HAAGA-HELIA
ammattikorkeakoulu

HAAGA-HELIA ammattikorkeakoulun opiskelijoiden käsitys sosiaalisen median tietoturvasta ja sen riskeistä

Katariina Nuotio

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2012

HAAGA-HELIA ammattikorkeakoulu

Tiivistelmä

Raportin palautuksen tai esityksen päivämäärä

Koulutusohjelma

Tekijä tai tekijät Katariina Nuotio	**Ryhmätunnus tai aloitusvuosi** 2008
Raportin nimi HAAGA-HELIA ammattikorkeakoulun opiskelijoiden käsitys sosiaalisen median tietoturvasta ja sen riskeistä	**Sivu- ja liitesivumäärä** 35 + 9
Opettajat tai ohjaajat Titta Ahlberg	

Opinnäytetyön tarkoituksena oli selvittää sosiaalisen median tietoturvaa ja HAAGA-HELIA ammattikorkeakoulun opiskelijoiden suhtautumista siihen. Opinnäytetyö toteutettiin keräten tietoa kirjallisuudesta ja HAAGA-HELIA ammattikorkeakoulun kolmen eri koulutusohjelman opiskelijoille lähetetyllä kyselyllä. Kyselyssä keskityttiin yksityisyyteen liittyviin uhkiin ja käyttäjien tietoisuuteen niistä. Kyselyyn vastasi noin 12 prosenttia opiskelijoista.

Opinnäytetyön teoreettisissa osioissa käsitellään sosiaalisen median eri määritelmiä sekä suosituimpia sosiaalisen median palveluja, kuten Facebook, YouTube ja Twitter. Teoreettisissa osioissa käsitellään myös sosiaalisen median tietoturvaa ja käydään läpi sosiaalisen median yleisimpiä uhkakuvia jaoteltuina teknisiin uhkiin ja yksityisyyteen liittyviin uhkiin. Opinnäytetyön pääpaino on ollut yksityisyyteen liittyvissä uhissa.

Opiskelijoille suunnattu kysely analysoitiin kysymyksittäin ja koulutussuunnittain. Tutkimuskysymykset jaoteltiin kolmeen kokonaisuuteen eli opiskelijoiden käsitykseen sosiaalisen median tietoturvasta, opiskelijoiden tietoisuuteen siitä ja kolmanneksi muuttuivatko opiskelijoiden käsitykset tutkimuskyselystä johtuen.

Kyselyyn saatuihin tuloksiin on suhtauduttava varauksella, koska vastausprosentti jäi pieneksi. Tuloksista voidaan kuitenkin päätellä, että vastaajat suhtautuivat hieman varauksella sosiaalisen median tietoturvaan yleensä, mutta pitivät omaa tietämystänsä siitä suhteellisen hyvänä. Julkisuudessa esillä olleista asioista tiedetään jonkin verran enemmän kuin niistä, jotka mainitaan esimerkiksi vain käyttöehdoissa.

Asiasanat
sosiaalinen media, tietoturva, yksityisyys

HAAGA-HELIA
University of Applied Sciences

Abstract

Date of presentation

Degree programme

Authors Katariina Nuotio	**Group or year of entry** 2008
The title of thesis The perception of the students at HAAGA-HELIA University of Applied Sciences of the information security of social media and of the related risks	**Number of pages and appendices** 35 + 9
Supervisor(s) Titta Ahlberg	

The purpose of this thesis was to examine the information security of social media and the perceptions that the students of HAAGA-HELIA UAS have of it. The main focus was on the threats to privacy in social media.

The thesis was based on the research of relevant literature and a questionnaire sent to students of three different study programmes at HAAGA-HELIA UAS. The questionnaire focused on threats to privacy and the users' awareness thereof. Approximately 12 percent of the students replied to the questionnaire.

The theoretical sections of the thesis addressed the definition of social media as well as the most popular social media services such as Facebook, YouTube and Twitter. The theoretical sections also discussed the information security in social media and the most common threats to it. These threats were divided into technical and privacy - related threats.

The replies to the questionnaire were analysed question by question and based on the study programme of the subject. The questions included in the questionnaire were divided into three groups, i.e. the students' perception of the information security of social media; their knowledge thereof; and whether their perceptions changed as a result of taking part in the study.

The results of the questionnaire are to be viewed with reservation due to the low percentage of replies received. The conclusion can, however, be drawn that the subjects had a somewhat reserved attitude toward the information security of social media but considered their own knowledge of it to be relatively good. Information security issues that have been the topic of public attention are understood somewhat better than issues that are, for example, only mentioned in the sites' terms of use.

Key words
social media, information security, privacy

Sisällys

1 Johdanto

Tutkimuksen tarkoituksena on selvittää kyselyn avulla HAAGA-HELIA ammattikorkeakoulun opiskelijoiden tietoisuutta sosiaalisen median tietoturvasta ja opiskelijoiden suhtautumista sosiaalisen median tietoturvariskeihin. Tutkimuksessa käsitellään sosiaalisen median yleisimpiä tietoturvauhkia kirjallisuutta lähteenä käyttäen. Tutkimus painottuu ennen kaikkea niihin uhkiin, jotka koskevat käyttäjien yksityisyyttä.

Tutkimuksessa käsitellään aluksi teoreettisesti sosiaalisen median käsitettä ja kuvataan suosituimpia sosiaalisen median palveluita. Facebook, YouTube ja Twitter valittiin sen vuoksi, että ne kaikki ovat erittäin suosittuja, edustavat erilaisia sosiaalisen median palveluiden tyyppejä ja niiden suosion takia monet teoriataustassa olevista esimerkeistä koskevat kyseisiä palveluita. Sosiaalisen median tietoturvaan liittyviä uhkia käsitellään myös kirjallisuuteen perustuen luvussa 3. Vaikka tämän tutkimuksen pääpaino on yksityisyyteen liittyvissä uhissa, niin työssä haluttiin myös käsitellä jonkin verran sosiaaliseen mediaan liittyviä teknisiä uhkia, koska niistä on puhuttu paljon.

Tutkimukseen sisältyy myös kyselyosio HAAGA-HELIA ammattikorkeakoulun opiskelijoille. Kyselyn avulla pyrittiin saamaan vastaus kolmeen eri aihekokonaisuuteen. Aihekokonaisuuksista ensimmäinen koski HAAGA-HELIA ammattikorkeakoulun opiskelijoiden käsitystä sosiaalisen median tietoturvasta ja toinen opiskelijoiden tietoisuutta sosiaalisen median tietoturvariskeistä. Kolmas aihekokonaisuus koski sitä, muuttuiko opiskelijoiden suhtautuminen sosiaalisen median tietoturvaan kyselyn jälkeen. Saatuja vastauksia pyrittiin analysoimaan myös sen mukaan, mihin koulutusohjelmaan opiskelija kuuluu.

2 Yleistä sosiaalisesta mediasta ja tietoturvasta

Tutkimuksen teoreettisena taustana käsitellään ensinnäkin sosiaalisen median käsitettä, joka ei ole yksiselitteinen. Lisäksi tarkastellaan joitain sosiaalisen median suosituimpia ja yleisimpiä palveluita (Facebook, YouTube ja Twitter). Lisäksi selostetaan tietoturvan perusteena pidettyä muistiosääntöä (CIA).

2.1 Sosiaalisen median käsite

Käsite "sosiaalinen media" ei ole yksiselitteinen ja sille löytyy useampia hieman toisistaan poikkeavia määritelmiä. Sanastokeskus TSK ry:n (2010, 14) määritelmän mukaan sosiaalinen media on tietoverkkoja ja tietotekniikkaa hyödyntävä viestinnän muoto, jossa käsitellään vuorovaikutteisesti ja käyttäjälähtöisesti tuotettua sisältöä sekä luodaan ja ylläpidetään ihmisten välisiä suhteita. Sosiaalinen media voidaan määritellä myös vuorovaikutteisuuteen ja käyttäjälähtöisyyteen perustuviksi viestintävälineiksi, viestintäkanavaksi tai -ympäristöksi.

Tyypillisimpiä sosiaalisen median verkkopalveluita ovat sisällönjakopalvelut, verkkoyhteisöpalvelut ja keskustelupalstat. Sosiaalisen median piiriin kuuluvaa toimintaa on esimerkiksi kollektiivinen sisällöntuotanto, blogien kirjoittaminen ja lukeminen, tiedostojen jakaminen vertaisverkossa sekä verkkopelien pelaaminen usean eri henkilön kesken. (Sanastokeskus TSK 2010, 14.)

Sosiaalisen median määrittelyssä painotetaan joskus teknisiä ratkaisuja, jolloin yleensä tarkoitetaan Web 2.0:aa. Web 2.0 on Internetin hyödyntämisessä käytettävien tietoteknisten ratkaisujen kokonaisuus, joka mahdollistaa sosiaalisen median palvelut. Siihen sisältyy muun muassa sellaiset sovellukset, jotka mahdollistavat vuorovaikutteisuuden ja käyttäjälähtöisyyden. Web 2.0:n ajatuksena on sen lisäksi, että Internet toimii sisältöjen tallennuspaikkana, niin Internet toimii myös eri sovellusten alustana. (Sanastokeskus TSK 2010, 14–15.)

Kotimaisten kielten tutkimuskeskuksen mukaan sosiaalinen media on monimutkaisempi käsite kuin yhteisöllinen media ja että yhteisöllinen media avaa käsitteen sisällön pa-

remmin asiaa tuntemattomalle kuin sosiaalinen media. Joidenkin näkemysten mukaan yhteisöllinen media ei kuitenkaan kuvaa kaikkea sosiaalisen median toimintaa, koska kaikki sosiaalisen median toiminta ei ole välttämättä yhteisöllistä. (Sanastokeskus TSK 2010, 14.)

Yleisesti ottaen sosiaaliseen mediaan liittyy käyttäjien tuottama sisältö, vertaistuotanto ja käyttötuotanto, mikä tarkoittaa sitä, että sisällön käyttö ja tuotanto sekoittuvat. Sosiaaliseen mediaan liittyykin vahvasti se, etteivät ihmiset ole enää ainoastaan sisällön kuluttajia vaan myös sisällön tuottajia. Tästä seuraa myös se, että ihmiset ovat myös proharrastajia eli että he tekevät harrastuksekseen ammattilaistason tuotantoja. (Kalliala & Toikkanen 2009, 18.)

2.2 Sosiaalisen median suosituimmista palveluista

Facebook on verkkoyhteisöyhteisöpalvelu, johon ihmiset kirjautuvat omalla nimellään ja voivat siten pitää yhteyttä esimerkiksi ystäviinsä tai perheenjäseniinsä. Palvelun kehitti Mark Zuckerberg yhdessä kolmen opiskelukollegansa kanssa Harvardin yliopistossa Amerikan Yhdysvalloissa. Aluksi Facebookin käyttöoikeus oli rajoitettu vain Harvardin yliopiston opiskelijoihin, mutta vähitellen käyttöoikeuksia laajennettiin myös muihin yhdysvaltalaisiin yliopistoihin. Facebookin käyttöoikeuksien laajennettua myös muihin yliopistoihin, sen käyttöoikeudet avattiin lopulta kaikille yli 13-vuotiaille.

Facebook on nykyisin Internetin suosituin sosiaalisen median palvelu ja sillä yli 900 miljoonaa käyttäjää (Hachman 2012). Facebook tarjoaa käyttäjilleen mahdollisuuden jakaa henkilökohtaisia tietoja ja pitää yhteyttä muiden palvelun käyttäjien kanssa. Facebookia pidetään verkkoyhteisöpalveluna. Verkkoyhteisöpalvelulla tarkoitetaan palvelua, joka tarjoaa ihmisille mahdollisuuden muodostaa ihmisten välisiä suhteita ja ylläpitää niitä verkon kautta. (Sanastokeskus TSK 2010, 43, 26.)

YouTube on sisällönjakopalvelu, joka antaa käyttäjille mahdollisuuden julkaista videoita ja katsoa muiden käyttäjien julkaisemia videoita YouTubessa. Sisällönjakopalvelulla tarkoitetaan palvelua, joka tarjoaa mahdollisuuden sisällön jakamiseen tietoverkossa. (Sanastokeskus TSK 2010, 44, 27.)

YouTuben kehitti kolme entistä PayPalin työntekijää Chad Hurley, Steve Chen ja Jawed Karim helmikuussa 2005 (Hopkins 2006). Lokakuussa 2006 Google ilmoitti, että se haluaisi ostaa YouTuben. Osasyynä kauppaan oli YouTubeen ladattu tekijänoikeuksien piiriin kuuluva materiaali. Yksi YouTuben perustajista, Chad Hurley, kertoi ennen kauppaa, että kauppa Googlen kanssa antaa YouTubelle mahdollisuuden keskittyä paremmin tekijänoikeuksiin, koska Googlella on enemmän taloudellisia ja teknologisia resursseja asian hoitamiseen. (La Monica 2006.)

YouTubeen ladataan nykyisin maailmanlaajuisesti tarkasteltuna 60 tuntia videoita tunnissa, katsotaan päivittäin yli neljä miljardia videota ja YouTubessa käy kuukauden aikana yli 800 miljoonaa erillistä käyttäjää (YouTube 2012). Koska Google omistaa YouTuben, Googlen 1. päivänä maaliskuuta 2012 voimaan tulleet uudet käyttöehdot koskevat myös YouTuben käyttäjiä (Google 2012).

Twitter on verkkopalvelu, joka yhdistää yhteisöpalvelun ja mikroblogin ominaisuuksia. Mikroblogilla tarkoitetaan blogia, johon voi tehdä vain lyhyitä merkintöjä. Twitterissä käyttäjä voi lähettää lyhyitä viestejä, joita kutsutaan twiiteiksi (englanniksi tweet), ja jakaa ne muiden käyttäjien kanssa. Käyttäjä voi myös lukea muiden käyttäjien lähettämiä blogimerkintöjä. Blogimerkintöjä voidaan lähettää joko Twitterin verkkosivujen kautta tai matkapuhelimella. (Sanastokeskus TSK 2010, 44, 31.)

Twitterin perustivat Jack Dorsey, Evan Williams ja Biz Stone vuonna 2006 ja se syntyi Odeo-nimisen podcasting-palvelun sivutuotteena. Twitterin kehittämisen taustalla oli Jack Dorseyn ajatus siitä, että helppo tapa lähettää status-päivityksiä kollegojen kesken olisi tekstiviesti. Twitterin perustajat tekivät sen prototyypin kahdessa viikossa. Twitterin idea oli ainutlaatuinen sosiaalisen median maailmassa, koska käyttäjät pystyivät seuraamaan muita käyttäjiä ilman, että heitä seurattaisiin takaisin. Twitterissä kaikkien viestien oletus on julkinen ja viestien pituus on rajattu 140 merkkiin, jotta viesti mahtuu tekstiviestin pituuteen. (Miller 2010)

2.3 Tietoturvasta yleensä

Tietoturvan perusteena voidaan pitää CIA:ta. Tämä on helppo muistisääntö, koska CIA tarkoittaa tiedon luottamuksellisuutta (confidentiality), eheyttä (integrity) ja saatavuutta (availability). (Järvinen 2002, 22.)

Luottamuksellisuudella tarkoitetaan sitä, että tietoa ei pääse oikeudettomasti käyttämään kukaan sellainen henkilö, jolle tietoa ei ole tarkoitettu. Tietoa saavat muokata ja lukea vain ne, joille on annettu siihen lupa. (Järvinen 2002, 22.)

Tiedon eheydellä tarkoitetaan sitä, ettei mikään ulkopuolinen taho voi luvatta muuttaa tiedon sisältöä. Tässä tapauksessa muuttamisella tarkoitetaan esimerkiksi tiedostojen poistamista tai asiattomien muutosten tekemistä niihin. (Järvinen 2002, 22.)

Tietojärjestelmien toiminnan turvaamiseen liittyy tärkeänä osana tietojen ja palveluiden saatavuus. Verkkoyhteyksien ja tietokoneiden täytyy toimia silloin, kun tietoa halutaan käyttää. Tämä tarkoittaa verkkopalveluiden osalta käytännössä usein sitä, että verkkopalveluiden täytyy toimia 24 tuntia päivässä ja seitsemän päivää viikossa. (Järvinen 2002, 24.)

Tietosuoja on myös tärkeää tietoturvan kyseessä ollessa. Tietosuoja on erityisesti henkilötietojen käsittelyyn liittyvä termi. Internetissä kysytään usein käyttäjien henkilötietoja, vaikka kaikki kysytyt tiedot eivät välttämättä ole salaisia kuten henkilön nimi tai osoite. Tietojen aiheeton rekisteröinti ja yhdistely erilaisista lähteistä voi tuottaa tuloksen, josta on haittaa henkilölle itselleen. (Järvinen 2002, 30.)

3 Sosiaalisen median tietoturvasta

Sosiaaliseen mediaan liittyy paljon riskejä, jotka koskevat myös muuta Internetissä oloa, mutta joiden vaikutus on kasvanut sosiaalisen median myötä. On myös sellaisia potentiaalisia riskejä, joiden leviämisessä sosiaalisella medialla on ollut merkitystä. Tällaisia uhkia ovat esimerkiksi teknisissä uhissa erilaiset linkkien välityksellä leviävät uhat, jotka leviävät sosiaalisen median avulla nopeammin kuin aikaisemmin.

Suurin osa sosiaalisen median tietoturvariskeistä liittyy käyttäjän omaan toimintaan sosiaalisessa mediassa. Omasta toiminnasta mahdollisesti aiheutuvista riskeistä voidaan mainita esimerkiksi se, mitä käyttäjä itse päättää kertoa ja näyttää itsestään sekä keiden käyttäjä antaa nähdä kyseiset tiedot.

Tässä työssä käydään läpi yleisimpiä sosiaaliseen mediaan liittyviä tietoturvauhkia, mutta painopiste on yksityisyyteen liittyvissä uhissa.

3.1 Sosiaalisen median tekniset uhat

Sosiaalisen median teknisiä uhkia ovat esimerkiksi ne uhat, jotka koskevat palvelun teknistä toteutusta, sekä perinteiset virukset ja madot. Myös roskapostin leviäminen on ongelma. Esimerkiksi Facebookin koodia on vuodettu Internetiin siten, että hakkereille annettiin ehkä mahdollisuus päästä käsiksi käyttäjien yksityiseen informaatioon (Vander Veer 2008, 204). Facebookin ohjelmoinnissa on myös tapahtunut virheitä, joista johtuen käyttäjien yksityisiksi tarkoitetut tiedot ja kuvat näkyivätkin kaikille toisin kuin oli tarkoitettu (Järvinen 2012, 234).

Ohjelmia ja sovelluksia tehdään myös niin nopealla aikataululla, etteivät tietoturva ja testaus välttämättä pysy perässä. Tämä voi johtaa siihen, että palvelussa on haavoittuvuuksia, jotka johtuvat käytettävästä ohjelmointi- tai sovelluspalvelinteknologiasta. Myös käytettävässä selaimessa ja selaimen lisäohjelmistossa voi olla sellaisia haavoittuvuuksia, jotka mahdollistavat edellä mainittujen riskien toteutumisen. Esimerkiksi Firefoxiin julkaistiin vuonna 2010 lisäosa nimeltä Firesheep, joka kuunteli käyttäjän verkko-

liikennettä ja kaappasi sosiaalisessa mediassa käytettävät evästeet, minkä seurauksena oli mahdollista tehdä identiteettivarkauksia. (Valtiovarainministeriö 2010, 16–17.)

Sosiaalisen median suuri ja jatkuvasti kasvava käyttäjämäärä on houkutteleva kohde haittaohjelmien levittäjille. Riski saada haittaohjelma on suurempi sellaisten sosiaalisten median palveluiden käytössä, jossa selaimen täytyy suorittaa ohjelmakoodia, kuin sellaisilla palveluilla, jotka koostuvat ainoastaan tekstisisällöstä. (Valtiovarainministeriö 2010, 17.)

3.2 Haittaohjelmien leviäminen ja roskaposti sosiaalisessa mediassa

VAHTI 4/2010 (Valtiovarainministeriö 2010, 17) aineistossa tuodaan esiin neljä eri syytä, jotka edistävät haittaohjelmien leviämistä sosiaalisessa mediassa. Ensimmäinen syy on se, että kun henkilö saa sosiaalisessa mediassa viestin ystävältään, tutunoloiselta kaverilta tai työtoverilta, hän ajattelee viestin olevan luotettava. Jos sama viesti vastaanotettaisiin esimerkiksi sähköpostin välityksellä, sitä ei ehkä miellettäisi yhtä luotettavaksi. Tämä koskee erityisesti erilaisia yhteisöpalveluja.

Toisena syynä mainitaan lyhennetyt url-osoitteet. Etenkin Twitterissä, jossa on 140 merkin rajoitus, lyhennetyt url-osoitteet ovat yleisiä, koska pitkä osoite pitää saada lyhyemmäksi. Silloin käytetään url-osoitteen lyhentämispalvelua, esimerkiksi tinyurl.com. Haittapuolena linkin lyhentämisellä on se, että kun linkki on lyhennetty, ei voi tietää, minne linkki johtaa, ennen kuin linkin on avannut. Tällöin ei voi myöskään tietää, onko sivulla, jonne ollaan johdattamassa haittaohjelmia. Voi olla myös niin, että jos url-osoitteen lyhentämispalvelu ei olekaan luotettava, alun perin turvallisen ja luotettavan linkin tilalle voikin tulla linkki jonnekin haittaohjelmia sisältävälle sivulle. (Valtiovarainministeriö 2010, 17.)

Kolmantena syynä mainitaan, että sosiaalisen median palvelun tarjoaja ei ole välttämättä kiinnittänyt riittävästi huomiota oman palvelunsa tietoturvaan. Tällöin palveluun voi jäädä tietoturva-aukkoja, jotka mahdollistavat palvelun käyttäjän koneen saastuttamisen. (Valtiovarainministeriö 2010, 17.)

Neljäs mainittu syy on uudenlaiset haittaohjelmat, jotka on kehitetty hyödyntämään käytetyimpien sosiaalisen median palveluita. Näiden haittaohjelmien tarkoitus on ohjata käyttäjä hyökkääjän ylläpitämälle sivustolle henkilön luottamusta omaan verkostoonsa hyväksi käyttäen. (Valtiovarainministeriö 2010, 18.)

Roskapostin levittäjät osaavat myös käyttää sosiaalisen median palveluita hyväkseen. Sosiaalisen median kautta levitetyllä roskapostilla on ominaista se, että käytetään hyväksi hakukoneiden mahdollistamaa roskapostien kohdentamista tietyille ryhmille tai hyödynnetään suosittuja sivustoja tai ryhmiä roskapostin levittämisessä. (Valtiovarainministeriö 2010, 18.)

Tärkeimmät teknisten uhkien torjumiskeinot ovat maalaisjärki sekä ajantasainen virustorjuntaohjelma ja palomuuri. Myös muut tietokoneessa olevat ohjelmat on hyvä pitää ajan tasalla, kuten Internet-selain. Linkkihuijauksien osalta paras torjuntakeino on maalaisjärki eli käyttäjän kannattaa harkita tarkkaan linkin avaamista. (Tietoturvaopas 2012c.)

Roskapostilta voi suojautua ensinnäkin siten, että omaa sähköpostiosoitetta ei julkaista ainakaan perusmuodossa, vaan mieluummin esimerkiksi kuvatiedostona tai kaikki osat erotettuina, jotta automaattiset sähköpostiosoitteiden keräysohjelmat eivät pysty lukemaan osoitetta (Tietoturvaopas 2012b). Toinen hyvä tapa suojautua roskapostilta on tehdä kokonaan oma sähköpostiosoite sosiaalisen median käyttöön, jolloin käyttäjä ei käytä omaa henkilökohtaista sähköpostiosoitettaan sosiaaliseen mediaan kirjautumiseen (Vander Veer 2008, 206).

3.3 Sosiaalisen median yksityisyyteen liittyvät uhat

Sosiaalisessa mediassa kannattaa huomioida tarkasti omat yksityisyysasetukset. Esimerkiksi Facebookissa yksityisyysasetukset ovat yleensä lähtökohtaisesti heikoimmalla mahdollisella tasolla silloin, kun käyttäjä rekisteröityy Facebookiin (Vander Veer 2008, 205). Tällöin kaikki ne henkilöt, jotka menevät käyttäjän profiilisivulle, näkevät kaiken, mitä käyttäjä on itsestään kertonut. Jos yksityisyysasetukset ovat heikoimmalla mahdollisella tasolla, tietoja pääsevät katsomaan myös sellaiset henkilöt, joilla ei ole Faceboo-

kia. Samalla tiedot näkyvät myös yleisten hakukoneiden kautta, jos joku hakee käyttäjän nimeä esimerkiksi Googlella.

Twitterissä kuka tahansa voi lukea käyttäjän Twitter-viestejä, jos vain tietää tilin osoitteen. Twitter -tilejä on myös helppo hakea yleisellä hakukoneella. Edellä sanottu yhdistettynä Twitterin toimintoon, jossa käyttäjä ilmoittaa sijaintinsa viestin yhteydessä, sai aikaan sivuston PleaseRobMe, johon kirjattiin ihmisten Twitter-viestejä, joissa ihmiset kertoivat olevansa poissa kotoaan. PleaseRobMe-sivustolla haluttiin kiinnittää huomiota siihen, mitä tietoa ihmiset jakavat sosiaalisessa mediassa. Esimerkiksi Yhdysvalloissa New Hampshiren Nashuan kaupungissa ryöstettiin 50 kotia, kun murtovarkaat olivat saaneet tiedot asuntojen tyhjillään olosta esimerkiksi Facebookin status-päivityksistä ja muista verkkoyhteisöistä. (Linnake 2010.)

On myös otettava huomioon, että vaikka käyttäjä itse laittaisi tiukat rajat sosiaalisen median palvelun yksityisyysasetuksiinsa, käyttäjän omat kaverit voivat levittää käyttäjän omia tietoja omaa harkitsemattomuuttaan tai vahingossa. Tällöin käyttäjä ei voi enää kontrolloida sitä kenelle kaikille tieto leviää. (Järvinen 2010, 234.)

Sosiaalisen median käyttäjät lataavat paljon kuvia ja videoita sosiaalisen median palveluissa. Kuvissa olevien henkilöiden nimeäminen on myös nykyisin yleistynyt. Jos käyttäjä nimeää jonkun tai useamman kuvassa olevan henkilön, myöhemmin voi olla mahdollista hakea kyseisestä henkilöstä kuvia muualta Internetistä. (Järvinen 2010, 241.)

Kuvien nimeämiseen liittyy myös sama ongelma kuin omiin henkilökohtaisiin kuviin. Käyttäjä voi itse hallinnoida, mitä kuvia tai videoita laittaa omaan profiiliinsa ja ketkä kuvissa nimeää, mutta hän ei välttämättä pysty kontrolloimaan sitä, mitä kaveri laittaa omaan profiiliinsa ja päättääkö kaveri nimetä käyttäjän jossain kuvassa tai videossa, joka on käyttäjälle epäedullinen.

Edellä kerrotusta voidaan mainita esimerkkinä Helsingissä asuva 20-vuotias Vilhelmiina Rahikainen. Vilhelmiina Rahikainen huomasi, että hänen kuvansa oli päätynyt virolaisen kirjan kanteen. Kuva oli luultavasti otettu Rahikaisen blogista, jota Rahikainen on

pitänyt 17-vuotiaasta saakka. Kuvan käyttöön ei oltu kuitenkaan pyydetty lupaa. (Lämsä 2012.)

Nykyisin kannattaa varautua siihen, että mikään Internetiin laitettu ei häviä sieltä koskaan. YouTubeen laitettu video, Facebookiin laitettu nolo kuva tai blogiin kirjoitettu asia tai mielipide, joka myöhemmin kaduttaa, voi löytyä vielä vuosienkin päästä. Sivuista on helppo tehdä kopioita, ottaa ruutukuvia tai kopioida kuva tai video ja myöhemmin levittää sitä. Monet palveluntarjoajat eivät välttämättä poista profiilia, vaikka palvelusta eroaisikin. Facebookista ei voinut aluksi lainkaan erota, mutta myöhemmin se tehtiin mahdolliseksi (Järvinen 2010, 239–241).

Muutenkin kannattaa ajatella, mitä sosiaaliseen mediaan kirjoittaa. Jos ei ole pitänyt huolta yksityisyysasetuksista, voivat sellaisetkin henkilöt, joiden kirjoittaja ei haluaisi näkevän viestejä, nähdä ne. Esimerkiksi Volvo antoi potkut kolmelle työntekijälleen, kun yksi työntekijä oli laittanut Facebookiin viestin " Vielä yksi päivä viikkoa jäljellä tässä hullujenhuoneessa." Kun työnantaja oli nähnyt kyseisen viestin sekä kahden muun työntekijän samansävyiset kommentit viestiin, työnantaja oli ilmoittanut työntekijöille, etteivät he olleet enää tervetulleita työpaikalle. Koska työtekijät olivat olleet vuokratyöntekijöitä, irtisanominen oli heti mahdollista. (Kotilainen, 2011.)

Suomessa on voimassa laki yksityisyyden suojasta työelämässä (759/2004). Lain mukaan työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa työntekijältä itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Edelleen lain mukaan työnantajan on ilmoitettava työntekijälle saamistaan tiedoista ennen kuin niitä käytetään työntekijää koskevassa päätöksenteossa, jos työntekijää koskevia tietoja on kerätty muualta kuin työntekijältä itseltään. Vaikka työntekijän tietojen etsiminen Internetistä onkin Suomessa lain vastaista, näin ei välttämättä ole muissa valtiossa.

Yhteisöpalveluun annetut tiedot voivat päätyä myös kolmansien osapuolten käyttöön. Esimerkiksi Facebookissa on mahdollista asentaa kolmansien osapuolten tekemiä sovelluksia. Jos käyttäjä asentaa kolmannen osapuolen tekemän sovelluksen, käyttäjän on samalla annettava sovelluksen tekijälle pääsy omiin henkilötietoihinsa. Sen jälkeen, kun

käyttäjä on antanut luvan sovelluksen tekijälle päästä käsiksi henkilötietoihinsa, Facebook ei enää hallinnoi niitä tietoja. Facebook ei enää siinä tapauksessa päätä mihin tietoja käytetään, vaan tietojen käyttö on sovelluksen tekijän päätettävissä. (Vander Veer, 205.)

Identiteettivarkaudet ovat yksi sosiaalisen median uhista. Facebookissa ollaan omalla nimellä ja monesti myös blogeissa jaetaan yksityiskohtaista tietoa omasta elämästä. Identiteettivarkaudella tarkoitetaan sitä, että joku hankkii haltuunsa toisen henkilön tietoja ja alkaa asioida verkossa kyseisen henkilön tiedoilla. (Aalto & Uusisaari 2009, 126.)

Yksityishenkilöitä vastaan saatetaan hyökätä esimerkiksi tekemällä valetili tämän tunnuksilla. Mitä yksityiskohtaisempia tiedot ovat, tili on sitä vakuuttavampi. Usein näin tehdään ajattelemattomuutta tai pilan päiten, mutta siitä voi olla haittaa sille henkilölle, jonka tietoja on käytetty (Valtiovarainministeriö 2010, 15). Kyseessä voi olla myös ns. Social Engineering -tapaus, jossa yritetään päästä toisen henkilön tiedoilla käsiksi tietoihin ja/tai omaisuuteen, joihin kyseisellä henkilöllä on pääsy (Cert.fi, 2011).

Identiteettivarkaudesta hyvänä esimerkkinä voidaan mainita MTV3:n 45-minuuttia ohjelmassa olleen Sharon Rubanovitschin tapaus. Joku tuntematon henkilö oli laittanut Rubanovitschin nimissä Internetin deittisivustoille ilmoituksia, joihin tiedot oli luultavasti saatu Rubanovitschin omasta elämästään kertovasta blogista. Tapaus tuli Rubanovitschin tietoon, kun hänen Facebook profiiliinsa alkoi tulla viestejä miehiltä, jotka pyysivät lainaamaansa rahaa takaisin, vaikka Rubanovitsch ei tuntenut kyseisiä miehiä eikä ollut lainannut heille rahaa. Samassa lähetyksessä käsiteltiin myös Veera Korhoseen liittyvää tapausta, josta Viestintäviraston tietoturva-asiantuntijat etsivät Korhosesta kaiken tiedon minkä pystyi löytämään verkkoa selailemalla. (Tikkanen 2010.)

Paras tapa suojautua omaan yksityisyyteen liittyviin uhkiin on maalaisjärki. Kannattaa mieluummin olla kitsas sen kanssa, mitä Internetissä jakaa, oli se sitten videoita, kuvia tai tekstiä. Kannattaa myös pitää mielessä, mitä itse haluaa palvelulta ja ainoastaan se. Tällöin henkilö muistaa paremmin, mikä on tarpeellista materiaalia ja mikä on sellaista

materiaalia, jota ei tarvitse tai kannata jakaa. On myös hyvä muistaa pitää yksityinen yksityisenä.

Jos henkilö haluaa antaa itsestään tietyn kuvan Internetissä, tietoa ja materiaalia tulisi antaa tämän mukaan. Jos jokin tieto on valinnaista ja samalla arkaa tietoa, jota ei haluta satunnaisten henkilöiden vahingossakaan saavan tietää, se kannattaa jättää kertomatta. Edellä mainittuja tietoja voivat olla esimerkiksi puhelinnumero ja kotiosoite. (Tietoturvaopas 2012a; Vander Veer 2008, 206)

On myös hyvä käydä omat yksityisyysasetukset tarkoin läpi niissä palveluissa, joita käyttää. Esimerkiksi Facebookissa ei tarvitse kaikkea kaikkien muiden kanssa ja YouTubessa voidaan rajata ne henkilöt, jotka voivat nähdä palveluun laitetun videon. Hyvä sääntö pitää mielessä silloin, kun laittaa Internetiin jotain on se, että kun on laittanut jotain Internetiin, sitä ei välttämättä koskaan voi saada sieltä pois (Cert.fi 2011).

3.4 Muut riskit

Sosiaalisen median palveluissa, kuten muissakin rekisteröintiä vaativissa palveluissa, pyydetään ennen rekisteröintiä hyväksymään palvelun käyttöehdot. Palveluiden käyttöehtoihin sisältyy muun muassa kenelle palveluun ladatun ja kirjoitetun aineiston käyttöoikeudet kuuluvat. Usein voi olla niin, että laitettaessa esimerkiksi kuva johonkin palveluun, tällä palvelulla on käyttöoikeus kuvaan kunnes kuva poistetaan.

Facebookin käyttöehtoihin sisältyy esimerkiksi ehto siitä, että kun käyttäjä laittaa Facebookiin immateriaalioikeuksien piiriin kuuluvaa sisältöä, kuten esimerkiksi kuvat tai videot, käyttäjä antaa Facebookille luvan käyttää kaikkea sitä materiaalia, joka kuuluu siihen immateriaalioikeuksien lisenssiin, jonka käyttäjä on laittanut Facebookiin. Facebookin käyttöoikeus kyseisiin materiaaleihin loppuu vasta silloin, kun käyttäjä poistaa kyseisen tiedon Facebookista. Jos materiaalin Facebookin laittanut henkilö on kuitenkin jakanut materiaalin muiden käyttäjien kanssa ja muut käyttäjät eivät ole poistaneet sitä, Facebookin käyttöoikeus ei poistu ennen kuin kaikki muut käyttäjät ovat poistaneet materiaalin. (Facebook 2012.)

Käyttöoikeuksien ongelmana voidaan pitää myös sitä, että ne voivat muuttua hyvin usein, jolloin käyttäjän on itse pidettävä huoli siitä, että on tietoinen uusista muutoksista käyttöehtoihin. Muutoksiin voi sisältyä myös sellaisia kohtia, joita ei aikaisemmin ollut ja joita käyttäjä ei hyväksy (Järvinen 2010, 246). Jos palvelun tarjoaja pidättää itsellään kaikki oikeudet käyttäjän palveluun laittamaan materiaaliin, tämä mahdollistaa tiedon levittämisen ja edelleen välittämisen tai tiedon myynnin myös kolmansille osapuolille.

Yksi palveluun liittyvä asia, mikä kannattaa tarkistaa ennen kuin liittyy palveluun, on yksityisyyspolitiikka. Yksityisyyspolitiikan palveluun liittymisen ehtoihin sisältyy muun muassa, mihin palvelu käyttää keräämiänsä henkilötietoja ja millä tavalla palvelu kerää kyseisiä henkilötietoja. Ongelma yksityisyyspolitiikan ehtojen osalta on useimmiten se, että yksityispolitiikan ehtoja koskeva teksti on pitkä ja vaikeaselkoinen. Petteri Järvisen kirjassa Yksityisyys – Turvaa digitaalinen kotirauhasi todetaan, että yhdysvaltalainen tutkijaryhmä kävi läpi 75 suosittua amerikkalaispalvelua ja laski niiden yksityisyyspolitiikan pituuden. Tekstien keskipituus oli 250 sanaa, mutta pisimmät tekstit olivat 15 sivua ja 8000 sanaa. Facebookin teksti oli 5438 sanan pituinen. (Järvinen 2010, 246.)

Käyttäjän kannalta ongelmallista on myös palvelun sijaitseminen ulkomailla. Jos sosiaalisen median palveluiden tarjoaja sijaitsee ulkomailla, Suomen lainsäädäntö ei päde ja palvelun normaalien sopimusehtojen lisäksi noudatettavat lainsäädännön vaatimukset voivat poiketa huomattavasti Suomen lainsäädännöstä. Tällöin esimerkiksi suomalaisilla viranomaisille ei ole automaattisesti toimivaltaa poistaa laitonta aineistoa ulkomaisesta palvelusta. (Valtiovarainministeriö 2010, 19.)

4 Tutkimuksen empiirinen toteutus

Tutkimusmenetelmänä käytettiin HAAGA-HELIA ammattikorkeakoulun opiskelijoille suunnattua kyselyä, jonka tarkoituksena oli kartoittaa opiskelijoiden tietosuutta sosiaalisen median tietoturvasta ja heidän suhtautumistaan sosiaalisen median tietoturvauhkiin. Alkuperäinen idea oli tarkastella tuloksia myös vertailemalla sitä, onko sukupuolten välisissä vastauksissa eroja, mutta tästä luovuttiin vähäisestä vastausmäärästä johtuen.

4.1 Tutkimustehtävän jäsentyminen kysymyksiksi

Ensimmäinen tutkimuskysymys koski sitä, millaisia ovat eri koulutusohjelman opiskelijoiden käsitykset sosiaalisen median tietoturvasta. Aineiston saamiseksi tähän kysymykseen käytettiin kolmea mittarin kysymystä. ”Minkälainen käsitys sinulla on sosiaalisen median tietoturvasta?”. Vastaajille annettiin myös mahdollisuus antaa vapaamuotoisia perusteluja tähän kysymykseen. Jokaista opiskelijaa pyydettiin vastaamaan myös avoimeen kysymykseen: ”Minkälaisia tietoturvauhkia koet sosiaalisessa mediassa olevan?”. Tähän kysymykseen sai vastata omin sanoin. Kysymys ”Kuinka huolissasi olet sosiaalisen median tietoturvasta?” koski myös opiskelijoiden käsitystä sosiaalisen median tietoturvasta, mutta siltä näkökannalta, aiheuttaako sosiaalisen median tietoturva huolta opiskelijoissa. Edellä kuvatut kysymykset ovat mittarin kysymyksiä 4,7,6 ja 5 (Liite 1).

Toinen tutkimuskysymys koski eri koulutusohjelmien opiskelijoiden tietoisuutta erilaisista sosiaalisen median riskeistä. Tässä kysymyksessä keskityttiin erityisesti niihin riskeihin, jotka koskivat käyttäjän henkilökohtaisia tietoja ja yksityisyyttä. Kysymykset, joilla haettiin tähän ongelmaan vastausta, ovat mittarin kysymyksiä 8-13. (Liite 1).

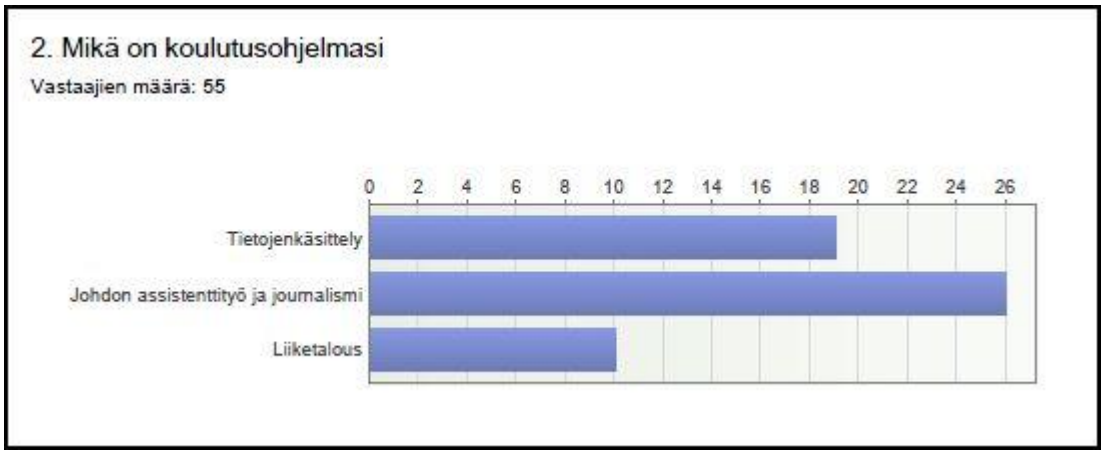
Kolmas vaihtoehtoinen tutkimuskysymys oli se, muuttuivatko eri koulutusohjelmien opiskelijoiden käsitykset sosiaalisen median tietoturvasta ja opiskelijoiden sosiaalisen median käyttö tutkimuksen aikana. Tähän ongelmaan aineisto saatiin mittarin kysymyksistä 14 ”Muuttuiko käsityksesi sosiaalisen median tietoturvasta tämän kyselyn jälkeen?” ja 16 ”Muuttuiko suhtautumisesi sosiaalisen median käyttöön tämän kyselyn jälkeen?”. Kysymykset 15 ja 17 olivat vapaaehtoisia kysymyksiä ”Jos muuttui niin miten?”, joihin sai perustella edellisen kysymyksen vastauksen omin sanoin (Liite 1 ja 2).

Tutkimuskysymykset ovat kokoavasti seuraavat:

1. Minkälainen opiskelijoiden käsitys sosiaalisen median tietoturvasta on?
2. Mikä on opiskelijoiden tietoisuus sosiaalisen median tietoturvariskeistä?
3. Muuttuiko opiskelijoiden suhtautuminen sosiaalisen median tietoturvaan ja sen käyttöön tutkimuskyselystä johtuen?

4.2 Kohderyhmä

Kohderyhmänä oli 450 HAAGA-HELIA ammattikorkeakoulun opiskelijaa. Näistä 150 oli tietojenkäsittelyn koulutusohjelmasta, 150 johdon assistentti ja journalismin koulutusohjelmasta ja 150 liiketalouden koulutusohjelmasta. Vastauksia kyselyyn saatiin 55 kappaletta, joista naisopiskelijoiden määrä oli 39 ja miesopiskelijoiden määrä oli 16. Kohderyhmä jakautui koulutusohjelmittain kuvion 1 osoittamalla tavalla. Vastauksia saatiin eniten johdon assistentin ja journalismin koulutusohjelman opiskelijoilta. Kaikista vastaajista tietojenkäsittelyn koulutusohjelman opiskelijoita oli 35 prosenttia, johdon assistentti ja journalismin koulutusohjelman opiskelijoita oli 47 prosenttia ja liiketalouden koulutusohjelman opiskelijoita oli 18 prosenttia.



Kuvio 1 Vastaajien koulutusohjelmat

4.3 Mittari, aineiston kerääminen ja käsittely

Kysymykset oli laadittu teoria-aineistoon perustuen. Muutamaa poikkeusta lukuun ottamatta kysymyksiin oli annettu monivalintakysymyksen asteikkoon perustuvat vasta-

usvaihtoehdot. Kysymyksissä suhtautumista sosiaalisen median tietoturvaan on kysytty pyytämällä arvioimaan sitä, huolettaako sosiaalisen median tietoturvassa jokin asia ja mahdollisesti sitä, mikä kyseinen asia on. Samalla kysyttiin myös, onko vastaajan suhtautuminen sosiaalisen median tietoturvaan muuttunut kyselyn jälkeen ja jos on niin miten.

Tietoisuutta on vaikeampi kysyä, joten niihin kysymyksiin käytettiin esimerkkejä yleisimmistä sosiaalisen median tietoturvaan liittyvistä asioista. Esimerkeillä oli tarkoitus täsmentää kysymystä sillä tavalla, että vastaaja ymmärtää kysymyksen idean kuitenkaan vastaajaa johdattelematta. Esimerkkeihin on käytetty teoriaosuutta ja kysymysten tarkoitus oli saada vastuksia teoriaosuudessa mainittuihin sosiaalisen median tietoruvariskeihin ja siihen, ovatko HAAGA-HELIA ammattikorkeakoulun oppilaat niistä kuinka tietoisia.

Ensimmäiseen tutkimuskysymykseen saatiin vastauksia kysymyksistä 4-7. Kysymykset 4, 6 ja 7 olivat pakollisia kysymyksiä ja kysymys 5 oli vapaaehtoinen avoin kysymys, jossa annettiin mahdollisuus perustella vastaus kysymykseen 4. Kysymykset 4 ja 7 olivat monivalintakysymyksiä, joissa käytettiin neliportaista asteikkoa. Kysymys 6 oli pakollinen kysymys, mutta siihen vastattiin omin sanoin. Kysymyksissä kysyttiin vastaajan käsitystä sosiaalisen median tietoturvasta, sosiaalisen median tietoturvauhista sekä siitä, kuinka huolissaan vastaaja on sosiaalisen median tietoturvasta.

Toiseen tutkimuskysymykseen kerättiin vastauksia kysymyksillä 8-13, joissa kysyttiin erilaisten esimerkkien avulla opiskelijoiden tietoisuutta erilaisista sosiaaliseen mediaan liittyvistä riskeistä, jotka koskevat käyttäjien yksityisyyttä ja tietoja. Kysymyksissä oli tarkoitus antaa esimerkki asiasta ja kysyä sen jälkeen, kuinka tietoinen opiskelija oli juuri kyseisestä asiasta. Kysymyksissä kysyttiin Facebookin käyttöehdoista, Facebookin kolmansien osapuolten sovellusten tietojenkeruusta, Googlen yksityisyyspolitiikasta, sosiaalisen median palveluiden sijainnista ja siitä miten, se vaikuttaa käyttäjään, jaetun materiaalin pysyminen ja myöhemmin mahdollinen löytyminen Internetistä ja identiteettivarkauden uhriksi joutumisen huolesta. Monet edellä mainituista ovat sellaisia, jotka koskevat useita sosiaalisen median palveluita. Esimerkiksi käyttöehdot, aineiston jakaminen, palveluiden sijainti ja tietojen pysyvyys Internetissä koskevat kaikkia suosittuja

sosiaalisen median palveluita. Kaikki kysymykset olivat pakollisia ja kysymysten tyyppi oli monivalinta. Jotta kysymyksiin saatiin vaihtelua, vastausvaihtoehtoja oli kolme.

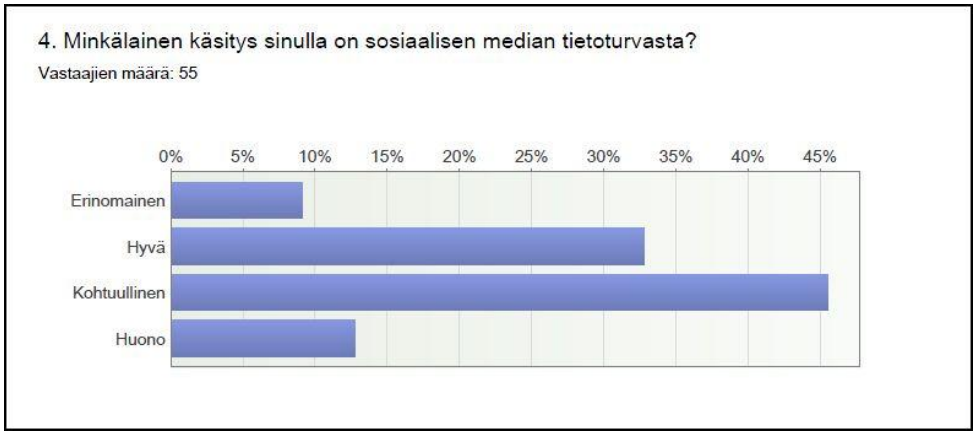
Kolmanteen tutkimuskysymykseen kerättiin vastauksia kysymyksillä 14–17. Kysymyksistä 14 ja 16 olivat pakollisia ja ne olivat monivalintakysymyksiä, joissa oli kolme eri vastausvaihtoehtoa. Kysymykset 15 ja 17 olivat vapaaehtoisia ja niissä annettiin mahdollisuus perustella kysymysten 14 ja 16 vastaukset omin sanoin. Kysymyksillä pyrittiin saamaan tietoa sitä, muuttuiko vastaajan käsitys sosiaalisen median tietoturvasta tai sosiaalisen median käytöstä tämän kyselyn jälkeen.

5 Tulokset ja niiden tarkastelu

Tuloksia tarkastellaan tutkimuskysymysten mukaisessa järjestyksessä ja tulokset havainnollistetaan kuvioiden avulla. Monivalintakysymyksiin saatujen vastausten tulokset esitetään prosentuaalisesti. Lisäksi käsitellään sanallisesti avoimiin kysymyksiin saatuja vastauksia.

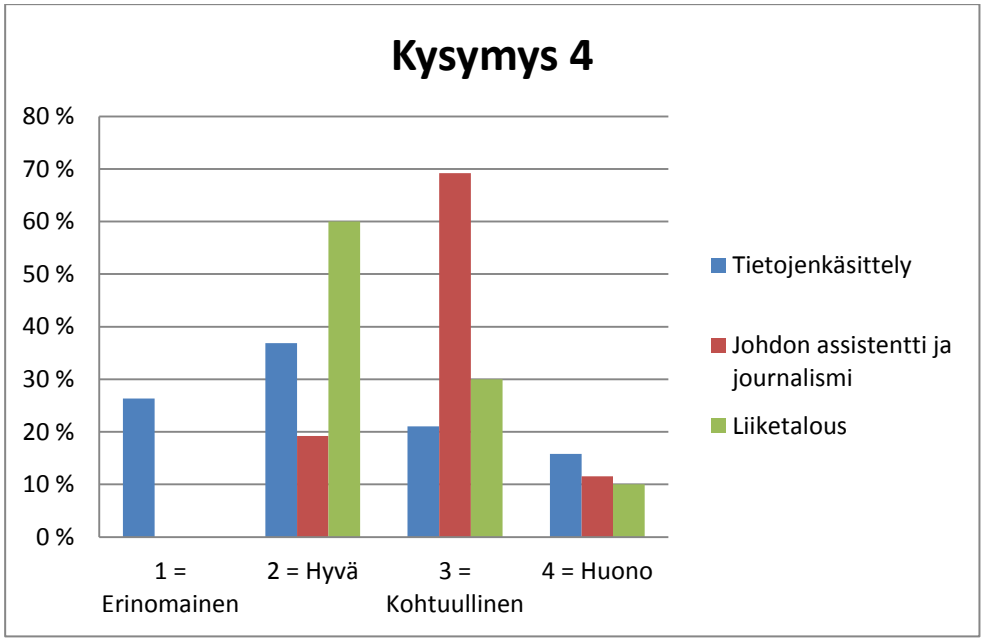
5.1 Opiskelijoiden käsitys sosiaalisen median tietoturvasta

Ensimmäiseen tutkimuskysymykseen liittyviin kysymyksiin annetuista vastauksista paljastuu se, että oppilaiden käsitys sosiaalisen median tietoturvasta ei ole yleisesti ottaen kovin hyvä. Yli puolet vastaajista oli sitä mieltä, että sosiaalisen median tietoturva on kohtuullista tai huonoa (Kuvio 2).



Kuvio 2 Vastaajien käsitys sosiaalisen median tietoturvasta

Jos käsityksiä sosiaalisen median tietoturvasta tarkastellaan koulutusohjelmittain, havaitaan eroja saatujen vastausten perusteella (Kuvio 3). Yli puolella tietojenkäsittelyn opiskelijoilla oli erinomainen tai hyvä käsitys sosiaaliseen median tietoturvasta. Sen sijaan johdon assistentti ja journalismin opiskelijoista noin 80 prosentilla on kohtuullinen tai huono käsitys sosiaalisen median tietoturvasta (Kuvio 3).



Kuvio 3 Vastaajien käsitys sosiaalisen median tietoturvasta koulutusohjelmittain

Kysymys 5 oli vapaamuotoinen kysymys ja siinä annettiin mahdollisuus perustella kysymyksen 4 vastausta omin sanoin. Muutama vastaaja ilmoitti, että hän pitää omaa tietoansa sosiaalisen median tietoturvasta erinomaisena tai hyvänä sen vuoksi, että sosiaalisen median tietoturvaan liittyvät kysymyksen kuuluivat työnkuvaan tai että vastaaja opiskeli alaa. Muutama vastaaja ilmoitti, että hänen tietonsa tulivat lähinnä kavereilta tai uutisista. Jotkut vastaajista totesivat myös, että he ovat tietoisia riskeistä ja siten myös yrittävät välttää niitä (Liite 2).

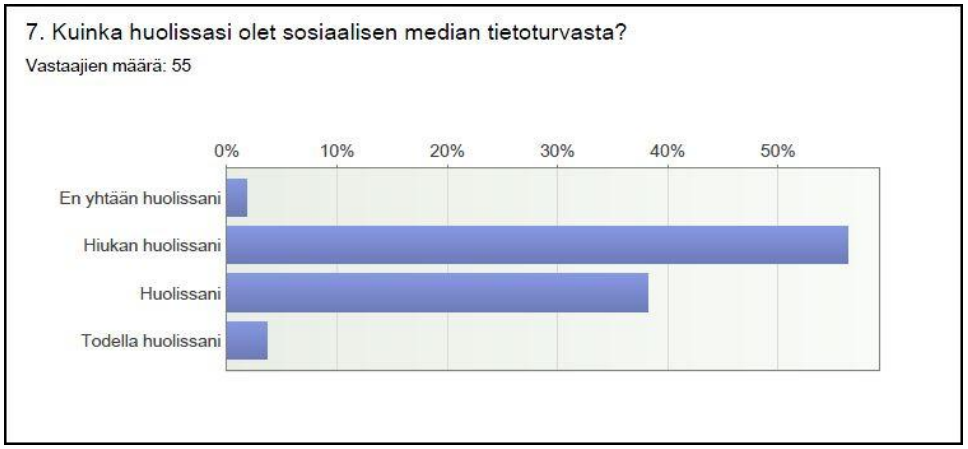
Kysymykseen 5 vastattiin vapaamuotoisesti esimerkiksi seuraavasti:
”Sosiaalista mediaa useita vuosia käyttäneenä ja tietoturva-alalla työskentelevänä käsitykseni tietoturvasta yleensäkin on hyvä.”
”En jaksa lukea käyttäjäehtoja, käsitykseni perustuu siihen mitä olen kuullut ystäviltäni ja uutisista.”
”Ko sovellusten tarkoitus on tehdä omistajilleen tuottoa kaupallisten sovellusten kautta, joten pääpaino lienee siinä, ei tietoturvassa tms.”
”Tiedot monien ihmisten saatavilla, käyttäjillä ei käsitystä kokonaisuudesta.”

Kysymys 6 oli pakollinen vapaamuotoinen kysymys, jossa pyydettiin kertomaan, minkälaisia tietoturvauhkia vastaaja kokee sosiaalisessa mediassa olevan. Vastauksissa esiintyi usein identiteetin kaappaus (identiteettivarkaus) ja tiedon leviäminen sellaisille tahoille,

joille tieto ei ollut tarkoitettu. Kysymykseen saaduissa vastauksissa mainittiin myös erilaiset phishing yritykset, tietojen kalastelu, virukset sekä hakkerit, jotka yrittävät hankkia yksityistä tietoa (Liite 2).

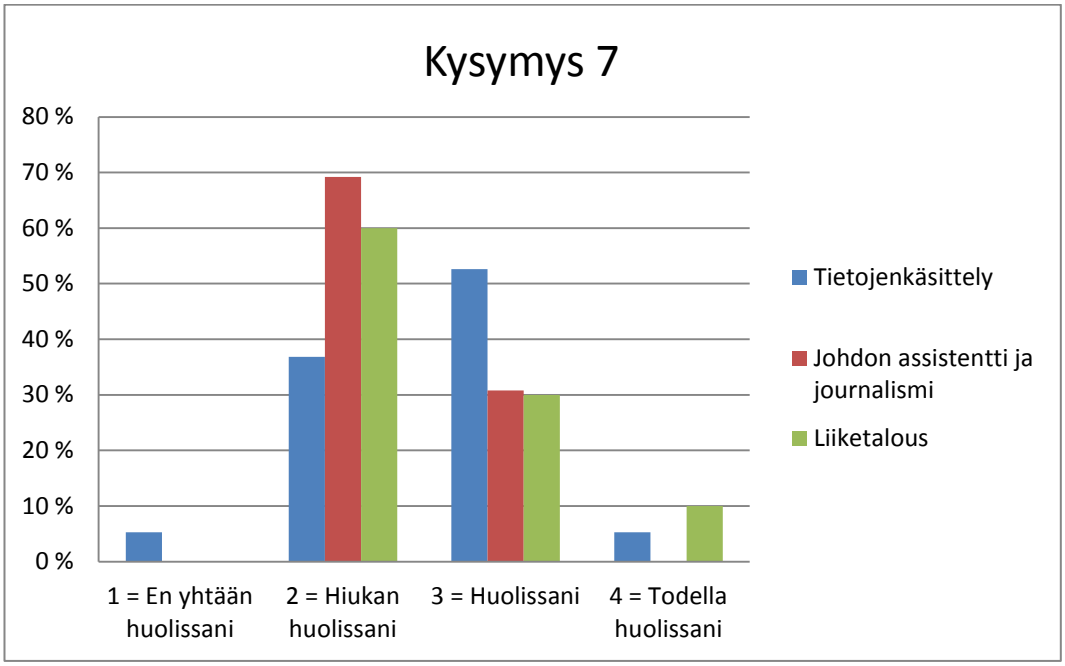
Kysymykseen 6 vastattiin vapaamuotoisesti esimerkiksi seuraavasti:
”identiteettivarkaudet”
”Samanlaisia kuin muuallakin, viruksia. Sosiaalisessa mediassa uhat voivat vielä olla vakavampiakin koska saadaan henkilökohtaisia tietoja helposti.”
”Suurimpana uhkana koen sen, että tietojani päätyy sellaisten ihmisten käsiin, joihin niitä ei ole tarkoitettu”
”Henkilökohtaisten tietojen leviäminen vääriin käsiin, tietojen "säilyvyys" eli et voi välttämättä poistaa olemassa olevia tietojasi”
”Hakkeroinnit ja muut tietomurrot ja -vuodot. Virukset ja muut jotka kaappaavat salasanoja.”

Valtaosa vastaajista oli ainakin hiukan huolissaan sosiaalisen median tietoturvasta. Vain kaksi prosenttia ei ollut yhtään huolissaan sosiaalisen median tietoturvasta ja vain neljä prosenttia vastaajista oli todella huolissaan sosiaalisen median tietotuvasta (Kuvio 4).



Kuvio 4 Vastaajien huoli sosiaalisen median tietoturvasta

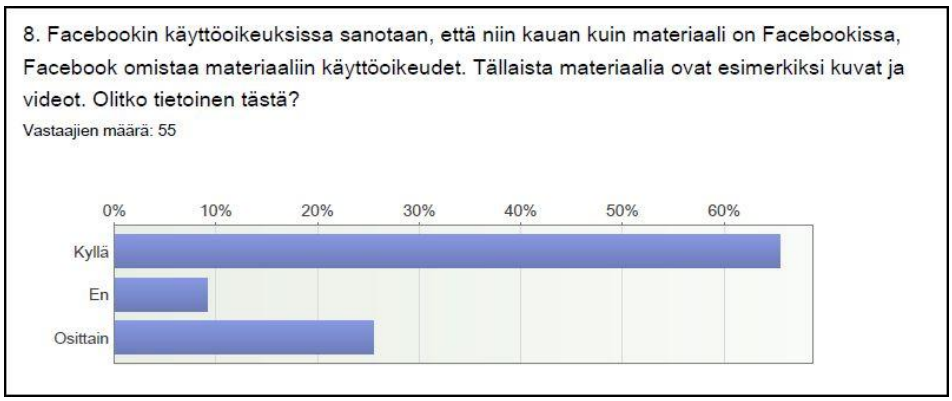
Kun tarkastellaan vastauksia koulutusohjelmittain, voi huomata, että ääriarvot olivat harvinaisia ja että hajontaa oli kahden keskimmäisen vaihtoehdon välillä. Tietojenkäsittelyn opiskelijat ovat enemmän huolissaan sosiaalisen median tietoturvasta kuin muiden koulutusohjelmien opiskelijat.



Kuvio 5 Vastaajien huoli sosiaalisen median tietoturvasta koulutusohjelmittain

5.2 Opiskelijoiden tietoisuus sosiaalisen median tietoturvariskeistä

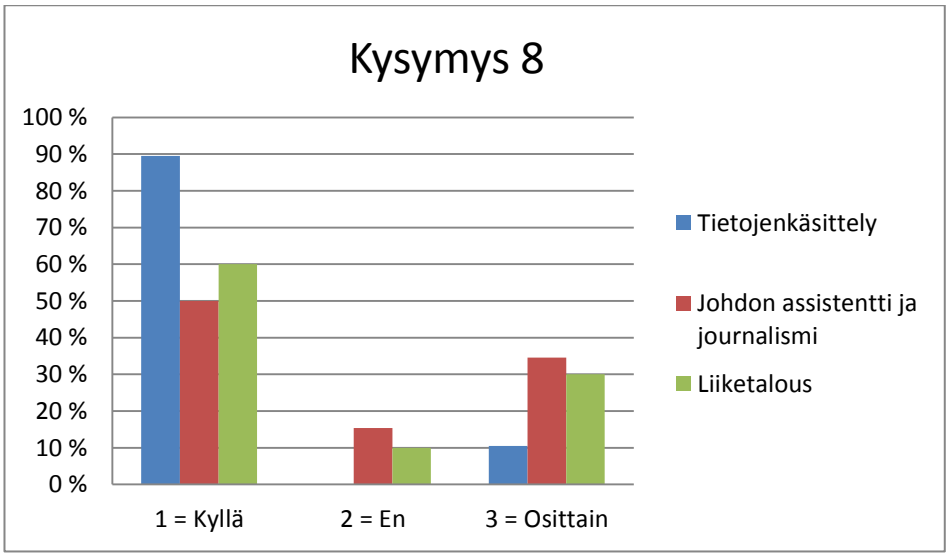
Toisen tutkimuskysymyksen ongelmiin käytettiin mittarin kysymyksiä 8, 9, 10, 11, 12 ja 13. Kysymyksessä 8 kysyttiin sitä, kuinka hyvin vastaajat tiesivät esimerkkinä käytetyn Facebookin käyttöehdoista löytyneestä ehdosta. Vastaajat olivat hyvin perillä kyseisestä ehdosta, sillä yli 60 prosenttia oli tietoinen kyseisestä ehdosta. Tosin lähes kymmenen prosenttia vastaajista ei tiennyt mitään kerrotusta käyttöehdosta (Kuvio 6).



Kuvio 6 Tietoisuus Facebookin käyttöoikeuksiin sisältyvästä omistajuusehdosta

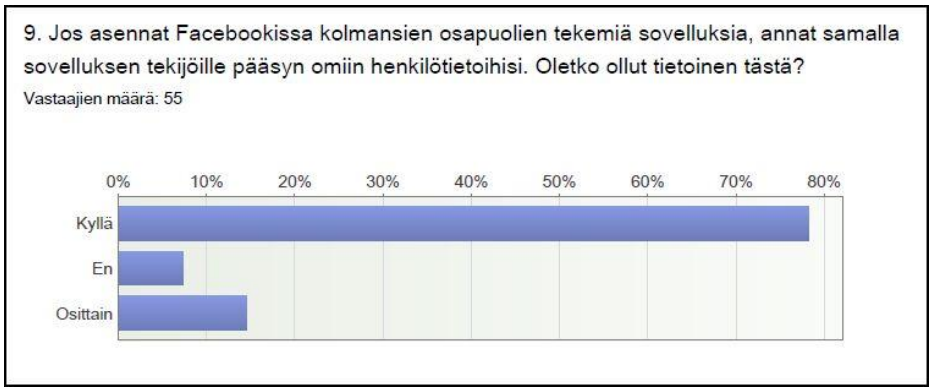
Koulutusohjelmittain eroja löytyi jonkin verran. Vastanneista tietojenkäsittelyn opiskelijoista 90 prosenttia tiesi Facebookin ehdosta. Puolet vastanneista johdon assistentti ja

journalismin opiskelijoista tiesi ehdosta ja liiketalouden opiskelijoista 60 prosenttia. Osittain ehdosta tiesi 30 prosenttia johdon assistentti ja journalismi sekä liiketalouden vastanneista opiskelijoista (Kuvio 7).



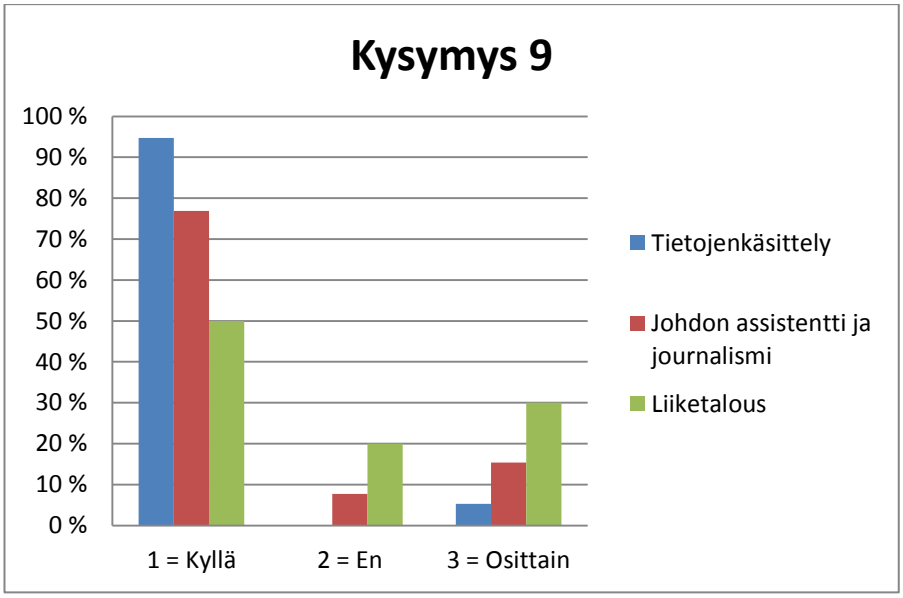
Kuvio 7 Tietoisuus Facebookin käyttöoikeuksiin sisältyvästä omistajuusehdosta koulutusohjelmittain

Kysymyksessä 9 kysyttiin, tiesivätkö vastaajat Facebookin kolmansien osapuolien tekemien sovellusten tietojenkeruusta. Lähes 80 prosenttia vastaajista vastasi tietävänsä siitä (Kuvio 8).



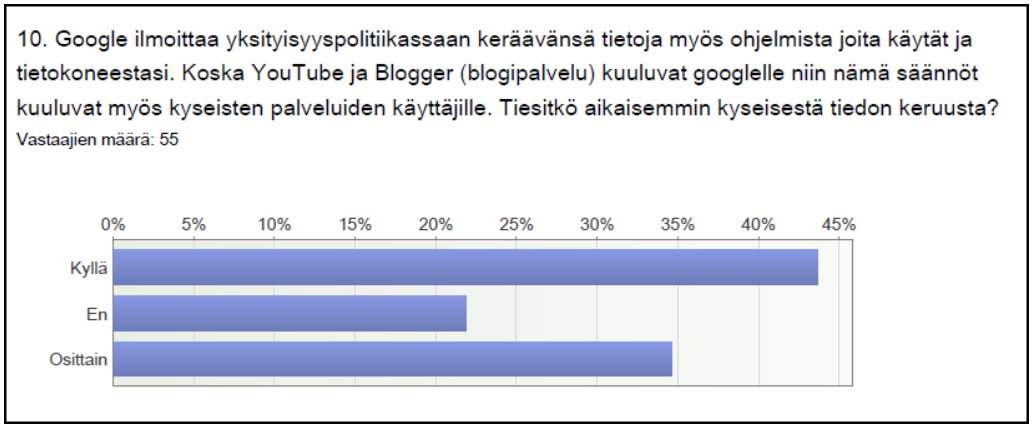
Kuvio 8 Tietoisuus omiin henkilötietoihin pääsystä Facebookissa

Valtaosa kysymykseen vastanneista opiskelijoista koulutusohjelmasta riippumatta tiesi tietojenkeruusta (Kuvio 9).



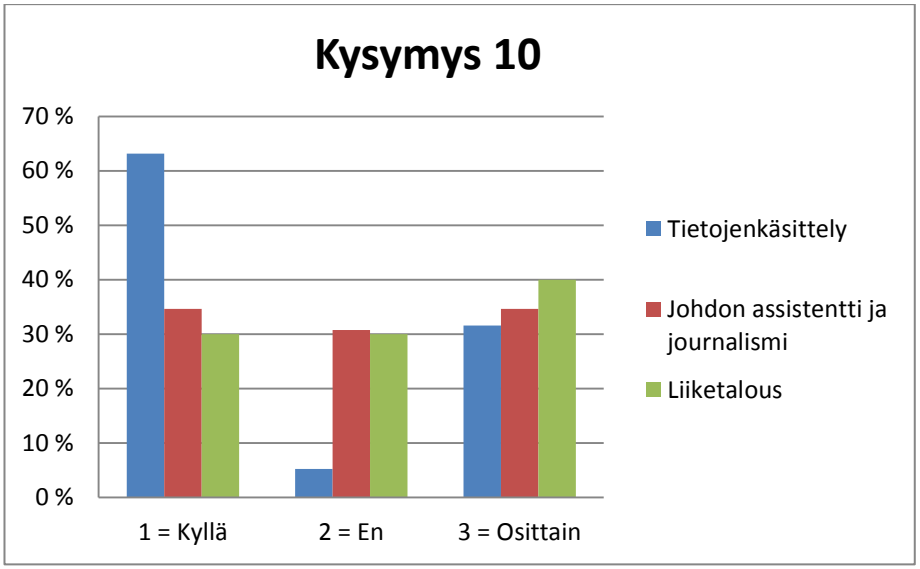
Kuvio 9 Tietoisuus omiin henkilötietoihin pääsystä Facebookissa koulutusohjelmittain

Kysymyksessä 10 kysyttiin Googlen yksityisyyspolitiikan ehtoja koskevasta ehdosta, jonka mukaan Google kerää tietoja myös käyttäjän tietokoneesta sekä ohjelmista, joita käyttäjä käyttää. Alle puolet kyselyyn vastaajista ilmoitti tietävänsä kyseisestä ehdosta ja osittain siitä tiesi lähes 35 prosenttia vastaajista (Kuvio 10).



Kuvio 10 Tietoisuus Googlen keräämistä tiedoista

Varmimmin asiasta ilmoitti tietävänsä tietojenkäsittelyn koulutusohjelman vastaajat, joista yli 60 prosenttia ilmoitti tietävänsä ehdosta. Sekä johdon assistentti ja journalismin että liiketalouden koulutusohjelman vastaajista 30 prosenttia vastasi, että he eivät tienneet kyseisestä ehdosta (Kuvio 11).

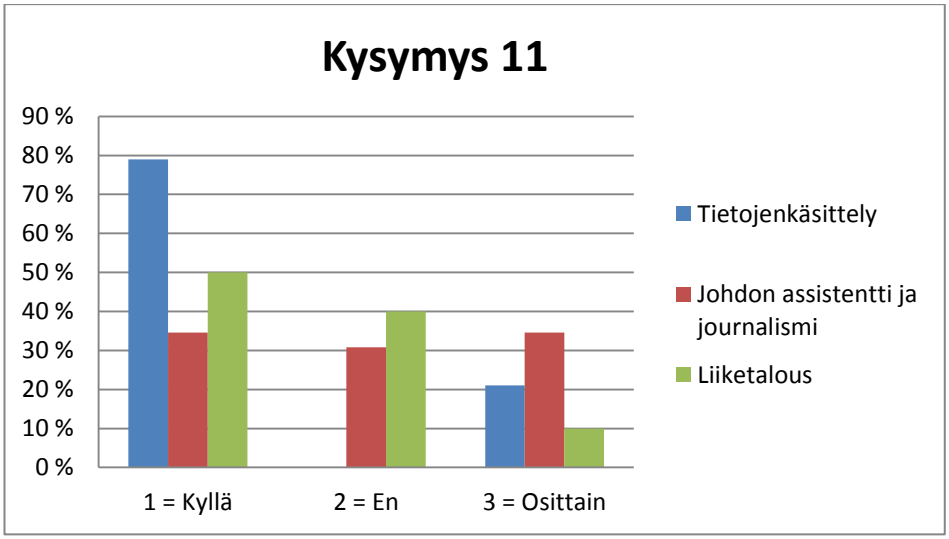


Kuvio 11 Tietoisuus Googlen keräämistä tiedoista koulutusohjelmittain

Kysymyksessä 11 kysyttiin sitä, kuinka tietoisia vastaajat olivat siitä, että palveluiden sijaitseminen ulkomailla tarkoittaa, että mahdollisissa riitatilanteissa noudatetaan sen valtion lakeja, jossa palvelu sijaitsee. Hieman yli 50 prosenttia vastaajista vastasi olevansa tietoisia asiasta ja vähän yli 20 prosenttia ilmoitti että eivät tienneet siitä (Kuvio 12).

Kuvio 12 Tietoisuus ulkomaisen lainsäädännön soveltamisesta

Kun vertaillaan koulutusohjelmakohtaisia tuloksia keskenään, tietojenkäsittelyn koulutusohjelman vastaajista melkein 80 prosenttia ilmoitti tietävänsä asiasta. Johdon assistentti ja journalismin koulutusohjelman opiskelijoiden vastaukset jakautuivat tasaisesti, sillä vastauksiin kyllä, ei ja osittain tuli melkein sama määrä vastauksia (Kuvio 13).

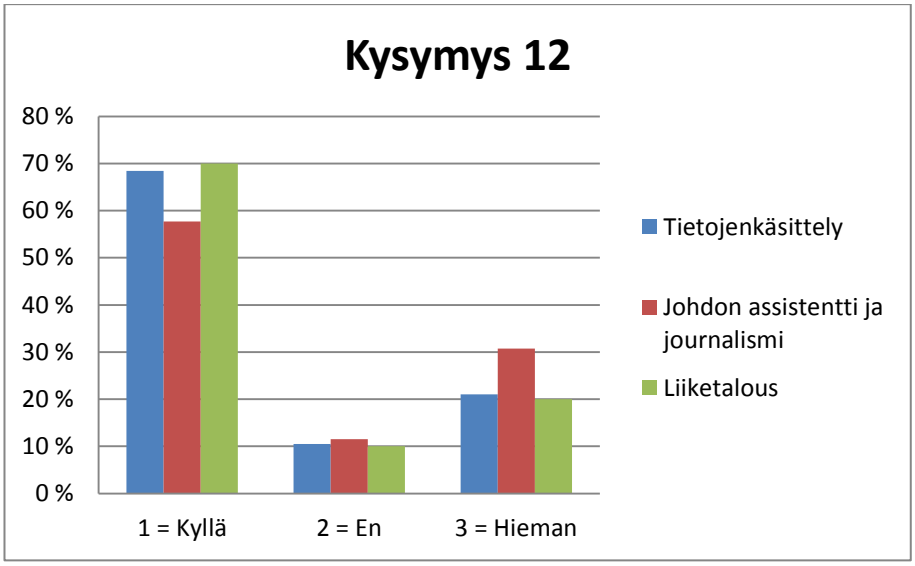


Kuvio 13 Tietoisuus ulkomaisen lainsäädännön soveltamisesta koulutusohjelmittain

Kysymyksessä 12 kysyttiin, onko vastaaja ajatellut sitä, että Internetistä voi löytyä myöhemmin jokin epäedullinen häntä koskeva asia, jonka tämä on sinne laittanut aikaisemmin. Vastaajista enemmistöä tuntui huolettavan se, että joskus heistä voisi löytyä jokin kuva/teksti/video joka antaa heistä epäedullisen kuvan sillä hetkellä. Vastaajista vain kymmentä prosenttia ei huolettanut sellaisen materiaalin löytyminen Internetistä joskus tulevaisuudessa (Kuvio 14).

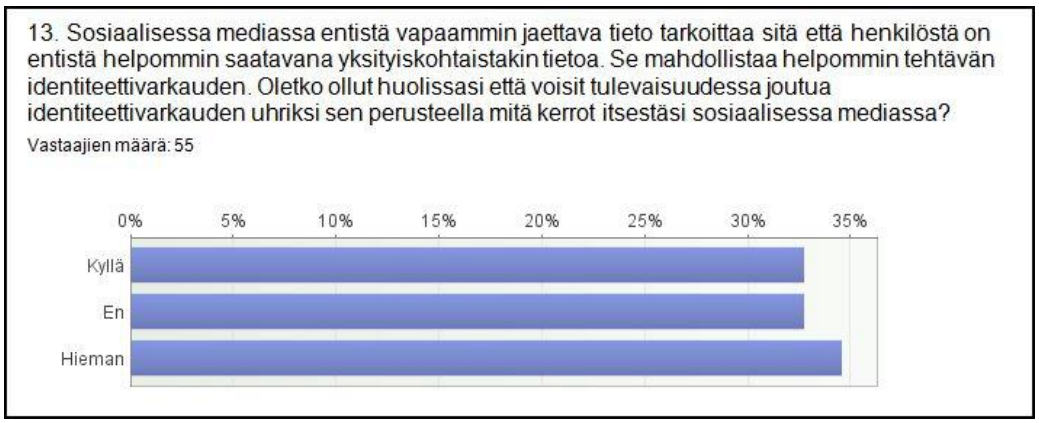
Kuvio 14 Huoli itselle epäedullisen aineiston löytymisestä myöhemmin Internetistä

Jokaisesta eri koulutusohjelmasta vastanneista vain hyvin pientä osaa asia ei huolettanut. Suhteellisesti vähiten ”kyllä” vastasi johdon assistentti ja journalismin koulutusohjelman opiskelijat, mutta toisaalta saman koulutusohjelman vastaajista oli myös suhteellisesti eniten valinnut vaihtoehdon ”hieman” (Kuvio 15).



Kuvio 15 Huoli itselle epäedullisen aineiston löytymisestä myöhemmin Internetistä koulutusohjelmittain

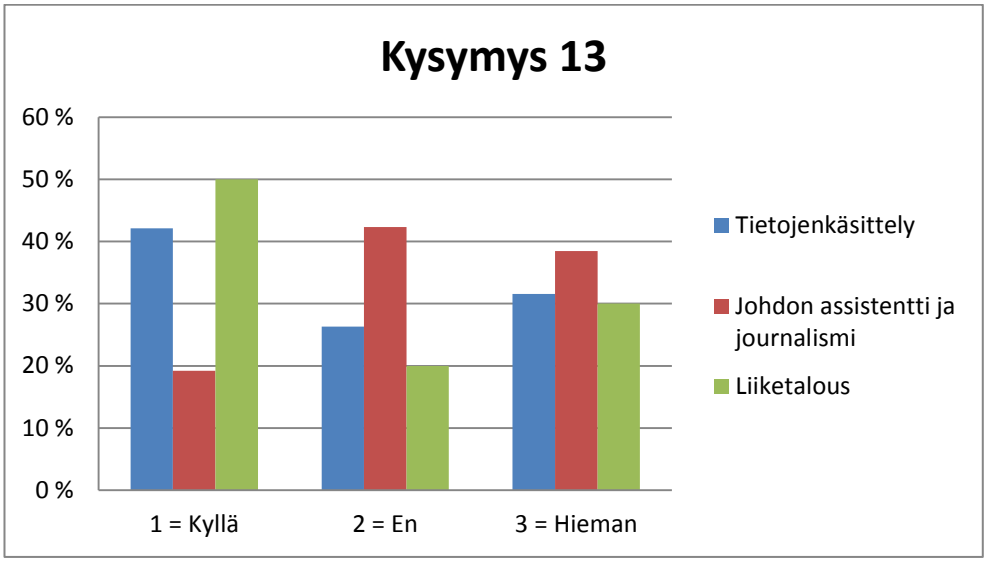
Kysymyksessä 13 kysyttiin, onko vastaaja huolissaan siitä, että voisi joutua identiteettivarkauden uhriksi. Kysymyksen 13 vastaukset jakautuivat hyvin tasaisesti. Jos kuitenkin tarkastellaan vastausvaihtoehtoja kyllä ja hieman, niin selvä enemmistö eli yli kaksi kolmasosaa vastaajista on ainakin hieman huolissaan identiteettivarkaudesta (Kuvio 16).



Kuvio 16 Huoli identiteettivarkaudesta

Suhteellisesti vähiten selvästi huolissaan identiteettivarkauksista oli johdon assistentti ja journalismin vastaajat, joista vähän alle 20 prosenttia vastasi ”kyllä”. Tietojenkäsittelyn koulutusohjelman vastaajista vähän yli 40 prosenttia ja liiketalouden koulutusohjelman vastaajista 50 prosenttia vastasi olevansa huolissaan identiteettivarkauksista. Toisaalta johdon assistentti ja journalismin koulutusohjelman vastaajista yli 40 prosenttia vastasi, että he eivät ole huolissaan identiteettivarkauksista, kun esimerkiksi tietojenkäsittelyn

koulutusohjelman vastaajista alle 30 prosenttia vastasi, että vastaaja ei ole huolissaan identiteettivarkauksista (Kuvio 17).



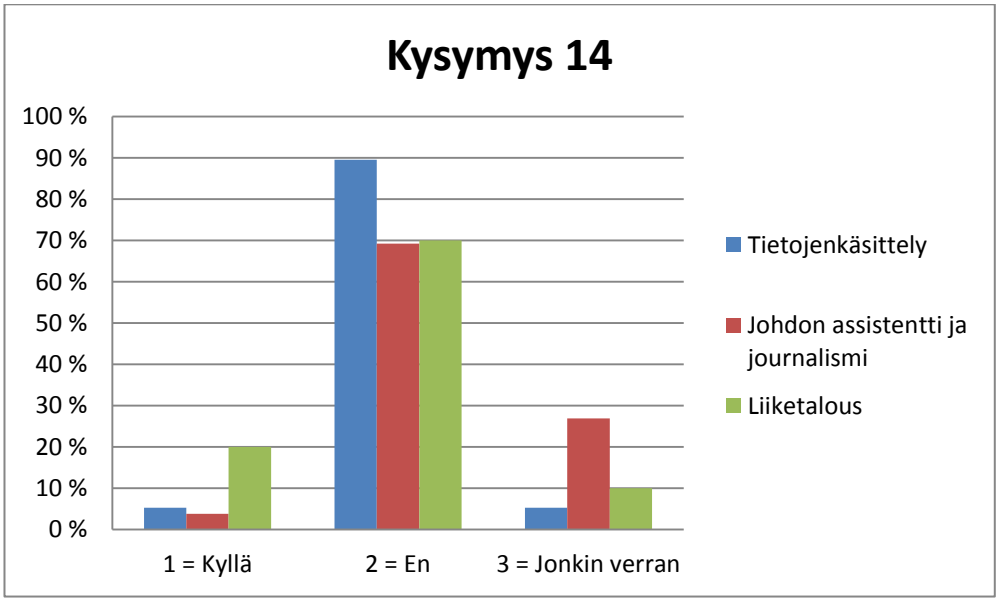
Kuvio 17 Huoli identiteettivarkaudesta koulutusohjelmittain

5.3 Muuttuiko opiskelijoiden suhtautuminen kyselyn jälkeen

Tutkimuskysymykseen 3 eli siihen, vaikuttiko kysely vastanneiden opiskelijoiden asenteisiin sosiaalisen median tietoturvaan ja sosiaalisen median käyttöön, käytettiin kysymyksiä 14, 15, 16 ja 17.

Kysymyksessä 14 kysyttiin, muuttuiko vastaajan käsitys sosiaalisen median tietoturvasta tämän kyselyn jälkeen. Monivalintakysymyksiin saatujen vastausten perusteella kysely vaikutti opiskelijoiden käsityksiin vain vähän. Kuitenkin joidenkin opiskelijoiden käsitys muuttui ainakin jonkin verran (Kuvio 18). Vastauksissa ei ollut myöskään suurempia eroja koulutusohjelmittain (Kuvio 19).

Kuvio 18 Käsityksen muuttuminen sosiaalisen median tietoturvaan kyselyn jälkeen



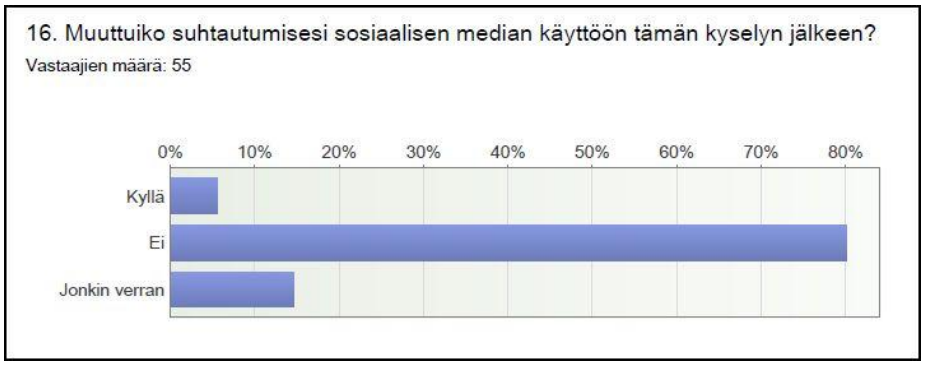
Kuvio 19 Käsityksen muuttuminen sosiaalisen median tietoturvaan kyselyn jälkeen koulutusohjelmittain

Kysymys 15 oli avoin kysymys, jossa voitiin perustella kysymykseen 14 annettua vastausta. Vastaajien kommenteista kävi aika usein ilmi, että kysely oli kuitenkin toiminut joillekin muistutuksena siitä, että sosiaalisen median tietoturvaan pitää kiinnittää enemmän huomiota. Toisista vastauksista kävi ilmi, että vastaajille ei ollut kyselystä vaikutusta sen takia, että olivat jo aikaisemmin hyvin perillä sosiaalisen median tietoturvaan mahdollisesti liittyvistä uhista (Liite 2).

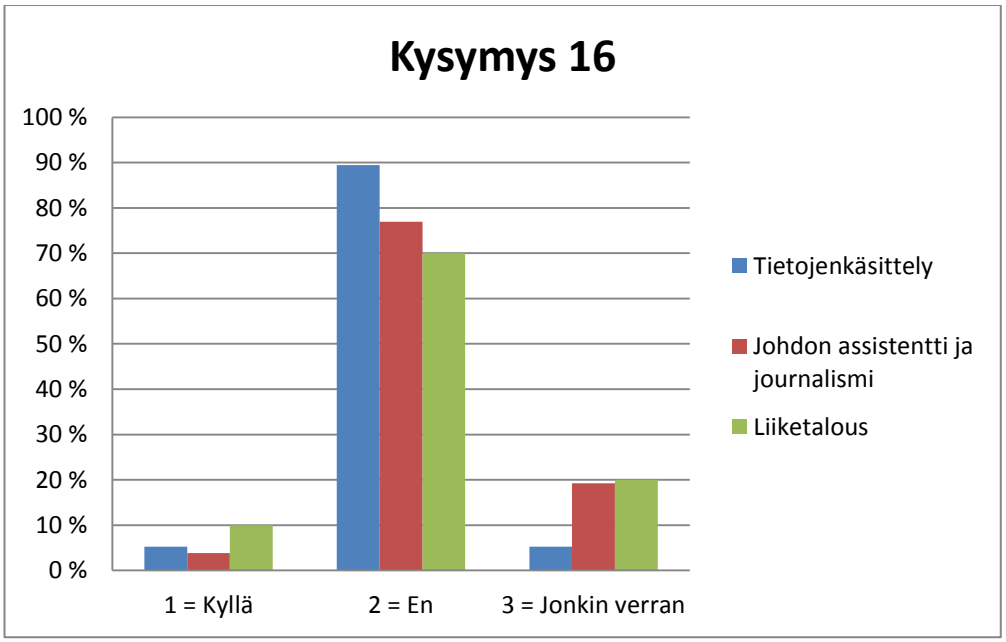
Avoimiin kysymyksiin annetuissa vastauksissa kirjoitettiin muun muassa seuraavaa: ”Olen tietoinen ongelmista, mutta minulla ei ole tarvittavaa tieto-taitoa asian parantamiseksi. Kysely oli minulle muistutus siitä, että pitää olla tarkempi.”

”Pitää olla varaivainen. Uhkat tuntee, mutta ne aina helposti unohtaa ja niin ei saisi käydä.”

Kysymyksessä 16 kysyttiin, muuttuiko vastaajan suhtautuminen sosiaalisen median tietoturvasta tämän kyselyn jälkeen. Monivalintakysymyksiin saatujen vastausten perusteella tehdyllä kysymyksellä ei ollut vaikutusta sosiaalisen mediankäyttöön vastanneiden keskuudessa (Kuvio 20). Vastauksissa ei myöskään ollut erityisiä koulutusohjelmakohtaisia eroja (Kuvio 21).



Kuvio 20 Suhtautumisen muuttuminen sosiaalisen median käyttöön kyselyn jälkeen



Kuvio 21 Suhtautumisen muuttuminen sosiaalisen median käyttöön kyselyn jälkeen koulutusohjelmittain

Kysymykseen 16 liittyi myös kysymys 17, joka oli avoin vapaamuotoinen kysymys, jossa sai kertoa syitä kysymyksen 16 vastaukseen. Näissä vastauksissa useat vastaajat ilmoittivat, että he saattavat jatkossa miettiä tarkemmin, mitä laittavat sosiaalisen median palveluihin (Liite 2).

Avoimiin kysymyksiin annetuissa vastauksissa kirjoitettiin muun muassa seuraavaa:
”Varmaan katson vielä tarkemmin, mitä tietoja itsestäni julkaisen netissä.”
”Pitäisi varmaan tiedottaa fb-ystäville, että mikäli he haluavat lisätä kuviani someen, siihen pitäisi kysyä lupa. Itse pyrin harkitsemaan tarkoin, mikäli laitan fb:hen kuvia ja esim. lasteni kuvien suhteen olen tarkka, ja lataan kuvia vasta kysyttyäni myös lasten isän mielipidettä.”
”Olen jo nyt passiivinen käyttäjä, joten luultavasti muutuin vielä passiivisemmaksi ;)”

6 Tulosten arviointia ja pohdintaa

Työssä tarkasteltiin kolmea eri kysymyskokonaisuutta, joista ensimmäinen koski HAAGA-HELIA ammattikorkeakoulun opiskelijoiden käsitystä sosiaalisen median tietoturvasta. Toinen kysymyskokonaisuus koski opiskelijoiden tietoisuutta sosiaalisen median tietoturvariskeistä ja kolmas opiskelijoiden käsitystä siitä, muuttuiko heidän suhtautumisensa kyselyn jälkeen sosiaalisen median tietoturvaan tai sosiaalisen median käyttämiseen. Kysely lähetettiin 450 opiskelijalle, joista kyselyyn vastasi 55 opiskelijaa eli noin 12 prosenttia opiskelijoista.

Ensimmäiseen tutkimuskysymykseen, joka koski opiskelijoiden suhtautumista sosiaalisen median tietoturvaan, voisi kysymyksiin saatujen vastausten perusteella päätellä, että sosiaalisen median tietoturvaan suhtaudutaan yleisesti ottaen hieman varauksellisesti. Vastaajista tietojenkäsittelyn opiskelijat suhtautuivat kaikkein varautuneimmin sosiaalisen median tietoturvaan ja myös arvioivat omat tietonsa sosiaalisen median tietoturvasta paremmiksi kuin muiden koulutusohjelmien opiskelijat.

Toiseen tutkimuskysymykseen saatujen vastausten perusteella voidaan ehkä vetää se johtopäätös, että julkisuudessa esillä olleista asioista tiedetään jonkin verran enemmän kuin niistä, jotka mainitaan esimerkiksi ainoastaan sosiaalisen median palveluntarjoajan käyttöehdoissa. Tietojenkäsittelyn koulutusohjelman opiskelijat tuntuivat olleen parhaiten perillä kyseisistä seikoista.

Kolmanteen tutkimuskysymykseen saatujen vastausten perusteella vastaajien suhtautuminen ei muuttunut siitä johtuen, että vastaajilta kysyttiin näkemystä sosiaalisen median tietoturvasta tai sen käytöstä. Suuria koulutusohjelmakohtaisia eroja ei ollut myöskään havaittavissa. Avoimiin kysymyksiin annettujen vastausten perusteella useat vastaajat kuitenkin huomasivat, että sosiaalisen median tietoturvariskeihin pitää kiinnittää huomiota ja että kysely muistutti heitä tästä.

Koska vastaajajoukko oli pieni, tuloksiin on suhtauduttava varauksella eikä niistä pidä vetää laajempia johtopäätöksiä. Vastaajajoukosta oli kuitenkin huomattavissa, että yleisesti ottaen tietojenkäsittelyn opiskelijat olivat paremmin perillä kysytyistä asioista ja

että he arvioivat omat tietonsa sosiaalisen median tietoturvasta keskimäärin paremmiksi kuin muiden HAAGA-HELIA ammattikorkeakoulun koulutusohjelmien opiskelijat.

Ne opiskelijat, jotka vastasivat esitettyihin kysymyksiin, vastasivat hyvin ja perusteellisesti jopa vapaaehtoisiin avoimiin kysymyksiin Tämä parantaa saatujen vastausten luotettavuutta, koska kysymykset olivat joko monivalintakysymyksiä tai avoimia kysymyksiä. Vaikka kyselyyn vastaajia oli suhteellisesti vähän, saadut vastaukset osoittavat, että opiskelijoiden käsityksissä sosiaalisen median tietoturvasta on hajontaa.

Saaduista tuloksista voidaan päätellä, että vastaajat suhtautuivat hieman varauksella sosiaalisen median tietoturvaan yleensä, mutta pitivät omaa tietämystänsä siitä suhteellisen hyvänä. Vastaajat tuntuivat olevan yleisesti ottaen suhteellisen hyvin perillä myös erilaisista sosiaalisen median tietoturvan alueista. Pelkästään se, että henkilö tietää sosiaalisen median tietoturvasta, tämä vaikuttaa suhtautumiseen sosiaaliseen mediaan ja sen käyttämiseen siten, että jatkossa vastaaja ehkä miettii tarkemmin, mitä asioita hän laittaa sosiaalisen median palveluihin.

Kyselyyn saatujen vastausten perusteella voi päätellä, että opiskelijoiden mielestä sosiaalisen median tietoturvaan pitäisi kiinnittää enemmän huomiota, kun sitä käyttää. Muista kuin tietojen julkisuuteen liittyvistä erilaisista tietoturvariskeistä ei myöskään välttämättä tiedetä kovin hyvin. Sosiaalisen median tietoturvaan, kuten muuhunkin tietoturvaan, liittyviä kysymyksiä ja riskejä olisi hyvä tuoda esille aina, kun puhutaan tietotekniikasta ja sen käyttämisestä.

Lähteet

Aalto, T. & Uusisaari M. 2009. Nettielämää. BTJ Kustannus. Jyväskylä.

Cert.fi, 2011. Omien tietojen jakaminen Facebookissa. Luettavissa: http://www.cert.fi/tietoturvanyt/2011/01/ttn201101211318.html. Luettu: 25.3.2012

Facebook 2012. Statement of Rights and Responsibilities. Luettavissa: http://fi-fi.facebook.com/legal/terms. Luettu 15.3.2012

Google Official Blog 2012. Google's new Privacy Policy. Luettavissa: http://googleblog.blogspot.com/2012/02/googles-new-privacy-policy.html#!/2012/02/googles-new-privacy-policy.html. Luettu: 2.4.2012

Hachman, M. 2012. Facebook Now Totals 901 Million Users, Profits Slip. PCMag. Luettavissa: http://www.pcmag.com/article2/0,2817,2403410,00.asp. Luettu 20.4.2012

Hopkins, J. 2006. Surprise! There's a third YouTube co-founder. USA Today. Luettavissa: http://www.usatoday.com/tech/news/2006-10-11-youtube-karim_x.htm. Luettu: 20.4.2012

Järvinen, P. Tietoturva & Yksityisyys. 2002. Docendo Finland Oy. Jyväskylä.

Järvinen, P. Yksityisyys – Turvaa digitaalinen kotirauhasi. 2010. WSOYPro. Jyväskylä.

Kalliala, E. & Toikkanen, T. Sosiaalinen media opetuksessa. 2009. Oy Finn Lectura Ab. Tampere.

Kotilainen, S. 2011. Ikävä Facebook-viesti – Volvo antoi potkut kolmelle. Tietokone. Luettavissa: http://www.tietokone.fi/uutiset/ikava_facebook_viesti_volvo_antoi_potkut_kolmelle. Luettu: 19.3.2012

Laki yksityisyyden suojasta työelämässä 13.8.2004/759

La Monica, P. R. 2006. Google to buy YouTube for $1.65 billion. CNNMoney. Luettavissa: http://money.cnn.com/2006/10/09/technology/googleyoutube_deal/index.htm?cnn=yes. Luettu 20.4.2012

Linnake, T. 2010. Murtovarkaat iskivät Facebookin avulla. IT-viikko. Luettavissa: http://www.itviikko.fi/uutiset/2010/09/14/murtovarkaat-iskivat-facebookin-avulla/201012699/7. Luettu 20.3.2012

Lämsä, H. 2012. Nuori suomalaisnainen järkyttyi nähtyään naamansa yllättävässä paikassa. Ilta-Sanomat. Luettavissa: http://www.iltasanomat.fi/kotimaa/nuori-suomalaisnainen-jarkyttyi-nahtyaan-naamansa-yllattavassa-paikassa/art-1288462502783.html. Luettu: 16.4.2012

Miller, C. C. 2010. Why Twitter's C.E.O. Demoted Himself. The New York Times. Luettavissa: http://www.nytimes.com/2010/10/31/technology/31ev.html?pagewanted=1&_r=1. Luettu 20.4.2012

Sanastokeskus TSK. 2010. Sosiaalisen median sanasto (TSK 40). Luettavissa: http://www.tsk.fi/tiedostot/pdf/Sosiaalisen_median_sanasto.pdf. Luettu: 2.3.2012

Tietoturvaopas. 2012a. Ajattele ennen kuin >klik<. Luettavissa: http://www.tietoturvaopas.fi/perusohjeet.html. Luettu: 26.2.2012

Tietoturvaopas. 2012b. Roskaposti. Luettavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/roskaposti.html. Luettu: 26.2.2012

Tietoturvaopas 2012c. Miten haittaohjelmilta suojaudutaan?. Luettavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haitoiltasuojautuminen.html. Luettu: 26.2.2012

Tikkanen, E. 2010. 22.9. Yksityisyys on verkossa kaupan. Luettavissa: http://www.mtv3.fi/uutiset/45min/jaksot.shtml?1189994. Luettu 5.3.2012

Valtiovarainministeriö. VAHTI 4/2010. Sosiaalisen median tietoturvaohje. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf. Luettu: 3.3.2012

Vander Veer, E.A. Facebook The Missing Manual. 2008. O'Reilly Media, Inc. Sebastopol, Canada.

YouTube. 2012. Tilastot. Luettavissa: http://www.youtube.com/static?gl=US&template=press_statistics&hl=fi. Luettu 26.3.2012

Liitteet

Liite 1. Opiskelijoille lähetetty kysely

Sosiaalisen median tietoturva

Tämän kyselyn tarkoitus on selvittää Haaga-Helian oppilaiden tietoisuutta sosiaalisen median tietoturvasta ja suhtautumista sosiaalisen median tietoturvaan. Kyselyn painopiste on käyttäjän yksityisyyttä uhkaavissa tietoturvauhissa.

Tähdellä merkittyihin kysymyksiin on pakko vastata.

Taustatiedot

1. Sukupuoli *

- Mies
- Nainen

2. Mikä on koulutusohjelmasi *

- Tietojenkäsittely
- Johdon assistenttityö ja journalismi
- Liiketalous

3. Käytätkö sosiaalista mediaa? *

Sosiaaliseksi mediaksi lasketaan tässä sellaiset palvelut kuin Facebook, Twitter, YouTube, Google+, blogit, MySpace ja muut vastaavanlaiset palvelut.

- Kyllä
- En

Seuraava -->

Sosiaalisen median tietoturva

Kysely

4. Minkälainen käsitys sinulla on sosiaalisen median tietoturvasta? *

- ○ Erinomainen
- ○ Hyvä
- ○ Kohtuullinen
- ○ Huono

5. Perustele vastauksesi.

Voit perustella edellisen kysymyksen vastauksen tähän.

6. Minkälaisia tietoturvauhkia koet sosiaalisessa mediassa olevan? *

7. Kuinka huolissasi olet sosiaalisen median tietoturvasta? *

- ○ En yhtään huolissani
- ○ Hiukan huolissani
- ○ Huolissani
- ○ Todella huolissani

<-- Edellinen | Seuraava –>

Sosiaalisen median tietoturva

8. Facebookin käyttöoikeuksissa sanotaan, että niin kauan kuin materiaali on Facebookissa, Facebook omistaa materiaaliin käyttöoikeudet. Tällaista materiaalia ovat esimerkiksi kuvat ja videot. Olitko tietoinen tästä? *

- Kyllä
- En
- Osittain

9. Jos asennat Facebookissa kolmansien osapuolien tekemiä sovelluksia, annat samalla sovelluksen tekijöille pääsyn omiin henkilötietoihisi. Oletko ollut tietoinen tästä? *

- Kyllä
- En
- Osittain

10. Google ilmoittaa yksityisyyspolitiikassaan keräävänsä tietoja myös ohjelmista joita käytät ja tietokoneestasi. Koska YouTube ja Blogger (blogipalvelu) kuuluvat googlelle niin nämä säännöt kuuluvat myös kyseisten palveluiden käyttäjille. Tiesitkö aikaisemmin kyseisestä tiedon keruusta? *

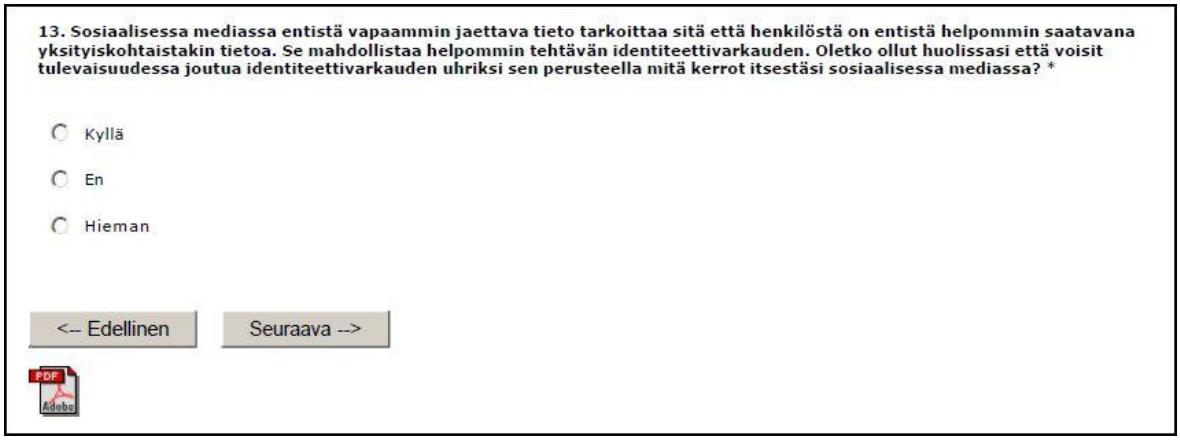
- Kyllä
- En
- Osittain

11. Useimmat sosiaalisen median palvelut sijaitsevat ulkomailla, jolloin lainsäädäntö jota noudatetaan mahdollisissa riitatilanteissa voi olla sen maan jossa palvelu sijaitsee. Oletko tietoinen tästä? *

- Kyllä
- En
- Osittain

12. Nykyisin Internetistä on hyvin vaikeaa, jollei mahdotonta saada kaikkea tietoa poistettua vaikka haluaisikin. Oletko ajatellut että joskus myöhemmin jokin video/kuva/teksti jonka olet joskus laittanut sosiaaliseen mediaan ja sitten poistanut koska se antaa sinusta epäedullisen kuvan, löytyisi myöhemmin netistä mahdollisesti antaen sinusta väärän kuvan sillä hetkellä? *

- Kyllä
- En
- Hieman


13. Sosiaalisessa mediassa entistä vapaammin jaettava tieto tarkoittaa sitä että henkilöstä on entistä helpommin saatavana yksityiskohtaistakin tietoa. Se mahdollistaa helpommin tehtävän identiteettivarkauden. Oletko ollut huolissasi että voisit tulevaisuudessa joutua identiteettivarkauden uhriksi sen perusteella mitä kerrot itsestäsi sosiaalisessa mediassa? *
Kyllä
En
Hieman
<-- Edellinen
Seuraava -->

Sosiaalisen median tietoturva

14. Muuttuiko käsityksesi sosiaalisen median tietoturvasta tämän kyselyn jälkeen? *

- Kyllä
- Ei
- Jonkin verran

15. Jos muuttui niin miten?

Voit perustella edellisen kysymyksen vastauksen tähän.

16. Muuttuiko suhtautumisesi sosiaalisen median käyttöön tämän kyselyn jälkeen? *

- Kyllä
- Ei
- Jonkin verran

17. Jos muuttui niin miten?

Voit perustella edellisen kysymyksen vastauksen tähän.

<-- Edellinen Lähetä

Liite 2. Avointen kysymysten vastaukset

5. Perustele vastauksesi.

Vastaajien määrä: 29

- Myyvät tietoja eteenpäin
- periaatteessa se on hyvä, mutta jos ottaa huomioon, että kaikki, mitä syötät erinäisiin sosiaalisen median sivustoihin, joutuu kuitenkin kolmansien osapuolten käsiin, ei tietoturvalla juurikaan ole väliä
- Ymmärrän, että järjestelmät sisältävät tietoturva-aukkoja.
- Sosiaalisen median seuranta ja sen eri toimijoiden sääntöjen tunteminen kuuluvat työtehtäviini.
- Olen tehnyt sosiaalisten verkostojen kehitystyötä ja sitä kautta tutustunut aiheeseen.
- Olen käyttäny esim. facebookia, IcQ ja windows messngeriä yms. jo pitkään
- En ole löytänyt vielä yhtäkään varmaa ja vankkaa perustelua siihen, miksi sos.median tuotteet ja palvelut olisivat tietoturvattu yhtään paremmin kuin muutkaan netin palvelut. Fakta on se, että mitä enemmän käyttäjiä ja kiinnostusta, sitä enemmän mahdollisuutta käyttää hyväkseen tietoja, aukkoja ja muutenkin tehdä pahaa käyttäjille/ylläpitäjille.
- Asiaan voi itse vaikuttaa paljon, mutta lähtötaso esim facebookissa on todella köykäinen.
- Facebookin ja Googlen bisneshän on kerätä tietoja käyttäjien liikkeistä ja mieltymyksistä ja myydä niitä mainostajille. Mistä voi olla varma, että tietoja ei kertätä vaikka asetukset olisivat tietoturva-asetukset nimellisesti päällä.
- Käyttäjä ei voi millään vaikuttaa siihen, että ketkä oikeasti näkevät käyttäjän tiedot. En luota palveluiden rehellisyyteen.
- En jaksa lukea käyttäjäehtoja, käsitykseni perustuu siihen mitä olen kuullut ystäviltäni ja uutisista.
- Sosiaalista mediaa useita vuosia käyttäneenä ja tietoturva-alalla työskentelevänä käsitykseni tietoturvasta yleensäkin on hyvä.
- En ole perehtynyt erityisesti sosiaalisen median tietoturvaan, mutta tietoturvaan yleisellä tasolla kyllä.
- Kaikkea ei olla otettu huomioon kaikkialla.
- Pysyn ajan tasalla lukemalla tietoturvapäivityksiä ja chekkailemalla välillä miten toiminnot ovat käytännössä muuttuneet.

  Mietin myös ennen kuin jaan mitään sosiaalisessa mediassa, että kenellä se näkyy ja pidän mielessä, että myös sellaiset tahot, joiden en halua tietävän asioista saattavat silti saadan asioita tietoonsa.
- En luota esim. facebookiin, koska se aina on temppuillut.
- Ko sovellusten tarkoitus on tehdä omistajilleen tuottoa kaupallisten sovellusten kautta, joten pääpaino lienee siinä, ei tietoturvassa tms.
- Tiedot monien ihmisten saatavilla, käyttäjillä ei käsitystä kokonaisuudesta.
- Tiedon olen saanut lähinnä uutisista tai kavereilta
- Facebookin kohdalla se on hieman laskenut, mutta muihin palveluihin luotan.
- Opiskelen tietojenkäsittelyä ja tehtäväni on tietää nämä asiat.
- Kaikki mitä nettiin laittaa, jää aina nettiin. Joten ei tulisi mieleenkään laittaa puhelinnumeroa, osoitetta ym. Vaikka ne näkyisi vain kavereille. Jaan sosiaalisessa mediassa vain sellaista mitä esimiehenikin voisi nähdä. Kuvakansioni on rajatut, niin että vain lähimmät ystäväni näkevät ne, mutta niiden sisältö on silti sellasta, että vaikka joku hakkeroisi asetusta ohi, niin se ei olisi maailman loppu.
- Asun Suomessa.
- Haluaisin oppia lisää, mutta tuntuu että tietoturvaa käsittelevät asiat on aina ilmaistu verkkosivuilla hankalalla tavalla.
- Tiedän jonkin verran, mutten ole vaivautunut ottamaan kauheasti selvää.
- Esimerkiksi Facebookissa en ole täysin varma toteutuuko kaikki tietoturva-asetukset. Välillä olen huomannut, että heidän tehdessä päivityksiä ym. asetukset muuttuvat, profiilini on ollut julkinen (vaikka sen olisi laittanut suojatuksi).
- kokemusta
- Olen tietoinen somen tietoturvariskeistä
- Tiedostan riskit mitä sosiaalisen median tietoturvaan liittyy, yritän välttää mahdollisia selkeitä uhkia.

6. Minkälaisia tietoturvauhkia koet sosiaalisessa mediassa olevan?

Vastaajien määrä: 55

- Kaikki tiedot menee eteenpäin.

- - väärää tietoa
  - kuka tahansa voi esittää ketä tahansa
  - tietosuoja ja käyttöehdot
- periaatteessa siis, jos me käyttäjinä emme olisi "tuotteita", eikä kaikki tieto välittyisi mainostajille, voisi tietoturva näiden sivustojen osalta olla hyväkin. enpä usko, että krakkerit ainakaan vielä ovat saaneet käyttäjätunnuksia rikki näissä sivustoissa, ellei niiden varsinaiset omistajat syötä salasanoiksi kissa1 tai aut0 tms
- Kirjoitetun tiedon leviäminen julkiseen verkkoon.
- Identiteettivarkaus, käyttäjätilin tai yrityksen Twitterin hashtagin kaappaus ja haitta- sekä vakoiluohjelmien tms. levittäminen somesisällön mukana. Katson uhkaksi myös sen, että työntekijä saattaa sometoiminnallaan yrityksen maineen kyseenalaiseksi tai että vahvan henkilöbrändin omaava yrityksen työntekijä vie firmasta poislähtiessään mukanaan esim. firman Twitter-seuraajat.
- Salasanat voivat päätyä vääriin käsiin. Ei muisteta kirjautua ulos sivustolta.
- Identiteettikaappaua, virus
- identiteettivarkauksia, väärän tiedon levitystä, hoaxit. yksityisten tietojen väärinkäyttö.
- phishingiä, troijalaisia yms.
- Virukset
- Esim identiteetin riisto
- Pelkään jatkuvasti että mm. yksityisviestini vuotaisivat julki, kuviani käytettäisiin väärin jne.
- Vakoilut, huijaukset, tietomurrot jne
- Mikään ei ole tärkeämpää kuin ihmiset omat ja yksilölliset (muista erottavat) tiedot. Sos.media on onnistunut kadottamaan käyttäjien oman kiinnostuksen omiin tietoihin ja niiden leviämiseen. Asenne on muuttunut "kuka nyt mun tiedoista kiinnostuisi". Pelottavaa.
- En pidä siitä että tietojani luovutetaan kolmansille osapuolille. myös tietojen säilyminen netissä ikuisesti huolestuttaa.
- Kuvamateriaali ja mahdolliset tilapäivitykset jne. päätyvät tahoille, joille ne eivät ole tarkoitettu jaettaviksi.
- Yksityisyyden suoja.
- Tietojen päätyminen vääriin käsiin, ilkivalta, hlötietokaappaus.
- Sinun nimelläsi voi joku muu perustaa profiilin ja tätä kautta saada aikaan harmia. Myöskään ei voi olla täysin varma mihin antamiasi tietoja ja kuvia tallennetaan ja käytetäänkö niitä myös muihin tarkoituksiin, mihin itse olit tarkoittanut.
- Yksityisyyden suojaus ja tietojen mahdollinen leviäminen ulkopuolisille tahoille.
- Samanlaisia kuin muuallakin, viruksia. Sosiaalisessa mediassa uhat voivat vielä olla vakavampiakin koska saadaan henkilökohtaisia tietoja helposti.
- Sosiaalisen median yhteisöt vaihtelevat turvallisuus- ja yksityisyysasetuksiaan usein ja päivittävät ohjelmistoja. Joskus on vaikea pysyä perillä muutoksissa, vaikka osaisikin suojata profiilinsa.
- Suurimpana uhkana koen sen, että tietojani päätyy sellaisten ihmisten käsiin, joihin niitä ei ole tarkoitettu
- Hakkerit
- Suurin tietoturvariski on käyttäjä itse. Lähes kaikki sosiaalisen median palvelut tarjoavat mahdollisuuden oman näkyvyyden rajoittamiseen mutta suuri osa ei hyödynnä niitä. Käyttäjien pitäisi myös tajuta että kaikkea ei välttämättä kannata jakaa itsestään netissä.
- Tietojen leviäminen ulkopuolisille, tosin tämän voi minimoida huolellisella käytöllä.
- Aktiivinen somen käyttäjä voi vuodattaa koko ulkomaailmalle näkyvän identiteettinsä kaikkien tutkittavaksi sosiaaliseen mediaan. Hakkeri voi sen varastaa ja kasvottomassa internetissä tietoja voi hyödyntää helpostikin. Pankkitunnusten vuotaminen on ehkä eniten pelkäämäni yleinen tietoturvauhka. Sosiaalisen median vallankumous ei ainakaan vaikeuta varkaan urakkaa tällä saralla. Somessa leviävä tehokas pankkitunnustroijalainen olisi katastrofi.
- Hakkeroinnit ja muut tietomurrot ja -vuodot. Virukset ja muut jotka kaappaavat salasanoja.
- Pelkään,että yksityiset tiedot näkyvät kaikille
- Käyttäjätietojen jakamisen kolmansille osapuolille tai tietojen väärinkäyttö tulee ensimmäisenä mieleen.
- Internet on varmastikin aina haavoittuvainen ja se on hyvä muistaa. Tarkemmin en osaa lähteä tietoturvauhkia erittelemään. Varmuuden vuoksi en jaa tärkeitä tietojani (kuten tilinumero) viestinä esim. Facebookissa, vaikka monet ovat tilinumeronsa FB:ssä antaneetkin esim. bensarahojen maksua varten
- Onhan niitä, mutta en viitsi lähteä niitä tähän luettelemaan. Googlaamalla löytyy...

  Tärkeintä on tehdä itselle selväksi, että kaikki tiedot, jotka internettiin laitat, ovat siellä ikuisesti ja kaikkien saatavilla. Tämän kun ymmärtää, ja jokaisen kuvan, lauseen, statuspäivityksen ym. kohdalla itselleen selvittää, on melko hvin turvassa. Identiteettivarkaudet on toinen juttu, mutta toisaalta sen riskin on ottanut, kun tietojaan on internettiin laittanut (ja saa ne tiedot kaivettua vaikka roskiksestakin vanhoista kirjeista jne.).
- ns. identiteetin kaappaaminen
- Mietin onko mahdollista että sosiaalisen median sivustot tunkeutuvat koneelle, asentavat haittaohjelmia

tai milloin esim facebookissa käyty keskustelu tulee julkiseksi.

- Omat tiedot jaetaan laajasti. Lienee vain ajankysymys milloin hakkerit hyökkäävät sovelluksiin tekemään kiusaa...
- Henkilökohtaisten tietojen leviäminen vääriin käsiin, tietojen "säilyvyys" eli et voi välttämättä poistaa olemassa olevia tietojasi
- Tietoturvauhka ei ole tiedon puutteen takia kovinkaan selvä. En ole osannut ajatella, että esim. facebookin tietoja joku haluaa käyttää hyväksi tai että sitä kautta voi päästä muihin tietoihin käsiksi. Nämäkin mahdollisuudet ovat tulleet tietoon lähinnä median kautta.
- Henkilökohtaisten tietojen väärinkäyttö ja kuvien joutuminen epäedullisiin yhteyksiin.
- Linkkihuijaukset
  Identiteetin varastaminen
  Yksityistietojen vuotaminen
    -osoite
    -henkilötunnus
    -numero
    -henkilökohtaiset kuvat
    -pankkitiedot
- Kaikki voi vuotaa sieltä. Siksi siellä ei pidäkään jakaa mitä vaan. Isoin huoli on ehkä "yksityisissä" viesteissä palvelun sisällä. Kuka niihin voi päästä käsiksi ja mitä niissä voi jakaa? Jos kaveri haluaa maksaa velat takaisin, voitko antaa tilinumeron Facebook-viestin kautta?
- Tietojenkalasteluhuijaukset
- Pelkään että henkilökohtaisia asioita leviää kuulumattomiin paikkoihin.
- Tietojen vuotaminen kolmansille osapuolille, tietojen varastointi ja keräily useista eri lähteistä.
- Omien kuvien väärinkäyttöä ja identiteettivarkauksia.
- Henkilökohtaisten tietojen, kuten salasanojen ja kuvien vuotaminen.
- Tietokalastelua
- Sellaisen tiedon vuotaminen ulkopuolisille, mitä ei haluaisi muiden tietoon.
- ylläoleva kertoi huolen, mutta se että palveluntarjoajat eivät todellakaan pidä huolta siitä, että tietoturva säilyy. Tämä on laajempikin ilmiö, ei vain sosiaalisessa mediassa mutta ylipäätään sähköisessä maailmassa. Pankeillakin on jo ongelmia asian kanssa.
- Salasanalistoja yms. tuntuu joidenkin olevan helppo saada käsiinsä.
- identiteettivarkaudet
- Esimerkiksi Facebookissa on hieman epäselvää, mitkä tiedot ja toimet näkyvät muille ja kenelle näkyvät. Timelinen tullessa käyttöön joidenkin käyttäjien yksityisviesteistä tuli kuulemani mukaan julkisia, vaikka Facebookin ylläpito väittää muuta. Mielestäni on vakava virhe, jos yksityiset, kahden ihmisen välillä käydyt keskustelut tulevat muidenkin nähtäville.

  Välillä mietityttää myös se mahdollisuus, että joku hakkeroituisi jonkun palvelun tiliini ja saisi tietojani.
- Tietojen vapaa-ehtoinen jakaminen ja myöhempi katumus
- Käyttäjien lisäämä tieto on palvelun järjestäjälle kauppatavaraa ja palveluissa usein kehotetaan lisäämään niin paljon tietoa kuin mahdollista "käyttäjän oman edun vuoksi". Käyttöehdossakin on usein käyttäjän oikeuksien kannalta kyseenalaisia kohtia.
- Omia tietoja, viestejä yms. ei pysty hallitsemaan ts. poistamaan varmasti ja tietämään kenelle kaikille tiedot kulkeutuvat
- Liikkeellä on ollut mm. viruksia, kalasteluviestejä, ja tietty jos oman salasanansa jakaa jollekin toiselle henkilölle tai käyttää sitä muualla niin se lisää riskiä. Koen myös uhkana mm. sen että Facebook säilyttää kaikki tietoni vaikka poistaisinkin itseni sieltä.

15. Jos muuttui niin miten?

Vastaajien määrä: 18

- -
- Ei muuttunut, koska olen ollut hyvin tietoinen näistä kaikista asioista ja mahdollisista uhista.
- En tiennyt tietojenkeruun olevan näin laajaa.
- Tieto googlen keräämistä tiedoista itse tietokoneesta ja ohjelmista yllätti.
- Olen jo aiemminkin ollut tietoinen siitä, että sosiaalisessa mediassa kannattaa tarkkaan miettiä, mitä tietoa itsestään kertoo. En toisaalta ole koskaan jaksanut silti hirveästi välittää aiheesta.
- Käsitykseni muuttui jo aikaisemmin, kun jouduin identiteettivarkaan "uhriksi"
- Olin hyvin pitkälti tietoinen kyseisistä asioista ja tehnyt päätökseni tavoista käyttää sosiaalista mediaa niiden tietojen mukaan.
- Tuli mieleeni, että saa taas olla todella varovainen netin kanssa.

- Kaikki mitä laittaa internetiin, on käytännössä vapaata riistaa. Kuka tahansa voi ottaa tiedot käyttöönsä ja käyttää nitä haluamallaan tavalla.
- Olen tietoinen ongelmista, mutta minulla ei ole tarvittavaa tieto-taitoa asian parantamiseksi. Kysely oli minulle muistutus siitä, että pitää olla tarkempi.
- Pitää olla varaivainen. Uhkat tuntee, mutta ne aina helposti unohtaa ja niin ei saisi käydä.
- Osittain vastauksista tuli kyllä vastauksia.
- Olen entistäkin huolestuneempi :) vaikka olenkin hyvin tarkka, mitä kirjoitan facebookiin (käytännössä postailen hyvin vähän), niin ei tule enää helposti lisättyä kuvia.
- En ollut ajatellut ulkomaisen lainsäädännön kannalta asiaa.
- -
- Lehdissä ja muussa mediassa on ollut paljon puhetta esim. Facebookin tietoturvakäytännöistä ja niiden heikkouksista. Asia kyllä tiedetään, mutta ei välttämättä tiedosteta riittävästi.
- En ollut tietoinen kohdan 11 lainsäädäntöasiasta. Muista asioista olen ollut kohtuullisen tietoinen ja olenkin melko epäluuloinen sosiaalisen median tietoturvan suhteen.
- Olen ollut hyvin tietoinen kaikista tietoturvauhkista joita esimerkiksi facebook -palveluun liittyy. Googlen keräämät tiedot olivat uutta, mutta eivät yllättäviä sillä tiesin Googlen keräävän paljon tietoa käyttäjistään.

17. Jos muuttui niin miten?

Vastaajien määrä: 14

- käytän edelleen hyvin vähän sosiaalisia medioja / en lisää itse sisältöä
- Olin jo varsin tietoinen kyselysssä ilmenneistä seikoista.
- Olen hyvin rajoittavasti käyttänyt sos.median palveluita juurikin tästä syystä. Vaikuttaa siltä, että ihmiset nykyään luopuvat yksityisyydestä melko köykäisin perustein. Näitä perusteita on esim. kaveripiirin laajuus ja tunne jäädä juttujen ulkopuolelle. Voivoi :)
- Luotan googleen paljon vähemmän.
- En julkaise sosiaalisessa mediassa mitään kovin henkilökohtaista. Enemmän huolestuttaa sovellusten "salaa" keräämä sisältö....
  Onnea opinnäytetyöhön :-)
- Jäin miettimään sitä että jo poistetut kuvat voivat ilmestyä uudestaan ja myös Googlen omistamat palvelut keräävät tietoa.
- Pitäisi varmaan tiedottaa fb-ystäville, että mikäli he haluavat lisätä kuviani someen, siihen pitäisi kysyä lupa. Itse pyrin harkitsemaan tarkoin, mikäli laitan fb:hen kuvia ja esim. lasteni kuvien suhteen olen tarkka, ja lataan kuvia vasta kysyttyäni myös lasten isän mielipidettä.
- Olen jo nyt passiivinen käyttäjä, joten luultavasti muutuin vielä passiivisemmaksi ;)
- Kysely oli minulle muistutus siitä, että pitää olla tarkempi.
- Sama vastaus kuin edellinen.
- Osittain vastauksista tuli kyllä vastauksia, joten ajattelumallini muuttui, joten saatan toimia eri tavalla kysyttyjen asioiden suhteen.
- sama vastaus kuin edellisessä
- Katsoisin tarkemmin mitä kirjoitan sosiaalisessa mediassa. Olen kyllä tietoinen, että liian henkilökohtaisia asioita, varsinkin salaisia en kirjoita siellä ollenkaan.
- Varmaan katson vielä tarkemmin, mitä tietoja itsestäni julkaisen netissä.