VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Annika Henriksnäs

SOSIAALINEN MEDIA JA YKSITYISYYS

Liiketalous
2020

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Annika Henriksnäs
Opinnäytetyön nimi	Sosiaalinen media ja yksityisyys
Vuosi	2020
Kieli	suomi
Sivumäärä	58 + 2 liitettä
Ohjaaja	Päivi Rajala

Tämä opinnäytetyö käsittelee sosiaalista mediaa muutamasta eri näkökulmasta. Ensimmäisessä luvussa esitellään internetin käytetyimmät sosiaalisen median sivustot – Facebook, Instagram, Twitter ja YouTube. Seuraavassa luvussa sosiaalista mediaa tutkitaan tietoturvan kannalta. Lopuksi tutkitaan käyttäjälle saatavilla olevia suojauskeinoja internetissä. Opinnäyteyön tavoitteena on antaa yleiskuva sosiaalisesta mediasta, tietoturvauhista, sekä suojauskeinoista verkossa.

Teoriaosuudessa tutkitaan sosiaalisten medioiden taustoja, historiaa ja olennaisia ominaisuuksia. Työssä tutkitaan tavallisimmat keinot, joilla sivusto kerää dataa käyttäjästä ja tämän laitteista. Nämä keinot ovat muun muassa evästeet, laitteen sijaintitiedot ja ohjelmointirajapinnat. Työssä tutkitaan, miten kukin somesivusto käyttää keräämäänsä käyttäjädataa ja mihin tarkoitukseen. Lopuksi käydään läpi eri suojauskeinoja, kuten VPN-sovelluksia, kaksivaiheista varmennusta, sekä selaimen laajennuksia ja lisäosia.

Teoreettinen viitekehys muodostuu muun muassa verkkoturvallisuutta käsittelevistä kirjoista, someyhtiöiden virallisista käyttöehdoista, sekä viranomaisten sivuista, kuten Liikenne- ja viestintävirastosta ja Europolista. Käytännön osuus koostuu kyselytutkimuksesta, jossa selvitetään Vaasan ammattikorkeakoulun opiskelijoiden somekäyttöä ja verkkoturvallisuutta.

Tutkimuksessa havaittiin, että sosiaalisen median käyttö on hyvin yleistä vastaajien keskuudessa. Valtaosa ilmoitti käyttävänsä jonkinlaista sosiaalista mediaa hyvin usein. Kävi myös ilmi, että moni käyttää useita eri suojauskeinoja verkossa. Selaintietojen tyhjennys, VPN-sovelluksien ja kasivaiheisen varmennuksen käyttö, sekä selaimen lisäosat (kuten mainostenestäjät) olivat yleisiä suojauskeinoja vastaajien keskuudessa.

Avainsanat Yksityisyys, sosiaalinen media, tietoturva, verkkoseuranta

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Business Information Technology

ABSTRACT

Author	Annika Henriksnäs
Title	Social Media and Privacy
Year	2020
Language	Finnish
Pages	58 + 2 Appendices
Name of Supervisor	Päivi Rajala

This bachelor's thesis studied social media from a few different viewpoints. The most used social media sites – Facebook, Instagram, Twitter and YouTube – are introduced in the first chapter. Social media and its data security are studied in the next chapter. The last chapter examines different security measures the user can take online. The objective of this study was to give the reader an overview of social media, information security and security measures on the Web.

The theoretical section of the study examines the history, backgrounds and relevant features of social media sites. The common methods through which sites collect data of the user and their devices are presented. These methods include cookies, location data and application programming interfaces (API). The study explores how different social media sites use user data, and for which purposes. Finally, different security measures are explored, including VPN applications, two-factor authentication and browser extensions and addons.

The conceptual framework consists of books about Internet security, the official terms of use of websites, and the websites of official agencies, such as The Finnish Transport and Communications Agency and Europol. The practical part of the study consists of a survey sent out to the students of Vaasa University of Applied Sciences. The survey explores the students' use of social media, as well as their Internet security.

The survey revealed that the use of social media is very common among those who replied. The majority reported using some form of social media very frequently. It was also revealed that many take several different security measures online. Common measures were deleting browsing data, the use of VPN applications, two-factor authentication and browser extensions (such as ad blockers).

Keywords Privacy, social media, data security, internet tracking

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

LIITELUETTELO

1 JOHDANTO

Yksityisyys ja sen varjeleminen verkossa on nykymaailmassa aina ajankohtainen aihe. Sosiaalisesta mediasta on melko lyhyessä ajassa tullut jokapäiväinen ilmiö, jota suurin osa meistä – sekä yksityishenkilöistä että yrityksistä – käyttää.

Vuonna 2018 arviolta 2,65 miljardia ihmistä ympäri maailman käytti jonkinlaista sosiaalista mediaa, ja numeron arvioidaan ylittävän kolmen miljardin vuonna 2021 (Clement 2020a). Tällaiset määrät – miltei puolet maapallon asukkaista – houkuttelevat kaikenlaisia tahoja, joiden päämääränä on hyödyntää verkossa käyvien yksityistietoja. Tavoitteet voivat olla melko jokapäiväisiä ja harmittomia, kuten kohdennetut mainokset verkkosivuilla, mutta pahimmassa tapauksessa yksityishenkilö voi menettää rahansa ja henkilötietonsa.

Edward Snowdenin paljastukset vuonna 2013 yksityishenkilöihin kohdistuvasta vakoilusta nostivat verkkoyksityisyyden merkityksen pöydälle. Hän toi julkisuuteen Yhdysvaltojen kansallisen turvallisuusviraston NSA:n (National Security Agency) suorittamat tietourkinnat, joita perusteltiin terrorismin vastaisella sodalla.

Yhdysvaltalaiset puhelinyhtiöt, kuten Verizon, olivat luovuttaneet NSA:lle miljoonien asiakkaiden puhelinlokeja. Tiedonkeruuohjelma nimeltä Prism oli koonnut dataa verkkojättiläisiltä kuten Googlelta, Facebookilta, Yahoolta ja Applelta.

Snowdenin paljastukset herättivät maailmanlaajuista kritiikkiä sekä yksityishenkilöiden, että poliitikkojen parissa. Saksan kansleri Angela Merkel syytti Yhdysvaltoja häneen kohdistuvasta vakoilusta. (Macaskill & Dance 2013.)

Vuoden 2013 jälkeen verkkoyksityisyys on ollut keskustelujen ja kiistojen kohteena eri tahojen puolesta, ja asia on tärkeä kaikille sosiaalisen median käyttäjille.

Tässä työssä tietoturvauhkiin perehdytään syvemmin, ja pyritään selvittämään yksityishenkilöihin kohdistuvia tietoturvauhkia – sekä miten niiltä voi suojautua. Painopiste on yksityisellä käyttäjällä, ja pyrkimyksenä on antaa lukijalle kattava peruskäsitys aiheesta, vaikka henkilöllä ei ole aiheesta aiempaa kokemusta.

Tutkimuskysymyksiä on kolme:

- Mitkä tahot seuraavat verkkokäyttäytymistämme?
- Miten nämä tahot seuraavat meitä?
- Minkälaisia suojakeinoja on olemassa verkkoseurannan estämiseksi?

Työssä tutkitaan verkkoseurannan suorittajia, näiden toimintatapoja ja lopulta olemassa olevia suojakeinoja. Tietoturvatietoisuus on hyödyllinen taito kaikille ihmisille nyky-yhteiskunnassa, jossa internetiä käytetään jokapäiväisissä tehtävissä, sekä yksityiselämässä että työelämässä. Vankat perustiedot uhkien tunnistamisessa ja torjunnassa vähentävät tietoturvauhkien vaaraa.

Työssä käydään läpi suosituimmat sosiaaliset mediat – niiden historia, toiminta, käyttäjämäärät ja yksityisyyteen liittyvät asiat. Luvut etenevät loogisessa järjestyksessä. Aluksi tutustutaan käytetyimpiin sosiaalisiin medioihin, ja perehdytään niiden toimintaperiaatteisiin. Sivustoista annetaan yleiskatsaus, mutta niiden yksityisyyskäytäntöjä käsitellään vasta seuraavassa luvussa.

Opinnäytetyössä selvitetään eri metodeja käyttäjän verkkotoiminnan suojaamiseksi. Näihin kuuluvat muun muassa perustoimet kuten selaimen valinnat ja yksityisasetukset, sekä niin kutsutut VPN-ohjelmat (Virtual Private Network).

Opinnäytetyöhön kuuluu kyselyn lähettäminen VAMK:in eri koulutusyksiköille – tekniikka, liiketalous ja sosiaali- ja terveysala. Kyselyssä tutkitaan yksittäisten oppilaiden tietoja verkkoyksityisyydestä, sosiaalisen median käytöstä, ja suojauskeinoista. Lähettämällä kyselyn eri alojen opiskelijoille saadaan selville, onko ryhmien välillä eroja tietotasoissa.

Kyseessä on määrällinen tutkimus, jonka avulla saadaan yleiskäsitys ryhmien tietoisuudesta aiheeseen liittyen. Tavoitteena on saada ainakin 30 vastausta.

Kysely suoritetaan sähköisesti verkkolomakkeen kautta, ja lähetetään oppilasryhmille sähköpostilla. Päämääränä on luoda mahdollisimman lyhyt ja ytimekäs kysely, jolloin vastauskynnys on alempi. Kyselyssä ei perehdytä liiaksi yksittäisiin vastaajiin, vaan tavoitteena on luoda yleinen käsitys eri alojen verkkotietotaidoista.

Kyselyn tulokset esitetään graafimuodossa, esimerkiksi Microsoft Excelissä, joista helposti nähdään vastaajan ikä, sukupuoli, koulutusala ja muut vastaukset. Vapaamuotoisten vastauksien määrä pidetään minimissä, jotta tuloksien analysointi ja kaaviointi pysyy suoraviivaisena.

Opinnäytetyön viimeisissä luvuissa tutkitaan kyselytuloksia. Vastaukset analysoidaan, ja loppupäätelmät kirjataan. Lopullisena tavoitteena on saada selville, onko eri alojen opiskelijoilla huomattavia eroja yksityisyystietoisuudessa.

2 SOSIAALINEN MEDIA

Sosiaalinen media, arkikielessä some, on nykymaailmassa tuttu käsite. Se kattaa useat verkkosivustot, joita suuri osa ihmisistä käyttää päivittäin. Facebook, Twitter, Instagram, eri blogialustat, nettifoorumit, chattiohjelmat, ynnä muut ovat jokapäiväisiä käsitteitä internetin selaajalle. Sosiaalisen median käyttäjäluku lasketaan miljardeissa, ja luku on noussut vuosi vuodelta. Siitä on tullut merkittävä osa nykymaailmaa – sekä yksityisessä elämässä että työssä. Erilaiset sosiaalisen median sivustot ovat hyvin tärkeitä muun muassa internetiin perustuville yrityksille, ja sosiaalisen median voimaa mainonnassa ja kuluttajakäyttäytymisessä ei tule sivuuttaa.

Vuonna 2008 Jussi-Pekka Erkkola määritteli sosiaalisen median seuraavasti:

”... sosiaalinen media on teknologiasidonnainen ja rakenteinen prosessi, jossa yksilöt ja ryhmät rakentavat yhteisiä merkityksiä sisältöjen, yhteisöjen ja verkkoteknologioiden avulla vertais- ja käyttötuotannon kautta (Erkkola 2008).”

Maallikkokielellä se merkitsee ihmisten luomaa sisältöä ja kommunikaatiota eri verkkosivustoilla. Voidaankin sanoa, että sosiaalinen media ei riipu niinkään itse alustasta, vaan sen sisällöstä ja viestinnästä. Erään näkökulman mukaan sosiaalinen media ei ole varsinaisesti uusi käsite, ainoastaan moderni jatke ihmiskunnan kaukokommunikoinnin historialle, aina sähketeknologiasta puhelimiin. Itse ydinajatus on sama, ainoastaan teknologia on muuttunut. Siksi sosiaalista mediaa ei pidä pitää erillisenä ”oikeasta” maailmasta, aivan kuten emme pidä puhelinsoittoja erillisenä oikeasta maailmasta. Yksilöt ja ryhmät ovatkin internetin kehityksen myötä vaihtaneet alustaa useaan otteeseen.

Daniel Miller ja Mirca Madianou loivat käsitteen ”polymedia”. Tämä termi syntyi ihmisten tavasta käyttää tiettyjä some-alustoja riippuen siitä, mitä haluttiin sanoa. Koska useimmilla henkilöillä on mahdollisuus käyttää montaa eri (tai kaikkia) sosiaalisia medioita ilman rajoituksia, valinnoilla alkaa olla merkitystä. Henkilön valintaa voidaan arvostella, ja henkilö voi punnita tietyn viestintätavan hyödyt ja haitat. Onko esimerkiksi parempi kertoa vanhemmille hylätystä arvosanasta tekstiviestitse, sähköpostilla, vai Facebookissa? Oppilas saattaa valita viestintämetodin, joka

ei mahdollista äkkipikaista reaktiota, vaan pakottaa vastaanottajan miettimään vastaustaan.

Ihmiset käyttävät hyväkseen eri sosiaalisten medioiden ominaisuuksia kommunikoidakseen tehokkaasti ja mielekkäästi. Tekstiviestillä voidaan kysyä hyvää hetkeä videopuheluun, Twitterissä alkanutta keskustelua voidaan jatkaa Skypessä, Facebookissa kirjoitettuun kysymykseen voidaan vastata virallisesti sähköpostilla, ja niin edelleen. Sosiaaliset mediat täydentävät toisiaan, ja Millerin mukaan alustan valinnalla on merkitystä viestin sävyyn ja tärkeyteen. Arkielämässä sosiaaliset mediat siis sulautuvat toisiinsa, ja niiden tarkastelua erillisinä, toisistaan riippumattomina alustoina voidaan pitää hieman vanhentuneena käsitteenä. (Miller 2016.)

Teknologian kehitys ajan mittaan on mahdollistanut kommunikoinnin entistä monimuotoisimmilla tavoilla. 1970-, 1980- ja 1990-luvun alussa sosiaalista mediaa sen nykyisessä muodossa ei ollut olemassa, mutta sähköiseen kommunikointiin pystyttiin sähköpostitse ja eri postilistoilla. IRC (Internet Relay Chat) luotiin vuonna 1988, ja ”irkki” olikin suosittu chattiohjelma 90-luvun lopulla ja 2000-luvun alussa. Monet blogisivustot, kuten Livejournal, Blogger ja WordPress, saivat alkunsa vuosituhannen vaihteessa. 2000-luvun alkupuoliskolla tietokoneet ja internet alkoivat yleistyä kodeissa merkittävästi, ja näihin aikoihin moni nykyään suuri sivu syntyi. Wikipedia, verkon tietokirjajättiläinen, luotiin 2001, ja työelämään keskittyvä LinkedIn pari vuotta myöhemmin. (McFadden 2018.) Tunnetuin sivu on kuitenkin Facebook, joka perustettiin vuonna 2004 Harvardin yliopistossa Yhdysvalloissa (Phillips 2007). Se onkin noussut maailman suosituimmaksi sosiaalisen median sivuksi – vuonna 2020 aktiivisia käyttäjiä on yli 2,45 miljardia (Clement 2020b).

Sosiaalisten medioiden käyttäjiä on liki 3 miljardia maailmanlaajuisesti. Käyttäjämäärä on kasvanut vuosittain, ja sama kehitys näyttää jatkuvan tulevaisuudessakin. Suuri osa ihmisistä käyttää jonkinlaista sosiaalista mediaa päivittäin, ja Millerin (2016) mukaan sosiaalista mediaa voi pitää teknologian ja kommunikoinnin lisäksi paikkana, jossa moni viettää aikaa. Siksi ei olekaan yllättävää, että internetin eri sivustoista on tullut hyvin tärkeä tekijä nykymaailman tapahtumissa. Internetissä yhdistyvät nopea kommunikointi ja nopea tiedonkulku, ja eri aikavyöhykkeillä ja

maanosilla on hyvin vähän merkitystä tiedonkulun suhteen. Internet on maailma ilman rajoja.

Rajattomuus tuo mukanaan monta hyötyä. Verkkokommunikoinnilla voi olla suuri vaikutus ”oikeassa” maailmassa. Tunnettu esimerkki internetin vallasta on Edward Snowden, entinen Yhdysvaltojen tiedustelupalvelun työntekijä. Vuonna 2013 hän paljasti Yhdysvaltain kansallisen turvallisuusviraston NSA:n (National Security Agency) suorittamat maailmanlaajuiset joukkovalvonnat. Tietovuodossa paljastui, että NSA oli vakoillut ja tehnyt yhteistyötä monen teknologiajättiläisen kanssa. Näihin lukeutui muun muassa Facebook, Skype, Microsoft, Apple, Twitter ja eri puhelinyhtiöt. Nämä olivat luovuttaneet asiakkaiden tietoja NSA:lle, ja paljastukset saivat aikaan suuren, maailmanlaajuisen kritiikkivyöryn. Snowdenin paljastukset nostivat sosiaalisen median yksityisyyden tapetille, ja teki tavallisen ihmisen tietoiseksi mahdollisista tietoturvauhista liittyen jokapäiväisiin tuotteisiin ja palveluihin. (Macaskill & Dance 2013.)

Toinen esimerkki sosiaalisen median vaikutusvallasta löytyy Pohjois-Afrikasta ja Lähi-idästä, vuoden 2011 niin kutsutusta arabikeväästä. Toisinaan sitä kutsuttiin myös ”Facebook-vallankumoukseksi” ja ”Twitter-kansannousuksi” näiden sivujen tärkeän roolien vuoksi. Egyptissä mielenosoittajat käyttivät hyödykseen sosiaalisen median viestintävoimaa suunnitellakseen protesteja ja kertoakseen niistä maailmalle.

”Käytämme Facebookia mielenosoitusten aikatauluttamiseen, Twitteriä koordinointiin ja YouTubea kertoaksemme maailmalle,” kirjoitti mielenosoittaja Fawaz Rashed Twitterissä keväällä 2011. Sosiaalisen median käyttö protesteissa oli erittäin tehokasta Egyptissä, jossa 60 % väestöstä oli alle 30-vuotiaita. Maan protestit johtivat presidentti Mubarakin eroon. (Shearlaw 2016.)

Internet mahdollisti tavallisten ihmisten mahdollisuuden saada äänensä kuuluviin ympäri maailman, mikä myös mahdollistaa poliittisen painostuksen. Tämä tapahtui Hong Kongissa vuonna 2019. Alkukesällä alettiin pitää suuria mielenilmaisuja Kiinaa vastaan, joiden syynä oli Kiinan esittämä laki, joka olisi mahdollistanut Hong Kongin asukkaiden luovuttamisen Manner-Kiinaan. Itsenäisyyttä vaativat

hongkongilaiset alkoivat järjestäytyä sosiaalisen median, usein chattiohjelmien WhatsAppin ja Telegramin avulla. Protesteja lähetettiin reaaliaikaisena suoratoistona (live streaming) muun muassa Periscopessa (Twitterin omistamassa videosovelluksessa), Twitchissä (videopelisivustolla) ja Instagramissa (Kharpal 2019). Kirjoitushetkellä (maaliskuu 2020) protesteihin johtaneet ongelmat eivät ole ratkenneet (Tam & Jim 2020).

Sosiaalisella medialla oli suuri vaikutus Yhdysvaltojen presidenttivaaleissa vuonna 2016. Loppuehdokkaina vastakkain olivat Hillary Clinton ja Donald Trump, ja tiukan kilpailun voitti Trump. Vaalikisa oli kiivas ja vaaleissa esille nousi moni kiistanalainen asia, kuten maan rasismiongelmat, laiton maahanmuutto sekä ehdokkaiden käyttäytyminen ja historia. Konservatiiviset ja liberaalit olivat vastakkain, ja kyseessä oli hyvin kiistanalainen vaali. Venäjä käytti hyödykseen tätä vastakkaisasettelua puuttumalla vaalikampanjoihin salaa. Pietarilainen yhtiö IRA (Internet Research Agency) alkoi levittää Clintonin vastaista propagandaa sosiaalisessa mediassa.

Twitteriin luotiin tuhansia valetilejä ja botteja, jotka levittivät konservatiivista sanomaa, tukivat ehdokas Trumpia ja yllyttivät eri ihmisryhmiä toisiaan vastaan. IRA:aa kutsuttiin ”trollifarmiksi”, ja se oli tunnettu valeuutisten levittäjä. IRA:lla oli yhteyksiä Kremliin, ja koko kampanjan tarkoituksena oli vaikuttaa äänestämiseen – joko saamalla ihmiset äänestämään tiettyä ehdokasta, tai olla äänestämättä ollenkaan. Kampanjan alkuperäismaa peitettiin käyttämällä VPN (Virtual Private Network)-sovelluksia. (Lee 2018.)

2.1 Facebook

Verkkojättiläinen Facebook on ylläpitänyt asemaansa maailman suosituimpana sosiaalisena mediana jo yli kymmenen vuoden ajan. Se on tuttu sivusto useimmille ihmisille, ja lause ”Oletko Facebookissa?” on nykyään yhtä normaali kuin puhelinnumeron kysyminen. Työnantajat etsivät työhaastatteluun tulevia Facebookista, ja saattavat pitää profiilin puuttumista outona tai jopa epäilyttävänä. Sivun kautta voidaan löytää entisiä luokka- ja työkavereita, kaukaisia sukulaisia, uusia ja vanhoja ystäviä, parisuhteita, yhteisöjä ja harrastuksia, ja paljon muuta. Sivun perusideana

on kirjoittaa ja jakaa julkaisuja omasta elämästään. Se voi olla hyvä työkalu yhteydenpitoon henkilöiden kanssa, jotka asuvat kaukana. Ei olekaan ihme, että Facebook on saavuttanut suuren suosion miltei ensihetkiltä alkaen. Noin 1/3 maailman asukkaista käyttää Facebookia, joten kyseessä on todellakin maailmanlaajuinen ilmiö. (Clement 2020c.)

Facebook sai alkunsa vuonna 2004 Bostonissa, Harvardin yliopistossa. Se perustettiin helmikuussa oppilas Mark Zuckerbergin toimesta, ja rahoitettiin aluksi toisen Harvard-oppilaan, brasilialaisen Eduardo Saverinin avulla. Kolmas oppilas, Dustin Moskowitz, värvättiin mukaan hieman myöhemmin. Zuckerbergillä oli entuudestaan kokemusta tietoverkostosivujen luomisesta. Coursematchissa oppilas pystyi etsiä ja ottaa yhteyttä muihin oppilaihin, jotka opiskelivat samaa ainetta. Toinen sivusto, Facemash, oli tarkoitettu muiden henkilöiden viehättävyyden arvioimiseen.

Aluksi Facebook tunnettiin nimellä ”The facebook”, ja se oli tarkoitettu ainoastaan Harvardin oppilaille. Se mahdollisti omien profiilien luomisen ja jakamisen verkossa. Sivusta tuli lyhyessä ajassa hitti. Vain 24 tunnin sisällä sivulle oli rekisteröitynyt 1200 oppilasta, ja kuukauden kuluttua yli puolet olivat luoneet profiilin. Suuren kysynnän myötä sivu laajeni nopeasti. Muut Bostonin yliopistot liittyivät Facebookiin hieman sen jälkeen, ja yliopistot kautta maan seurasivat perässä. Vuonna 2005 Facebook saatiin käyttöön yläaste- ja lukiokoulutuksissa (engl. high school), ja vuotta myöhemmin kaikille yli 13-vuotiaille. Samana vuonna Zuckerberg osti nykyään tunnetun osoitteen facebook.com (Carlson 2012; Phillips 2007). Alunperin yläkouluille tarkoitettu sivusto oli nyt vapaasti kaikkien käytettävissä, ja vuoden 2006 loppupuoliskolla sivulla oli jo 12 miljoonaa käyttäjää. (Albarran 2013, 36.)

Facebookin luojien keskelle oli kuitenkin syntynyt kitkaa. Saverin, Facebookin aikainen rahoittaja, joutui epäsuosioon Zuckerbergin silmissä. Saverin oli laittanut Facebookiin mainoksia ilman Zuckerbergin lupaa, mutta asiaa pahensi se, että näissä mainostettiin Saverinin omaa työnhakusivustoa, Joboozlea. Tämä koettiin luottamuksen rikkomisena, koska Facebookille kaavailtiin samantyyppistä työnhakutoimintoa.

Ratkaiseva asia Saverinin erottamisessa johtui taloudellisista asioista. Facebook oli kasvanut nopeasti ja tarvitsi lisää rahoitusta, mutta Saverin viivytteli tärkeissä asioissa, kuten muiden perustajien luo muuttamisessa, tärkeiden papereiden allekirjoittamisessa ja yhtiösuunnitelmien luomisessa. Erilaisia liiketoiminnallisia porsaanreikiä ja ”likaisia temppuja” käyttäen Zuckerberg osti vaivihkaa Saverinin ulos yhtiöstä. Tästä seurasi liuta kanteita, jotka lopulta ratkaistiin. Facebook oli aiemmin kieltänyt Saverinin osuuden sivun perustamisessa, mutta listasi hänet nyt virallisena Facebookin perustajana. Osana tuomioistuimen päättämässä ratkaisussa Saverin puolestaan suostui olemaan puhumatta medialle. Facebookin ansiosta Saverin on nykyään miljardööri ja asuu Singaporessa. (Carlson 2012.)

Zuckerberg ja Facebook joutuivat oikeuteen toisenkin kerran. Veljekset Cameron ja Tyler Winklevoss sekä Divya Narendra syyttivät Zuckerbergia heidän oman sosiaalisen median alustansa kopioimisesta. Zuckerberg oli työskennellyt heidän alaisuudessaan ConnectU -sivuston parissa ennen Facebookin luomista, ja kolmikko haastoi Zuckerbergin oikeuteen. Muodollisuuden takia tapaukseen ei saatu ratkaisua oikeudessa, ja Winklevossit ja Narendra sopivat noin 65 miljoonan dollarin arvoisesta hyvityksestä. (Phillips 2007; Arthur 2011.)

Winklevossin kaksoset sijoittivat oikeudessa voittamansa rahat Bitcoiniin, vuonna 2008 perustettuun kryptovaluuttaan, ja heistä tuli maailman ensimmäiset Bitcoin-miljardöörit (Berr 2017). He työskentelevät vieläkin Bitcoinin ja kryptovaluutan parissa, Gemini-nimisen yhtiön kanssa. Facebook on myös suunnittelemassa omaa kryptovaluuttaansa, Libraa, ja Winklevossien mukaan yhteistyö Geminin ja Libran välillä on mahdollista. (Duffy 2019.)

2.2 Twitter

Twitter on internetin eniten käytetty niin kutsuttu mikroblogipalvelu. Sen perusidea on merkkirajoitettujen päivitysten julkaisu, jakaminen ja kommentointi. Mikrobloggaus yhdistää tavallisen bloggaamisen pikaviestintään. Toisin kuin tavallisissa blogeissa (esim. Livejournal, Wordpress), mikroblogien ideana on pitää julkaisut lyhyinä ja ytimekkäinä. Ne voivat koostua kirjoitetusta tekstistä, kuvista, linkeistä, videoklipeistä, äänitiedostoista tai lainauksista. ”Kirjoita lyhyesti, mutta

usein” voisi olla helppo tapa kuvailla Twitterin perusideaa. Blogipalvelu Tumblr sekä Instagram lasketaan myös mikroblogeiksi. (Nations 2019.)

Tämä käytäntö muistuttaa Facebookia, mutta Twitter eroaa suuresta sukulaisestaan siinä, että Twitterissä julkaisujen merkkimäärä on rajattu 280:een. Ennen vuotta 2017 suurin sallittu merkkimäärä oli 140, mutta tämä määrä tuplattiin lyhyen testikauden jälkeen. Tapa, jolla ihmiset kommunikoivat internetissä, oli muuttunut hieman Twitterin alkuajoista, ja ”twiittien” pidennys heijasti tätä muutosta. Twitter perusteli päätöstään sillä, että pidemmät twiitit rohkaisisivat käyttäjiä twiittaamaan useammin. Se myös lisäisi kanssakäymistä, eli statusten tykkäämistä, kommentoimista ja jakamista käyttäjien kesken (Tsukayama 2017). Myöhemmin kävi kuitenkin ilmi, että käyttäjien julkaisujen pituudet pysyivät melko samoina verrattuna aiempaan. Vain 1% twiiteistä ylsi 280 merkkiin, ja ainoastaan 12% twiiteistä ylitti 140 merkin rajan. (Perez 2018.)

Vaikka merkkirajan nostaminen sai aikaan vastustusta, ei sillä ollut merkittäviä vaikutuksia Twitterin käyttäjämäärään. Vuonna 2019 käyttäjiä oli maailmanlaajuisesti 330 miljoonaa. Käyttäjämäärä on pysynyt melko tasaisena vuodesta 2015 lähtien. (Clement 2019c.)

Twitter perustettiin maaliskuussa vuonna 2006 kolmen henkilön toimesta – Evan Williams, Christopher ”Biz” Stone ja Jack Dorsey. He työskentelivät Odeossa, Williamsin startup-yrityksessä. Odeo oli suunniteltu podcast-alustaksi, mutta tämä idea ei menestynyt monesta syystä. Odeon luojat testasivat ja kehittivät alustaansa, mutta ymmärsivät etteivät käyttäneetkään podcastia niin paljon kuin olivat luulleet. Suurin vastoinkäyminen oli kuitenkin Applen julkaisema iTunes, joka sisältäisi podcast-toiminnon. He tiesivät, etteivät voisi kilpailla Applen kaltaisen jättiläisen kanssa. Vuosi oli 2005, ja Odeo oli vaikeuksissa. Odeolla oli tähän aikaan 14 työntekijää, ja yrityksen piti löytää uusi suunta.

Työntekijä Jack Dorseylla oli idea tuotteesta, jonka perusajatuksena oli statusten kirjoittaminen ja jakaminen. Toinen työntekijä, Noah Glass, keksi nimen ”Twttr”, josta myöhemmin tulisi Twitter. Glass, Dorsey ja saksalainen Florian Weber alkoivat työstää tätä projektia, ja sen tuloksena Twitter sai syntynsä. Maaliskuussa 2006

heillä oli toimiva prototyyppi, ja tulevien kuukausien aikana Twitteristä kirjoitettiin tekniikkasivustoilla internetissä. Kesällä 2006 San Franciscoon iski maanjäristys, ja Twitteriä käytettiin uutisten ja päivitysten nopeaan levittämiseen. Tämä sai käyttäjät ja IT-yritykset tietoiseksi Twitterin potentiaalista, ja Twitter onkin osoittautunut erinomaiseksi ruohonjuuritason uutislähteeksi. Ei ole harvinaista, että Twitter raportoi uusista tapahtumista nopeammin kuin perinteiset uutiskanavat. (Albarran 2013; Carlson 2011.)

Näin onkin tapahtunut useasti. Twitterillä on tärkeä rooli katastrofien ja onnettomuuksien tiedottamisessa. Ihmiset paikan päällä voivat kertoa tilanteen kehittymisestä alusta alkaen, toisin kuin esimerkiksi toimittajat, jotka joutuvat joko matkaamaan sinne tai etsiä tietoja ennen uutisointia.

Twitter oli yksi ensimmäisistä raportoijista Bostonin maratonin pommihyökkäyksessä vuonna 2013, jossa kuoli kolme ihmistä ja satoja loukkaantui. Kaoottisesta tilanteesta saatiin ajankohtaista ja reaaliaikaista tietoa paikan päältä, mistä oli apua sekä siviileille, että virkavallalle ja pelastusryhmille.

Notre Damen katedraalin tulipaloa vuonna 2019 pystyttiin seuraamaan livenä Twitterissä. Twitter-tilien suoratoistovideoiden avulla maailma sai nähdä historiallisen rakennuksen osittaisen tuhon, mikä sai aikaan suuren sympatiavyöryn ympäri maailman. (Cresci 2016.)

Moni julkinen henkilö kuuluu nykyään Twitteriin. Muun muassa poliitikoilla, presidenteillä, näyttelijöillä, kirjailijoilla ja YouTube-persoonilla on omat tilinsä, joita käytetään mielipiteiden, uutisten ja muun sisällön kirjoittamiseen. Viralliset tilit erotetaan fani- ja feikkitileistä sinisellä pukkimerkillä.

Eräs kohutuimmista virallisista Twitter-tileistä kuuluu Yhdysvaltain nykyiselle presidentille, Donald Trumpille. Hän on ahkera Twitterin käyttäjä, ja hänen twiittinsä ovat aika ajoin aiheuttaneet konflikteja ja jopa poliittisia vaaratilanteita. Vuoden 2020 alussa Yhdysvallan armeija surmasi Iranin kenraalin Qasem Soleimanin pommi-iskussa. Presidentti Trump ilmoitti Twitterissä, että Iranin mahdollisiin kostoiskuihin vastattaisiin vahvasti ja suhteettomasti. Tämä twiitti oli myös suunnattu

Yhdysvaltain kongressille, jolle ei oltu ilmoitettu presidentin aikeista virallisesti tai erikseen. Twiitti oli poliittisesti herkkäluonteinen ja maailma on yleisesti pitänyt Yhdysvaltain presidentin käyttäytymistä Twitterissä sopimattomana ja riskialttiina. (Rupar 2020.)

Tämä piti paikkansa myös koronapandemian kohdalla. Twitterissä Trump vähätteli koronaviruksen vakavuutta, ja väitti median lietsovan paniikkia. Lausunnoillaan Twitterissä ja muilla alustoilla Trumpin on sanottu sabotoivan tiedemiesten ja asiantuntijoiden uskottavuutta, ja sosiaalisen median maailmassa tällaiset ideat voivat nopeasti saada kannattajia. (Stelter 2020.)

2.3 YouTube

Suosittu videosivusto YouTube perustettiin vuonna 2005 kolmen entisen PayPal-työntekijöiden toimesta. Steve Chen, Chad Hurley ja Jawed Karim kehittivät idean verkossa toimivasta videopalvelusta vuoden 2005 alkupuoliskolla. Ajatus syntyi kahdesta vuoden 2004 tapahtumasta – Janet Jacksonin vaatetusvahingosta Yhdysvaltain Super Bowl-urheilutapahtumassa, sekä Intian valtameren tsunamista. Karim ymmärsi videokuvan tärkeyden tällaisissa tilanteissa, ja ajatus YouTuben kaltaisesta palvelusta sai syntynsä.

Hurley rekisteröi YouTuben verkkotunnuksen, logon ja tavaramerkin helmikuussa 2005, ja sivuston betaversio julkaistiin saman vuoden toukokuussa. Karim julkaisi YouTuben ensimmäisen videon. Sen nimi oli ”Me at the Zoo” (”minä eläintarhassa”), ja se on vieläkin nähtävissä.

Marraskuussa 2005 YouTube sai 3,5 miljoonan dollarin rahoituksen Sequoia Capital-yritykseltä, minkä ansiosta YouTube paransi servereitään ja kaistanleveyksiään. YouTuben betavaihe päättyi, ja sivusto julkaistiin virallisesti 15. joulukuuta 2005.

YouTube tuli yhä suositummaksi. Yhdysvaltalainen televisioyhtiö NBC oli yksi ensimmäisistä suurista mediayhtiöistä, joka ryhtyi yhteistyöhön YouTuben kanssa. Yhteistyösopimuksen takana oli tekijänoikeuskiista. NBC-sarjan videoklippi oli saanut osakseen suosiota YouTubessa, mutta NBC vaati YouTubea poistamaan videon tekijänoikeusrikkomuksen vuoksi. Tämän seurauksena YouTube loi

sisällönvahvistusohjelman, jonka kautta yritykset ja muut tahot voivat ilmiantaa tekijänoikeuksia rikkovia videoita.

Verkkojätti Google pani merkille YouTuben potentiaalin, ja osti yhtiön vuonna 2006 1,65 miljardilla dollarilla. Google kuvaili YouTubea seuraavasti: ”seuraava askel internetin evoluutiossa.” Ottaen huomioon YouTuben nykyisen roolin maailmassa, voidaan sanoa, että Google oli oikeassa. (Dickey 2013.) Time-lehden vuoden henkilö vuonna 2006 oli ”Sinä” - eli jokainen YouTuben käyttäjä, joka luo sisältöä sivustolle (Ricke 2014, 15).

YouTubesta on tullut suuri tekijä politiikassa, varsinkin Yhdysvalloissa. Eri poliittiset ryhmät pääsevät helposti jakamaan sanomaansa massoille sivuston kautta. YouTuben interaktiivinen toimintaperiaate edesauttaa aatteiden ja ajatusten kehitystä ja jakamista. YouTuben kautta on helpompaa kommunikoida ja olla yhteydessä mahdollisiin äänestäjiin, mikä on houkuttelevaa politiikkaan pyrkiville henkilöille.

Videoklippien nopealla leviämisellä on toinenkin puoli. Mahdolliset poliittiset kömmähdykset ja virheet leviävät yhtä nopeasti, elleivät nopeammin kuin ”viralliset” videot. Aikainen esimerkki tästä ilmiöstä tapahtui vuonna 2006 Yhdysvalloissa. Senaattori George Allen Virginian osavaltiosta saatiin taltioitua videolla tämän kutsuessa intialaisperäistä miestä rasisminsävytteisellä nimellä. Mies julkaisi videopätkän YouTubessa, ja siitä tuli nopeasti suosittu. Se aiheutti suurta poliittista kohua ja vahingoitti Allenin poliittista kampanjaa. Tapaus sai ihmiset kiinnostumaan vaaleista enemmän kuin normaalisti, ja äänestysprosentti nousi 14,6% verrattuna aiempiin vaaleihin. Allen hävisi vaaleissa sinä vuonna, sekä uudelleen vuonna 2012. Virheiden täydellinen poistaminen internetistä on hyvin vaikeaa. (Ricke 2014, 17.)

Kuten muut sosiaaliset mediat, YouTube mahdollistaa nopeiden vastausten ja reaktioiden julkaisun suurille ryhmille. Tästä on hyötyä julkisuuden henkilöille, yrityksille ja virallisille tahoille. Ennen internetin aikakautta jouduttiin useimmiten odottamaan seuraavan päivän uutislehteä ennen päivitystä tai vastausta ajankohtaiseen tapahtumaan. YouTube on luonut vuorovaikutteisemman toimintatavan

nykymaailmaan. Nykyään kaikilla suurilla mediayhtiöillä on myös oma YouTube-profiili, ja sen puuttumista voidaan pitää poikkeuksena.

2.4 Instagram

Instagram on maailman suosituin valokuvasovellus. Se on saatavina älypuhelinsovelluksena sekä Vuonna 2018 se rikkoi yhden miljardin käyttäjärajan, ja päivittäin aktiivisia käyttäjiä oli 500 miljoonaa. Kevin Systrom ja Mike Krieger perustivat sivun vuonna 2010, ja siitä tuli nopeasti hitti. (Clement 2019d.)

Instagram sai alkunsa Systromin mielenkiinnosta valokuvaukseen. Hän opiskeli insinööriksi Stanfordin yliopistossa, mutta vietti yhden lukukauden Italian Firenzessä opiskellen valokuvaamista. Siellä hän käytti vanhanaikaista kameraa, jolla sai otettua vintage-tyylisiä kuvia. Tämä toimi myöhemmin inspiraationa Instagramin ikonisille kuvasuodattimille (engl. *filter*).

Systrom oli työharjoittelussa podcastyhtiö Odeossa, jossa Twitterin tulevat perustajat Evan Williams ja Jack Dorsey työskentelivät. Hän liikkui samoissa piireissä kuin monet nykyään tunnetut henkilöt, kuten Facebookin perustaja Mark Zuckerberg. Tämä tarjosi aikaisessa vaiheessa Systromille työpaikkaa Facebookissa, mutta Systrom kieltäytyi tarjouksesta. Hän oli vielä collegessa ja halusi suorittaa opintonsa loppuun.

Opintojensa jälkeen Systrom palkattiin Googlen työntekijäksi. Näihin aikoihin hän kehitti oman sovelluksensa nimeltä Burbn. Siinä yhdistyivät paikallinen verkostoituminen ja valokuvaus, ja sovellus kiinnitti muutaman investoijan huomion. Burbnille myönnettiin puolen miljoonan dollarin rahoitus. Mike Krieger liittyi yhtiöön, ja yhdessä hän ja Systrom kehittivät sovelluksen perusideaa. He päätyivät rajaamaan sovelluksen pääpainon valokuvaamiseen, karsien muut ylimääräiset toiminnot. Instagramille ominaiset suodattimet saivat alkunsa Systromin ja tämän vaimon keskustelusta, jolloin mietittiin miten saada heidän sovelluksensa erottumaan joukosta. Ensimmäinen suodatin oli nimeltään X-Pro II, ja se on vieläkin käytössä. (Hartmans 2020.)

3 YKSITYISYYS SOSIAALISESSA MEDIASSA

Yksityisyys sosiaalisessa mediassa on aihe, joka on jatkuvasti ajankohtainen. Tutkimukset osoittavat, että huoli omasta yksityisyydestä verkossa on kasvanut. Vuonna 2019 julkaistu tutkimus kertoo, että 53% maailman internetkäyttäjistä on enemmän huolissaan verkkoyksityisyydestä verrattuna edelliseen vuoteen. Suurin kasvu oli tapahtunut Nigeriassa, jossa luku oli 82%. Saksalaiset olivat vähiten huolissaan – ainoastaan 26% väestöstä ilmaisi huolensa verkkoyksityisyydestään kasvaneen. Suomi ei ollut mukana tässä tutkinnassa, mutta Ruotsissa luku oli 36%. Voitaneen olettaa, että suomalaiset ovat jokseenkin samalla kannalla kuin Ruotsi. (Clement 2019.)

Toukokuussa 2018 EU:ssa astui voimaan uudet tietosuoja-asetukset. General Data Protection Regulation (yleinen tietosuoja-asetus), eli GDPR, oli uusi laki, joka sääteli EU:n kansalaisten henkilötietojen käsittelyä. Se yhtenäisti Euroopan unionin maiden tietosuojalait, ja antoi kansalaisille enemmän tietosuojaa internetissä.

Lisäksi se antoi henkilölle paremmat mahdollisuudet hallinnoida omia henkilötietojaan. Henkilötiedoilla tarkoitetaan muun muassa nimiä, osoitetta, potilastietoja, puhelinnumeroa, auton rekisterinumeroa ja paikannustietoja. GDPR takaa EU:n kansalaiselle oikeuden tietää, mitä henkilötietoja organisaatiolla hänestä on, sekä oikeuden muuttaa tai vastustaa tietojen käsittelyä. Lisäksi kansalaisella on oikeus tietää mihin ja miten näitä henkilötietoja käytetään. Järjestön on pyydettäessä toimitettava nämä tiedot kysyjälle. (Findwise 2020.)

GDPR:n tavoitteena oli lisäksi vastata digitaalisen ja globalisoituneen nykymaailman tietoturvahaasteisiin. Laki päivitti mahdolliset vanhentuneet lait, ja toi EU:n tietosuojasäännökset nykypäivään. Suomessa GDPR kumosi sitä edeltävän henkilötietodirektiivin. (Liikenne- ja viestintävirasto 2020a; Tietosuojavaltuutetun toimisto 2020.)

3.1 Evästeet

Evästeet (engl. *cookie*) ovat yleisiä internetissä, ja niitä käyttävät useimmat verkkosivustot. Evästeet ovat pieniä tekstitiedostoja, jotka tallennetaan käyttäjän laitteelle internetselaimen toimesta. Evästeet tallentavat käyttäjän eri tietoja tämän siirtyessä sivulta toiselle. Tallennettavat tiedot voivat olla esimerkiksi henkilön selaintyyppi, IP-osoite, kellonaika, minkä sivun tai palvelun kautta henkilö on tullut sivulle, sekä henkilön selainhistoria.

Evästeiden käyttö vaatii käyttäjän suostumuksen. Sivuston tulee kertoa evästeiden käyttötarkoituksesta, tallentamisesta ja toiminta-ajasta selkeästi ja kattavasti. Lisäksi pitää tulla ilmi saavatko kolmannet osapuolet käyttää evästeiden tallentamia tietoja. Evästeiden käyttö vaatii käyttäjän luvan. Suomessa sivujen ei tarvitse ilmoittaa evästekäytöstään ponnahdusikkunalla.

Evästeistä on olemassa useita eri tyyppejä. Istuntokohtaiset evästeet (engl. *session cookie*) ovat toiminnassa ainoastaan henkilön aktiivisesti käyttäessä verkkosivua. Istunnon jälkeen tämä eväste katoaa. Pysyvät evästeet (engl. *stored cookie*) säilyvät istunnon jälkeenkin ja tallentuvat laitteelle pysyvästi. Jos ne halutaan poistaa, pitää se tehdä manuaalisesti.

Evästeet eivät itsessään ole haitallisia. Niistä on usein hyötyä – esimerkiksi verkkokauppaa selatessa evästeet säilyttävät kauppakorin sisällön, vaikka siirtyisikin pois kauppakorisivulta. Evästeet säilyttävät myös sijainnin sääsivustoja varten, minkä ansiosta paikkakuntaa ei tarvitse syöttää joka kerta uudelleen. (Liikenne- ja viestintävirasto 2020b; Norton LifeLock 2020.)

3.2 Kolmannet osapuolet

Kolmannella osapuolella tarkoitetaan tahoa, joka ei ole käyttäjä tai palvelun tarjoaja, mutta joka kuitenkin on osa palvelua. Tavallinen esimerkki tällaisesta kolmannesta osapuolesta on Facebookin pelisovellukset. Pelien kehittäjät ovat usein Facebookin ulkopuolisia tahoja, jotka ovat Facebookin palkkalistoilla. Pelisovelluksilla on usein pääsy tiettyihin käyttäjän tietoihin, kuten tämän ystävälistalle. Pelit

kuten Farmville on tarkoitettu sosiaalisiksi peleiksi, joita voidaan pelata Facebook-ystävien kanssa.

Monet verkkosivustot käyttävät integroitua Facebook-ominaisuutta – sivulla voi esimerkiksi kommentoida tai tykätä julkaisusta omalla Facebook-profiilillaan. Verkkosivu on täten kolmas osapuoli, ja Facebookin käytäntöjen mukaan sivusto saa pääsyn julkiselle Facebook-profiilille, sekä tietoja käyttäjän kommentti-/aktiivisuushistoriasta. Myös ystävälistat kuuluvat kolmansien osapuolien keräämiin tietoihin. Kolmannet osapuolet saavat itse päättää, mitä ja miten näitä tietoja käsitellään, eivätkä Facebookin omat tietosuojakäytännöt päde heihin. (Facebook 2020a.)

Facebook kerää yhteistyökumppaniensa ja kolmansien osapuolien kautta tietoa käyttäjän toimista Facebookin ulkopuolella. Esimerkkejä kerättävistä tiedoista ovat esimerkiksi tietoa käyttäjän laitteesta, verkko-ostoksista, selaushistoriasta ja palvelujen käyttötavasta. Näitä tietoja kerätään riippumatta siitä, onko henkilö kirjautunut sisään Facebookiin, tai jos hänellä edes on Facebook-tiliä. (Facebook 2020b.)

Kolmannet osapuolet Twitterissä ovat yhtiön ulkopuolisia kehittäjiä, eikä Twitter omista tai operoi niitä. Sovelluksessa tai verkkosivulla voi löytyä vaihtoehtoina kirjautua tai yhdistää Twitteriin, ja käyttämällä näitä kolmannen osapuolen sovelluksia henkilö hyväksyy sovelluksen käyttöehdot. Käyttöehdot antavat joskus luvan melko mittaviin tietojen keräyksiin. Sovellus voi esimerkiksi lukea twiittejä, kerätä sähköpostiosoitteen ja ystävälistan, muokata profiilia, nähdä yksityisviestit ja jopa twiitata käyttäjän puolesta. Kolmannen osapuolen sovellus voi toisin sanoen toimia oikean käyttäjän tavoin hallinnoimalla ja olemalla vuorovaikutuksessa muiden käyttäjien ja twiittien kanssa. (Twitter 2020a.)

3.3 Ohjelmointirajapinta

API (*Application Programming Interface*), suomeksi ohjelmointirajapinta, on ryhmä toimintoja, käskyjä ja protokollia, joilla ohjelmoija voi luoda ohjelmia tai kommunikoida ulkoisen järjestelmän kanssa. Esimerkiksi käyttöjärjestelmä Windowsin rajapintaan kuuluvat dialogi-ikkunat, vierityspalkit ja ikkunat. (TechTerms 2020.) API määrittelee tavat, jolla ohjelmisto tarjoaa tietoja tai palveluita

käyttöjärjestelmille ja sovelluksille. Ohjelmointirajapintaa voi kutsua välikädeksi, jonka avulla sovellukset voivat kommunikoida keskenään.

Tavallinen esimerkki API:n toiminnasta löytyy vertailuverkkosivuilta – sivuilta, jotka kokoavat ja vertaavat tietyn palvelun tai tuotteen. Käyttäjä haluaa ehkä vertailla eri lentoyhtiöiden hintoja keskenään, joten hän käyttää matkahakukonetta. Tämä hakukone hyödyntää lentoyhtiöiden ohjelmointirajapintaa hakeakseen ja esitelläkseen lippuhinnat ja matkatiedot.

API:a voi verrata ravintolan tarjoilijaan, joka kuljettaa asiakkaan tilaaman tuotteen (datan) asiakkaan ja keittiön (palvelimen) välillä.

Rajapinnat ovat jaettavissa kahteen tyyppiin – datarajapintaan ja toiminnalliseen rajapintaan. Datarajapinta on rajoitettu pelkkään datan lukemiseen toisiin järjestelmiin, kun taas toiminnallisessa rajapinnassa järjestelmän tietoja voidaan muuttaa rajapinnan kautta. (MuleSoft 2020; Poikola, Kivekäs & Kettunen 2014.)

Sosiaaliset mediat käyttävät tietorajapintoja muun muassa ulkopuolisten sovelluksien integroimiseen. Sovelluksen kehittäjä lähettää hakemuksen Twitterille päästäkseen käyttämään Twitterin API:a. Oletuskohtaisesti sovelluksilla on ainoastaan pääsy julkisiin Twitter-tietoihin, ja vaatii Twitter-käyttäjän suostumuksen päästäkseen käyttämään yksityisviestitoimintoa. Käyttäjä voi säädellä sovelluksien käyttöoikeuksia oman tilinsä asetuksista. (Twitter 2020b.)

Facebook, Instagram ja YouTube käyttävät API:a samankaltaisesti. Ulkopuoliset sovellukset vaativat käyttäjän suostumuksen moniin toimintoihin, kuten tilannepäivitysten julkaisuun Facebookissa. Facebookilla onkin laajat säännöt ulkopuolisten sovelluksien luojille. Ne koskevat kaikkea sovelluksen laadusta ja käyttäjien antamasta arvosanasta tietojen keräämiseen. Sovellusten kehittäjät sitoutuvat noudattamaan yli 100 Facebookin säännöstä. (Facebook 2020c.)

Googlen omistamalla YouTubella on tarkat säännöt ohjelmointirajapintoihin liittyen. Käyttäjän henkilökohtaisia tietoja, kuten nimiä, yhteystietoja, uskontoa ja poliittisia näkemyksiä ei saa kerätä ilman käyttäjän suostumusta. Käyttäjän tietoja ei saa tallentaa loputtomasti, ja tiedot tulee poistaa käyttäjän pyynnöstä. Käyttäjän

tulee myös helposti päästä käsiksi ja hallinnoida sovelluksen keräämää dataa. Tietoja ei myöskään saa myydä kolmansille osapuolille. (Google 2020a.)

Monia käyttäjän tietoja voidaan kuitenkin kerätä, jos henkilö antaa siihen suostumuksensa. Tämän vuoksi käyttäjän tulisi perehtyä käyttöehtoihin ennen ”hyväksy”-napin painamista.

3.4 Sijaintitiedot

Sijaintitietoja käytetään useassa eri teknologiassa. Se on puhelimen tai muun mobiililaitteen asetus, joka kerää tietoja laitteen sijainnista muun muassa GPS:n, puhelinmastojen tai julkisten WiFi-verkkojen kautta. Niiden avulla verkkosivu tai palvelu voi tarjota käyttäjälle lähellä sijaitsevia tuotteita, nähtävyyksiä, kauppoja ja muita kohteita. Tilastokeskus määrittelee sijaintitiedon seuraavasti: ”...paikkatietokohteen sijaintia, geometriaa tai topologiaa kuvaileva ominaisuus. Sijaintitieto ilmoitetaan koordinaatteina, osoitteena, paikkakuntana tai muuna tunnettuna kohteena” (Tilastokeskus 2020).

Useimmat sosiaaliset mediat hyödyntävät sijaintitietoja mobiilisovelluksissaan. Facebookissa monet toiminnot perustuvat sijaintitietojen käyttämiseen. Julkaisut, jotka sisältävät merkinnän käyttäjän sijainnista sekä lähellä olevien kaverien löytäminen kuuluvat näihin toimintoihin. Sijaintipalvelulla henkilö voi löytää läheisiä WiFi-verkkoja tai paikkoja, joiden uskotaan kiinnostavan kyseistä käyttäjää. Facebook käyttää myös asiakkaidensa sijaintitietoja luodakseen tarkennettuja mainoksia. Toinen tärkeä toiminto on taustasijainti. Se sallii sovelluksen käyttävän laitteen tarkkaa sijaintia, vaikka henkilö ei käyttäisi Facebookia sillä hetkellä. Taustasijainti tulee olla aktivoituna, jos käyttäjä haluaa hyödyntää muutamia mobiilisovelluksen keskeisiä ominaisuuksia, kuten lähellä olevien kavereiden tai WiFi-verkkojen löytämistä.

Käyttäjän sijaintitiedot kootaan Facebook-sovelluksen sijaintihistoriaan. Se on kokoelma henkilön tarkoista sijaintitiedoista, jotka on kerätty sijaintitietojen ja taustasijainnin kautta. Sijaintihistoriaan kerääntyy tietoja myös muilla tavoilla, kuten tapahtumakutsujen vastauksista, kuvien sijaintimerkinnöistä ja henkilön julkaisujen

paikkamerkinnöistä. Sijaintihistorian tietojen perusteella Facebook räätälöi ehdotuksiaan ja mainoksiaan. Sijaintihistorian voi tyhjentää, ja se näkyy ainoastaan käyttäjälle. (Facebook 2020d.)

Facebook omistaa Instagramin, joten tämän sijaintikäytännöt ovat laajalti samoja kuin Facebookilla. Instagram kerää monenlaisia tietoja käyttäjästä ja tämän laitteesta. Näihin tietoihin kuuluu muun muassa henkilön julkaisemat valokuvat, videot ja muu sisältö, henkilön sosiaalinen kanssakäyminen Instagramissa (mihin ryhmiin hän kuuluu, kenen kanssa hän kommunikoi), mobiililaitteen tai tietokoneen tekniset tiedot, henkilön käyttäytyminen selatessa sisältöä (hiiren liikkeet, onko selainikkuna minimoitu vai ei), sekä luonnollisesti sijaintitietoja.

Sijaintitietoja kerätään valokuvien ja videoiden metadatasta. Laitteen GPS-koordinaatit, valokuvien sijainnit ja päivämäärät kuuluvat näihin tietoihin. Instagram saa myös tietoja käyttäjän laitteen lähellä olevista puhelinmastoista ja WiFi-verkoista. (Instagram 2020a.)

Twitterissä käyttäjä voi lisätä sijaintitiedon twiitteihinsä. Tämä asetus kytketään päälle erikseen, ja oletusarvoisesti sijaintitietoja ei liitetä twiitteihin. Tarkan sijainnin salliminen antaa Twitterille luvan kerätä, tallentaa ja käyttää laitteen GPS- ja muita sijaintitietoja. Sijaintitietoja voi kerätä myös pöytäkoneen selaintiedoista, jolloin käyttäjän kotiosoitteen voi saada selville. Tämä tulee pitää mielessä twiittejä julkaistaessa.

Sijaintitietoja on kahdenlaisia – yleisiä (esim. kaupungin nimi tai kaupunginosa) ja tarkkoja tietoja, joihin liitetään kaupungin nimen lisäksi tarkat GPS-tiedot. GPS-tietoja voidaan ainoastaan lisätä mobiililaitteella. GPS-tietojen, eli geologisen leveys- ja pituuspiirin käyttäminen voi olla avuksi julkisten tapahtumien tai hyödyllisen infon jakamisessa. Kuten aiemmin todettiin, Twitter on usein nopeampi uutisten välittäjä kuin perinteiset mediat, ja esimerkiksi onnettomuuspaikan tarkan sijainnin jakaminen voi olla avuksi sekä lähellä oleville, että pelastushenkilöstölle.

Twitter käyttää hyväksi kolmansia osapuolia joidenkin sijaintitietojen yhteydessä. Sijaintiteknologiaan erikoistunut yhdysvaltalainen yhtiö Foursquare tarjoaa tietoja

muun muassa maamerkeistä, yrityksistä ja muista tunnetuista paikoista, joita voidaan käyttää Twitterin sijaintimerkinnöissä. (Twitter 2020c.)

Googlen omistama YouTube seuraa emoyhtiönsä tiedonkeräyskäytäntöjä. YouTube kerää käyttäjän sijaintitietoja laajalti samoilla tavoilla kuin muut sosiaaliset mediat. Yhtiö tallentaa ja käyttää GPS-koordinaatteja, IP-osoitteita, lähellä sijaitsevia WiFi-pisteitä ja puhelinmastoja saadakseen selville henkilön sijainnin. IP-osoitteet määrittyvät maan mukaan, joten käyttäjän maan voi usein päätellä tämän IP-numerosarjasta.

Googlen palvelut keräävät myös dataa mobiililaitteen anturitiedoista – kiihtyvyysmittarista ja gyroskoopista. Näistä voidaan päätellä henkilön matkasuunta, nopeus (matkustustapa) sekä sijainti. (Google 2020b.)

Suurin osa yrityksistä käyttää kuluttajan sijaintitietoja räätälöidäkseen mainoksensa ja tuotteensa henkilölle sopivaksi. Niillä voidaan muokata internetkäyttäjän näkemää sisältöä Facebookin ja Twitterin aikajanoilla ja näyttää lähellä sijaitsevia tapahtumia.

4 SUOJAUTUMINEN VERKOSSA

Internetin käyttäjille on saatavilla useita apuvälineitä, jotka auttavat yksityisyyden varjelemisessa ja turvallisuuden ylläpitämisessä. Teknologia kehittyy jatkuvasti. Verkkorikolliset ja turvallisuudesta vastaavat tahot kilpailevat kehityksessä. Jokainen internetin käyttäjä on osa tätä maailmaa, ja jokaisen tulisi tuntea verkkoturvan perusteet. Kyberrikollisuus on osa jokapäiväistä elämää internetissä, ja sitä mukaa kun älykotimme, tietokoneistetut automme ja yhteiskuntamme integroituvat lisää verkkomaailmaan, sitä enemmän mahdollisuuksia rikolliset saavat. Kuluttajan olisi hyödyllistä pysyä ajan tasalla verkkoturvallisuudessa. Turvakeinoina on kaikkea omasta maalaisjärjestä teknisiin sovelluksiin.

Sosiaalisten medioiden käyttäjän tulisi tarkistaa oman tilinsä yksityisyysasetukset säännöllisesti. Internetiä, ja varsinkin sosiaalisia medioita käyttäessä voi olla varsin helppoa unohtaa yksityisyyden varjelemisen perusteet. Facebookiin kirjoitetuista tiedoista ja julkaistuista kuvista voi luoda profiilin henkilöstä, ja saada selville muun muassa tämän täyden nimen, syntymäpäivän, perheenjäsenet, työpaikan ja asuinpaikan. Henkilön statuspäivityksistä voi saada selville tietoa tämän tulevista lomista ja kalliista ostoksista. Murtovarkaat voivat käyttää tätä hyväkseen ja iskeä taloon, jonka omistajat ovat lomalla tai hankkineet uuden, kalliin television.

Facebookissa omat henkilökohtaiset tiedot tulisi pitää yksityisinä, tai pelkästään näkyvillä kavereille. Hyvä nyrkkisääntö on, että jos ei kertoisi tietoja satunnaiselle ohikulkijalle, ei myöskään pitäisi kirjoittaa siitä julkisesti sosiaalisessa mediassa.

Facebookilla on useita apuvälineitä yksityisyyden hallinnoimisessa. Tietosuojatarkistus tarkistaa tärkeimmät yksityisyysasetukset ja pitää käyttäjän ajan tasalla omien asetuksiensa suhteen. Tarkistuksessa tarkistetaan useita asetuksia. Näihin kuuluvat käyttäjän jakaman sisällön näkyvyys (ketkä voivat nähdä sen), profiilitietojen näkyvyys, sekä miten henkilön voi löytää Facebookista ja kenen toimesta. Tiettyä henkilöä voi hakea käyttämällä tämän sähköpostiosoitetta tai

puhelinnumeroa, ja nämä hakumetodit voidaan rajoittaa tai estää. Tässä voidaan myös määrittää, ketkä voivat lähettää kaveripyyntöjä.

Tietosuojatarkistus voi avustaa uuden ja vahvan salasanan luomisessa. Myös sisäänkirjautumishälytyksen voi ottaa käyttöön. Tämä ilmoittaa käyttäjälle, jos tilille kirjaudutaan tunnistamattomasta sijainnista. (Facebook 2020e.)

Instagram-tilin voi asettaa yksityiseksi. Tällöin ainoastaan tilin hyväksytyt seuraajat voivat nähdä käyttäjän julkaiseman sisällön ja vuorovaikutukset toisten käyttäjien kanssa. Kommentit toisten käyttäjien julkisissa kuvissa kuitenkin näkyvät kaikille. Yksityisen tilin kuvat eivät näy hauissa, vaikka käyttäjä olisi lisännyt kuvaan avainsanan (hashtag). Instagramin yksityisyyshallinnointi on suppeampi kuin Facebookin, ja ainoa tapa poistaa seuraaja on estää tämän tili. (Instagram 2020b.)

Twitterin suojausasetukset toimivat pitkälti samalla periaatteella kuin Instagramissa. Oman tilinsä voi asettaa yksityiseksi, jolloin kaikki käyttäjän twiitit ovat suojattuja eivätkä näy henkilöille, jotka eivät ole hyväksyttyjä seuraajia. Näitä suojattuja julkaisuja ei myöskään voi uudelleentwiitata. Kaikki käyttäjän twiitit muuttuvat joko julkisiksi tai suojatuiksi asetuksen muuttamisen myötä, eikä yksittäisten twiittien näkyvyysstatusta voi muuttaa kuten Facebookissa. (Twitter 2020d.)

Toisen käyttäjän voi joko mykistää tai estää. Mykistäminen pelkästään piilottaa mykistetyn käyttäjän twiitit näkyvistä, näyttäen ainoastaan julkaisut, joissa henkilö mainitaan. Mykistäminen ei estä toista käyttäjää seuraamasta tai näkemästä twiittejä, eikä mykistetty käyttäjä voi nähdä tulleensa mykistetyksi. Estetty käyttäjä ei voi nähdä henkilön julkaisuja, ja käyttäjä näkee, että on tullut estetyksi. (Twitter 2020e.)

Rajaamalla omien julkaisujensa ja tietojensa yleisön, sekä harkitsemalla, mitä verkkoon kirjoittaa on hyvä ensiaskel yksityisyyden hallitsemisessa. Mitä vähemmän tietoja henkilöstä voi saada selville yksinkertaisella Google-haulla, sen parempi.

Internetkäyttäjän olisi hyvä pysyä ajan tasalla tietomurroista. Käyttäjänimien, sähköpostiosoitteiden ja salasanojen joutuminen vääriin käsiin voi olla vaaraksi omalle verkkoturvallisuudelle. Vuonna 2019 tietomurto nimeltä ”Collection #1 breach”

tuli ilmi. Yli miljardi eri sähköposti- ja salasanayhdistelmää oli julkaistu MEGA-pilvipalveluun. Tiedot olivat peräisin useilta eri verkkosivuilta ja palveluilta. Tietomurron havaitsi kyberturvallisuuden tutkija Troy Hunt, joka on perustanut palvelun ”Have I Been Pwned” (haveibeenpwned.com). Tämä on verkkosivu, josta voi tarkistaa onko tietty sähköpostiosoite tai salasana vaarantunut tietomurrossa. Vaarantuneen tilin salasana tulisi vaihtaa, ja jos tietty salasana on paljastunut tietomurrossa, ei sitä tulisi enää käyttää millään sivulla.

Vahvan salasanan luominen vaikeuttaa luvatonta pääsyä tilille. Salasanan tulisi olla pitkä, sisältää suuria ja pieniä kirjaimia, numeroita ja symboleita satunnaisessa järjestyksessä. Kuluttajalle on saatavilla sovelluksia, jotka auttavat vahvojen salasanojen luomisessa ja hallinnoimisessa. Nämä luovat eri tileille salasanan, joka tallentuu sovelluksen muistiin ja kirjaa käyttäjän tilille automaattisesti. Google Chrome- ja Mozilla Firefox-selaimilla on sisäänrakennettu salasanojen hallinta. Nämä tallentavat käyttäjän sisäänkirjautumistiedot, ja ehdottavat myös vahvaa salasanaa uuden tilin luomisen yhteydessä.

Salasanojen kirjoittaminen analogiseen muistivihkoon on toinen varteenotettava menetelmä. Se ei ole digitaalisesti hakkeroitavissa, ja murron yhteydessä kohteina ovat yleensä kalliit elektroniikkalaitteet, ei lehtiöt. (Hunt 2019; O'Flaherty 2019.)

Kaksivaiheinen tunnistautuminen (*two-factor authentication* tai *multi-factor authentication*, myös 2FA tai MFA) on tehokas suojauskeino yleisiltä tietosuojariskeiltä, kuten tietojen kalastelulta ja bottihyökkäyksiltä. Kaksivaiheisessa tunnistautumisessa käytetään hyväksi kahta eri suojauskerrointa – käyttäjän omaa salasanaa, sekä tekstiviestitse tai mobiilisovelluksen kautta saatua varmennuskoodia, joka pitää syöttää sivulle sisäänkirjautumisen onnistumiseksi. Tämä menetelmä vaikeuttaa tietomurtoyrityksiä, koska suojaus ei ole täysin digitaalinen. Jos käyttäjä ei halua vastaanottaa varmennuskoodia tekstiviestitse, on saatavilla eri tunnistautumissovelluksia. Googlella ja Microsoftilla on omat sovelluksensa, Google Authenticator ja Microsoft Authenticator. Näiden lisäksi on lukuisia muita, kuten Authy, LastPass ja Duo Mobile.

Google on kehittänyt kehotemenetelmän sisäänkirjautumisessa. Se lähettää varmenteen käyttäjän puhelimelle uuden sisäänkirjautumisen yhteydessä, ja käyttäjä voi sallia tai hylätä pyynnön. Kehote ei vaadi varmennuskoodeja, vaan kehotteen ponnahdusikkuna ilmestyy jokaiselle Google-tilille kirjautuneelle mobiililaitteelle. (Google 2020c.)

Googlen teettämän analyysin mukaan kaksivaiheinen varmennus esti jopa 100% automatisoiduista bottihyökkäyksistä, 96% tiedonurkintayrityksistä ja 76% kohdistetuista haittaohjelmahyökkäyksistä. Laitekohtaiset varmennukset, kuten varmennussovellukset ja Google-kehotteet, olivat turvallisempia kuin SMS-koodit. Näillä menetelmillä yli 90% kohdistetuista haittaohjelmahyökkäyksistä tuli estetyksi. Tiedonurkinnan ja bottihyökkäysten estoprosentit olivat melko samat molemmilla menetelmillä. (Thomas & Moscicki 2019.)

Selaimen laajennukset ja lisäosat voivat antaa käyttäjälle lisää turvaa verkkomaailmassa. Selainten sovelluskaupoissa on laaja valikoima eri sovelluksia eri käyttötarkoituksiin, kosmeettisista muutoksista verkkoturvallisuuteen. Laajennukset luodaan HTML:llä, JavaScrptilla tai CSS:llä, ja ne käyttävät sivun API:a, sekä omaa API-osiota. Tämän ansiosta koodaaja saa lisää vapautta laajennuksen toimintojen suhteen, koska laajennus ei ole riippuvainen pelkästään verkkosivun sallimasta koodista. (Mozilla 2020.)

Mainoksenestäjät (adblocker) ovat suosittu laajennuskategoria. Ne estävät kuva-, teksti- ja videomainokset verkkosivulta, mikä voi nopeuttaa sivun lataamista ja toimintaa. Mainoksenestäjät estävät esimerkiksi YouTuben mainokset keskellä videota.

Mainoksenestäjät antavat käyttäjälle suojakertoimen haittaohjelmia vastaan. Haittaohjelmien piilottaminen mainoksiin, niin kutsuttu ”malvertising” (englannin sanoista *malware* ja *advertising*), on ongelma, joka voi vaivata jopa kunnollisia verkkosivuja. MSN, Yahoo ja London Stock Exchange ovat olleet malvertising-hyökkäysten kohteena. Haitallisen mainoksen klikkaaminen voi aiheuttaa monenlaista vahinkoa. Se voi tartuttaa tietokoneen haittaohjelmilla, vakoiluohjelmilla, troijalaisilla ja viruksilla, joskus käyttäjän huomaamatta. Koneelle saattaa asentua

näppäilytallennin (engl. *keylogger*) – ohjelma, joka tallentaa ja jakaa henkilön näppäinpainallukset. Haitallinen mainos voi johdattaa käyttäjän tiedonurkintasivustolle, joka imitoi esimerkiksi pankin tai kaupan sivua. Tavoitteena on saada henkilö syöttämään pankkitietonsa tai muita tietoja sivustolle, jolloin kyberrikolliset voivat päästä käsiksi uhrin pankkitilille. (Malwarebytes 2020.)

Vuonna 2009 luotu AdBlock -laajennus on yksi suosituimmista mainoksenestäjistä. Se on saatavilla kaikille käytetyimmille selaimille, ja sillä on yli 65 miljoonaa käyttäjää. Laajennus estää häiritsevät ja haitalliset mainokset, mutta sallii tietynlaiset mainokset. Yritys on kuulunut vuodesta 2015 lähtien Acceptable Ads (”hyväksyttävät mainokset”) -ohjelmaan.

Ohjelman päämääränä on luoda tasapaino hyvän verkkomaailman ja mainonnan välille, antaen yrityksille keinon tavoittaa yleisönsä ja lisätä liikevaihtoaan. AdBlock päästää läpi mainokset, jotka sopivat Acceptable Ads:in vaatimuksiin. Mainosten ei tulisi häiritä lukukokemusta, vaan ne tulee sijoittaa sisällön alle, yläpuolelle tai sivulle. Niille on laadittu kokovaatimukset. Sivun ylälaitaan sijoitettu mainos ei saa viedä enemmän kuin 15 % sivun tilasta. Tämä luku on 25 %, jos mainos sijaitsee alempana sivulla. Sivun ylälaidassa olevan mainoksen korkeusrajoitus on 200 pikseliä, sivun reunassa 350 pikseliä leveä, ja sisällön alapuolella korkeusrajoitus on 400 pikseliä. Mainokset tulee myös merkitä selvästi, jotta käyttäjä tunnistaa ne mainoksiksi. Suurimmat yritykset maksavat saadakseen mainoksensa näkyville Acceptable Adsin kautta, kun taas pieniltä ja keskisuurilta yrityksiltä ei peritä maksua. (AdBlock 2019; Acceptable Ads 2020.)

AdBlock Plus on toinen suosittu mainoksenestäjä. Nimestään huolimatta se on täysin erillään AdBlock-sovelluksesta. AdBlock Plusin ensiversio julkaistiin 2006, ja siitä tuli nopeasti suosittu. Laajennuksen perustaja Wladimir Palant halusi omien sanojensa mukaan ”luoda paremman internetin kaikille, ja huonojen mainosten karsiminen on hyvä ensiaskel.” Palantin päämääränä oli jo vuonna 2007 tehdä mainoksista parempia, eikä niinkään estää kaikkia mainoksia näkymästä. AdBlock Plusin kasvun myötä kehittäjäryhmä palkkasi lisää työntekijöitä, ja he perustivat yrityksen Eyeo vuonna 2011. AdBlock Plus on nykyään Eyeon tuote, ja Eyeo on myös

Acceptable Ads-ohjelman perustaja. Palant kehitti ideaansa hyväksyttävistä mainoksista, ja Acceptable Ads-hanke julkaistiin 2011. AdBlock Plus sallii täten AdBlockin tavoin AA:n vaatimukset täyttävät mainokset. Laajennus on saatavilla kaikille selaimille, sekä PC- että mobiiliversiona.

Eyeon tiedotuspäällikön mukaan sovelluksen nimi hämää käyttäjiä. AdBlock Plus ei ole niinkään mainoksenestäjä, vaan verkkomaailman kustomointityökalu. (Eyeo 2020; Maheshwari 2016.)

Mainosten- ja muun haitallisen sisällön estäjä uBlock Origin ei salli minkäänlaisia mainoksia, eikä kuulu Acceptable Ads-ohjelmaan. Se eroaa täten muista mainostenestäjistä. uBlockia ei lasketa pelkäksi mainostenestäjäksi, sillä se estää myös muita haitallisia toimintoja. Oletuksena uBlock suojaa käyttäjää mainoksilta, seurantapalvelimilta (*tracker*) ja haittaohjelmasivuilta suodatinlistoja käyttäen. Näihin listoihin kuuluvat muun muassa EasyList, EasyPrivacy, Online Malicious URL Blocklist sekä uBlockin omat suodatinlistat. Käyttäjä voi valita RequestPolicy Continued -tilan, jolloin uBlock automaattisesti estää verkkosivun kaikki kolmannen osapuolen pyynnöt. Verkkosivun toimimiseen vaadittavat kolmannet osapuolet voidaan hyväksyä erikseen. (GitHub 2020.)

VPN (Virtual Private Network), suomeksi virtuaalinen erillisverkko, voi antaa lisäturvaa internetin selaajalle. VPN:n perusperiaatteena on luoda erillinen, salattu ”käytävä” internetin käyttäjälle, jonka kautta henkilö voi selata verkkoa, ilman että internet-palveluntarjoaja (Internet Service Provider, eli ISP) näkee henkilön toimet verkossa. Verkkosivut eivät myöskään voi tunnistaa käyttäjän henkilökohtaista IP-osoitetta, ainoastaan VPN-palvelimen IP-osoitteen. VPN-palvelimen IP-osoitteet ovat yleensä useiden henkilöiden käytössä, mikä vaikeuttaa erillisen käyttäjän tunnistamista.

Verkkosivujen näkökannalta käyttäjä sijaitsee fyysisesti siinä maassa, missä VPN-palvelin sijaitsee. Tämän takia VPN-sovellukset ovat suosittuja suoratoistopalveluiden käytössä, kuten Netflixissä. VPN-palvelut voivat antaa käyttäjälle pääsyn muiden maiden elokuva- ja sarjatarjontaan. (Crawford 2020.)

VPN-sovellukset estävät internet-palveluntarjoajaa keräämästä tietoa käyttäjän toimista verkossa, mutta käyttäjän tulisi selvittää, mitä tietoja VPN-palveluntarjoaja mahdollisesti kerää ja tallentaa. Selaustietojen yksityisyys riippuu näistä toimintaperiaatteista. Käyttöehtoihin ja yksityisyyskäytäntöihin tutustuminen on tärkeää ennen VPN-sovelluksen valitsemista. Maksulliset VPN-sovellukset ovat yleisesti ottaen parempia kuin ilmaiset versiot, sekä ominaisuuksien, että luotettavuuden näkökannalta. Ilmaisissa versioissa on usein rajoituksia esimerkiksi nopeuden, datankäytön tai palvelinvaihtoehtojen suhteen. (SafetyDetectives 2020.)

VPN-palveluntarjoajan alkuperämaalla on väliä. Yhdysvaltalaiset yhtiöt ovat maan valvontalakien alaisena, ja varsinkin etsintälupa nimeltä National Security Letters (NSL) voi vaarantaa asiakkaiden yksityisyyden. NSL-etsintäluvan saaneiden yhtiöiden on luovutettava asiakastietonsa sekä muut tarvittavat tiedot, mikä käytännössä tarkoittaa, että yhtiö on muuttunut joukkovalvontatietokannaksi. Yhtiöt eivät myöskään saa ilmoittaa joutuneensa NSL:n kohteeksi. Yhdysvaltalaisia (sekä Englantiin sijoittuvia) VPN-palveluntarjoajia tulee tämän takia välttää. Tunnetut maksulliset VPN-sovellukset, kuten ExpressVPN, NordVPN ja Surfshark toimivat maista, jotka eivät vaadi käyttäjä- tai muun datan keräämistä. Näiden yhtiöiden kotimaat ovat Brittiläiset Neitsytsaaret ja Panama. (ExpressVPN 2020; NordVPN 2020; Privacy Tools 2020; Surfshark 2020.)

VPN-palvelimet tarjoavat lisää vapautta yksittäisille käyttäjille, ja jopa kokonaisille kansoille, joilta on evätty pääsy tietyille sivuille. Esimerkiksi Kiinan hallitus on estänyt kansalaisiltaan pääsyn ulkomaalaisille internetsivustoille, ja VPN-sovellusten vapaa käyttö on kiellettyä. On olemassa luettelo hallituksen hyväksymistä ja hallitsemista VPN-sovelluksista. Luvattoman VPN-sovelluksen käytöstä voi saada 145 dollarin sakot. Tiukoista rajoituksista huolimatta 31% Kiinan kansalaisista käyttää VPN-sovellusta. (Humphries 2019; Marvin 2018.)

VPN-sovelluksista on monta hyötyä. Kaikki data, joka kulkee VPN-palvelimen kautta on salattua, mikä voi suojata käyttäjää hakkereilta. Julkista WiFi-yhteyttä käytettäessä oma yhteys tulisi aina salata VPN:n avulla. Avoimet WiFi-verkot esimerkiksi kahviloissa tai kauppakeskuksissa voivat sisältää tietoturvariskejä.

Käyttäjä ei voi koskaan tietää onko yhteys turvallinen. Kyberrikollinen voi luoda oman avoimen WiFi:n jakamalla yhteydensä, eli luoden hotspotin. Käyttämällä tunnettua tai kaupallista verkkotunnusta (Service Set Identifier, eli SSID) rikollinen voi luoda näennäisesti luotettavan WiFi-yhteyden. Tämän valeyhteyden kautta syötetyt henkilökohtaiset tiedot ja salasanat päätyvät suoraan rikolliselle.

Man-in-the-Middle -hyökkäys (lyhennettynä MiTM), suomeksi välistävetohyökkäys tai väliintulohyökkäys, on toinen vaara avoimissa WiFi-yhteyksissä. Väliintulohyökkäyksessä kolmas osapuoli (rikollinen) puuttuu uhrin ja esimerkiksi pankin väliseen verkkoyhteyteen. Molempien osapuolien data kulkee rikollisen kautta. Uhri ja pankki lähettävät tietämättään datansa rikolliselle. Avoimet WiFi-verkot ovat avoimuutensa takia alttiita tämän kaltaisille hyökkäyksille. Varsinkin lentokentät ovat alttiita WiFi-yhteyshuijauksille suurten ihmismäärien ja verkkoyhteyttä tarvitsevien henkilöiden takia.

VPN-sovelluksen käyttö julkisissa WiFi-verkoissa on hyvin suositeltavaa. Tällöin data kulkee suojatun VPN-käytävän kautta, eivätkä rikolliset tai muut tahot pääse lukemaan sitä. Pääsääntöisesti avoimia WiFi-yhteyksiä tulisi kuitenkin välttää. (Europol 2020.)

5 SOSIAALISEN MEDIAN KYSELYTUTKIMUS

Opinnäytetyön empiirinen osa koostui kyselytutkimuksesta, jolla selvitettiin Vaasan ammattikorkeakoulun opiskelijoiden kokemuksia sosiaalisesta mediasta ja verkon suojauskeinoista. Päämääränä oli lähettää kysely VAMK:in eri alan opiskelijoille, ja vertailla ryhmien välisiä vastauksia.

5.1 Kyselyn suunnittelu

Tämän opinnäytetyön empiiristä osiota varten oli kaksi vaihtoehtoa – laadullinen (kvalitatiivinen) tai määrällinen (kvantitatiivinen) tutkimus. Molemmilla vaihtoehdoilla olisi ollut hyvät puolensa, mutta määrällinen tutkimus sopi paremmin kyselyn tarkoitukseen. Tavoitteena oli saada mahdollisimman monta vastausta ja mahdollisimman paljon dataa, jota analysoida ja vertailla.

Kysely koostui 11 kysymyksestä, mukaan lukien perustietokysymyksistä (mm. sukupuoli ja ikä). Kyselystä ei haluttu tehdä liian pitkää, jotta kysymysten määrä ei karkottaisi mahdollisia vastaajia. Liian pitkä ja monimutkaisen näköinen lomake ei yleensä innosta vastaamaan, ja tätä kyselyä varten haluttiin saada mahdollisimman monta vastaajaa.

Kyselylomake oli jaettu kolmeen osioon – perustietoihin, sosiaaliseen mediaan ja yksityisyyteen ja turvallisuuteen. Joka osio koostui noin kolmesta kysymyksestä, jotka liittyivät osion aiheeseen. Perustiedoissa kysyttiin vastaajan ikää, sukupuolta, hänen aiempaa koulutustasoaan ja sen hetkistä opiskelualaa Vaasan ammattikorkeakoulussa. Opiskelualat oli jaettu liiketalous-, tekniikka- ja sosiaali- ja terveyskategorioihin. Vastausvaihtoehtoihin ei lisätty tarkennettuja opiskelusuuntauksia (esim. sosionomi, ympäristöteknologia, tietojenkäsittely), sillä tämä olisi paisuttanut vastauksia liikaa.

Sosiaalinen media -kategoriassa kysyttiin vastaajan some-tottumuksista. Käyttääkö hän ensinnäkin sosiaalista mediaa? Kuinka tärkeä sosiaalinen media hänelle on, ja kuinka usein hän käyttää sitä? Vastausvaihtoehdoiksi ei annettu tarkkoja lukumääriä (esim. ”viisi kertaa päivässä”), sillä käyttökertojen lukumääriä voisi olla vaikea

arvioida tai muistaa. Sen sijaan vaihtoehtoina oli kuusi valintaa, joista ensimmäinen oli ”jatkuvasti” ja viimeisenä ”en ollenkaan”. Vastaaja sai täten itse arvioida omaa käyttöään. Jokaisella henkilöllä on oma käsityksensä siitä, mitä ”usein” tarkoittaa, joten vastausdata ei ole täten yhtä ”puhdasta” kuin numeroarvioinnilla saatu data. Numeroarvioinnin katsottiin loppujen lopuksi olevan huonompi näistä kahdesta vaihtoehdoista. Sosiaalisen median käyttäjät tarkistavat yleensä tilinsä pitkin päivää älypuhelimellaan, ja käyttökertojen määrä voi nopeasti paisua kaksinumeroisiin lukuihin.

Viimeisessä osiossa vastaajilta kysyttiin heidän tietoturvatoimistaan. Miten tärkeänä he pitävät verkkosivun yksityisyyskäytäntöjä? Heitä pyydettiin arvioimaan oma mielipiteensä 1 – 5-tyyppisellä asteikolla, ”hyvin tärkeästä” ”ei yhtään tärkeään”. Heiltä kysyttiin minkälaisia suojakeinoja he käyttävät verkossa, ja valitsemaan käyttämänsä keinot valintalaatikkovalikosta. Näihin keinoihin kuuluivat muun muassa incognito-ikkunan käyttäminen verkossa, VPN-sovelluksen käyttö, kaksivaiheinen varmennus sisäänkirjautumisen yhteydessä ja selaintietojen tyhjennys. Vaihtoehtona oli myös ”en käytä yhtään näistä”.

Lomakkeen kysymykset laadittiin opinnäytetyön sisällön perusteella. Kyselyssä ei täten käsitelty kaikkia sosiaalisen median sivustoja, ainoastaan niitä sivustoja, joihin opinnäytetyö keskittyi. Nämä sivustot olivat Facebook, Instagram, Twitter ja Facebook.

5.2 Kyselyn toteutus

Kyselylomake toteutettiin E-lomakkeella (e-lomake.puv.fi). Kirjoittaja oli käyttänyt tätä lomakesivustoa muilla kursseilla, ja se oli todettu helppokäyttöiseksi ja luotettavaksi. E-lomakkeella tehtyyn kyselyyn voisi myös tarvittaessa vaatia Vaasan ammattikorkeakoulun sisäänkirjautumistunnukset, mikä rajaisi vastaajat oppilaitoksen opiskelijoihin.

Kyselyssä päädyttiin kuitenkin sallimaan vastaukset ilman VAMK-tunnistautumista. Sisäänkirjautumisvaatimus ei olisi sallinut nimetöntä vastaamista, ja vastaaminen omalla käyttäjätunnuksella olisi saattanut alentaa vastaajien määrää.

Kysymykset eivät olleet henkilökohtaisia tai muutenkaan herkkäluontoisia, mutta nimettömyys koettiin kuitenkin parhaaksi vaihtoehdoksi.

Useimmat kysymykset laadittiin radionappivalikoksi. Vastaaja sai valita yhden, parhaiten sopivan vaihtoehdon. Kysymyksen niin vaatiessa monivalintavalikko oli tarpeen. Näin tehtiin esimerkiksi niiden kysymysten kohdalla, joissa kysyttiin millä sosiaalisen median sivustoilla vastaaja käy. Vaihtoehdoiksi annettiin opinnäytetyössä läpikäydyt Facebook, Instagram, Twitter ja YouTube, sekä ”muu”. Vaihtoehtoja olisi ollut liikaa, jos mukaan olisi otettu kaikki suositut sosiaalisen median sivustot.

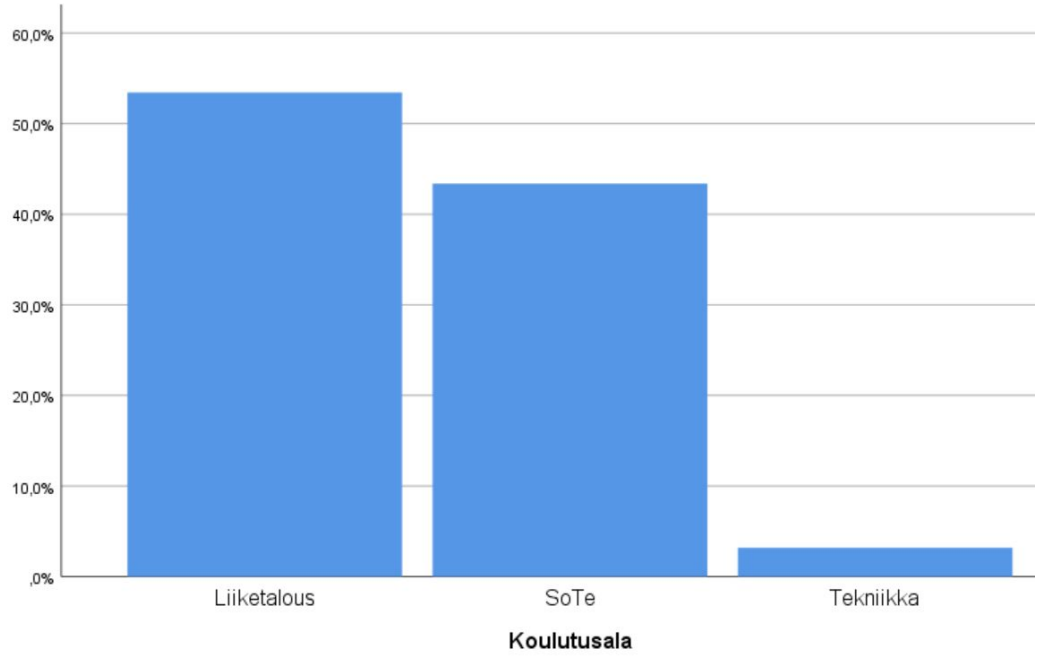
Kyselylomakkeessa ei ollut vapaamuotoisia vastauksia ikävalintaa lukuun ottamatta. Datan analysointia varten kaikki vastaukset tuli pystyä muuttamaan numeromuotoon, mikä hieman rajasi kysymysten laatimista. Kvantitatiivisessa kyselyssä vastausten määrä on kuitenkin tärkeintä, eivät niinkään analysoivat tekstivastaukset.

Kyselylomake lähetettiin opiskelijaryhmille VAMK:in opintosihteerin kautta. Vastausaikaa annettiin noin kuukausi, 28.9.2020 – 30.10.2020.

5.3 Kyselyn tulokset

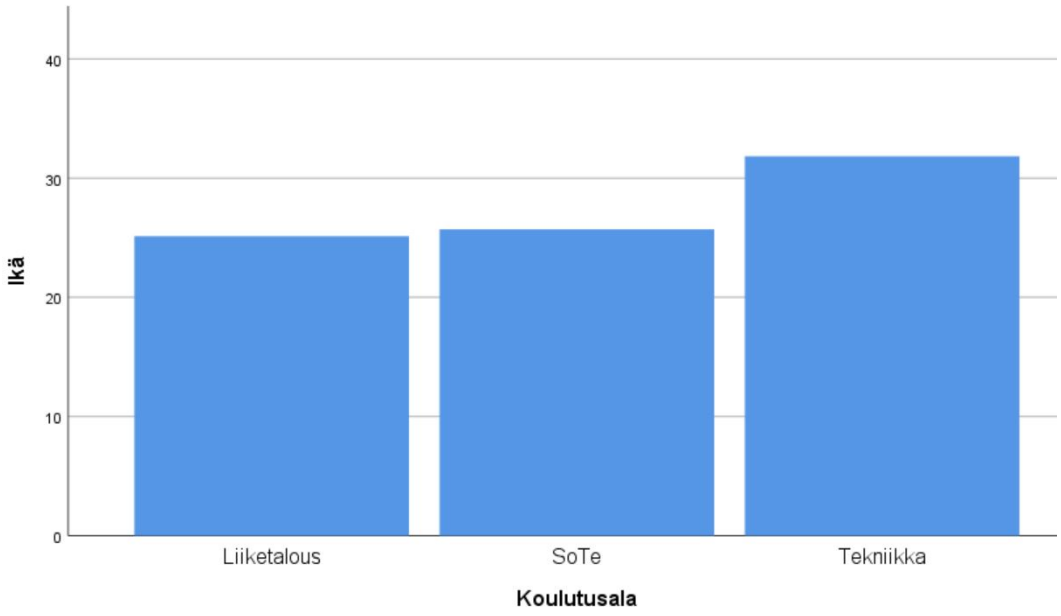
Kysely lähetettiin kaikille VAMK:in opiskelualoille ja näiden alaryhmille. Vastauksia saatiin 190 kappaletta. Valtaosa niistä saapui muutaman päivän sisällä lomakkeen lähetyksestä. Kyselyn tulokset olivat mielenkiintoisia, ja tässä osiossa käydään läpi tärkeimmät löydökset.

Vastausdata käsiteltiin ensiksi Microsoft Excelissä, ja sen jälkeen IBM SPSS Statistics-ohjelmalla. Kaikki kuviot luotiin IBM SPSS:llä.



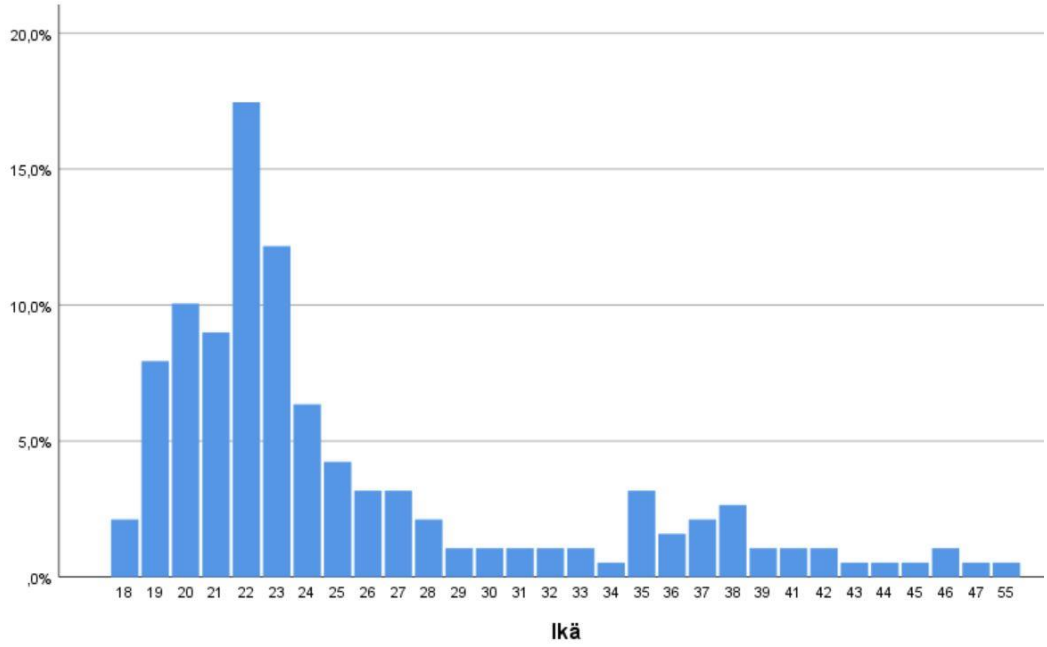
Kuvio 1. Eri koulutusalojen osuus kaikista vastauksista.

Suurin osa vastauksista, yli 50%, saatiin liiketalouden opiskelijoilta (kuvio 1). Liiketalouden alat ovat näistä kolmesta alasta eniten painottuneita tietokoneiden ja internetin käyttöön, mikä saattaa selittää tulokset. Sosiaali- ja terveysalan (SoTe) opiskelijat olivat myös melko aktiivisia vastaajia – heidän vastausmääränsä oli hieman yli 40%. Tekniikan alan opiskelijoiden vastausten vähyys oli yllättävää. On vaikea sanoa, mistä tämä johtui. Myöhemmillä kyselyvastauksilla voi kuitenkin olla osuutta tähän alhaiseen vastausprosenttiin. Tekniikan alan vastaajien keskivertoikä oli korkein, ja osa heistä ei käyttänyt lainkaan sosiaalista mediaa. Näillä tuloksilla voi olla yhteyttä vastausprosenttiin.

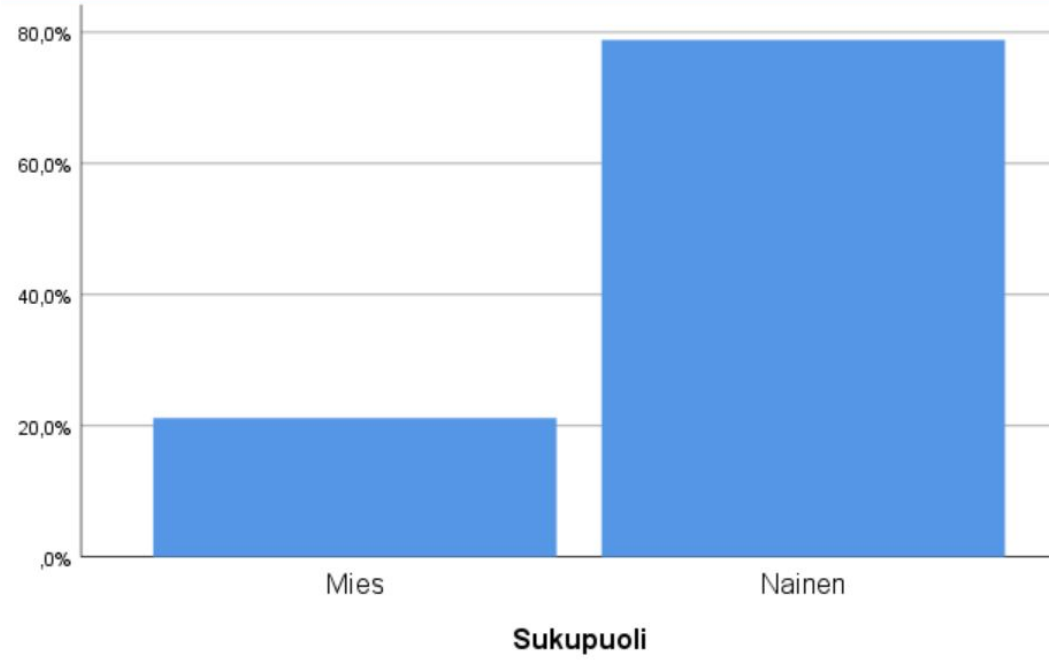


Kuvio 2. Vastaajien keskivertoikä koulutusaloittain.

Kuviossa 2 kuvataan opiskelualojen keskivertoikä. Tekniikan alan vastaajien ikä on suurin, yli 30. Liiketalous ja sosiaali- ja terveysalan vastaajien iät ovat melko samantasoiset. Korkeammalla keskivertoiällä saattoi olla vaikutusta tekniikan opiskelijoiden vähäiseen vastausintoon.

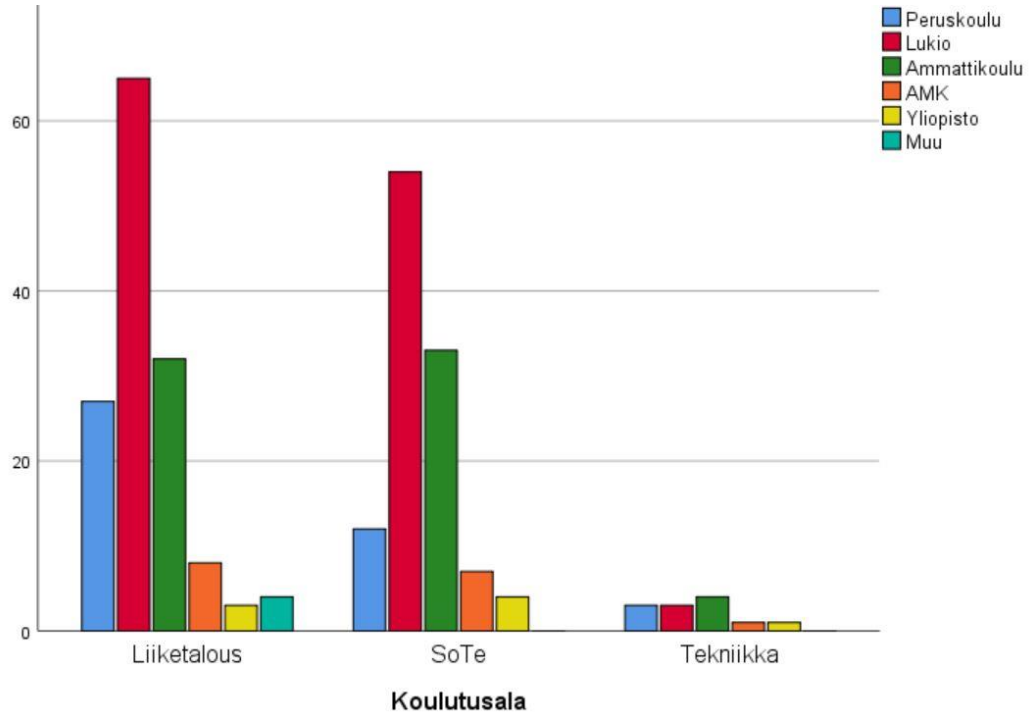


Kuvio 3. Vastaajien tarkempi ikäjakauma. Kuviossa 3 on esitetty tarkempi ikäjakauma, jonka mukaan suurin osa vastaajista oli 22 – 23-vuotiaita. Vastaajista valtaosa oli nuoria, alle 25-vuotiaita.



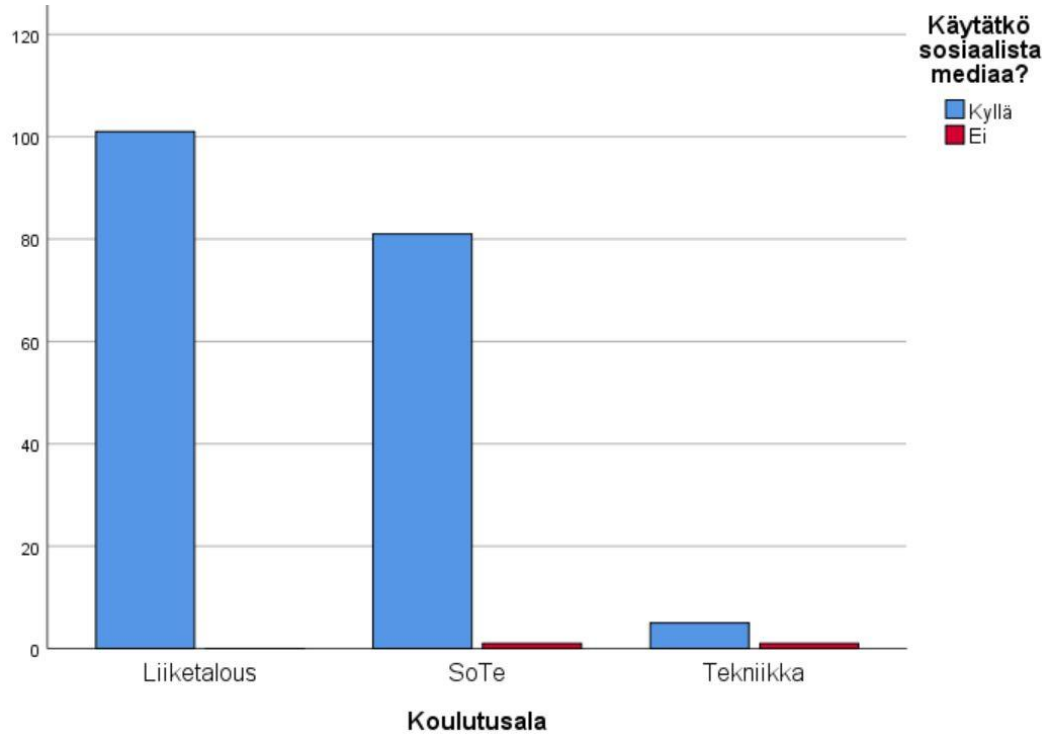
Kuvio 4. Vastaajien sukupuolijakauma.

Suurin osa vastaajista, 80%, oli naisia (kuvio 4). Olisi kiinnostavaa tietää kaikkien opiskelijoiden sukupuolijakauma, jotta tätä tietoa voitaisiin vertailla kyselyn dataan. Onko naispuolisia opiskelijoita enemmän, vai vastasivatko he vain innokkaammin kyselyyn?



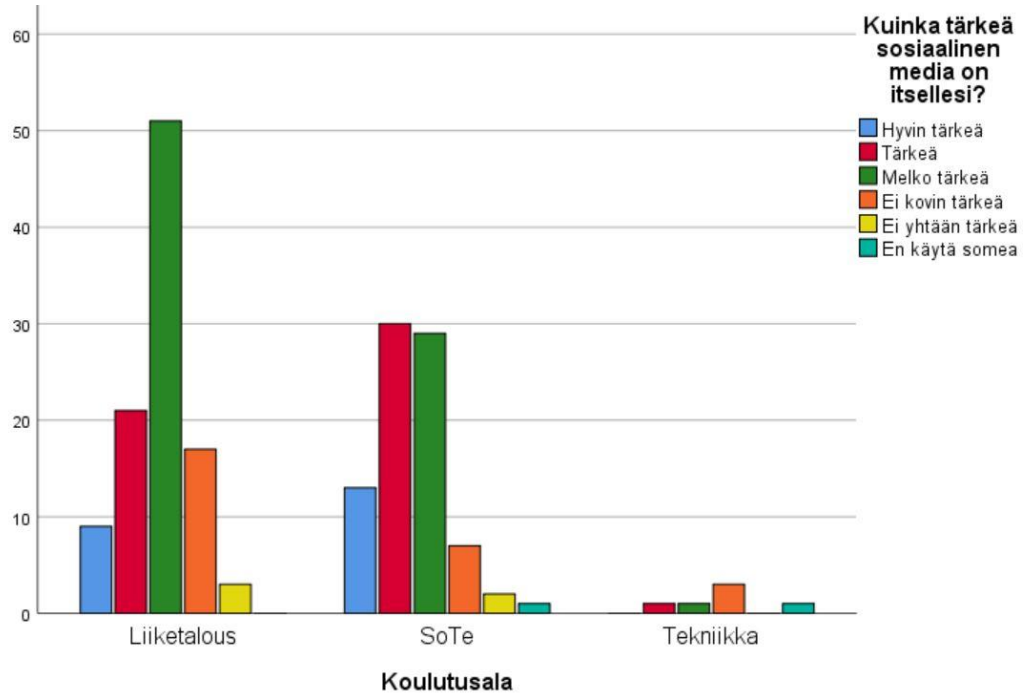
Kuvio 5. Vastaajien aiempi koulutus.

Kyselyssä haluttiin tietää vastaajien aiempi koulutustaso ennen Vaasan ammattikorkeakoulua. Suurin osa vastaajista oli käynyt lukion, lukuun ottamatta tekniikan alan opiskelijoita (kuvio 5). Heidän kohdallansa ammattikoulutausta oli yleisin. Pieni osa vastaajista oli aiemmin suorittanut toisen ammattikorkeakoulututkinnon, tai käynyt yliopistoa.



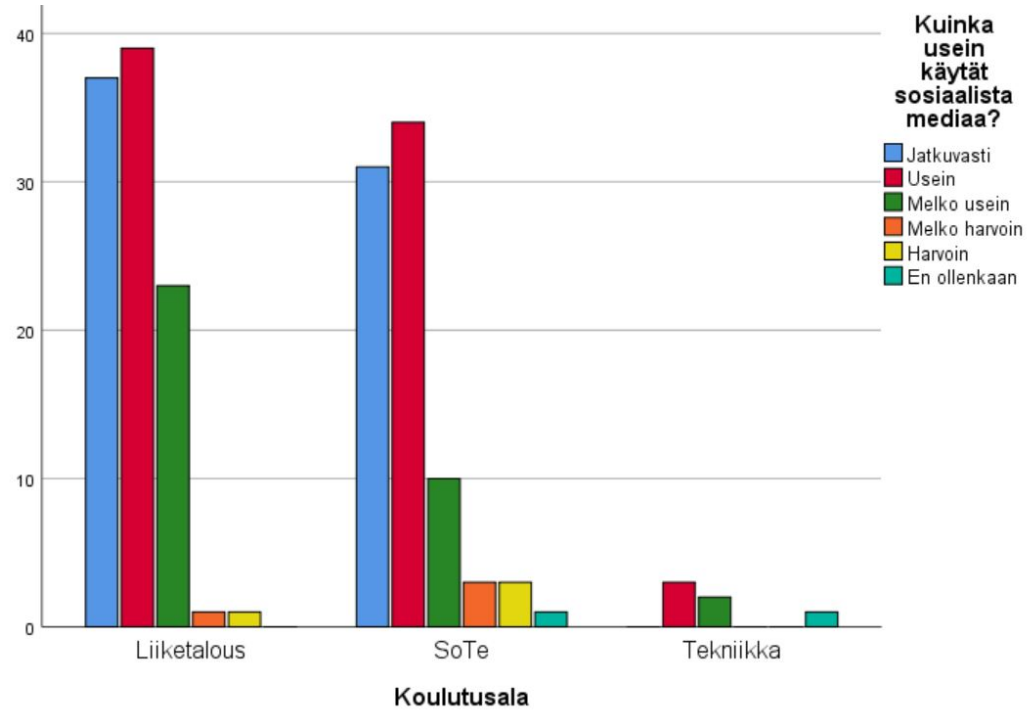
Kuvio 6. Sosiaalisen median käyttö opiskelualoittain.

Peruskysymys kyselyssä oli, käyttääkö vastaaja sosiaalista mediaa. Valtaosa kaikista vastaajista vastasi kyllä, ja harvat kielteiset vastaukset löytyivät SoTe- ja tekniikan aloilta (kuvio 6). Liiketalousalan opiskelijat vaikuttavat jälleen olevan aktiivisimpia tietokoneiden käyttäjiä. Ei ole yllättävää, että sosiaalisen median käyttö on näin yleistä opiskelijoiden keskuudessa. Olisi ollut mielenkiintoista teettää tämä kysely kymmenen vuotta sitten, ja verrata tuloksia 2010-luvun alulta ja 2010-luvun lopulta.



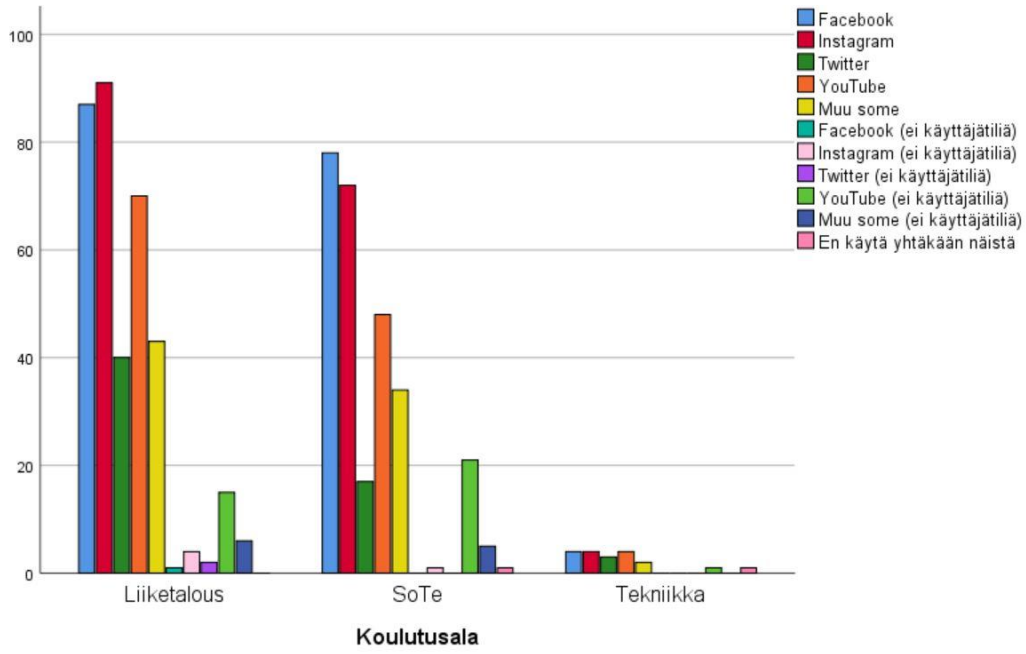
Kuvio 7. Sosiaalisen median tärkeys vastaajille.

Kyselyssä vastaajaa pyydettiin arvioimaan sosiaalisen median tärkeyttä itselleen. Sosiaali- ja terveysalan opiskelijat arvioivat somen tärkeyden korkeimmaksi (kuvio 7). Suurin osa heistä piti sosiaalista mediaa tärkeänä tai melko tärkeänä. On kiinnostavaa huomata, että liiketalouden opiskelijat pitävät keskimäärin sosiaalista mediaa vain melko tärkeänä. Tästä huolimatta jokainen vastaajista ilmoitti käyttävänsä jonkinlaista sosiaalista mediaa. Sosiaalisen median tärkeys on vähäisin tekniikan opiskelijoilla. Tämän alan vastaajien vähäisestä määrästä johtuen johtopäätösten vetäminen on hieman vaikeaa.



Kuvio 8. Kuinka usein vastaajat käyttävät sosiaalista mediaa.

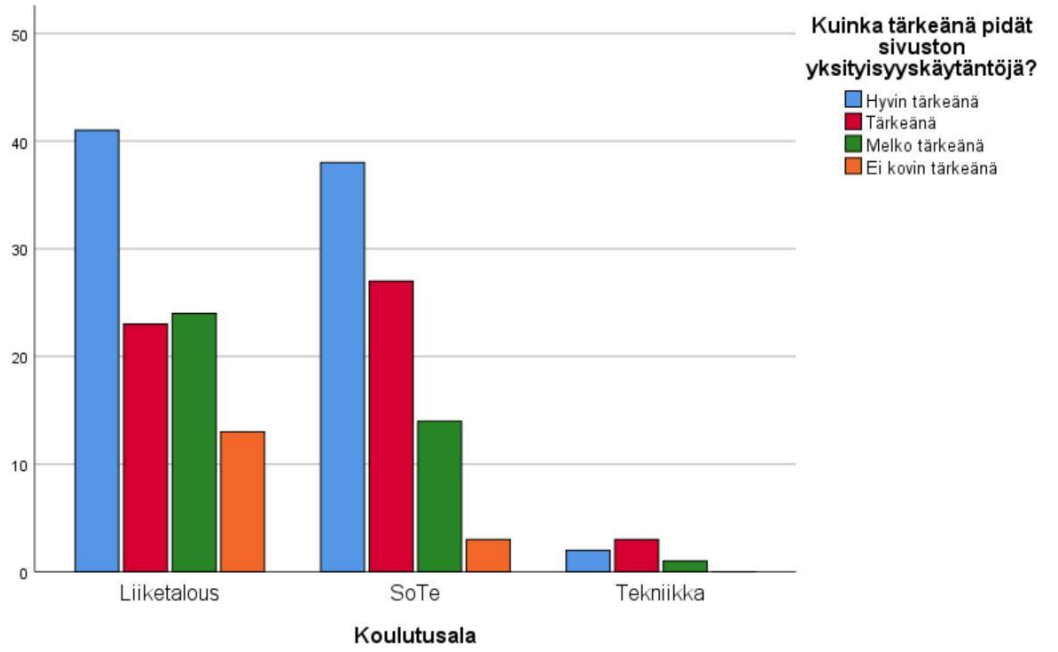
Liiketalouden ja sosiaali- ja terveysalan opiskelijat käyttävät sosiaalista mediaa hyvin aktiivisesti (kuvio 8). Suuri osa sanoi olevansa somessa ”jatkuvasti”, mikä ei ole kovin yllättävää. Älypuhelimien ansiosta henkilö on periaatteessa aina yhteydessä verkkoon, ja Facebookin tai Instagramin nopea tarkistus päivän mittaan on yleistä. Hyvin pieni osuus vastaajista käytti sosiaalista mediaa vain harvoin. Olisi ollut yllättävämpää, jos nämä luvut olisivat olleet päinvastaisia.



Kuvio 9. Vastaajien käyttämät somesivustot.

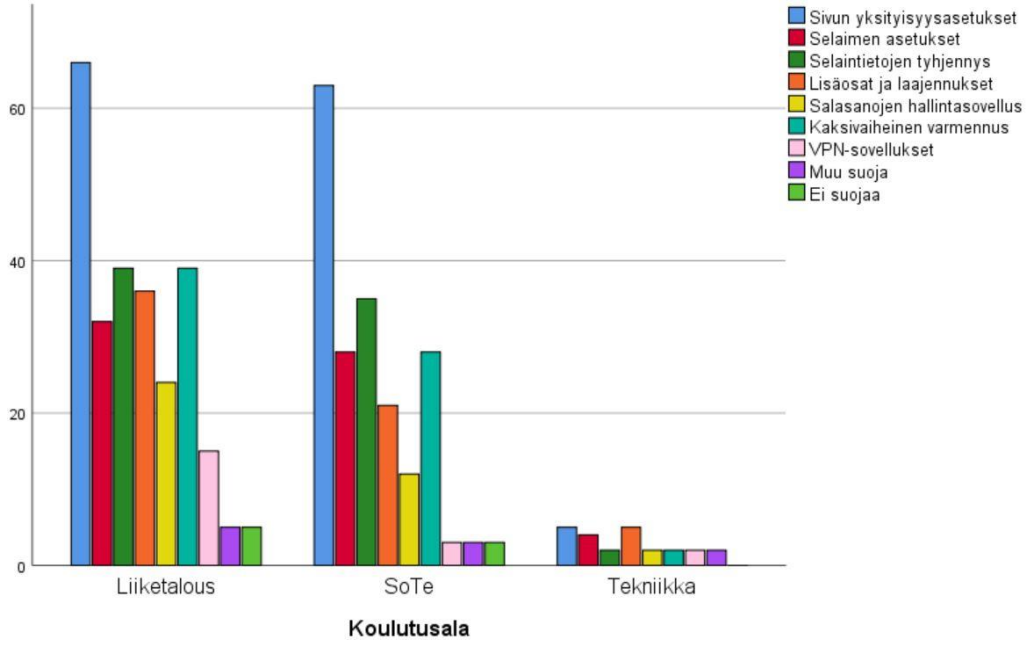
Kyselylomakkeessa kysyttiin opiskelijoiden käyttämiä sosiaalisen median sivuja, joille he ovat luoneet käyttäjätilin. Vaihtoehtoina oli myös valita sivut, joita he käyttävät ilman rekisteröityjä tunnuksia. Liiketalouden ja sosiaali- ja terveysalan opiskelijat olivat aktiivisia Facebookin ja Instagramin käyttäjiä, ja nämä sivustot olivat selvästi muita suositumpia (kuvio 9). YouTube oli kolmanneksi suosituin näiden alojen opiskelijoiden keskuudessa, mutta tekniikan alan vastaajilla YouTube oli yhtä suosittu kuin Facebook ja Instagram. Twitter oli vähiten käytetty sosiaalinen media kaikkien alojen vastaajilla.

Monet olivat valinneet ”muu some”-vaihtoehdon, ja olisi ollut mielenkiintoista saada tästä enemmän tietoa. Työn rajaamisen vuoksi tätä ei kuitenkaan tehty. Sosiaalisten medioiden käyttö ilman käyttäjätiliä ei ollut kovin tavallista, ja useiden sivujen käyttöominaisuudet ovat hyvin rajallisia ilman käyttäjätunnuksia. YouTuben käyttö ilman rekisteröityjä tunnuksia oli eniten valittu vaihtoehto. YouTubea voi helposti käyttää ilman rekisteröitymistä, mikä selittää tämän tuloksen.



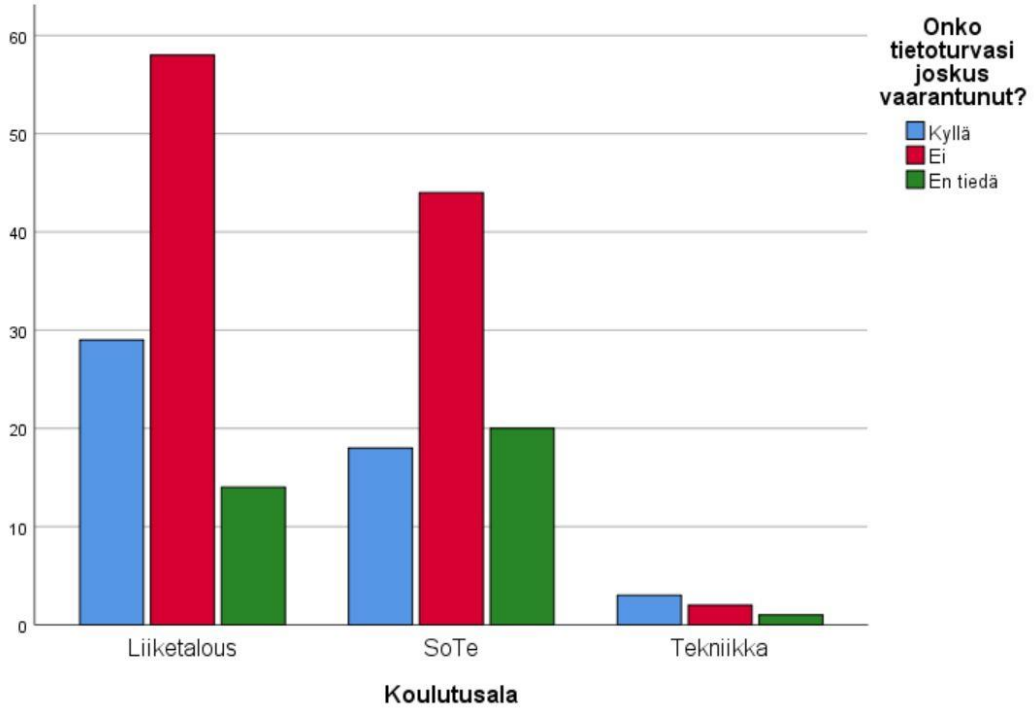
Kuvio 10. Kuinka tärkeänä vastaajat pitävät sivustojen yksityisyyskäytäntöjä.

Kyselyssä haluttiin tietää vastaajien asenteet sivustojen yksityisyyskäytäntöjä kohtaan. Kyselylomakkeessa vastaajille annettiin lyhyt selitys yksityisyyskäytännöistä, jotta he ymmärtäisivät, mitä kysymyksellä tarkoitettiin. ”Yksityisyyskäytännöillä tarkoitetaan sivun käytäntöjä koskien käyttäjätietojen keräämistä, käyttämistä ja tallentamista, laitteen sijaintitietojen keräämistä, sekä sivun evästeitä, joiden perusteella esim. käyttäjän näkemät mainokset ja sisältö räätälöidään.” Useimmat vastaajat pitivät yksityisyyskäytäntöjä hyvin tärkeinä, mikä on positiivista (kuvio 10). Käyttäjien olisi tärkeää tietää käyttämiensä sivujen käytännöt käyttäjädatan suhteen, ja näiden tulosten perusteella VAMK:in opiskelijat ovat tietoisia tästä.



Kuvio 11. Vastaajien käyttämät suojauskeinot verkossa.

Opiskelijoilta kysyttiin heidän käyttämistään suojaustoimista verkossa, ja heitä pyydettiin valitsemaan kaikki käyttämänsä suojauskeinot. Valtaosa on suojannut sometilinsä sivuston yksityisyysasetuksien kautta (kuvio 11), esimerkiksi rajaamalla ulkopuolisilta pääsyn heidän henkilökohtaisiin tietoihinsa. Selaintietojen manuaalinen tyhjennys verkkosession jälkeen on toiseksi yleisin suojauskeino. Tämä onkin hyvä tehdä julkisilla tietokoneilla, kuten oppilaitoksen koneilla. Selaimen asetuksien käyttö, kuten Do Not Track-asetus tai incognito-ikkuna, on myös melko yleistä vastaajien keskuudessa. Kaksivaiheisen varmennuksen käyttö sisäänkirjautumisen yhteydessä on yleistä, mikä on hyvin positiivinen asia tilin suojaamisen kannalta. Liiketalouden opiskelijat olivat aktiivisimpia salasanojen hallinta- ja VPN-sovelluksien käyttäjiä. Liiketalous painottuu näistä aloista eniten tietokoneen käyttöön, millä luultavasti on osuutta tähän tulokseen. Suojaa käyttämättömien vastaajien osuus oli hyvin pieni.



Kuvio 12. Vastaajien tietoturvan vaarantuminen.

Lisäksi opiskelijoilta kysyttiin heidän kokemuksistaan tietoturvan vaarantumisesta. Onko heidän tiliään koskaan esimerkiksi hakkeroitu, tai onko heidän tilinsä vaarantunut tietomurrossa? Tulosten perusteella suurin osa vastaajista ei ole kohdannut tietoturvariskejä (kuvio12), mikä kertoo hyvistä turvallisuuskäytännöistä. Melko suuri osa ei tosin tiedä, onko heidän verkkoturvallisuutensa vaarantunut. Sen selvittäminen voi olla hankalaa, varsinkin henkilölle, joka ei aktiivisesti käytä internetiä.

6 YHTEENVETO JA POHDINTA

Tämän opinnäytetyön tavoitteena oli tutkia aihetta, josta kirjoittaja itse halusi saada tietää lisää. Olettamuksena oli, että sosiaalinen media on osa jokaisen opiskelijan elämää ainakin jollain tasolla. On varsin harvinaista törmätä opiskeluikäiseen henkilöön, jolla ei ole profiilia esimerkiksi Facebookissa tai Instagramissa. Siksi oli mielenkiintoista tutkia juuri Vaasan ammattikorkeakoulun opiskelijoiden kokemuksia sosiaalisesta mediasta, ja nähdä pitikö tämä olettamus paikkansa.

Työn tutkimuskysymykset olivat seuraavat:

1) Mitkä tahot seuraavat verkkokäyttäytymistämme?

2) Miten nämä tahot seuraavat meitä?

3) Minkälaisia suojakeinoja on olemassa verkkoseurannan estämiseksi?

Näihin kysymyksiin saatiin vastaukset. Vastaukset eivät tosin olleet tyhjentäviä, ja aiheen laajuuden vuoksi vastaukset piti rajata. Verkkoseurantaa harjoittavien tahojen suhteen keskityttiin suurimpiin some-jättiläisiin ja näiden yhtiöiden taustoihin, vaikka tutkittavaa olisi ollut miltei rajattomasti. Kyseessä on perustutkimus sosiaalisten medioiden verkkoseurantaan, ei syventävä tutkimus. Työssä käsiteltiin tavallisimmat verkkoseurantametodit ja keinot, joiden avulla käyttäjä voi suojautua. Nämäkin osiot sisältävät perustiedot kyseisistä aiheista, ja niistä voisi olla hyötyä esimerkiksi verkkoturvallisuuteen perehtymättömälle.

Jälkikäteen ajateltuna työtä olisi voinut rajata vielä enemmän, ja keskittyä syvemmin kahteen tai kolmeen osioon. Varsinkin teknisiin yksityiskohtiin olisi voitu perehtyä enemmän. Tekstistä olisi täten tullut teknisempi, mutta aihealueiltaan kapeampi. Tavoitteena oli kuitenkin löytää tasapaino näiden kahden välillä, ja antaa lukijalle yleiskatsaus suosituimmista sivustoista, suojauskeinoista ja näiden teknisistä yksityiskohdista.

Yksi syy yleiskatsausmaiseen näkökulmaan opinnäytetyössä oli sen kuviteltu kohdeyleisö. Varsinkin asiakaspalvelussa ja helpdesk -tehtävissä voi vastaan tulla

asiakkaita, joiden tietokone-/internettaidot eivät ole ajan tasalla. Ajatuksena oli luoda perusopas tämän kaltaisille henkilöille sosiaalisen median maailmaan. Tekstistä löytyy myös ohjeet verkon vaarojen ja suojausmenetelmien suhteen.

Työtä voisi tulevaisuudessa hioa ja kehittää tarpeen tullen, jos tulevalla työpaikalla olisi siihen tarvetta. Tietokoneet ovat nykyään osa jokaista alaa, vaikka itse ammatilla ei olisi mitään tekemistä IT:n kanssa. Tämän vuoksi useimmilta työntekijöiltä tulisi löytyä ainakin perustiedot tietokoneen käytöstä. Esimerkiksi vanhemmilta toimistotyöntekijöiltä ei aina löydy tarvittavia tietotaitoja verkkomaailmassa.

Opinnäytetyön kirjoittaminen oli mukava haaste. Joidenkin aihealueiden kirjoittaminen sujui helpommin kuin toisten, riippuen esimerkiksi omasta kiinnostuksestani ja lähteiden laadusta. Juuri kunnollisten lähteiden löytäminen oli ajoittain haastavaa. Yhtiöiden luomista sovelluksista voi olla vaikeaa löytää tieteellisiä ja puolueettomia artikkeleita, varsinkin jos sovellus on uusi. Verkkomaailman nopean kehittymisen takia on myös tärkeää löytää mahdollisimman uusia lähteitä. Jo muutaman vuoden ikäiset lähteet voivat sisältää vanhentunutta tietoa.

Opinnäytetyöllä ei ollut toimeksiantajaa, mikä antoi lisävapautta työn kirjoittamiseen. Ajatuksena oli kuitenkin luoda ohjelehti some-turvallisuuteen. Tämä auttoi pitämään suunnan kirjoitusprosessin aikana.

Kyselylomakkeen luominen oli mielenkiintoista. Se ei saanut olla liian lyhyt, muttei myöskään liian pitkä. Liian monimutkaiselta näyttävä lomake saa helposti vastaajan luovuttamaan, ja tämä haluttiin välttää. Ohjaajan palautteen avulla saatiin luotua sopiva kyselylomake (liite 2), ja se lähetettiin opiskelijaryhmille opintosihteerin kautta (liite 1). Vastauksien määrä yllätti positiivisesti. Toiveena oli ollut saada ainakin 20 vastausta, mutta tämä määrä ylittyi moninkertaisesti. Vastauksia saatiin 190, minkä ansiosta tulokset kuvasivat opiskelijoiden keskivertomielipiteitä paremmin. Kyselyyn vastattiin nimettömänä, mikä luultavasti nosti vastaajien lukumäärää. Nimen tai opiskelijatunnuksen liittäminen yksittäiseen vastaukseen ei ollut tarpeellista.

En ollut aiemmin kirjoittanut näin laajaa työtä, ja prosessin aikana opin uusia asioita kirjoittamisesta ja suuren projektin työstämisestä. Työn jakaminen pienempiin osiin helpotti kirjoittamisprosessia paljon. Tästä strategiasta on hyötyä mahdollisissa tulevaisuuden työtehtävissä. Opinnäytetyön kirjoittaminen oli kaiken kaikkiaan miellyttävä kokemus, ja sen tuomat hyödyt painoivat enemmän kuin ajoittaiset vaikeudet prosessin aikana.

LÄHTEET

Albarran, A. 2013. The Social Media Industries. ProQuest Ebook Central. https://ebookcentral-proquest-com.ezproxy.puv.fi/lib/vamklibrary-ebooks/reader.action?docID=1143700&ppg=1

Acceptable Ads. 2020. The Acceptable Ads Standard. Acceptable Ads. Viitattu 24.9.2020. https://acceptableads.com/standard/

AdBlock. 2019. About AdBlock. AdBlock. Viitattu 24.9.2020. https://getadblock.com/

Arthur, C. 2011. Winklevoss Twins end Facebook Lawsuit. The Guardian. Viitattu 3.4.2020. https://www.theguardian.com/technology/2011/jun/23/winklevoss-twins-end-facebook-lawsuit

Berr, J. 2017. Winklevoss Twins Become First "bitcoin billionaires". CBS News. Viitattu 3.4.2020. https://www.cbsnews.com/news/winklevoss-twins-bitcoin-billionaires-investment-price-surges/

Carlson, N. 2012. Exclusive: How Mark Zuckerberg Booted His Co-founder Out of the Company. Business Insider. Viitattu 1.4.2020. https://www.businessinsider.com/how-mark-zuckerberg-booted-his-co-founder-out-of-the-company-2012-5?op=1&r=US&IR=T

Carlson, N. 2011. The Real History of Twitter. Business Insider. Viitattu 8.4.2020. https://www.businessinsider.com/how-twitter-was-founded-2011-4?op=1&r=US&IR=T

Clement, J. 2020a. Number of Social Network Users Worldwide From 2010 to 2023. Statista. Viitattu 27.3.2020. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Clement, J. 2020b. Most Popular Social Networks Worldwide as of January 2020, Ranked by Number of Active Users. Statista. Viitattu 28.3.2020. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Clement, J. 2020c. Number of monthly active Facebook users worldwide as of 2nd quarter 2020. Statista. Viitattu 16.11.2020. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Clement, J. 2019d. Number of Monthly Active Twitter Users Worldwide From 1st Quarter 2010 to 1st Quarter 2019. Statista. Viitattu 8.4.2020. https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

Clement, J. 2019e. Instagram - Statistics & Facts. Statista. Viitattu 11.5.2020. https://www.statista.com/topics/1882/instagram/

Clement, J. 2019f. Share of internet users who are more concerned about their online privacy compared to a year ago as of February 2019, by country. Statista. Viitattu 15.10.2020. https://www.statista.com/statistics/373322/global-opinion-concern-online-privacy/

Crawford, D. 2020. What is a VPN and Why Use One? A Non-Technical Beginner's Guide to Virtual Private Networks. ProPrivacy. Viitattu 7.10.2020. https://proprivacy.com/vpn/guides/what-is-vpn-beginners-guide

Cresci, E. 2016. 12 Ways Twitter Changed our Lives. The Guardian. Viitattu 11.4.2020. https://www.theguardian.com/technology/2016/mar/21/12-ways-twitter-changed-our-lives-10th-birthday

Dickey, M.R. 2013. The 22 Key Turning Points in the History of YouTube. Business Insider. Viitattu 3.5.2020. https://www.businessinsider.com/key-turning-points-history-of-youtube-2013-2?op=1&r=US&IR=T

Duffy, C. 2019. The Winklevoss Twins May Work with Facebook Again. CNN Business. Viitattu 3.4.2020. https://edition.cnn.com/2019/08/19/tech/winklevoss-boss-files/index.html

Erkkola, JP. 2008. Sosiaalisen median käsitteestä. Aalto University Learning Centre. Viitattu 28.3.2020. https://aaltodoc.aalto.fi/handle/123456789/12480

Europol. 2020. Risks of Using Public Wi-Fi. Europol - European Union Agency for Law Enforcement Cooperation. Viitattu 7.10.2020. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/risks-of-using-public-wi-fi

ExpressVPN. 2020. Corporate Accountability & Business Model. ExpressVPN. Viitattu 17.10.2020. https://www.expressvpn.com/trust/cdt-trust-questions

Eyeo. 2020. Frequently Asked Questions. Eyeo GmbH. Viitattu 28.9.2020. https://eyeo.com/about/

Facebook. 2020a. Data Policy. Viitattu 8.6.2020. https://www.facebook.com/policy.php

Facebook. 2020b. Data Policy. Viitattu 8.6.2020. https://www.facebook.com/about/privacy

Facebook. 2020c. Facebook Platform Policy. Facebook About. Viitattu 7.7.2020. https://developers.facebook.com/policy/

Facebook. 2020d. Facebook ja sijainti. Viitattu 27.8.2020. https://www.facebook.com/help/337244676357509

Facebook. 2020e. Yksityisyyden perusasetukset ja työkalut. Viitattu 14.9.2020. https://www.facebook.com/help/325807937506242/

Findwise. 2020. Mitä jokaisen kuuluu tietää EU:n uudesta tietosuoja-asetuksesta GDPR? Viitattu 16.11.2020. https://findwise.com/en/gdpr-fi

GitHub. 2020. uBlock Origin. GitHub, Inc. Viitattu 2.10.2020. https://github.com/gorhill/uBlock/blob/master/README.md

Google. 2020a. YouTube API Services Terms of Service. Google Developers. Viitattu 8.7.2020. https://developers.google.com/youtube/terms/api-services-terms-of-service

Google. 2020b. Tietosuoja ja käyttöehdot. Google. Viitattu 3.9.2020. https://policies.google.com/privacy?hl=fi

Google. 2020c. Sisäänkirjautuminen Google-kehotteilla. Google. Viitattu 22.9.2020. https://support.google.com/accounts/answer/7026266?co=GENIE.Platform%3DAndroid&hl=fi

Hartmans, A. 2020. The Life and Rise of Kevin Systrom, Instagram's Former CEO who Shocked Facebook by Quitting 6 Years After Selling his Company to Mark Zuckerberg for $1 Billion. Business Insider. Viitattu 25.5.2020. https://www.businessinsider.com/kevin-systrom-instagram-ceo-life-rise-2018-9?op=1&r=US&IR=T

Humphries, M. 2019. China Starts Issuing $145 Fines for Using a VPN. PCMag. Viitattu 12.10.2020. https://uk.pcmag.com/news/119084/china-starts-issuing-145-fines-for-using-a-vpn

Hunt, T. 2019. The 773 Million Record "Collection #1" Data Breach. Viitattu 21.9.2020. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Instagram. 2020a. Data Policy. Instagram, Inc. Viitattu 31.8.2020. https://help.instagram.com/519522125107875

Instagram. 2020b. Näkyvyyden hallinta. Instagram, Inc. Viitattu 14.8.2020. https://help.instagram.com/116024195217477/?helpref=hc_fnav&bc[0]=Instagramin%20ohje&bc[1]=Yksityisyys-%20ja%20turvallisuuskeskus

Kharpal, A. 2019. How Social Media is Shaping what People Know — and Don’t Know — about the Hong Kong Protests. CNBC. Viitattu 30.3.2020. https://www.cnbc.com/2019/06/13/hong-kong-protests-role-of-technology-and-china-censorship.html

Lee, D. 2018. The Tactics of a Russian Troll Farm. BBC News. Viitattu 31.3.2020. https://www.bbc.com/news/technology-43093390

Liikenne- ja viestintävirasto. 2020a. Luottamuksellinen viestintä. Viitattu 3.6.2020. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta

Liikenne- ja viestintävirasto. 2020b. Luottamuksellinen viestintä. Viitattu 4.6.2020. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta

Macaskill, E., Dance, G. 2013. NSA Files: Decoded. The Guardian. Viitattu 30.3.2020. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Maheshwari, S. 2016. Adblock Plus, Created to Protect Users from Ads, Instead Opens the Door. The New York Times. Viitattu 28.9.2020. https://www.nytimes.com/2016/09/19/business/media/adblock-plus-created-to-protect-users-from-ads-opens-the-door.html

Malwarebytes. 2020. Keyloggers - What is a keystroke logger? Malwarebytes. Viitattu 17.11.2020. https://www.malwarebytes.com/keylogger/

Marvin, R. 2018. Breaking Down VPN Usage Around the World. PCMag. Viitattu 12.10.2020. https://uk.pcmag.com/vpn/117532/breaking-down-vpn-usage-around-the-world

McFadden, C. 2018. A Chronological History of Social Media. Interesting Engineering. Viitattu 28.3.2020. https://interestingengineering.com/a-chronological-history-of-social-media

Miller, D., Madianou, M. 2016. Social Media in an English Village. JSTOR. Viitattu 29.3.2020. https://www.jstor.org/stable/j.ctt1g69xs1.6

Mozilla. 2020. What Are Extensions? MDN Web Docs. Viitattu 23.9.2020. https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/What_are_WebExtensions

MuleSoft. 2020. What is an API? (Application Programming Interface). MuleSoft LLC. Viitattu 3.7.2020. https://www.mulesoft.com/resources/api/what-is-an-api

Nations, D. 2019. What Is Microblogging? A definition of microblogging with examples. Lifewire. Viitattu 8.4.2020. https://www.lifewire.com/what-is-microblogging-3486200

NordVPN. 2020. Jurisdiction We Operate In. NordVPN. Viitattu 17.10.2020. https://support.nordvpn.com/General-info/Features/1061811142/Jurisdiction-we-operate-in.htm

Norton LifeLock. 2020. What are Cookies? Norton LifeLock Inc. Viitattu 4.6.2020. https://us.norton.com/internetsecurity-privacy-what-are-cookies.html

O'Flaherty, K. 2019. Collection 1 Breach -- How to Find Out if Your Password Has Been Stolen. Forbes. Viitattu 17.9.2020. https://www.forbes.com/sites/kateoflahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#58ee7c532a2e

Perez, S. 2018. Twitter's Doubling of Character Count from 140 to 280 had Little Impact on Length of Tweets. TechCrunch. Viitattu 7.4.2020. https://techcrunch.com/2018/10/30/twitters-doubling-of-character-count-from-140-to-280-had-little-impact-on-length-of-tweets/

Phillips, S. 2007. A Brief History of Facebook. The Guardian. Viitattu 28.3.2020. https://www.theguardian.com/technology/2007/jul/25/media.newmedia

Poikola, A., Kivekäs, O., Kettunen, J. 2014. Avoimen rajapinnan määritelmä. Avoin rajapinta. Viitattu 1.7.2020. http://avoinrajapinta.fi

Privacy Tools. 2020. Why is it Not Recommended to Choose a US-based Service? Privacy Tools. Viitattu 15.10.2020. https://www.privacytools.io/providers/

Rashed, F. 2011. @FawazRashed. Twitter. Viitattu 30.3.2020. https://twitter.com/FawazRashed/status/48882406010257408?s=20

Ricke, L.D. 2014. The Impact of YouTube on U.S. Politics. ProQuest Ebook Central. https://ebookcentral-proquest-com.ezproxy.puv.fi/lib/vamklibrary-ebooks/reader.action?docID=1809830&ppg=1

Rupar, A. 2020. "These Media Posts Will Serve as Notification": Trump's dangerous Iran tweets, briefly explained. Vox. Viitattu 18.4.2020. https://www.vox.com/2020/1/6/21051550/trump-iran-tweets-soleimani-war-powers-act

SafetyDetectives. 2020. VPN Comparison by That One Privacy Guy. SafetyDetectives. Viitattu 17.11.2020. https://www.safetydetectives.com/best-vpns/

Shearlaw, M. 2016. Egypt Five Years On: was it ever a 'social media revolution'? The Guardian. Viitattu 30.3.2020. https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution

Stelter, B. 2020. Analysis: Trump's War on Truth Takes a Dangerous Turn as He Attacks the Media's Coronavirus Coverage. CNN. Viitattu 22.4.2020. https://edition.cnn.com/2020/02/26/media/trump-attacks-media-coronavirus/index.html

Surfshark. 2020. Surfshark Privacy Policy. Surfshark. Viitattu 17.10.2020. https://surfshark.com/privacy-policy

Tam, F., Jim, C. 2020. Exclusive: Support for Hong Kong protesters' demands rises even as coronavirus halts rallies: poll. Reuters. Viitattu 31.3.2020. https://www.reuters.com/article/us-hongkong-protests-poll-exclusive-idUSKBN21E11L

Thomas, K., Moscicki, A. 2019. New research: How effective is basic account hygiene at preventing hijacking. Google Security Blog. Viitattu 22.9.2020. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Tietosuojavaltuutetun toimisto. 2020. Usein kysyttyä EU:n tietosuoja-asetuksesta. Viitattu 25.5.2020. https://tietosuoja.fi/gdpr

Tsukayama, H. 2017. Twitter is Officially Doubling the Character Limit to 280. The Washington Post. Viitattu 7.4.2020. https://www.washingtonpost.com/news/the-switch/wp/2017/11/07/twitter-is-officially-doubling-the-character-limit-to-280/

Twitter. 2020a. About Third-party Apps and Log in Sessions. Twitter, Inc. Viitattu 11.6.2020. https://help.twitter.com/en/managing-your-account/connect-or-revoke-access-to-third-party-apps

Twitter. 2020b. About Twitter’s APIs. Twitter, Inc. Viitattu 4.7.2020. https://help.twitter.com/en/rules-and-policies/twitter-api

Twitter. 2020c. Tweet Location FAQs. Twitter, Inc. Viitattu 28.8.2020. https://help.twitter.com/en/safety-and-security/tweet-location-settings

Twitter. 2020d. About Public and Protected Tweets. Twitter, Inc. Viitattu 15.9.2020. https://help.twitter.com/en/safety-and-security/public-and-protected-tweets

Twitter. 2020e. How to Control your Twitter Experience. Twitter, Inc. Viitattu 15.9.2020. https://help.twitter.com/en/safety-and-security/control-your-twitter-experience

LIITE 1

SAATEKIRJE

Hei!

Opiskelen tietojenkäsittelyä avoimessa AMK:ssa. Opinnäytetyöni sekä tämä kysely koskee sosiaalista mediaa ja yksityisyyttä. Kyselylomake sisältää noin 10 kysymystä, ja tavoitteena on vertailla eri koulutusalojen vastauksia keskenään. Kysely on vapaaehtoinen, ja vastaukset ovat nimettömiä. Tulokset julkaistaan opinnäytetyössä.

Kysely on auki 28.9.2020 - 30.10.2020.

Kiitos ajastanne!

LIITE 2

KYSELYLOMAKE

Perustiedot

Tässä kyselyssä sosiaalinen media kattaa Facebookin, Twitterin, Instagramin, YouTuben, keskustelufoorumit, blogit, ja muut sosiaalisen kanssakäymisen sivustot. Videopelejä ei lasketa sosiaalisiin medioihin.

Sukupuoli:

- Mies
- Nainen

Ikä: ___

Koulutusala:

- Liiketalous
- Sosiaali- ja terveys
- Tekniikka

Aiempi koulutus:

- Peruskoulu
- Lukio
- Ammattikoulu
- Ammattikorkeakoulu
- Yliopisto
- Muu

Sosiaalinen media

Käytätkö sosiaalista mediaa?

- Kyllä
- Ei

Kuinka tärkeä sosiaalinen media on itsellesi?

- Hyvin tärkeä
- Tärkeä
- Melko tärkeä
- Ei kovin tärkeä

- Ei yhtään tärkeä
- En käytä sosiaalista mediaa

Kuinka usein käytät sosiaalista mediaa?

- Jatkuvasti
- Usein
- Melko usein
- Melko harvoin
- Harvoin
- En ollenkaan

Valitse kaikki sivustot, joille olet luonut tilin ja joita käytät:

- Facebook
- Instagram
- Twitter
- YouTube
- Muu
- Minulla ei ole tiliä, mutta käytän Facebookia
- Minulla ei ole tiliä, mutta käytän Instagramia
- Minulla ei ole tiliä, mutta käytän Twitteriä
- Minulla ei ole tiliä, mutta käytän YouTubea
- Minulla ei ole tiliä, mutta käytän muita sivustoja
- Minulla ei ole tiliä yhdellekään sivustolle, enkä käytä yhtään niistä

Yksityisyys ja turvallisuus

Yksityisyyskäytännöillä tarkoitetaan sivun käytäntöjä koskien käyttäjätietojen keräämistä, käyttämistä ja tallentamista, laitteen sijaintitietojen keräämistä, sekä sivun evästeitä, joiden perusteella esim. käyttäjän näkemät mainokset ja sisältö räätälöidään.

Kuinka tärkeänä pidät sivuston yksityisyyskäytäntöjä?

- Hyvin tärkeänä
- Tärkeänä
- Melko tärkeänä
- Ei kovin tärkeänä
- En yhtään tärkeänä

Millaisia suojatoimia käytät verkossa?

- Sivuston yksityisyysasetukset (esim. kuvien ja tietojen piilottaminen ulkopuolisilta)
- Selaimen asetukset (esim. incognito-ikkuna, Do Not Track-asetus)

- Selaintietojen tyhjennys
- Selaimen lisäosat ja laajennukset (esim. mainoksenestäjät)
- Hallintasovellus salasanoille
- Kaksivaiheinen varmennus sisäänkirjautuessa
- VPN-sovellus
- Muu
- En käytä yhtään näistä

Onko tietoturvasi joskus vaarantunut? (Esim. tilin hakkerointi, tietomurto, virus, kiristysohjelma.)

- Kyllä
- Ei
- En tiedä