunne koettiin niin voimakkaaksi, että sille haluttiin tarjota myös lievempi vaihtoehto. Myös avoimista vastauksista tuli ilmi, että vastaajat eivät kokeneet tietomurtoja niin suurena uhkana, että se vaikuttaisi merkittävästi heidän internetin käyttöönsä. Tietomurtoja pidettiin jopa normaalina haittapuolena internetin käytölle. Näin ollen ärsyyntymistä voidaan pitää sopivampana tunteena kuin vihaa – omien tietojen päätyminen vääriin käsiin ärsyttää, mutta palveluista saatu hyöty koetaan silti riskin arvoiseksi.

Vihan tunteen esiintyminen vaihteli melko voimakkaasti eri tietoturvahuolien ulottuvuuksissa. Esimerkiksi luvattoman käytön ulottuvuuden väittämissä viha nousi voimakkaammin esiin kuin muissa tietoturvahuolien ulottuvuuksissa. Tulosta voi mahdollisesti selittää se, että luvaton käyttö liittyy usein yrityksen pyrkimykseen hyötyä taloudellisesti keräämistään henkilötiedoista. Kuluttajalle voi siis syntyä käsitys, että yritys saa taloudellista hyötyä tiedoista, jotka sille on luovutettu ilmaiseksi, eikä kuluttaja itse koe hyötyvänsä omien tietojensa jakamisesta. Tätä tukee myös ero tässä tutkimuksessa käytettyjen väittämien ”Yritys luovuttaa kuluttajista keräämiään tietoja muille yrityksille” ja ”Yritys myy kuluttajista keräämiään tietoja muille yrityksille” välisissä tuloksissa. Tietojen myyminen herätti vastaajissa enemmän vihaa kuin tietojen luovuttaminen muille yrityksille.

Erityisesti luvaton pääsy tietoihin herätti vastaajissa ahdistusta, mutta myös muissa ulottuvuuksissa ahdistus oli paljon valittu tunne. Luvattomalla pääsyllä on selkeä ero luvattoman käytön ulottuvuuteen: luvaton pääsy tarkoittaa käyttäjän tietojen vuotamista muiden nähtäville, kun taas luvattoman käytön ulottuvuudessa keskeisimpänä ongelmana on yrityksen päätöksenteko kuluttajien henkilötietoihin liittyen ja taloudellisen hyödyn tavoittelu niiden avulla. Luvattoman pääsyn herättämää ahdistusta voidaan siis mahdollisesti selittää sillä, että vaikutukset ovat henkilökohtaisempia ja tiedot voivat päätyä yritysten lisäksi myös muiden internetin käyttäjien nähtäville.

Huomionarvoista on, että tietojen luvaton käyttö ja luvaton pääsy tietoihin herättivät selkeästi eniten ja laajimmin eri tunteita. Tietojen kerääminen ja mahdolliset virheet tiedoissa ärsyttivät vastaajia, mutta muita tunteita näihin ulottuvuuksiin liittyen ei noussut erityisen voimakkaasti esiin. Tulosta voidaan selittää esimerkiksi sillä, että tietojen kerääminen on nykyään yleistä kaikissa internetissä käytettävissä palveluissa ja käyttäjät ovat todennäköisesti jo hyväksyneet, että heidän on luovutettava tietojaan, mikäli he haluavat käyttää palveluita. Bergströmin (2015) mukaan tietoturvahuolien määrä riippuu myös siitä, minkälaisista tiedoista on kysymys ja missä kontekstissa niitä pyydetään. Esimerkiksi sähköpostin tai hakukoneen käytön todettiin Bergströmin (2015) tutkimuksessa herättävän vähemmän tietoturvahuolia kuin pankkikortin tietojen luovuttaminen verkkopalveluille.

Myös virheiden osalta riskit voidaan kokea normaaleiksi ja vähäisiksi. Avoimista vastauksista kävi ilmi, että jotkut käyttäjät antavat myös tarkoituksella vääriä tietoja yrityksille, koska haluavat suojata omia henkilötietojaan. Virheet tiedoissa voivat siis olla myös käyttäjän puolelta toivottuja. Tulokset tämän ulottuvuuden kohdalla voisivat mahdollisesti muuttua radikaalistikin, jos vastaajia ohjattaisiin ajattelemaan virheellisiä tietoja esimerkiksi terveydenhuollon järjestelmien kontekstissa, koska pahimmillaan virhe potilastiedoissa voi uhata potilaan henkeä.

Tässä tutkimuksessa haluttiin myös selvittää, onko tietomurron uhriksi joutumisella vaikutusta käyttäjän tunteisiin. Tietomurron uhriksi joutuneet reagoivat voimakkaammin tietojen keräämiseen liittyviin väittämiin. He ilmaisivat muita enemmän ahdistusta siitä, että yritys pyytää heidän henkilötietojaan ja

enemmän ärsyyntymistä siitä, että he joutuvat luovuttamaan näitä tietoja usealle eri yritykselle. Yritysten keräämän tiedon suuri määrä herätti tietomurron uhreissa enemmän pelkoa ja vihaa kuin muissa vastaajissa. Myös luvattoman käytön ulottuvuudessa tietomurron uhriksi joutuneet ilmaisivat muita enemmän pelon tunteita useammassa eri väittämässä ja vihaa ja ahdistusta liittyen yrityksen epäselvään tapaan ilmaista kerättyjen tietojen käyttötarkoitus.

Tietomurron uhreilla pelon tunne nousi eniten esiin verrattuna muihin vastaajiin. Aiemmalla tietomurron uhriksi joutumisella on tulosten mukaan yhteys tietojen keräämisen ja luvattoman käytön herättämään pelkoon ja vihaan. Uhrit voivat mahdollisesti pelätä, että luovuttamalla tietojaan he altistuvat uudelleen tietomurron uhalle.

6.2 Tietomurtojen vaikutus internetin käyttäjien luottamukseen ja käytökseen

Toinen tämän tutkimuksen keskeisistä tutkimusongelmista oli selvittää, miten tieto tietoturvariskeistä vaikuttaa ihmisten käytökseen ja halukkuuteen luovuttaa tietojaan yrityksille tai muille organisaatioille verkossa. Keskeisimpänä havaintona tutkimuksessa selvisi, että erityisesti harrastuneisuus ja mielenkiinto tietoturva-asioita kohtaan, tietomurtoihin liittyvän uutisoinnin seuraaminen ja pyrkimys huolehtia omien laitteiden tietoturvasta vaikuttavat internetin käyttäjien luottamukseen ja käytökseen.

Internetin käyttäjän omalla mielenkiinnolla ja perehtymisellä tietoturva-asioihin havaittiin olevan yhteys harkintaan omia tietoja luovutettaessa. Omien laitteiden tietoturvan huomiointi, tietoturva-asioihin perehtyminen omaehtoisesti ja tietomurtoihin liittyvän uutisoinnin seuraaminen vaikuttavat siihen, kuinka paljon käyttäjä harkitsee ennen tietojensa luovuttamista verkossa. Tässä tutkimuksessa tiedolla viitattiin tietoon tietomurtouhkien olemassaolosta, eikä tarkempaan ymmärrykseen tietomurtojen syntymisestä tai teknisistä yksityiskohdista. Tulokset kuitenkin viittaavat siihen, että tarkemmalla ymmärryksellä ja internetin käyttäjän henkilökohtaisella kiinnostuksella tietoturva-asioita kohtaan on suurempi vaikutus luottamukseen kuin työn tai opiskelun kautta saadulla tiedolla.

Ne vastaajat, jotka ilmoittivat pitävänsä huolta omien laitteidensa tietoturvasta, olivat luottavaisempia omien tietojensa turvallisuudesta. Omalla toiminnalla siis koettiin olevan vaikutusta tietojen suojaamisessa. Tietojen suojaaminen on kuitenkin myös niitä keräävien yritysten vastuulla. Tutkimuksessa kysyttiin vastaajilta heidän käsitystään yrityksen vastuusta, mutta näiden muuttujien yhteys selittäviin muuttujiin jäi vähäiseksi. Ainostaan tietomurtoihin liittyvän uutisoinnin seuraamisella ja omien laitteiden tietoturvasta huolehtimisella oli yhteys siihen, että käyttäjä kokee yrityksen olevan vastuussa säilyttämistään henkilötiedoista ja sitä tulisi rangaista tietomurtotilanteessa. Näihin tuloksiin voi vaikuttaa tietomurtouutisoinnin tyyli mediassa. Mikäli yrityksen toiminnalla tai

huolimattomuudella on ollut tietomurron mahdollistava vaikutus, se nostetaan usein myös mediassa esiin. Kuluttaja voi myös kokea, että hän on tehnyt osansa pitäessään huolta omien laitteidensa tietoturvasta, ja syyttää yritystä siitä, ettei se ole toiminut yhtä huolellisesti.

Tiedolla havaittiin olevan vaikutusta internetin käyttäjien käytökseen. Työn tai opiskelun kautta saadulla tiedolla oli heikko yhteys varovaiseen tietoturvakäyttäytymiseen, mutta myös käytöksen suhteen suurin vaikutus oli vapaa-ajalla oma-aloitteisesti hankitulla tiedolla. Palvelujen tietosuojakäytäntöjen huomioimista ja sitä, kuinka voimakas vaikutus käyttäjän käsityksellä palvelun tietoturvasta on palvelun käyttämispäätökseen, voidaan tulosten mukaan selittää usealla tietoa mittaavalla muuttujalla. Harrastuneisuus ja mielenkiinto tietoturva-asioita kohtaan, tietomurtoihin liittyvän uutisoinnin seuraaminen ja pyrkimys huolehtia omien laitteiden tietoturvasta nousivat esiin merkittävimpinä käytökseen vaikuttavina tekijöinä.

Regressioanalyysin avulla luodut käytöstä ja luottamusta selittävät mallit jäivät suurelta osin selitysasteeltaan niin alhaisiksi, että niiden perusteella ei voitu tehdä luotettavia ja yleistettäviä päätelmiä. Ainoastaan kahdelle käytöstä mittaavalle muuttujalle saatiin mallit, joiden selitysasteita voidaan pitää kohtuullisina. Huomionarvoista regressioanalyysin tuloksissa on, että ne tukevat muilla analyysimenetelmillä saatuja tuloksia siitä, kuinka harrastuneisuuden ja oman kiinnostuksen vaikutus käytökseen on suurempi kuin työn tai opintojen kautta saatu tieto.

Aiempi tutkimus erityisesti tiedon merkityksestä tietoturvahuoliin ja varovaiseen tietoturvakäytökseen on vähäistä, joten vertailukohtia tämän tutkimuksen tuloksille on niukasti. Hwang ym. (2012) ovat tutkineet tiedon vaikutusta tietoturvahuoliin terveydenhuollon kontekstissa. He havaitsivat sähköisiin potilastietoihin liittyvän tiedon ja perehtyneisyyden lisäävän internetin käyttäjien tietoturvahuolia erityisesti luvattoman käytön ja luvattoman pääsyn ulottuvuuksissa. Vaikka tässä tutkimuksessa ei erikseen mitattu tietomurtoihin perehtyneisyyden tasoa, tulokset tiedon merkityksestä ovat samankaltaisia Hwangin ym. (2012) tutkimuksen kanssa. Tiedon siitä, miten henkilötietoja käsitellään ja suojataan, on havaittu vaikuttavan internetin käyttäjien halukkuuteen käyttää palvelua (Zorotheos & Kafeza, 2009). Tätä tukevia tuloksia saatiin myös tässä tutkimuksessa, sillä 80,9 % vastaajista ilmoitti käsityksensä palvelun tietoturvasta vaikuttavan palvelun käyttöön joskus tai useammin.

Vastaajia pyydettiin monivalintakysymysten lisäksi kertomaan omin sanoin perusteluita, mikäli he ovat jatkaneet jonkin tietomurron kohteeksi joutuneen palvelun käyttöä. Sosiaalisen median palvelut ja pelit ja pelaamiseen liittyvät sivustot mainittiin yleisimpinä tietomurron kohteeksi joutuneina palveluina, joiden käyttöä vastaajat ovat jatkaneet. Tätä tulosta voi osaltaan selittää myös kyselylomakkeen levittäminen pääasiassa sosiaalisen median kautta, vastaajien ikäjakauma ja sosiaalisen median ja pelien suosio.

Perusteluissa yleisimpiä mainittuja syitä olivat palvelusta saatu hyöty, tietomurrosta syntyvän uhkan kokeminen vähäiseksi, varovaisuus omien tietojen luovuttamisessa ja luottamus ja palveluntarjoajan suhtautuminen tietomurtoon.

Koettu hyöty ja kuluttajan henkilökohtaiset odotukset tietoturvan tasosta on nostettu esiin myös Budakin ym. (2021) artikkelissa, jonka mukaan nämä yksilölliset asenteet internetin käyttöä kohtaan vaikuttavat käyttäjän yksityisyysloukkauksiin liittyvään resilienssiin.

Bansalin ja Zahedin (2015) mukaan yrityksen reaktiolla asiakkaisiin kohdistuvaan yksityisyysloukkaukseen on suuri merkitys asiakkaiden luottamuksen palautumiselle. He toteavat anteeksipyynnön olevan paras reagointitapa. Tässä tutkimuksessa saaduissa avoimissa vastauksissa mainittiin luottamus siihen, että tietomurron jälkeen yritys todennäköisesti pyrkii entistä paremmin huolehtimaan säilyttämiensä tietojen turvallisuudesta. Tapahtuneen myöntäminen ja anteeksipyyntö ovat siis ensimmäinen askel luottamuksen palauttamiseksi ja herättävät asiakkaissa uskoa siihen, että yritys pyrkii korjaamaan virheensä.

6.3 Tutkimuksen rajoitteet

Tutkimuksen aineistonkeruu suoritettiin verkkokyselynä, jota levitettiin sosiaalisessa mediassa. Aineistonkeruutapa koettiin helpoksi, nopeaksi ja tutkimuksen kohderyhmän tavoittamiseen sopivaksi, mutta siihen liittyy myös aineiston luotettavuuden ja yleistettävyyden kannalta huomioitavia seikkoja.

Verkkokyselystä saatuja tuloksia ei voi yleistää koskemaan koko populaatiota, koska otantaa ei voi tehdä todennäköisyysotannan periaatteita noudattaen (Kananen 2014, s. 168-169; Valli & Perkkilä, 2015). Tässä tutkimuksessa kyselyä levitettiin sosiaalisessa mediassa ja suljetuissa työ- ja harrastusyhteisöjen keskusteluryhmissä. Sosiaalisessa mediassa levitetyssä verkkokyselyssä ei voida varmuudella tietää, onko vastaukset annettu rehellisesti ja kuuluuko vastaaja tutkimuksen kohderyhmään. Tutkimuksen kohderyhmänä olivat yli 18-vuotiaat internetin käyttäjät, mutta on mahdollista, että myös alle 18-vuotiaat ovat törmänneet kyselylinkkiin sosiaalisessa mediassa ja vastanneet kyselyyn. Vastaajien ikäjakauma painottui voimakkaasti alle 40-vuotiaisiin, vaikka tavoitteena oli saada vastauksia myös tätä vanhemmilta internetin käyttäjiltä. Sosiaalisen median käyttäminen kyselyn levittämisessä on mahdollisesti syynä myös ikäjakauman epätasaisuuteen.

Tietomurron uhriksi joutuneiden määrä vastaajista jäi myös toivottua vähäisemmäksi. Varmasti tietomurron uhriksi joutuneita ilmoitti olevansa vain 16,4 % vastaajista, joten ryhmien väliseen vertailuun on suhtauduttava varauksella epätasaisten ryhmäkokojen vuoksi. Huomattavan suuri osa vastaajista (67,2 %) ilmoitti, ettei ole koskaan joutunut tietomurron uhriksi, vaikka tietomurtoja on kohdistunut moneen suosittuun verkkopalveluun. On siis huomioitava, että tietomurtojen uhriksi joutumista selvitettiin vain kysymällä vastaajan käsitystä asiasta, ja todellisuudessa moni ei-vaihtoehdon vastannut voi olla tietomurron uhri tietämättään. Vastaajille annettiin myös ”en ole varma” -vaihtoehto, mutta sen valitsi vain 16, 4 % vastaajista.

Kyselylomakkeen laadinnassa tehtiin valintoja, jotka vaikuttivat tulosten analysointiin ja menetelmävalintoihin. Kyselyn suunnittelussa ei huomioitu

muuttujien tyyppejä ja mahdollisia analyysimenetelmiä, joten aineisto ei sopinut sellaisenaan esimerkiksi monimuuttujamenetelmille. Tästä johtuen kaikille muuttujille ei pystytty tekemään samoja analyysejä ja osaa muuttujista jouduttiin muokkaamaan regressioanalyysiin sopivammiksi.

Validiteetilla tarkoitetaan tulosten osuvuutta ja pätevyyttä, ja siihen vaikuttavat oikein valittu tutkimusmenetelmä, mittarit ja mitatut asiat (Kananen, 2014, s. 262). Luottamusta ja käsitystä yrityksen vastuusta mitattiin molempia vain kahdella eri muuttujalla. Lisäämällä validien muuttujien määrää olisi mahdollisesti parannettu tutkimuksen yleistä validiteettia. Myös muiden muuttujien kohdalla riskinä on, että ne eivät todellisuudessa sovellu tutkittavien asioiden mittaamiseen. Metsämuuronen (2005, s. 58) suosittelee käyttämään valmiita mittareita, mikäli sellaisia on olemassa. Tietoturvahuolien mittaamiseen käytettyjä CFIP- ja IUIPC-mittaristoja sovellettiin tunteita mittaavien kysymysten laadinnassa, mutta kumpaakaan ei käytetty suoraan sellaisenaan. Tietoa ja käytöksen varovaisuutta mittaamaan ei löydetty valmiita testattuja mittareita, joten näiden mittarien validiutta tukemaan ei ole olemassa aiempia tutkimustuloksia.

Lisäksi on huomioitava, että IUIPC- ja CFIP-mallien avulla selvitetään vain tutkittavien käyttäytymisaikomuksia eikä varsinaista käytöstä (Fodor & Brem, 2015). Myös tässä tutkimuksessa vastaajilta kysyttiin, miten he yleensä toimivat eri tilanteissa. On siis mahdollista, että vastaaja kertoo käyttäytyvänsä tietyllä tavalla, mutta todellisuudessa hän toimiikin toisin.

6.4 Jatkotutkimusaiheet

Tätä tutkimusta syventämään jatkotutkimuksissa voisi keskittyä erityisesti tietomurron uhrien kokemuksiin. Tarkempaa kuvausta tietomurtojen herättämistä tunteista ja niiden syistä voisi selvittää käyttämällä eri tutkimusmenetelmiä. Esimerkiksi laadullisia menetelmiä hyödyntäen voidaan tutkia pienempää joukkoa syvällisemmin ja ymmärtää eri tunteiden vaikutuksia käytökseen ja varovaisuuteen. Chatterjee ym. (2019) ovat tutkineet pelon ja vihan eroja verkko-ostamisen kontekstissa. Tulevissa tutkimuksissa myös muiden tunteiden vaikutuksia käytökseen voisi tutkia tarkemmin.

Tässä tutkimuksessa demografisten tekijöiden vaikutusta ei tutkittu, mutta jatkotutkimuksissa myös esimerkiksi sukupuolen, iän ja koulutustason mahdollinen vaikutus käytökseen kannattaa huomioida. Monissa tietoturvahuolien vaikutuksia käsittelevissä tutkimuksissa on tutkittu demografisten tekijöiden vaikutusta, mutta saadut tulokset ovat osittain ristiriitaisia.

Tutkimuksen tulokset viittaavat siihen, että käyttäjän motivaatiolla ja kiinnostuksella on vaikutusta tietoturvakäyttäytymiseen. Jatkotutkimuksissa tätä hypoteesia voisi testata, ja käyttäjän ennakkotietoja tietomurroista voisi kartoittaa tarkemmin kuin tässä tutkimuksessa on tehty.

7 YHTEENVETO

Tietomurrot ja niistä syntyvät tietovuodot ovat yksi lukuisista tietoturvauhkista, joille altistumme internetissä. Usein tällaisten kyberrikoksen uhrit eivät edes tiedä joutuneensa rikoksen kohteeksi (De Kimpe ym., 2020). Monet suositut palvelut ovat joutuneet tietomurron kohteeksi, ja nämä tapaukset ovat saaneet huomiota myös mediassa.

Tässä tutkimuksessa tavoitteena oli selvittää, millaisia tunteita tietomurrot ja niistä aiheutuneet tietovuodot herättävät tietomurtojen uhreissa ja yleisesti kaikissa internetiä käyttävissä ihmisissä. Lisäksi tutkittiin käyttäjällä tietoturvariskeistä olevan tiedon vaikutusta heidän käytökseensä ja halukkuuteen luovuttaa tietojaan yrityksille tai muille organisaatioille verkossa.

Ennen empiiristä tutkimusta tehtiin kirjallisuuskatsaus, jossa tutustuttiin aiempaan tietoturvahuoliin ja tietomurtoihin liittyvään tutkimukseen. Kirjallisuuden perusteella tähän tutkimukseen valittiin kuusi tunnetta: pelko, viha, stressi, ahdistus, suru ja häpeä. Lisäksi tutkimukseen sisällytettiin ärsyyntymisen tunne lievempänä vaihtoehtona voimakkaalle vihan tunteelle. Jotta tulokset kattaisivat kaikki tietoturvahuolien ulottuvuudet, tunteiden mittaamisessa sovellettiin Malhotran ym. (2004) luomaa IUIPC-mittaristoa ja Smithin ym. (1996) kehittämää CFIP-mittaristoa.

Tutkimuksen empiirinen osuus toteutettiin määrällisenä tutkimuksena. Tutkimusaineisto kerättiin verkkokyselyllä, jota levitettiin sosiaalisessa mediassa ja tutkijan omien verkostojen kautta. Kyselyyn saatiin 262 käyttökelpoista vastausta. Aineisto analysoitiin tilastollisin menetelmin IBM SPSS -ohjelmalla. Kyselyyn tulleet avoimet vastaukset käytiin läpi ja niistä etsittiin yhtäläisyyksiä ja toistuvia teemoja. Tietomurtojen herättämiä tunteita ja tietomurron uhriksi joutumisen vaikutusta niihin tutkittiin tarkastelemalla aineiston frekvenssejä sekä tekemällä ristiintaulukointi ja Khiin neliö -testi. Tiedon vaikutusta käytökseen ja luottamukseen selvitettiin ristiintaulukoinnin, Khiin neliö -testin, kontingenssikertoimen ja Spearmanin järjestyskorrelaatiokertoimen avulla. Aineiston muuttujia muokattiin myös monimuuttujamenetelmille sopiviksi ja niille tehtiin regressioanalyysi.

Tutkimuksessa saatiin selville, että tietomurrot herättävät internetin käyttäjissä eniten ärsyyntymistä, vihaa ja ahdistusta. Tunteet ja niiden voimakkuus vaihtelivat eri tietoturvahuolien ulottuvuuksien välillä. Luvaton pääsy tietoihin ja tietojen luvaton käyttö herättivät vastaajissa enemmän tunteita kuin virheet tiedossa ja tietojen kerääminen. Myös tietomurron uhriksi joutumisen havaittiin lisäävän pelon tunnetta ja negatiivista suhtautumista tietojen keräämiseen ja luvattomaan käyttöön. Tietomurtojen uhriksi joutuneiden osuus vastaajista oli kuitenkin niin pieni, että luotettavia päätelmiä ryhmien eroista ei voitu tehdä.

Tiedolla havaittiin olevan yhteys internetin käyttäjien varovaiseen käytökseen ja harkintaan tietojen luovuttamisessa. Erityisesti tuloksissa nousi esiin oman kiinnostuksen ja vapaa-ajalla hankitun tiedon merkitys käytöstä selittävänä tekijänä. Monien muuttujien väliset yhteydet jäivät kuitenkin heikoiksi, joten tulosten vahvistamiseksi vaaditaan vielä jatkotutkimuksia.

LÄHTEET

Avila, R., Khoury, R., Khoury, R. & Petrillo, F. (2021). Use of Security Logs for Data Leak Detection: A Systematic Literature Review. *Security and communication networks*, 2021.

Bansal, G. & Zahedi, F. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62.

Belanger, F. & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017-1041.

Belanger, F., Hiller, J. S. & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The journal of strategic information systems, 11*(3-4), 245-270.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in human behavior*, 53, 419-426.

Budak, J., Rajh, E., Slijepčević, S. & Škrinjarić, B. (2021). Conceptual Research Framework of Consumer Resilience to Privacy Violation Online. *Sustainability, 13*(3), 1238.

Chatterjee, S., Gao, X., Sarkar, S. & Uzmanoglu, C. (2019). Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of business research, 101*, 183-193.

Clouse, S. F., Wright, R. T. & Pike, R. E. (2010). Employee Information Privacy Concerns with Employer Held Data: A Comparison of Two Prevalent Privacy Models. *Journal of Information Privacy & Security*, 6(3), 47-71.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L. & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in human behavior,* Vol. 108.

Fodor, M. & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in human behavior, 53*, 344-353.

Gross, T. (2021). Validity and Reliability of the Scale Internet Users' Information Privacy Concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies*, 2021(2), 235-258.

Harborth, D. & Pape, S. (2020). How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor. *Database for Advances in Information Systems, 51*(1), 51.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2004). *Tutki ja kirjoita* (10. osin uud. laitos). Tammi.

Holopainen, M. & Pulkkinen, P. (2002). *Tilastolliset menetelmät*. WSOY.

Hoy, M. G. & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of interactive advertising*, 10(2), 28-45.

Hwang, H.-G., Han, H.-E., Kuo, K.-M. & Liu, C.-F. (2012). The Differing Privacy Concerns Regarding Exchanging Electronic Medical Records of Internet Users in Taiwan. *Journal of Medical Systems*, 36(6), 3783-3793.

Iovan, S. & Iovan, A. (2016). From cyber threats to cyber-crime. *Journal of Information Systems & Operations Management*, Winter 2016, 425-434.

Janakiraman, R., Lim, J. H. & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of marketing*, 82(2), 85-105.

Janda, S. & Fair, L. L. (2004). Exploring Consumer Concerns Related to the Internet. *Journal of Internet commerce*, 3(1), 1-21.

Jokivuori, P. & Hietala, R. (2015). *Määrällisiä tarinoita: Monimuuttujamenetelmien käyttö ja tulkinta*. Docendo.

Kananen, J. (2011). *Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas*. Jyväskylän ammattikorkeakoulu.

Kananen, J. (2014). *Verkkotutkimus opinnäytetyönä: Laadullisen ja määrällisen verkkotutkimuksen opas*. Jyväskylän ammattikorkeakoulu.

Karjalainen, L. (2010). *Tilastotieteen perusteet*. Pii-kirjat.

Khan, F., Kim, J. H., Mathiassen, L. & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management*, 58(1).

Koti, R., Kumar, R. & Srinivas, Y. (2017). A Survey on Data Leakage Techniques. *International Journal of Advanced Research in Computer Science*, 8(7), 627-631.

Kusyanti, A., Puspitasari, D. R., Ayu Catherina, H. P. & Lia Sari, Y. A. (2017). Information Privacy Concerns on Teens as Facebook Users in Indonesia. *Procedia computer science, 124*, 632-638.

Kyberturvallisuuskeskus. (2020a). Tietoturva. Haettu 25.4.2021 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Kyberturvallisuuskeskus. (2020b). Näin suojaudut tietomurroilta. Haettu 25.4.2021 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.

Malhotra, N., Kim, S. & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355.

Mattila, S. (27.10.2021). *Vastaamo-uhri Jenny Rostain kertoo nyt yli vuoden kestäneestä piinasta – "Tiettyä osaa yksityisyydestäni ei enää ole"*. MTV Uutiset. Haettu 2.11.2021 osoitteesta https://www.mtvuutiset.fi/artikkeli/vastaamo-uhri-jenny-rostain-kertoo-nyt-yli-vuoden-kestaneesta-piinasta-tiettya-osaa-yksityisyydestani-ei-enaa-ole/8275134#gs.f9yddl

Metsämuuronen, J. (2005). *Tutkimuksen tekemisen perusteet ihmistieteissä* (3. laitos.). International Methelp.

Metzger, M. J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer - Mediated Communication*, 9(4).

Nummenmaa, L. (2009). *Käyttäytymistieteiden tilastolliset menetelmät* (1. p., uud. laitos.). Tammi.

Ortiz, J., Chih, W. & Tsai, F. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior*, 80, 143.

Osatuyi, B. (2015). Personality Traits and Information Privacy Concern on Social Media Platforms. *The Journal of Computer Information Systems*, 55(4), 11-19.

Raggad, B. G. (2010). *Information security management: Concepts and practice*. CRC Press.

Reep-van den Bergh, C. M. M. & Junger, M. (2018). Victims of cybercrime in europe: A review of victim surveys. *Crime Science*, 7(1), 1-15.

Rikoslaki 19.12.1889/39.

Rosati, P., Deeney, P., Cummins, M., van Der Werff, L. & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in international business and finance*, 47, 458-469.

Sipior, J. C., T. Ward, B. & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management, 26*(6), 661-678.

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20*(2), 167-196.

Stewart, K. A. & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research, 13*(1), 36.

Tikkala, H. & Torkki, K. (10.11.2020). *Tietomurron uhrin elämä voi mullistua hetkessä, mutta henkilötunnuksen vaihto on piinallista – "Minulle ilmoitettiin,*

ettei sinua ole olemassakaan". Yle. Haettu 2.11.2021 osoitteesta https://yle.fi/uutiset/3-11635095

Valli, R. & Perkkilä, P. (2015). Nettikyselyt ja sosiaalinen media aineistonkeruussa. Teoksessa Valli, R. & Aaltola, J. (toim.), *Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu : virikkeitä aloittelevalle tutkijalle* (s. 109-120). PS-kustannus.

Yang, S. & Wang, K. (2009). The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioral Intention. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 40(1), 38-51.

Zhang, R., Chen, J. Q. & Lee, C. J. (2013). Mobile Commerce and Consumer Privacy Concerns. *The Journal of computer information systems*, 53(4), 31-38.

Zorotheos, A. & Kafeza, E. (2009). Users' perceptions on privacy and their intention to transact online: A study on Greek internet users. *Direct Marketing: An International Journal*, 3(2), 139-153.

LIITE 1 CFIP-MITTARISTO

Tietojen kerääminen (Collection)

1. Minua yleensä häiritsee, kun yritykset pyytävät minulta henkilötietoja.
2. Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.
3. Minua häiritsee luovuttaa henkilötietojani monelle yritykselle.
4. Olen huolissani siitä, että yritykset keräävät liikaa henkilökohtaisia tietoja minusta.

Virheet tiedoissa (Errors)

1. Kaikkien tietokannoissa säilytettävien henkilötietojen paikkansapitävyys tulisi tarkistaa useita kertoja – kustannuksista huolimatta.
2. Yritysten tulisi tehdä enemmän toimenpiteitä säilyttämiensä henkilötietojen oikeellisuuden varmistamiseksi.
3. Yrityksillä tulisi olla parempia menettelytapoja henkilötiedoissa olevien virheiden korjaamiseksi.
4. Yritysten tulisi käyttää enemmän aikaa ja vaivaa tietokannoissaan olevien henkilötietojen oikeellisuuden tarkistamiseen.

Tietojen luvaton käyttö (Unauthorized secondary use)

1. Yritysten ei tulisi käyttää henkilötietoja mihinkään muuhun tarkoitukseen kuin siihen, mihin tiedot luovuttanut henkilö on antanut luvan.
2. Kun ihmiset antavat tietojaan yrityksille johonkin tiettyyn tarkoitukseen, yritysten ei tulisi käyttää näitä tietoja mihinkään muuhun tarkoitukseen.
3. Yritysten ei tulisi koskaan myydä säilyttämiään henkilötietoja muille yrityksille.
4. Yritysten ei tulisi koskaan jakaa henkilötietoja muille yrityksille ilman tiedot luovuttaneen henkilön lupaa.

Luvaton pääsy tietoihin (Improper access)

1. Yritysten tulisi käyttää enemmän aikaa ja vaivaa estääkseen luvaton pääsy niiden säilyttämiin henkilötietoihin.
2. Tietokannat, jotka sisältävät henkilötietoja, tulisi suojata luvattomalta pääsyltä – kustannuksista huolimatta.
3. Yritysten tulisi tehdä enemmän toimenpiteitä estääkseen henkilötietoihin pääsyn niiltä, joilla ei ole siihen oikeutta.

Smithin ym. (1996) alkuperäisestä mallista suomentanut Riikka Puhakka.

LIITE 2 IUIPC-MITTARISTO

Tietojen hallinta (Control)

1. Kuluttajien yksityisyydessä internetissä on kyse siitä, että kuluttajalla on oikeus hallita itsenäisesti, miten heidän tietojaan kerätään, käytetään ja jaetaan.
2. Kuluttajan yksityisyyden ydin on kuluttajan mahdollisuus hallita omia tietojaan.
3. Uskon, että yksityisyyttä verkossa loukataan, kun hallinta omista tiedoista katoaa tai vähenee vastoin kuluttajan tahtoa markkinointitapahtuman seurauksena.

Tietoisuus kerättyjen tietojen käytöstä (Awareness)

1. Internetissä tietoja keräävien yritysten tulisi kertoa, miten dataa kerätään, käsitellään ja käytetään.
2. Tietosuojakäytäntö tulisi viestiä kuluttajalle selkeästi ja huomiota herättävästi.
3. Minulle on erittäin tärkeää, että tiedän, miten henkilötietojani käytetään.

Tietojen kerääminen (Collection)

1. En yleensä pidä siitä, kun yritykset pyytävät henkilötietojani internetissä.
2. Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.
3. Minua häiritsee luovuttaa henkilötietojani niin monelle eri yritykselle internetissä.
4. Olen huolissani siitä, että yritykset keräävät liikaa tietoja minusta internetissä.

Malhotran ym. (2004) alkuperäisestä mallista suomentanut Riikka Puhakka.

LIITE 3 KYSELYLOMAKE

Kysely tietomurtojen vaikutuksesta internetin käyttäjien tunteisiin ja käytökseen

Pakolliset kentät merkitään asteriskilla (*) ja ne tulee täyttää lomakkeen viimeistelemiseksi.

Tämä kysely on osa Jyväskylän yliopistossa tehtävää tietojärjestelmätieteen pro gradu -tutkimusta, jossa kartoitetaan tietomurtojen vaikutusta internetin käyttäjien tunteisiin ja käytökseen. Kyselystä saatuja vastauksia käytetään ainoastaan tutkimuskäyttöön. Kysely on täysin anonyymi, eikä yksittäistä vastaajaa voida tunnistaa raportoinnista. Vastaamalla kyselyyn ilmaiset suostumuksesi osallistua tähän tieteelliseen tutkimukseen.

Kyselyyn vastaaminen vie noin 5-10 minuuttia ja vastaamisen voi keskeyttää milloin tahansa. Kyselyyn vastaaminen on täysin vapaaehtoista.

Tutkimustiedotteen pääset lukemaan tästä linkistä ja tutkimuksen tietosuojailmoituksen tästä linkistä.

1. Sukupuoli *

- ◯ nainen
- ◯ mies
- ◯ muu / en halua kertoa

2. Ikä *

- ◯ 18-30 v
- ◯ 31-40 v
- ◯ 41-50 v
- ◯ 51-60 v
- ◯ yli 60 v

3. Koulutustaso *

- ◯ peruskoulu
- ◯ ammattikoulu / lukio
- ◯ alempi korkeakoulututkinto
- ◯ ylempi korkeakoulututkinto

4. Internetin käytön määrä keskimäärin *

- ◯ alle 1 h/päivä
- ◯ 1-4 h/päivä
- ◯ 4-8 h/päivä
- ◯ yli 8 h/päivä

5. Mihin tarkoitukseen käytät internetiä? Voit valita useamman vaihtoehdon. *

- ☐ työ
- ☐ viihde
- ☐ pankkiasiat ja muu verkkoasiointi (esim. sosiaali- ja terveyspalvelut)
- ☐ opiskelu
- ☐ uutisten seuraaminen
- ☐ sosiaalinen media
- ☐ verkkokaupoissa asiointi
- ☐ muu, mikä? _____

6. Olen joutunut tietomurron uhriksi internetissä. *

- ◯ kyllä
- ◯ ei
- ◯ en ole varma

7. Työ- tai opiskelupaikallani on käytössä tietoturvaan liittyvä ohjeistus.

- ◯ kyllä
- ◯ ei
- ◯ en osaa sanoa

8. Olen käynyt tietoturvaan liittyvän kurssin tai koulutuksen töideni tai opintojeni kautta. *

- ◯ kyllä
- ◯ ei

9. Olen perehtynyt tietoturva-asioihin harrastuksen tai oman mielenkiinnon vuoksi. *

- ◯ kyllä
- ◯ ei

10. Seuraan tietomurtoihin liittyvää uutisointia. *

En koskaan	Harvoin	Joskus	Melko usein	Usein
◯	◯	◯	◯	◯

11. Pyrin toiminnallani ylläpitämään henkilökohtaisten laitteideni (esim. älypuhelin, tietokone) tietoturvaa esimerkiksi käyttämällä tietoturvallisia salasanoja, ja huolehtimalla, että laitteen virustorjuntaohjelma on päivitetty. *

En koskaan	Harvoin	Joskus	Melko usein	Usein
◯	◯	◯	◯	◯

12. Minkälaisia tunteita seuraavat tilanteet ja väittämät sinussa herättävät? Voit valita useamman vaihtoehdon. *

	suru	ahdistus	viha	stressi	häpeä	ärsyyntyminen	pelko	ei mitään näistä
Yritys pyytää minulta henkilötietojani.	☐	☐	☐	☐	☐	☐	☐	☐
Joudun luovuttamaan henkilötietojani usealle yritykselle.	☐	☐	☐	☐	☐	☐	☐	☐
Yritykset keräävät paljon henkilökohtaisia tietoja kuluttajista.	☐	☐	☐	☐	☐	☐	☐	☐
Yrityksen säilyttämissä henkilötiedoissa on virheitä.	☐	☐	☐	☐	☐	☐	☐	☐
Yritys käyttää tietojani johonkin muuhun tarkoitukseen kuin mihin olen ne alun perin luovuttanut.	☐	☐	☐	☐	☐	☐	☐	☐
Yritys luovuttaa kuluttajista keräämiään tietoja muille yrityksille.	☐	☐	☐	☐	☐	☐	☐	☐
Yritys myy kuluttajista keräämiään tietoja muille yrityksille.	☐	☐	☐	☐	☐	☐	☐	☐
Yritys ilmaisee epäselvästi, mihin tarkoitukseen henkilötietoja kerätään.	☐	☐	☐	☐	☐	☐	☐	☐
Käyttämäni palvelu joutuu tietomurron kohteeksi.	☐	☐	☐	☐	☐	☐	☐	☐
Henkilökohtaiset tietoni päätyvät tietovuodon seurauksena kaikkien nähtäville.	☐	☐	☐	☐	☐	☐	☐	☐

13. Mitä mieltä olet seuraavista väittämistä? *

	täysin eri mieltä	jokseenkin eri mieltä	ei eri eikä samaa mieltä	jokseenkin samaa mieltä	täysin samaa mieltä
Uskon henkilötietojeni olevan turvassa.	◯	◯	◯	◯	◯
Kun yritys pyytää minulta henkilötietoja internetissä, harkitsen tarkoin ennen kuin luovutan tietojani.	◯	◯	◯	◯	◯
Tietomurron kohteeksi joutuminen kertoo yrityksen liian vähäisistä turvatoimista.	◯	◯	◯	◯	◯
Yritys on vastuussa säilyttämistään henkilötiedoista ja sitä tulisi rangaista tietovuodon sattuessa.	◯	◯	◯	◯	◯

14. Minulla on käytössäni maksullinen virustorjuntaohjelma. *

- ◯ kyllä
- ◯ ei

15. Kiinnitän huomiota internetissä käyttämieni palvelujen tietosuojakäytäntöihin. *

En koskaan	Harvoin	Joskus	Melko usein	Usein
◯	◯	◯	◯	◯

16. Käsitykseni palvelun tietoturvasta vaikuttaa valintaani käyttää palvelua. *

Ei koskaan	Harvoin	Joskus	Melko usein	Usein
◯	◯	◯	◯	◯

17. Käytän palveluita, vaikka niihin olisi aiemmin kohdistunut tietomurto. *

En koskaan	Harvoin	Joskus	Melko usein	Usein
◯	◯	◯	◯	◯

18. Mikäli käytät jotain palvelua tietomurrosta huolimatta: Mikä palvelu on kyseessä ja miksi olet jatkanut sen käyttöä?

LIITE 4 TUNTEIDEN FREKVENSSIT TIETOJEN KERÄÄMISEN ULOTTUVUUDESSA

		Olen joutunut tietomurron uhriksi internetissä.					
		kyllä (n=43)		ei (n=176)		en ole varma (n=43)	
		f	f %	f	f %	f	f %
TK1	suru	0	0,0%	1	0,6%	0	0,0%
	ahdistus	11	25,6%	17	9,7%	3	7,0%
	viha	2	4,7%	5	2,8%	1	2,3%
	stressi	3	7,0%	15	8,5%	2	4,7%
	häpeä	0	0,0%	1	0,6%	0	0,0%
	ärsyyntyminen	26	60,5%	72	40,9%	17	39,5%
	pelko	5	11,6%	9	5,1%	4	9,3%
	ei mitään näistä	13	30,2%	85	48,3%	21	48,8%
TK2	suru	0	0,0%	1	0,6%	0	0,0%
	ahdistus	11	25,6%	36	20,5%	9	20,9%
	viha	3	7,0%	6	3,4%	1	2,3%
	stressi	6	14,0%	23	13,1%	6	14,0%
	häpeä	0	0,0%	1	0,6%	0	0,0%
	ärsyyntyminen	32	74,4%	80	45,5%	21	48,8%
	pelko	9	20,9%	21	11,9%	8	18,6%
	ei mitään näistä	7	16,3%	60	34,1%	9	20,9%
TK3	suru	2	4,7%	3	1,7%	0	0,0%
	ahdistus	13	30,2%	33	18,8%	11	25,6%
	viha	13	30,2%	18	10,2%	5	11,6%
	stressi	9	20,9%	23	13,1%	5	11,6%
	häpeä	0	0,0%	2	1,1%	0	0,0%
	ärsyyntyminen	25	58,1%	102	58,0%	27	62,8%
	pelko	12	27,9%	17	9,7%	2	4,7%
	ei mitään näistä	6	14,0%	41	23,3%	6	14,0%

LIITE 5 TUNTEIDEN FREKVENSSIT VIRHEELLISTEN TIETOJEN ULOTTUVUUDESSA

		Olen joutunut tietomurron uhriksi internetissä.					
		kyllä (n=43)		ei (n=176)		en ole varma (n=43)	
		f	f %	f	f %	f	f %
VT	suru	0	0,0%	2	1,1%	0	0,0%
	ahdistus	1	2,3%	16	9,1%	7	16,3%
	viha	8	18,6%	14	8,0%	5	11,6%
	stressi	3	7,0%	17	9,7%	1	2,3%
	häpeä	0	0,0%	4	2,3%	0	0,0%
	ärsyyntyminen	31	72,1%	95	54,0%	24	55,8%
	pelko	2	4,7%	11	6,3%	1	2,3%
	ei mitään näistä	6	14,0%	52	29,5%	15	34,9%

LIITE 6 TUNTEIDEN FREKVENSSIT LUVATTOMAN KÄYTÖN ULOTTUVUUDESSA

		Olen joutunut tietomurron uhriksi internetissä.					
		kyllä (n=43)		ei (n=176)		en ole varma (n=43)	
		f	f %	f	f %	f	f %
LK1	suru	1	2,3%	4	2,3%	1	2,3%
	ahdistus	12	27,9%	36	20,5%	16	37,2%
	viha	32	74,4%	105	59,7%	28	65,1%
	stressi	6	14,0%	36	20,5%	6	14,0%
	häpeä	0	0,0%	2	1,1%	1	2,3%
	ärsyyntyminen	30	69,8%	131	74,4%	28	65,1%
	pelko	12	27,9%	34	19,3%	7	16,3%
	ei mitään näistä	2	4,7%	3	1,7%	2	4,7%
LK2	suru	1	2,3%	5	2,8%	0	0,0%
	ahdistus	9	20,9%	29	16,5%	10	23,3%
	viha	28	65,1%	82	46,6%	19	44,2%
	stressi	7	16,3%	21	11,9%	5	11,6%
	häpeä	0	0,0%	1	0,6%	0	0,0%
	ärsyyntyminen	30	69,8%	126	71,6%	28	65,1%
	pelko	13	30,2%	21	11,9%	6	14,0%
	ei mitään näistä	2	4,7%	9	5,1%	6	14,0%
LK3	suru	1	2,3%	12	6,8%	2	4,7%
	ahdistus	11	25,6%	31	17,6%	10	23,3%
	viha	31	72,1%	99	56,3%	25	58,1%
	stressi	9	20,9%	22	12,5%	5	11,6%
	häpeä	2	4,7%	7	4,0%	1	2,3%
	ärsyyntyminen	33	76,7%	123	69,9%	28	65,1%
	pelko	16	37,2%	23	13,1%	5	11,6%
	ei mitään näistä	0	0,0%	9	5,1%	2	4,7%
LK4	suru	0	0,0%	2	1,1%	0	0,0%
	ahdistus	14	32,6%	28	15,9%	11	25,6%
	viha	13	30,2%	24	13,6%	11	25,6%
	stressi	6	14,0%	22	12,5%	7	16,3%
	häpeä	0	0,0%	3	1,7%	0	0,0%
	ärsyyntyminen	34	79,1%	119	67,6%	27	62,8%
	pelko	8	18,6%	23	13,1%	2	4,7%
	ei mitään näistä	4	9,3%	22	12,5%	6	14,0%

LIITE 7 TUNTEIDEN FREKVENSSIT LUVATTOMAN PÄÄSYN ULOTTUVUUDESSA

		Olen joutunut tietomurron uhriksi internetissä.					
		kyllä (n=43)		ei (n=176)		en ole varma (n=43)	
		f	f %	f	f %	f	f %
LP1	suru	3	7,0%	10	5,7%	5	11,6%
	ahdistus	22	51,2%	92	52,3%	26	60,5%
	viha	10	23,3%	39	22,2%	9	20,9%
	stressi	21	48,8%	75	42,6%	16	37,2%
	häpeä	3	7,0%	13	7,4%	3	7,0%
	ärsyyntyminen	25	58,1%	85	48,3%	19	44,2%
	pelko	22	51,2%	76	43,2%	16	37,2%
	ei mitään näistä	3	7,0%	7	4,0%	4	9,3%
LP2	suru	12	27,9%	33	18,8%	9	20,9%
	ahdistus	28	65,1%	105	59,7%	29	67,4%
	viha	24	55,8%	85	48,3%	25	58,1%
	stressi	27	62,8%	88	50,0%	21	48,8%
	häpeä	15	34,9%	46	26,1%	13	30,2%
	ärsyyntyminen	27	62,8%	106	60,2%	26	60,5%
	pelko	24	55,8%	87	49,4%	21	48,8%
	ei mitään näistä	1	2,3%	7	4,0%	2	4,7%