Petra Komulainen

TIETOTURVA SOSIAALISESSA MEDIASSA

Centria ammattikorkeakoulun opiskelijoiden ja henkilökunnan käsitys tietoturvasta sosiaalisessa mediassa

Opinnäytetyö
CENTRIA AMMATTIKORKEAKOULU
Liiketalouden koulutusohjelma
Toukokuu 2013

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Yksikkö	**Aika**	**Tekijä**
Kokkola-Pietarsaari	Toukokuu 2013	Petra Komulainen
Koulutusohjelma Liiketalouden koulutusohjelma		
Työn nimi TIETOTURVA SOSIAALISESSA MEDIASSA. Centria ammattikorkeakoulun opiskelijoiden ja henkilökunnan käsitys tietoturvasta sosiaalisessa mediassa.		
Työn ohjaaja Marko Forsell	**Tekstin ohjaaja** Helvi Pääkkönen	**Sivumäärä** 59 + 11
Työelämäohjaaja Marko Ovaskainen		

Opinnäytetyöni tarkoitus on selvittää Centria ammattikorkeakoulun, opiskelijoiden ja henkilökunnan käsitystä tietoturvasta sosiaalisessa mediassa sekä heidän suhtautumistaan siihen. Tutkimuksessa keskityin yksityisyyteen liittyviin uhkiin ja käyttäjien tietoisuuteen niistä.

Opinnäytetyön teoreettinen osio käsittelee suosituimpia sosiaalisen median palveluita, kuten Facebook, Myspace, Twitter ja YouTube, sekä sosiaalisen median eri määritelmiä. Teoreettisessa osiossa käsitellään myös sosiaalisen median tietoturvaa ja tietosuojaa sekä käydään läpi yleisimpiä sosiaalisen median uhkakuvia ja pelkoja jaoteltuina teknisiin uhkiin ja yksityisyyteen liittyviin uhkiin. Opinnäytetyön pääpaino on yksityisyyteen liittyvissä uhissa.

Koska vastausprosentti jäi pieneksi, on kyselyssä saatuihin tuloksiin suhtauduttava varauksella. Voidaan kuitenkin päätellä, että vastaajat suhtautuivat hieman varauksella sosiaalisen median tietoturvaan yleensä, mutta pitivät omaa tietämystään siitä silti suhteellisen hyvänä.

Asiasanat
Facebook, Google, MySpace, sosiaalinen media, tietoturva, tietosuoja, Twitter, YouTube

ABSTRACT

DEPARTMENT Unit of Kokkola-Pietarsaari	Date May 2013	Author Petra Komulainen
Degree programme Business Administration		
Name of thesis DATA SECURITY IN SOCIAL MEDIA. Case Centria University of Applied Sciences, students and staff understanding in data security in social media.		
Instructor Marko Forsell	**Language instructor** Helvi Pääkkönen	**Pages** 59+11
Supervisor Marko Ovaskainen		

The aim of this thesis was to find out the Centria University of Applied Sciences, student and staff perception of security in social media as well as their attitudes towards it. The thesis focused on the threats to privacy and users' awareness of them.

The theory section deals with the most popular social media services such as Facebook, Myspace, Twitter and YouTube, as well as different definitions of social media. It deals with the theoretical part of the social media data security and protection, as well as the most common social media threats and fears broken down into technical threats, and privacy threats. The main focus of this thesis is related to privacy menace.

Because the response percentage was low, the survey on the results will be treated with caution. It can be concluded that the respondents were a little cautious on social media information security in general, but consider their own knowledge of it still relatively good.

Key words
data privacy, data security, Facebook, Google, MySpace, social media, Twitter, YouTube

TIIVISTELMÄ
ABSTRACT
SISÄLLYS

LÄHTEET
LIITTEET

KUVIOT

TAULUKOT

1 JOHDANTO

Opinnäytetyöni tarkoituksena on käsitellä sosiaalisen median tietoturvaa ja tietosuojaa. Opinnäytetyöni osana tein myös tutkimuksen Centria ammattikorkeakoulun Kokkola-Pietarsaaren yksikön Talonpojankadun toimipisteessä opiskelijoille ja henkilökunnalle heidän käsityksistään tietoturvasta sosiaalisessa mediassa. Tutkimus perustui ennen kaikkea niihin uhkiin, jotka koskevat käyttäjien yksityisyyttä.

Opinnäytetyöhöni sisältyi kysely, joka lähetettiin 575:lle liiketalouden ja 560:lle tekniikan opiskelijalle. Lisäksi kysely lähetettiin henkilökunnalle, jota tekniikan ja liiketalouden yksikössä on 60. Kysely toteutettiin 18.12.2012–18.1.2013. Kyselyyn vastasi 104 henkilöä. Liiketalouden opiskelijoista kyselyyn vastasi 61, tekniikan opiskelijoista 24 ja henkilökunnasta 19.

Kun mietin opinnäytetyötäni, minulla oli suuri halu tehdä sellainen työ, josta olisi hyötyä itselleni, mutta myös muille opiskelutovereilleni. Halusin tehdä opinnäytetyöhöni myös kyselyn, joka olisi pienimuotoinen tutkimus. Päädyin aiheeseen tietoturva sosiaalisessa mediassa. Tietoturva ja sosiaalinen media ovat olleet paljon esillä eri medioissa ja mielestäni niistä saisi erinomaisia opintojaksoja lisää kouluumme, niin liiketalouden kuin tekniikan puolelle. Centria ammattikorkeakoulussa on mahdollista opiskella kahdella opintojaksolla, joko tietoturvaa tai sosiaalista mediaa. Averkossa opiskelin opintojaksolla nimeltä ”Tietoturva yrityksen organisaatiossa” ja normaaliopiskeluna suoritin opintojakson nimeltä ”Sosiaalinen media liiketoiminnan tukena”. Näiltä kursseilta sain paljon lisää informaatiota opinnäytetyöhöni ja huomasin, kuinka opiskelijat ovat oikeasti kiinnostuneita tästä asiasta. Sen vuoksi halusin myös perehtyä aiheeseen lisää.

Etsiessäni tietolähteitä löysin Nuotion (2012) tekemän tutkimuksen Haaga-Helian ammattikorkeakoululle. Siitä sain idean tehdä samanlaisen kyselyn myös omaan kouluuni. Kyselyn avulla pyrittiin saamaan vastaus kolmeen eri aihekokonaisuuteen. Ensimmäiseksi halusin selvittää opiskelijoiden ja henkilökunnan käsitystä tietoturvasta sosiaalisessa mediassa. Sen jälkeen selvitin vastanneiden tietoisuutta sosiaalisen median tietoturvariskeistä. Viimeiseksi halusin selvittää, muuttuiko vastanneiden käsitys tietoturvasta sosiaalisessa mediassa kyselyn jälkeen. Lopuksi selvitin, oliko Centria ammattikorkeakoulun ja Haaga-Helian ammattikorkeakoulun vastanneiden kesken suuria eroja.

2 YLEISTÄ SOSIAALISESTA MEDIASTA JA TIETOTURVASTA

Tutkimukseni taustana käsitellen sosiaalisen median käsitettä, joka ei ole yksiselitteinen vaan hyvin monikäsitteinen. Tämän jälkeen perehdyn tietoturvan perusteena pidettyyn muistisääntöön CIA, joka tulee englannin sanoista confidentiality (luottamuksellisuus), integrity (eheys) ja availibility (käytettävyys). Lisäksi kerron sosiaalisen median yleisimmistä ja suosituimmista palveluista kuten Facebook, YouTube, Google, Twitter ja MySpace.

2.1 Sosiaalisen median käsite

Sosiaalinen media on uusi ja hyvin monikäsitteinen ilmiö, jonka takia sille on hankalaa esittää yhtä ainoaa sopivaa määritelmää. Sosiaalista mediaa käsittelevissä teoksissa ja artikkeleissa on usein viitattu englanninkielisen Wikipedian sosiaalisen median määritelmään. Tämän määritelmän mukaan *sosiaalinen media* on sateenvarjokäsite, joka pitää sisällään erilaisia verkkopohjaisia toimintatapoja, joissa teknologia, mediasisällöt ja sosiaalinen vuorovaikutus integroituvat. Määritelmän mukaan käyttäjät rakentavat yhteisiä merkityksiä sosiaalisen median avulla. (Alan.fi 2013.)

Erkkola (2008) on määritellyt 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. Samalla sosiaalinen media on jälkiteollinen ilmiö, jolla on tuotanto- ja jakelurakenteen muutoksen takia vaikutuksia yhteiskuntaan, talouteen ja kulttuuriin.

VTT:n sosiaalisen median liiketoimintamalleja koskevassa tutkimuksessa, sosiaalinen media määritellään seuraavasti: *Sosiaalisella medialla* tarkoitetaan prosessia, jossa yksilöt ja ryhmät rakentavat yhteisiä merkityksiä sisältöjen, yhteisöjen ja verkkoteknologioiden avulla vertais- ja käyttötuotannon kautta. Sosiaalisen median palveluissa käyttäjät jakavat keskenään mielipiteitä, näkemyksiä, kokemuksia ja näkökulmia. Vaikka erilaisia yhteisöpalveluita käytetään vielä pääsääntöisesti yksityisesti, on erilaisten sosiaalisten medioiden käyttö myös ammatillisiin tarkoituksiin voimakkaassa kasvussa. (Heikkilä 2012.)

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 koska Internet toimii sisältöjen tallennuspaikkana, niin Internet toimii myös eri sovellusten alustana. (Sanastokeskus TSK 2010a.)

O'Reilly alkoi ensimmäisenä käyttää nimeä Web 2.0 vuonna 2004. Tässä teknologiassa ei ole kyse mistään Webin toisesta tasosta, vaan pikemminkin uusista ajattelu-, toiminta- ja tuotantotavoista, joita sovelletaan Internetpalvelujen suunnittelussa, ohjelmoinnissa sekä strategiassa. Koko järjestelmänperustana ovat aktiiviset käyttäjät. Web 2.0 -tekniikat sekä muut ominaisuudet ovat toimineet käytännössä, mikä on lisännyt niiden suosiota. (Hintikka 2007, 6.)

Internet toimii ikään kuin alustana, jossa käyttäjät voivat verkostoitua ja olla yhteydessä keskenään sekä harrastaa muita aktiviteettejä. Web 2.0 -ilmiön määritteleminen on erittäin hankalaa ja monimutkaista, koska siihen kuuluu useita uusia ja vanhoja kehityssuuntaustoja. Sovellusten kannalta Web 2.0 -tekniikassa on hyvänä ominaisuutena muuntautumiskyvykkyys. Ilmiötä kuvaillaan yleensä siihen liittyvien termien avulla. Tässä muutamia Web 2.0 -teknologiaan liittyviä termejä:

- blogi
- kollektiivinen tuotanto ja kehitys
- omien sisältöjen ja palveluiden jakaminen maksutta
- ohjelmien ja sovellusten toteuttaminen www-alustalla
- yhteisöllisyys ja käyttäjien luomat sisällöt
- Rss-syöte. (Hintikka 2007, 10.)

Blogeissa henkilöt tai yritykset voivat kertoa elämästään, harrastuksistaan tai tuotteistaan. Rss-syötteet tarkoittavat lyhennettyjä uutispätkiä, joiden avulla on helppo levittää usein päivittyvää informaatiota tai vaikka markkinoida tuotteitaan. Yleisesti ottaen kaikki edellä mainitut tavat ovat helpottaneet tiedon kulkua eri tiedotusvälineissä, eritoten sosiaalisessa mediassa.

2.2 Tietoturvasta ja tietosuojasta

Tietoturvan edellytysten muistisääntö on CIA, joka tulee englannin sanoista confidentiality, integrity ja availability. Suomeksi nämä ominaisuudet ovat luottamuksellisuus, eheys ja käytettävyys tai saatavuus. Muita tietoturvan ominaisuuksia ovat kiistämättömyys, todennus ja pääsynvalvonta. (Heijaste 2013.)

Luottamuksellisuus tarkoittaa sitä, että verkossa olevaan tai liikkuvaan tietoon pääsevät käsiksi vain ne, joille on etukäteen annettu siihen oikeus. Emme pääse käyttämään tietoa, jota ei ole meille tarkoitettu. Käyttäjien tunnistaminen edellyttää todennusta. Tiedon säilymiseen muilta suojattuna taas tarvitaan salausta, joka toteutetaan teknisin keinoin. (Heijaste 2013.)

Eheys tarkoittaa sitä, että tiedon käsittelymekanismit takaavat tiedon virheettömän käsittelyn. Tieto ei siis voi huomaamatta muuttua siirtämisen tai säilyttämisen aikana, emmekä voi ilman lupaa muuttaa tiedon tai tiedostojen sisältöä saati poistaa niitä. Tiedon eheyden varmistamiseen liittyy aina lähettäjän todennus. Eheys ja todennus yhdessä varmistavat, että lähetty tieto saavuttaa vastaanottajan juuri siinä muodossa, missä se lähetettiinkin. (Heijaste 2013.)

Käytettävyys tarkoittaa sitä, että tieto on aina niiden käyttäjien saatavilla, jotka sitä tarvitsevat ja joille se on tarkoitettu. Käytettävyyden turvaamiseen kuuluvat mm. tietojärjestelmien toiminnan tekninen ja fyysinen varmistaminen sekä tiedostojen varmuuskopiointi, suojaus ja asianmukainen tallennus. Tiedon käytettävyys on vaikeimmin toteutettava tietoturvan muoto. (Heijaste 2013.)

Pääsynvalvonnalla tarkoitetaan, että käyttäjien pääsyä koneessa olevaan tietoon valvotaan ja rajoitetaan. Pääsynvalvonnalla tarkistetaan, onko osapuolella oikeus tiedon ja palvelun käyttöön, jolloin vain todennetut henkilöt pääsevät käyttämään tietoja. Pääsynvalvonnan tavoitteena on turvata tiedon luottamuksellisuus ja eheys. Pääsynvalvonta varmistaa myös tiedon käytettävyyttä, sillä se tekee järjestelmään hyökkäämisen vaikeammaksi. Osa pääsynvalvontaa on myös käytön seuranta. Järjestelmä kirjaa muistiin ns. lokitietoihin käyttäjien järjestelmässä tekemät

toimet. Lokitietoihin pääsee järjestelmänvalvoja, joka voi tarvittaessa niiden avulla selvittää tahallisia ja tahattomia tietoturvarikkomuksia. (Heijaste 2013.)

Todennuksella varmistetaan, että osapuolet ovat niitä, joita sanovat olevansa. Esimerkiksi sähköisessä viranomaispalveluissa ja kaupankäynnissä, sekä henkilöiden välisessä viestinnässä on usein tärkeää tietää varmasti, kuka toinen osapuoli on. Tällöin tarvitaan osapuolen ja tietolähteen eli tiedon alkuperän todennusta. Sähköpostissa todennus tehdään usein vain lähettäjän osoitteen perusteella, esimerkiksi tutulta tullutta viestiä ja sen liitettä avattaessa. Pelkän osoitteen perusteella todentaminen on kuitenkin turvatonta, sillä postin lähettäjän tiedot on hyvin helppo väärentää. Monet tietokoneesta toiseen leviävät matovirukset käyttävät tätä tapaa postin lukijoiden hämäämiseen. (Heijaste 2013.)

Kiistämättömyydellä tarkoitetaan, ettei tiedon lähettäjä voi kiistää lähettäneensä tietoa ja olleensa jossakin tapahtumassa osapuolena. Kiistämättömyys on tietolähteen todennuksen vahva muoto, ja se toteutetaan sähköisellä allekirjoituksella. Kiistämättömyys on edellytys monien palvelujen ja toimintojen, kuten sähköisen kaupankäynnin, toteuttamiselle tietoverkkojen kautta. (Heijaste 2013.)

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

Stranius (2012) kertoo blogissaan käynnistään Petteri Järvisen luennolla, kuudesta Järvisen listaamasta huomiosta tietoturvassa:

1. Mukavuus x turvallisuus = vakio.

2. Tietoturva on 80 % psykologiaa ja 20 % tekniikkaa.

3. Tieto huonosta tietoturvasta on parempi kuin luulo hyvästä.

4. Täydellistä turvaa ei ole, mutta siihen kannattaa silti pyrkiä.

5. Rutiini sekä lisää että heikentää turvallisuutta.

6. Odota odottamatonta. (Stranius 2012.)

Kannattaa siis aina pelata varman päälle. Tietoturvaa pitäisi opiskella enemmän, erityisesti sosiaalisen median osalta. On vielä paljon sellaisia tietoturvauhkia, joista kaikki sosiaalisen median käyttäjät eivät ole tietoisia. Aina on parempi varautua, kuin katua. Hyvä tietoturva takaa hyvän tietosuojan.

2.3 Sosiaalisen median suosituimmat palvelut

Tässä luvussa käsitellään sosiaalisen median suosituimpia palveluja, joista esimerkkinä verkkoyhteisöpalvelut, sisällönjakopalvelut ja verkkopalvelu. Ensin perehdyn teoriaan ja sen jälkeen kerron esimerkin jokaisesta edellä mainitusta palvelusta.

Verkkoyhteisöpalvelun kautta ihmiset voivat viestiä keskenään ja jakaa esimerkiksi kiinnostuksen kohteitaan koskevia mielipiteitä ja tietoja. Joissain verkkoyhteisöpalveluissa käyttäjä luo itselleen profiilin, johon hän liittää esimerkiksi kuvansa ja

tietoja itsestään. Hän voi pyytää ystäviään liittymään verkkoyhteisöpalveluun tai hyväksyä toisia palvelun käyttäjiä verkostoonsa. Verkkoyhteisöpalvelun avulla voi mm. etsiä vanhoja koulukavereitaan. Verkkoyhteisöpalveluja voidaan hyödyntää myös työelämään ja harrastuksiin liittyvässä viestinnässä. (Sanastokeskus TSK 2010b.)

Verkkoyhteisöpalveluja ovat esimerkiksi Facebook, MySpace ja IRC-Galleria. Termiä verkostoitumispalvelu käytetään toisinaan termin verkkoyhteisöpalvelu synonyymina, joskus sillä viitataan palveluihin, joiden avulla luodaan ja ylläpidetään tyypillisesti muita kuin yksityiselämään liittyviä ihmissuhteita. Esimerkki erityisesti työelämään liittyvästä verkostoitumispalvelusta on LinkedIn, jota voidaan hyödyntää mm. oman työhistorian kuvaamisessa ja esittämisessä, työnhaussa ja asiantuntijatiedon vaihdossa. (Sanastokeskus TSK 2010b.)

Sisällönjakopalvelu on palvelu, joka tarjoaa mahdollisuuden sisällön jakamiseen tietoverkossa. Sisällönjakopalveluita ovat esimerkiksi kuvanjakopalvelut, kuten Flickr, äänitallenteenjakopalvelut, kuten MySpace -verkkoyhteisöpalvelun musiikinjakopalvelu, videonjakopalvelut, kuten YouTube, diaesitysten jakopalvelu SlideShare ja yhteisöllisten kirjanmerkkien jakopalvelut, kuten Delicious. (Sanastokeskus TSK 40, 2010a.)

Verkkopalvelu on verkkosivuston kautta tarjottava palvelu. Verkkopalveluja ovat esimerkiksi selaimen kautta käytettävät sähköpostipalvelut, sähköinen kaupankäynti, pankki- ja viranomaisasiointi internetissä sekä internetpuhelut. Termillä verkkopalvelu viitataan usein myös verkkosivustoon, jonka kautta palvelua tarjo-

taan, esimerkiksi "X-verkkopalvelussa voit hoitaa pankki- ja vakuutusasiasi". (Sanastokeskus TSK 2012c.)

2.3.1 Facebook

Facebook on verkkoyhteisöyhteisöpalvelu, johon ihmiset kirjautuvat omalla nimellään ja voivat siten pitää yhteyttä esimerkiksi perheenjäseniinsä tai ystäviinsä. Nykyään Facebookiin voi rekisteröityä myös yrityksiä, jotka mainostavat palveluitaan tai tuotteitaan. Palvelun kehitti 19-vuotias Mark Zuckerberg vuonna 2004 yhdessä kolmen muun opiskelijan Eduardo Saverinin, Dustin Moskovitzin ja Chris Hughesin kanssa Harvardin yliopistossa Amerikan Yhdysvalloissa. Alun perin sivusto oli rajoitettu ainoastaan Harvardin yliopiston opiskelijoille, mutta sen jälkeen sivusto alkoi kattaa muidenkin yliopistojen opiskelijat. Ennen pitkää sivustolle sai rekisteröityä kuka tahansa yli 13-vuotias ja lopulta sivusto laajeni ympäri maailman kaikille halukkaille. (Carlson 2010.)

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. Facebookiin on mahdollista perustaa myös yksityisiä ryhmiä esimerkiksi opiskelua varten. Facebookia pidetään verkkoyhteisöpalveluna. Verkkoyhteisöpalvelulla tarkoitetaan palvelua, joka tarjoaa ihmisille mahdollisuuden muodostaa ihmisten välisiä suhteita ja ylläpitää niitä verkon kautta. (Sanastokeskus TSK 2010b, 43, 26.)

2.3.2 YouTube

YouTube on sisällönjakopalvelu, joka antaa käyttäjille mahdollisuuden julkaista videoita ja katsoa muiden käyttäjien julkaisemia videoita YouTubessa. Helmikuussa 2005 perustettu YouTube tarjoaa ihmisille paikan, jossa he voivat pitää yhteyttä, tiedottaa ja innoittaa muita ihmisiä ympäri maailman. Se toimii alkuperäisen sisällön luojien sekä pienten ja suurten mainostajien jakelukanavana. (YouTube 2013a.)

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 tähän oli YouTubeen ladattu tekijänoikeuksien piiriin kuuluva materiaali. Chad Hurley, kertoi ennen kauppaa, että yhteistyö 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 2013b). Koska Google omistaa YouTuben, Googlen 1. päivänä maaliskuuta 2012 voimaan tulleet uudet käyttöehdot koskevat myös YouTuben käyttäjiä (Google 2012.)

2.3.3 Google

Googlen pyrkimyksenä on maailman tietojen järjestely ja niiden tuominen mahdollisimman monien saataville. Googlen perustajat Larry Page ja Sergey Brin tapasivat Stanfordin yliopistossa vuonna 1995. Vuoteen 1996 mennessä he olivat jo

kehittäneet hakukoneen (alun perin nimeltään BackRub), joka määrittää verkkosivuston tärkeyden linkkien perusteella. Yritys on saanut aikaan paljon suhteellisen lyhyessä ajassa. Google perustettiin vuonna 1998, jonka jälkeen se on kasvanut nopeasti yritykseksi, joka palvelee asiakkaita ympäri maailman. (Google 2013a–b.)

2.3.4 Twitter

Twitter on verkkopalvelu, jossa on mikroblogin ja verkkoyhteisöpalvelun ominaisuuksia. Käyttäjä voi lähettää lyhyitä blogimerkintöjä, "tviittejä" (englanniksi tweet), palvelun verkkosivustolle matkapuhelimella tai selaimella. Merkinnät tulevat näkyviin käyttäjän palvelussa luomaan profiiliin. Muiden käyttäjien tekemät merkinnät voi nähdä palvelun verkkosivulla, tai niistä voi saada tiedon tekstiviestinä, verkkosyötteenä tai muiden sovellusten avulla. (Sanastokeskus TSK 40, 2010c.)

Twitter on myös yhteisöpalvelu. Se on perustettu vuonna 2006 Jack Dorseyn, Evan Williamsin ja Biz Stonen toimesta. Se syntyi Odeo-nimisen podcasting-palvelun sivutuotteena. Idea sivustoon lähti kokouksessa, jossa Dorsey toi esille idean tekstiviestipalvelusta, jonka avulla voitaisiin nopeasti kertoa ryhmässä oleville, mitä kukin sillä hetkellä tekee. Twitterissä kaikkien viestien oletus on julkinen ja viestien pituus on rajattu 140 merkkiin, jotta viesti mahtuu tekstiviestin pituuteen. Twitter-sanan idea tuli sen tarkoituksesta eli lyhyttä merkityksetöntä tietoa ja ääni, jota linnut tuottavat. Twitterin idea oli ainutlaatuinen sosiaalisen median maailmassa, koska käyttäjät pystyivät seuraamaan muita käyttäjiä ilman, että heitä seurattaisiin takaisin. (Sagolla 2009; Miller 2010.)

2.3.5 MySpace

MySpace LLC on johtava sosiaalisen viihteen kokoontumispaikka, jonka kantavana voimana on fanien intohimo. Y-sukupolvelle suunnattu MySpace kannustaa sosiaaliseen vuorovaikutukseen tarjoamalla yksilöllisen viihdekokemuksen ja yhdistämällä ihmiset heidän suosikkimusiikkiinsa, elokuviin, peleihin, julkkiksiin ja TV-ohjelmiin. Viihdekokemukset ovat saatavana usean eri kanavan kautta, mukaan lukien verkko, mobiililaitteet ja verkon ulkopuoliset tapahtumat. MySpacessa on myös MySpace-musiikkipalvelu, jonka vapaasti suoratoistettava musiikki- ja videokirjasto kasvaa jatkuvasti ja joka tarjoaa merkittäville, riippumattomille ja omakustanneartisteille erinomaiset välineet uuden yleisön tavoittamiseksi. Yhtiön päämaja sijaitsee Beverly Hills'issä Kaliforniassa, ja se on osa Specific Mediaa. (Myspace 2012.)

Kun vuonna 2002 perustettiin Friendster, useat eUniversen työtekijät, joilla oli Friendster -tili, näkivät sivuston potentiaalin ja päättivät kopioida muutamia sivuston suosituimpia ominaisuuksia. Näin syntyi vuonna 2003 MySpace, jonka ensimmäiset käyttäjät olivat eUniversen työntekijät. Tämän jälkeen yritys pisti pystyyn kilpailun, kuka saa sivustolle eniten käyttäjiä. Sitten ei kestänytkään enää kauaa ennen kuin sivusto alkoi kasvaa. (Douglas 2006.)

MySpace oli pitkään suosituin sosiaalisen median sivusto, mutta sen suosio alkoi laskea sen jälkeen, kun Facebook tuli uusine ominaisuuksineen ja vei MySpacen käyttäjiä. (Owyang 2008.)

3 SOSIAALISEN MEDIAN TIETOTURVA JA -SUOJA

Tässä luvussa perehdyn sosiaalisen median tietoturvaan ja -suojaan. Aluksi kerron teknisistä uhista ja sen jälkeen haittaohjelmista sekä roskapostista sosiaalisessa mediassa. Tämän luvun tarkoitus on auttaa ymmärtämään paremmin mitä sosiaaliseen mediaan kuuluu, jotta osaamme varautua paremmin riskeihin ja uhkiin ja mahdollisuuksien mukaan estää mitään pahempaa tapahtumasta ja löytää vahvuutemme niiden voittamiseen.

3.1 Sosiaalisen median tekniset uhat

Monet palvelin- (server) ja työasemasovellukset (client) sovellukset sisältävät haavoittuvuuksia. Ne mahdollistavat esimerkiksi käyttäjän koneen haltuunoton, haittaohjelmien levittämisen tai käyttäjän ohjaamisen saastuneille sivustoille. Tarjonta ja kilpailu sosiaalisen median palveluissa kehittyvät nopeasti. Tämä edellyttää nopeaa sovelluskehityksen ja palveluiden tuotantomallia. Nopeatempoisessa sovelluskehityksessä testaaminen ja tietoturvallisuus kärsivät, jolloin palveluihin voi jäädä haavoittuvuuksia, jotka mahdollistavat riskien toteutumisen. Lokakuussa 2010 julkaistiin uutinen Firefox -selaimen lisäosasta nimeltään Firesheep, joka kuuntelee verkkoliikennettä ja kaappaa sieltä sosiaalisen median palveluissa käytettäviä evästeitä mahdollistaen siten identiteettivarkaudet. (Valtiovarainministeriö 2010, 16–17.)

Etsiessäni lisää lähteitä tähän opinnäytetyöhön, löysin pari loistavaa esimerkkiä Cert.fi sivustolta, josta seuraavaksi esimerkit, jotka on päivätty 21.3.2013 ja 25.3.2013.

21.3.2013: "Aalto-Yliopiston tutkijat ovat käyttäneet verkon laitteiden tutkintaan hakukone Shodania, joka etsii avoimia laitteita verkosta ja on keskittynyt teollisuusautomaatiolaitteisiin. Tutkimuksessa on löydetty Suomen skannatusta IP-avaruusalueesta lähes 3000 automaatiolaitetta, joihin kuka tahansa pystyy ottamaan yhteyttä Internetin kautta. Näistä muutama tuhat on edelleen auki verkkoon. Shodan on verkkopalvelu, joka skannaa yleisimpiä portteja verkosta ja tallentaa niistä saadut tiedot tietokantaan, johon voidaan kohdistaa hakuja. Shodanista voi etsiä erilaisilla avainsanoilla tietoa eri järjestelmiin liittyen, esimerkiksi tiettyjen TCP/UDP porttien tai järjestelmän tunnisteen, kuten valmistajan nimen avulla. Tutkijoiden löytämien laitteiden joukossa on ollut mm. verkkokameroita, kiinteistönhallintajärjestelmiä ja teollisuusautomaatiojärjestelmiä. Osassa verkossa olevista laitteista on myös havaittu päivittämättömiä ohjelmistoja. Cert.fi:n tietoon on aikaisemmin tullut myös yksittäistapauksia avoimista automaatiolaitteista verkossa. Osa aiemmin tietoon tulleista järjestelmistä on ollut kytkettynä verkkoon tietoisesti ilman suojausta. Laitteiden ja verkkoon liitettyjen automaatiojärjestelmien suojaukseen julkisessa verkossa tulee kiinnittää huomiota. Laitteiden elinkaaren aikana on syytä huolehtia niiden päivityksestä.

Käyttöönoton yhteydessä on syytä:

- *rajata pääsyä palomuurin, VPN-yhteyksien tai sallittujen osoitteiden listan avulla*
- *vaihtaa pääkäyttäjän salasana tai luoda kokonaan uusi tili hallintaa varten*
- *poistaa vierailija- ja muut käyttämättömät tunnukset käytöstä*
- *käyttää riittävän vahvoja salasanoja käyttäjätilien suojaamiseen"* (Cert.fi 2013a.)

25.3.2013: "Yhdysvaltalaisen CloudFlare-palveluntarjoajan verkkoon on jo jonkin aikaa kohdistunut hyvin voimakas palvelunestohyökkäys. Hyökkääjien tarkoituksena näyttää olevan häiritä roskapostin torjuntaan erikoistuneen SpamHausin palvelinten toimintaa. Hyökkäyksessä käytetään hyväksi sellaisia nimenselvitykseen käytettäviä nimipalvelimia, jotka ovat avoimesti kenen tahansa käytettävissä. Hyökkäyksessä nimipalvelimelle lähetetään nimipalvelukyselyjä, joissa lähettäjän IP-osoitteeksi on väärennetty hyökkäyksen koh-

teena olevan palvelimen osoite. Nimipalvelin lähettää vastauksensa kyseiseen osoitteeseen. Tämä on mahdollista, koska nimipalvelussa käytetään UDP-protokollaa, joka ei TCP-protokollan tavoin vaadi kaksisuuntaista kättelyä yhteyttä avatessa. Koska nimipalveluvastaukset ovat moninkertaisesti kyselypaketteja isompia, saadaan melko vähäisellä dataliikenteellä aikaan paljon liikennettä kohdepalvelimelle. Hyökkäysliikenteestä on toistaiseksi tunnistettu yli sata suomalaista IP-osoitetta. Kyseisten osoitteiden haltijoihin otetaan yhteyttä Internetoperaattorien kautta. Tietojemme mukaan suomalaisissa verkoissa on vähintään 26000 sellaista laitetta, joita voi käyttää nimenselvitykseen, ja jotka löydyttyään ovat mahdollisesti käytettävissä palvelunestohyökkäyksiin. Suosittelemme, että omien nimipalvelinten ylläpitäjät tarkistavat omien palvelintensa asetukset. Avoimet resolver-nimipalvelimet helppoja kohteita. Resolver-nimipalvelimet on tavallisesti tarkoitettu tietyn asiakaskunnan käyttöön. Internetoperaattorilla on asiakkaitaan varten omat nimipalvelimet, joiden IP-osoitteet asentuvat DHCP-palvelun kautta asiakkaan laitteisiin ja tietokoneisiin. Koti- tai yritysverkon reititin tai ADSL-päätelaite toimii yleensä siten, että se ohjaa sisäverkon tietokoneiden nimipalvelukyselyt operaattorin palvelimelle. Laitteen tulisi sallia nimenselvitys vain sisäverkosta tuleville pyynnöille. Jos palvelu on avoinna myös Internetiin päin, laitetta tai tietokonetta voidaan käyttää hyväksi hyökkäysliikenteen vahvistajana. Nimipalveluohjelmiston (esimerkiksi BIND) asetuksissa on syytä rajoittaa niitä verkkoja, joista nimenselvitys on sallittu. Reitittimien tai ADSL-laitteiden ylläpitokäyttöliittymästä voi useimmiten valita, että mitä palveluja tarjotaan internetiin (WAN) ja mitkä palvelut ovat käytettävissä sisäverkosta (LAN). Väärennettyjen osoitteiden käyttämistä voitaisiin vaikeuttaa siten, että kaikki internetoperaattorit toteuttaisivat ns. BCP38 (Best Current Practices -dokumentti 38 ja sen korvannut versio 84, RFC 2827 ja 3704) mukaisen suodatuksen, jolloin kunkin operaattorin verkosta voisi liikennöidä ulospäin vain sellaisilla IP-lähdeosoitteilla, jotka kuuluvat sille itselleen. Valitettavasti läheskään kaikilla ulkomaisilla operaattoreilla tällaista suodatusta ei ole käytössä. Auktoritatiiviset palvelimet vastaavat omista verkkotunnuksistaan. Myös verkkotunnusten auktoritatiivisia nimipalvelimia ja juurinimipalvelimia käytetään hyväksi hyökkäyksissä. Jotta verkkotunnukseen liitetyt palvelut toimisivat, on verkkotunnuksen auktoritatiivisten nimipalvelinten vastat-

tava kyseiseen verkkotunnukseen kohdistuviin osoitekyselyihin. Tämän vuoksi kyselyjä ei voi estää IP-osoitteiden perusteella. Hyökkäyksen vaikutuksia voidaan torjua nimipalveluohjelmistojen ominaisuuksilla, joiden avulla vastaamista samoista osoitteista tulleisiin kyselyihin rajoitetaan (rate limiting). Rajoittamisen voi tehdä myös erillisellä palomuurilla tai muulla laitteella, joka sijoitetaan verkkoon nimipalvelimen eteen. Auktoritatiivisten nimipalvelinten ei tulisi vastata rekursiivisiin nimipalvelupyyntöihin, eli niiden ei tulisi vastata kyselyihin muista kuin itse hallitsemistaan verkkotunnuksista." (Cert.fi 2013b.)

Opimme tästä, että koskaan ei voi olla liian varovainen tietoturvan suhteen. Tietokoneilla pitäisi olla riittävät palomuurit, sekä virustentorjunnat. Käyttäjien pitäisi vaihtaa salasanojaan useammin, ja niiden pitäisi sisältää kirjaimia, numeroita sekä erikoismerkkejä, jotta niitä ei voisi hakkeroida helposti. Selvä järjen käyttö on aina paikallaan, kun mietitään teknisiin uhkiin varautumista.

3.2 Haittaohjelmien leviäminen ja roskaposti sosiaalisessa mediassa

Koska sosiaalisen median palveluiden käyttäjämäärä kasvaa nopeasti, tarjoaa se valitettavasti väärinkäyttäjille alustan yrittää nopeasti levittää uusia haittaohjelmia käyttäjän tietokoneisiin. Haittaohjelmariski koskee sellaisia sosiaalisen median palveluita, joissa palvelun käyttäminen edellyttää www-selaimessa ohjelmakoodin suorittamista. Sen sijaan esimerkiksi pelkästä tekstisisällöstä koostuvat palvelut muodostavat vähäisemmän haittaohjelmariskin. (Valtiovarainministeriö 2010, 17.)

Valtiovarainministeriön sivulta (2010), voidaan selvästi löytää neljä eri syytä, jotka edistävät haittaohjelmien leviämistä sosiaalisessa mediassa.

1. jos henkilö saa viestin sosiaalisessa mediassa henkilöltä jonka tuntee, se saatetaan kuvitella turvalliseksi
2. url-lyhenteet, eli nettisivujen osoitteiden lyhentäminen, niin että henkilö ei näe, mihin osoitteeseen on menossa
3. tietoturva-aukot omalla tietokoneella, tai ohjelmissa, joita käyttää
4. uudenlaiset haittaohjelmat, jotka käyttävät hyväkseen henkilön luottamusta tuntemiinsa ihmisiin (Valtiovarainministeriö 2010, 17.)

Haittaohjelmilta suojautumiseen tarvitaan maalaisjärkeä ja teknisiä apuvälineitä eli tietoturvaohjelmistoja. Tietoturvaohjelmistot koostuvat useista eri osista, joista tärkeimmät ovat virustentorjunta- ja palomuuriohjelmat. Näitä ohjelmia voi ostaa valmiina ohjelmistopaketteina tai operaattorien tarjoamina tietoturvapalveluina. Koneen käyttöjärjestelmä kannattaa myös pitää ajan tasalla, jotta mahdolliset haavoittuvuudet järjestelmässä saadaan korjattua nopeasti. Tietoturvan kolmen perussäännön (päivitä käyttöjärjestelmä ja pidä palomuuri ja virustorjunta ajan tasalla) noudattaminen auttaa tehokkaasti suojautumaan haittaohjelmilta. (Tietoturvaopas.fi 2008.)

Roskapostiksi kutsutaan ei-toivottua, suurina massoina lähetettyä, ei kenellekään erityisesti kohdistettua sähköpostiviestintää. Roskaposti ruuhkauttaa sähköpostijärjestelmiä ja tukkii ihmisten sähköpostilaatikoita. Roskapostittajien työkaluina käytetään sähköpostimatoja ja botteja. Seuraavaksi ohjeita roskapostin oikeaoppiseen käsittelyyn:

1. Älä koskaan avaa epäilyttäviä viestejä, vaan poista ne suoraan viestivalikosta.

2. Älä koskaan vastaa roskapostiviestiin.

3. Ota käyttöön operaattorin, sähköpostiohjelman tai tietoturva ohjelmistoon mahdollisesti sisältyvä roskapostin suodatusominaisuus.

4. Luovuta harkiten sähköpostiosoitteesi esimerkiksi Internet-sivujen kyselyihin ja keskustelupalstoille.

5. Älä lähetä ketjuviestejä ja kiertokirjeitä edelleen. (Tietoturvaopas.fi 2008.)

Roskaposti on muodostunut ongelmalliseksi myös sosiaalisen median palveluissa. Ominaista roskapostille on hakukoneiden mahdollistama roskapostien kohdentaminen tietyille käyttäjäryhmille. Viestit voivat sisältää linkkejä esimerkiksi tuotemyyntisivustoille tai pornografisiin sivustoihin. Roskapostin estäminen on usein hankalaa. Syksyllä 2010 Facebook-verkkopalvelussa levisi viesti, josta ”pitämällä” (like) huijausviesti pääsi käsiksi käyttäjän profiilitietoihin ja sai selville käyttäjän matkapuhelinnumeron. Huijauksen seurauksena käyttäjän matkapuhelinlaskuun tuli 19 € lisämaksu ylimääräisestä palvelusta. (Valtiovarainministeriö 2010, 18.)

Sähköpostiosoitteen julkaiseminen Internetissä on joskus tarpeellista yhteydenottojen mahdollistamiseksi. Niitä kerätään kuitenkin verkosta myös roskapostin ja muiden haittaohjelmien kartoittamiseksi. Kerätyt tiedot ovat rahanarvoista kauppatavaraa, jolle on myös olemassa olevat markkinat. Sähköpostiosoite kannattaa julkaista verkkosivulla siten, että automaattiset osoitteiden keräämiseen tarkoitetut ohjelmat eivät tunnista sitä sähköpostiosoitteeksi. Sähköpostiosoite voidaan liittää sivulle kuvatiedostona. Silloin se ei toimi linkkinä, vaan viestiä lähettävän on kirjoitettava sähköpostiosoite käsin. Toinen tapa toimia on kirjoittaa www-sivulla nimet erikseen, esimerkiksi etunimi.sukunimi@jotain.fi. Kolmas tapa on kirjoittaa koko osoite ja siihen kuuluvat välimerkit erikseen tekstinä, esimerkiksi etunimi piste sukunimi (at) jotain piste fi. (Tietoturvaopas.fi 2008.)

Tunnetuimpia haittaohjelmia ovat virukset, madot ja vakoiluohjelmat. Viruksia saadaan koneelle muun muassa sähköpostin kautta, ladattaessa tiedostoja Internetistä, pikaviestiohjelman välityksellä tai vertaisverkon kautta. Virukset leviävät myös cd- ja dvd-levyjen, levykkeiden sekä muistitikkujen välityksellä. (Tietoturvaopas.fi 2008.)

Seuraavaksi vielä selvennettynä miten eri haittaohjelmat ja edellä mainitut ongelmat voi tunnistaa. Haittaohjelmat aiheuttavat monenlaisia harmeja tietokoneen käytölle. Koneen käyttö hidastuu sekä sähköpostin käyttö ja verkkosurffailu hankaloituvat. Kone saattaa käynnistyä itsestään ilman käyttäjän toimenpiteitä tai ohjelmiston toimintaan tulee muita häiriöitä. Muita ongelmia ovat tietojen vaihtuminen tai häviäminen, selaimen kotisivun muuttuminen sekä muut käyttöhäiriöt. (Tietoturvaopas.fi 2008.)

Sähköpostimadot lähettävät itsensä käyttäjän osoitekirjassa oleviin osoitteisiin ja voivat liittää viestin mukaan tietokoneella olevia tietoja. *Virukset* muuttavat tietokoneen roskapostin välitystoimistoksi. Tällainen kone lähettää automaattisesti viestejä käyttäjän huomaamatta. *Verkkomadot*, kuten esimerkiksi Sasser ja Blaster, etsivät verkkoon kytkettyjä koneita, joihin ei ole asennettu uusimpia korjauspäivityksiä. Madot leviävät viruksia nopeammin suoraan koneelta toiselle. (Tietoturvaopas.fi 2008.)

Perinteisten virusten ja matojen lisäksi on myös muita haittaohjelmatyyppejä, kuten esimerkiksi botit ja troijan hevoset. Bot tulee sanasta robot, joka kuvastaa haittaohjelman leviämistapaa. Se on automaattinen ja muistuttaa verkkomatoa. Botis-

sa voi olla mukana myös muita ominaisuuksia, kuten takaportteja ja vakoiluohjelmia. *Botit* ovat haittaohjelmia, joiden avulla tietokonetta hallitaan käyttäjän huomaamatta verkon välityksellä. *Troijan hevoseksi* kutsutaan haittaohjelmaa, joka naamioidaan viattoman näköiseksi hyötyohjelmaksi tai peliksi. Pahimmillaan se tuhoaa tietokoneen kovalevyn sisällön. (Tietoturvaopas.fi 2008.)

Takaportiksi kutsutaan ohjelmaa, joka avaa ulkoisen tietoliikenneyhteyden suojaamattomaan tietokoneeseen. Takaportin kautta varastetaan käyttäjän henkilökohtaisia tietoja koneesta. *Vakoiluohjelmiksi* kutsutaan ohjelmia, jotka keräävät tietoa ohjelmistojen tai koneen käyttötavoista, käyttäjän tallentamista tiedoista ja vaikkapa näppäinpainalluksista. Vakoiluohjelma lähettää tiedon eteenpäin tai avaa pääsyn tietokoneeseen verkon kautta asentamalla koneeseen takaportin. Mainosohjelmat voidaan luokitella haittaohjelmiksi, joskin ne ovat monesti osana ns. ilmaisjakeluohjelmia. Mainosohjelman tavoitteena on saada käyttäjä menemään halutulle Internet-sivustolle. Uusimpia haittaohjelmia ovat ns. rootkitit eli piilohaittaohjelmat. *Rootkit* on ohjelma, joka osaa piilottaa oman toimintansa täysin näkymättömiin niin virustentorjuntaohjelmalta kuin käyttäjältä. (Tietoturvaopas.fi 2008.)

3.3 Sosiaalisen median yksityisyyteen liittyvät uhat ja pelot

Sosiaalisessa mediassa on huomioitava tarkasti omat yksityisyysasetukset. Esimerkiksi Facebookissa yksityisyysasetukset ovat yleensä lähtökohtaisesti heikoimmalla mahdollisella tasolla silloin, kun käyttäjä rekisteröityy palveluun. (Vander Veer 2008, 205.) Tällöin kaikki ne henkilöt, jotka menevät käyttäjän profiilisivulle, näkevät mitä käyttäjä on kertonut itsestään sekä hänen valokuvansa. Jos yksityisyysasetukset ovat heikoimmalla mahdollisella tasolla, tietoja pääsevät kat-

somaan myös sellaiset henkilöt, joilla ei ole Facebookia. Tiedot löytyvät suoraan myös kun kirjoittaa henkilön nimen Googlen hakukoneeseen. Samaiset tiedot löytyvät myös Twitteristä ja muista sosiaalisen median palveluista, jos yksityisyysasetuksia ei ole muutettu alkuperäisistä asetuksista.

Netti-identiteetti näyttelee yhä tärkeämpää roolia jokapäiväisessä elämässä, ja sosiaalinen media on mahdollistanut täysin uusia tapoja tehdä ihmisen yksityisyyttä loukkaavia rikoksia. Jokaisen itsemääräämisoikeus turvataan perustuslaissa, mutta käytännössä tämä ei toteudu netin globaalin luonteen ja nykyisen lainsäädännön takia. Lainsäädännön loogisuus on paperiajalta, ja sen myötä viranomaisilla on ongelmia vääntää ja venyttää lakeja sosiaaliseen mediaan sopivaksi. (Nettipoliisi 2013, 1.)

Sosiaalisen median käyttämisestä on olemassa kuitenkin myös menestystarinoita, joissa palveluun sitoutunut kävijäyhteisö pystyy lopulta tarjoamaan apua myös toisilleen. Yhteisön tuki toimii myös silloin, jos joku kävijöistä ”hyökkää” organisaatiota vastaan huutelemalla tai kirjoittelemalla asiattomuuksia. Kuitenkin sosiaalisessa mediassa pitää olla varautunut myös negatiiviseen palautteeseen, sillä tarkoitus on käydä tasavertaista keskustelua kuluttajan kanssa. (Viestintätoimisto Tulus Oy 2013, 11–12.)

Sosiaaliseen mediaan mentäessä kannattaa muistaa, että hyötyjen lisäksi sillä on myös mahdolliset riskinsä. Uhkien olemassaolo ja niihin liittyvän tietoisuuden kasvu sisältää myös positiivisen kääntöpuolen. Riskit tiedostamalla yritykset ja yksityiset henkilöt oppivat suhtautumaan sosiaaliseen mediaan riittävällä vaka-

vuudella ja oppivat käyttämään sitä pitkäjänteisesti ja strategisesti liiketoimintansa edistämisessä. (Viestintätoimisto Tulus Oy 2013, 11–12.)

Sosiaalinen media ei silti ole mikään mystinen paikka, jossa pitäisi pelätä kuluttajia. Siellä liikkuvat samat ihmiset, jotka soittavat asiakaspalveluun tai lähettävät kyselyjä sähköpostitse. Sosiaalisen median kautta kuluttajalla on mahdollisuus olla avoimessa dialogissa organisaation kanssa, kun taas organisaatioille on tärkeää saada suoraa palautetta. (Viestintätoimisto Tulus Oy 2013, 11–12.)

Useisiin sosiaalisen median palveluihin, kuten esimerkiksi Facebookiin tai MySpaceen, on mahdollista lisätä omia kiinnostuksen kohteita ja muita tietoja itsestään. Monille ei kuitenkaan ole täysin selvää, mihin jaettuja tietoja käytetään tai esimerkiksi millä tavoin jopa tuntemattomat ihmiset voivat nähdä jaettuja tietoja. Erilaisten Facebook-sovellusten tekijät voivat käyttää tietoja hyväkseen myös muissa web-palveluissa. (Cert.fi 2011.)

Yksityisyysasetuksien muokkaaminen voi olla tietokoneen käyttöön tottumattomalle hankalaa eikä termejä ymmärretä täysin. Sovellukset, joita käyttäjät asentavat, kuten tietovisat ja erilaiset pelit, pääsevät käsiksi käyttäjän profiiliin kysymällä lupaa. Ilman lupaa pelin tai tietovisan käyttöoikeutta ei välttämättä heru lainkaan. (Cert.fi 2011.)

Tällaisia käyttäjän omia tietoja, joita sovellukset voivat kysyä, ovat esimerkiksi käyttäjän kaverilista, nimi, verkostot, sähköpostiosoite, profiilikuva sekä käyttäjätunnus. Useimmat sovellukset hakevat myös kaikki käyttäjän julkiseksi määritte-

lemät tiedot. Sallimalla sovelluksen käyttää tietoja tulee myös hyväksyneeksi esimerkiksi palvelun käyttöehdot sekä yksityisyydensuojaperiaatteet. Sovellukset voivat myös käyttöehdoissaan pyytää lupaa käyttäjän sähköpostiosoitteen jakamiseen yhteistyökumppaneilleen. Tällöin sovellusten käyttäjät voivat saada roskapostiksi mieltämäänsä kohdennettua sähköpostia, jonka lähettämiseen ovat itse asiassa antaneet luvan. (Cert.fi 2011.)

Facebook-sovellukset voivat käyttää Facebookissa jaettuja tietoja hyväkseen myös muissa Internet-palveluissa, vaikka sitä ei suoraan missään sanottaisi. Omien tietojen jakamiseen sosiaalisen median palveluissa tulisikin suhtautua niin kuin mihin tahansa muuhun tietojen jakamiseen netissä. On myös muistettava, että pelkkä sovelluksen poistaminen ei välttämättä poista tietoja muista palveluista, joille käyttäjä on kerran antanut tietonsa. Nyrkkisääntönä tietojen ja netin jakamisen kanssa kannattaakin pitää sitä, että kun on kerran laittanut jotain verkkoon, sitä ei välttämättä koskaan saa pois sieltä. (Cert.fi 2011.)

Liian yksityiskohtaista julkista kuvausta itsestään ei nettiin kannata missään nimessä antaa. Pahimmassa tapauksessa se voi johtaa identiteettivarkauteen. Identiteettivarkaudella tarkoitetaan sitä, että joku esiintyy toisena henkilönä. Yksityiskohtaisia tietoja voidaan käyttää hyväksi myös niin kutsutuissa Social Engineering -tapauksissa, joissa esiintymällä toisena henkilönä pyritään pääsemään käsiksi tietoihin tai omaisuuteen, joihin tällä henkilöllä on pääsy. Muokkaamalla yksityisyysasetuksia määritellään, mitä tietoja muut näkevät meistä. (Cert.fi 2011.)

Twitterissä kuka tahansa voi lukea käyttäjän viestejä, jos vain tietää tilin osoitteen. Twitter-tilejä on myös helppo hakea yleisellä hakukoneella kuten Googlella. Twit-

ter -mikoroblogipalvelun tunnuksia voidaan myös kalastella verkossa. Niitä kalastellaan erilaisilla Twitter-viesteillä. Viesteissä oleva linkki johtaa urkintasivustolle, jossa kysellään Twitterin käyttäjätunnusta ja salasanaa. Mikroblogipalvelu Twitterissä kiersi helmikuussa 2013 viestejä, joissa kyseltiin "Did you see this pic of you?". Viestin liitteenä oli lyhytlinkki, jota klikkaamalla käyttäjä päätyi sivustolle, joka näytti erehdyttävästi Twitterin omilta sivuilta. Osoitepalkista kuitenkin voitiin huomata, ettei selain ole enää Twitterin omilla sivuilla. Jos käyttäjä on antanut kirjautumistietonsa sivustolle, kannattaa salasana käydä vaihtamassa välittömästi. Vietyjä kirjautumistietoja voidaan käyttää vastaavien viestien lähettämiseen muille Twitterin käyttäjille. On myös mahdollista, että myöhemmin lyhytlinkkiä klikanneen käyttäjän koneelle yritetään tartuttaa haittaohjelma. Vastaavanlaiset huijausyritykset ovat varsin yleisiä sosiaalisessa mediassa. Usein klikkauksilla yritetään kuitenkin ohjata käyttäjä asentamaan jotain, esimerkiksi Facebookin sovellus tai antamaan urkintasivustolle oikeuden käyttää palveluun tallennettuja yhteystietoja. (Cert.fi 2013c.)

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

Sosiaaliset yhteisöt ovat innoittaneet monet käyttäjät kertomaan ahkerasti, missä he kulloinkin ovat. Seurauksena yli 50 kotia ryöstettiin Nashuan kaupungissa New Hampshiressa. Uhka sosiaalisten yhteisöjen avulla tehtävistä murtovarkauksista on toteutunut aika ajoin. Huoli ihmisten kirjoittelusta kirvoitti verkkopalvelun nimeltä PleaseRobMe. Se julkaisi Twitter -viestejä ja listasi tyhjillään olevia

koteja. Verkkosivu on yhä olemassa, mutta viestien julkaisu on lopetettu. (Linnake 2010.)

Nykyisin kannattaa varautua siihen, että mikään Internetiin laitettu ei välttämättä häviä sieltä koskaan. Twitterin viesti, YouTubeen laitettu video, Facebookiin laitettu kuva tai blogiin kirjoitettu mielipide voi löytyä vielä vuosienkin päästä. Sivuista on helppo tehdä kopioita ja myöhemmin levittää tietoja niistä. Monet palveluntarjoajat eivät välttämättä poista profiilia, vaikka palvelusta eroaisikin. (Järvinen 2010, 239–241.)

Aina kannattaa miettiä tarkoin, mitä sosiaalisessa mediassa kirjoittaa. Esimerkiksi työpaikastaan ei kannata kirjoittaa mitään negatiivista. Esimerkiksi Volvo antoi Ruotsissa potkut kolmelle vuokratyöntekijälle, kun yksi työntekijä oli kirjoittanut Facebook-sivulleen viestin ”vielä yksi päivä viikkoa, tässä hullujenhuoneessa”. Toiset kaksi saivat potkut sen johdosta, kun kirjoittivat kommentteja vastaavaan sävyyn. (Kotilainen 2011.)

Suomessa on voimassa laki yksityisyyden suojasta työelämässä (759/2004). Lain 2. luvun 4. §:ssä sanotaan. ”*Työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa työntekijältä itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Suostumus ei kuitenkaan ole tarpeen silloin, kun viranomainen luovuttaa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi tai kun työnantaja hankkii henkilöluottotietoja tai rikosrekisteritietoja työntekijän luotettavuuden selvittämiseksi. Työnantajan on ilmoitettava työntekijälle etukäteen tätä koskevien tietojen hankkimisesta luotettavuuden selvittämistä varten. Jos työnantaja hankkii työntekijän henkilöluottotietoja, työnantajan tulee*

lisäksi ilmoittaa työntekijälle, mistä rekisteristä luottotiedot hankitaan. Jos työntekijää koskevia tietoja on kerätty muualta kuin työntekijältä itseltään, työnantajan on ilmoitettava työntekijälle saamistaan tiedoista, ennen kuin niitä käytetään työntekijää koskevassa päätöksenteossa. Työnantajan tiedonantovelvollisuudesta ja työntekijän oikeudesta tarkastaa itseään koskevia henkilötietoja on lisäksi voimassa se, mitä siitä muualla laissa säädetään." (Finlex.fi.)

Identiteettivarkaudet ovat yksi sosiaalisen median uhista. Blogeissa kerrotaan yksityiskohtaista tietoa omasta elämästä ja Facebookissa toimitaan omalla nimellä. 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 samalla tavalla kuin organisaatioitakin kohtaan eli luomalla henkilön nimissä väärennetty profiili. Väärennetty profiili saattaa vaikuttaa hyvinkin aidolta, jos väärentäjä on onnistunut keräämään riittävästi tietoa eri tietolähteistä. Vaikka tällaiset, usein ajattelemattomuudesta tai pilan päiten syntyneet ideat ja palvelut saattavat vaikuttaa harmittomilta, saattaa niillä olla merkittävä vaikutus identiteettivarkauden kohteelle. (Valtiovarainministeriö 2010, 15.)

Paras tapa suojautua sosiaalisen median uhilta on miettiä ja harkita tarkoin, mitä sinne kirjoittaa. Jo tällä suojatoimella pärjää pitkälle. On myös hyvä käydä läpi palvelun yksityisyysasetukset ja valita sieltä itselleen se sopivin. Ei julkaise kaikkia tietoja, vaan ainoastaan tietylle kaveripiirille tai perheelle. Sosiaalisessa mediassa voi perustaa myös ryhmiä, joihin pääsevät tietystä aiheesta kiinnostuneet

henkilöt, esimerkiksi ryhmä liikuntaa harrastaville tai sukututkimusta tekeville. Silloin voi vapaasti keskustella tästä aihepiiristä muiden samoista asioista kiinnostuneiden kanssa.

3.4 Muut riskit

Jokaisen tulisi sosiaalisen median palveluita käyttöön ottaessaan lukea ja seurata huolellisesti palvelun käyttöön liittyviä sopimus- ja palveluehtoja. Useissa palveluissa keskeinen haaste on toimittajan ja palvelun sijainti ulkomailla, jolloin palvelun tarjoaja ei ole halukas muuttamaan sopimusta ulkomaisen asiakkaan toiveiden vuoksi. Ulkomailla sijaitsevien sosiaalisen median palvelujen tarjoajat eivät ole Suomen lainsäädännön piirissä, jolloin sopimusehtojen lisäksi noudatettavat lainsäädännön vaatimukset voivat poiketa merkittävästi Suomessa totutuista. Suomalaisilla viranomaisilla ei ole automaattisesti toimivaltaa poistaa laitonta aineistoa ulkomaisesta palvelusta. (Valtiovarainministeriö 2010, 19.)

Jotkut henkilöt kertovat avoimesti tietoja itsestään ja omasta elämästään sosiaalisen median palveluissa. Osa palveluista on rakennettu niin, että hakukoneet, esimerkiksi Google, pystyvät hakemaan henkilöön liittyviä tietoja omaan tietokantaansa, jolloin tiedot ovat julkisesti nähtävissä ja löydettävissä. Henkilöön liittyvien tietojen joutuminen vääriin käsiin saattaa pahimmassa tapauksessa aiheuttaa henkilölle ja hänen lähipiirilleen fyysistä uhkaa. (Valtiovarainministeriö 2010, 20.)

Käyttäjä ei koskaan voi verkkoyhteisössä varmistua siitä, että yksityiseksi tarkoitettu sisältö pysyy luottamuksellisena. Palveluun tuotettua sisältöä voi tarkastella käyttäjän haluaman kaveripiirin lisäksi useita sellaisia silmäpareja, joille käyttäjä

itse ei ole halunnut kyseistä arkaluontoista tai yksityisyyttä loukkaavaa sisältöä jakaa. Käyttäjä itse voi haluta, että hänen yksityiseksi asiakseen mieltämänsä sisältö pysyy luottamuksellisena, kun taas sisällön vastaanottaja katsoo asiaa omasta perspektiivistään ja eikä välttämättä jaa lähettäjän näkemystä asian yksityisyydestä. Käyttäjä ei todellisuudessa voi olla varma siitä, miten toiset käyttäjät sosiaalisessa mediassa toimivat. Arkaluonteinen ja yksityinen sisältö voi toisen käyttäjän toimesta levitä milloin tahansa julkiseksi. (Aalto & Uusisaari 2009, 98–100.)

4 TUTKIMUKSEN TOTEUTUS

Tutkimusmenetelmänä käytettiin Centria ammattikorkeakoulun, Talonpojankadun, opiskelijoille ja henkilökunnalle suunnattua tutkimuskyselyä, jonka tarkoituksena oli kartoittaa heidän tietosuutta sosiaalisen median tietoturvasta ja tietosuojasta sekä heidän suhtautumistaan sosiaalisen median tietoturvauhkiin. Alkuperäinen idea oli tarkastella tuloksia myös vertailemalla niitä Katariina Nuotion (2012) opinnäytetyön, Haaga-Helian tuloksien kanssa, mutta tästä luovuttiin tutkimuksen edetessä, koska Nuotiolla oli eri koulutusalat eriteltyinä kuin tässä Centrialle tekemässäni tutkimuksessa. Olen kuitenkin tehnyt yleisvertailun kaikista vastauksista luvun 5 lopussa.

4.1 Tutkimuksen jäsentyminen kysymyksiksi

Ensimmäinen tutkimuskysymys koski sitä, millaisia ovat liiketalouden ja tekniikan opiskelijoiden sekä henkilökunnan käsitykset sosiaalisen median tietoturvasta. Aineiston saamiseksi tähän kysymykseen käytettiin kolmea kysymystä. ”Minkälainen käsitys sinulla on sosiaalisen median tietoturvasta?”. Vastaajille annettiin myös mahdollisuus antaa vapaamuotoisia perusteluja tähän kysymykseen. Jokaista vastaajaa pyydettiin antamaan vastaus 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 ja henkilökunnan käsitystä sosiaalisen median tietoturvasta, mutta siltä näkökannalta, aiheuttaako sosiaalisen median tietoturva huolta heissä. Edellä kuvatut kysymykset olivat kysymykset 4–7 (LIITE 1).

Toinen tutkimuskysymys koski kyselyyn vastanneiden tietoisuutta erilaisista sosiaalisen median riskeistä. Tässä kysymyksessä keskityttiin erityisesti niihin riskeihin, jotka koskivat käyttäjän henkilökohtaisia tietoja ja yksityisyyttä. Tähän ongelmaan haettiin vastausta kysymyksillä 8–13 (LIITE 1).

Kolmas vaihtoehtoinen tutkimuskysymys oli se, muuttuivatko vastanneiden käsitykset sosiaalisen median tietoturvasta ja sosiaalisen median käytöstä tutkimuksen aikana. Tähän ongelmaan aineisto saatiin 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 olivat seuraavat:

1. Minkälainen käsitys opiskelijoilla ja henkilökunnalla on tietoturvasta sosiaalisessa mediassa?

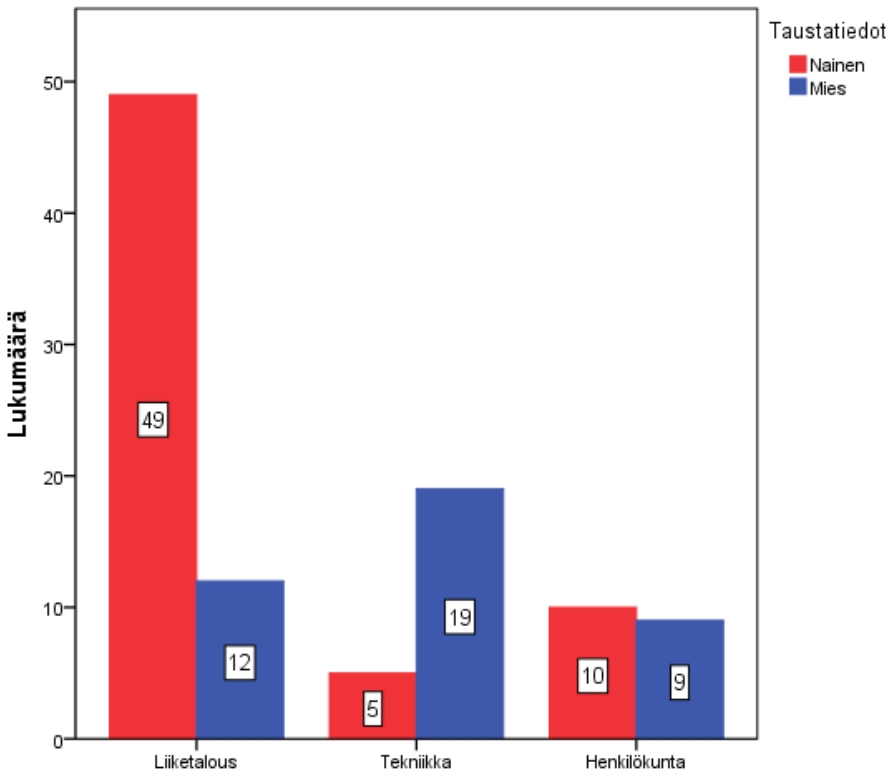
2. Mikä heidän tietoisuutensa on sosiaalisen median tietoturvariskeistä?

3. Muuttuiko kyselyyn vastanneiden suhtautuminen sosiaalisen median tietoturvaan ja sen käyttöön tutkimuskyselystä johtuen?

Kysymyksillä haluttiin saada selville, ovatko vastaajat tarpeeksi tietoisia sosiaalisen median tietoturvasta ja miten he suhtautuvat siihen.

4.2 Kohderyhmä ja vastaajien jakauma

Kohderyhmänä oli 1195 Centria ammattikorkeakoulun (Kokkola-Pietarsaaren yksikön, Talonpojankadun toimipisteen) tekniikan- ja liiketalouden opiskelijaa ja henkilökunnan jäsentä. Näistä 575 oli liiketalouden koulutusohjelmasta, 560 tekniikan opiskelijaa ja 60 henkilökunnan jäsentä. Vastauksia kyselyyn saatiin 104 kappaletta, joista naisia kyselyyn vastasi 64 kappaletta ja miehiä kyselyyn vastasi 40. Kohderyhmä jakautui kuvion 1 osoittamalla tavalla. Taulukossa 1 nähdään vastaajien prosentuaaliset jakaumat. Kuviot ja kaaviot on tehty SPSS -ohjelman ja Excelin avulla.



KUVIO 1. Vastaajien taustatiedot

TAULUKKO 1. Prosentuaaliset jakaumat

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Nainen	49 kpl	5 kpl	10 kpl	64 kpl
	80,3 %	20,8 %	52,6 %	61,5 %
Mies	12 kpl	19 kpl	9 kpl	40 kpl
	19,7 %	79,2 %	47,4 %	38,5 %
Yhteensä	61 kpl	24 kpl	19 kpl	104 kpl
	100 %	100 %	100 %	100 %

Olen oikein tyytyväinen vastausprosentteihin, sekä kaikkiin palautteisiin, joita olen saanut opinnäytetyöni edetessä.

4.3 Aineiston kerääminen ja käsittely

Kysymykset olen ottanut Nuotion (2012) tekemästä tutkimuksesta, jossa hän teki tutkimuksen Haaga-Helian ammattikorkeakoululle. Muutamaa poikkeusta lukuun ottamatta kysymyksiin oli annettu monivalintakysymyksen asteikkoon perustuvat vastausvaihtoehdot. 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. Kysymysten teoriaosuudet olen tarkistanut eri asiantuntijalähteistä.

Tietoisuutta on vaikeampi kysyä, joten kysymyksiin käytettiin esimerkkejä yleisimmistä sosiaalisen median tietoturvaan liittyvistä asioista. Esimerkeillä oli tarkoitus täsmentää kysymystä niin, että vastaaja ymmärtää kysymyksen idean vastaajaa johdattelematta. Esimerkkeihin on käytetty teoriaosuutta, ja kysymysten

tarkoitus oli saada vastauksia sosiaalisen median tietoruvariskeihin ja siihen, ovatko Centria ammattikorkeakoulun opiskelijat ja henkilökunta niistä 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 mm. 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 vastaajien tietoisuutta erilaisista sosiaaliseen mediaan liittyvistä riskeistä, jotka koskevat käyttäjien yksityisyyttä ja tietoja. Kysymyksissä oli tarkoitus antaa ensin esimerkki asiasta ja kysyä sen jälkeen, kuinka tietoinen vastaaja oli juuri kyseisestä asiasta. Kysymyksissä kysyttiin sosiaalisen median käyttöehdoista, kolmansien osapuolten sovellusten tietojenkeruusta, yksityisyyspolitiikasta, sosiaalisen median palveluiden sijainnista ja siitä miten ne vaikuttavat käyttäjään. Lisäksi tiedusteltiin, olivatko vastaajat huolissaan jaetun materiaalin pysymisestä ja myöhemmin sen mahdollisesta löytymisestä Internetistä ja identiteettivarkauden uhriksi joutumisesta. Monet edellä mainituista ovat sellaisia, jotka koskevat useita sosiaalisen median palveluita. Kaikki kysymykset olivat pakollisia, ja kysymysten tyyppi oli monivalinta. Koska halusin saada kysymyksiin vaihtelua, vastausvaihtoehtoja oli useampia.

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.

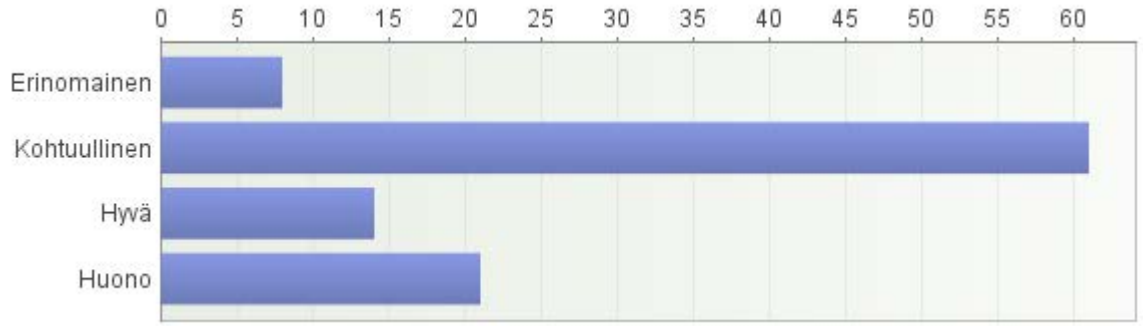
Kyselyn toteutin Webropol -ohjelmalla 18.12.2012–18.1.2013. Vastauksia tutkin SPSS-ohjelman avulla, jonka avulla myös tein prosenttilaskelmat ja tämän jälkeen siirsin tulokset Exceliin, jolla tein taulukot opinnäytetyötäni varten valmiiksi.

5 TULOKSET JA NIIDEN TARKASTELU

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

5.1 Käsitys tietoturvasta sosiaalisessa mediassa

Ensimmäisiin tutkimuskysymyksiin annetuista vastauksista paljastuu se, että vastanneiden käsitys sosiaalisen median tietoturvasta on kohtuullinen 58,7 %. Huono käsitys sosiaalisen median tietoturvasta oli kaikkiaan 20,2 %:lla vastaajista (KUVIO 2).



KUVIO 2. Käsitys sosiaalisen median tietoturvasta

Jos käsityksiä sosiaalisen median tietoturvasta tarkastellaan linjoittain, havaitaan eroja saatujen vastausten perusteella (TAULUKKO 2). Liiketalouden opiskelijoista 62,3 % on sitä mieltä, että heillä on kohtuullinen käsitys tietoturvasta sosiaalisessa mediassa. Erinomainen käsitys tietoturvasta sosiaalisessa mediassa oli liiketalou-

den opiskelijoilla 6,6 %, tekniikassa 8,3 % ja henkilökunnalla 10,5 %. (TAULUKKO 2).

TAULUKKO 2. Käsitys sosiaalisen median tietoturvasta

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Erinomainen	4 kpl 6,6 %	2 kpl 8,3 %	2 kpl 10,5 %	8 kpl 7,7 %
Kohtuullinen	38 kpl 62,3 %	13 kpl 54,2 %	10 kpl 52,6 %	61 kpl 58,7 %
Hyvä	7 kpl 11,5 %	4 kpl 16,7 %	3 kpl 15,8 %	14 kpl 13,5 %
Huono	12 kpl 19,7 %	5 kpl 20,8 %	4 kpl 21,1 %	21 kpl 20,2 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 %

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 kysymyksen kuuluivat työnkuvaan tai vastaaja opiskeli alaa. Muutama vastaaja ilmoitti, että tiedot tulivat lähinnä kavereilta tai uutisista. Jotkut vastaajista totesivat myös, että he ovat tietoisia riskeistä ja siten yrittävät välttää niitä (LIITE 2).

Kysymykseen 5 vastattiin vapaamuotoisesti esimerkiksi seuraavasti:
”Olen työskennellyt IT ympäristössä, joten mielestäni minulla on kohtuulliset tiedot tietoturvatekniikoista IT-ympäristössä ja esim. mitä tekniikoita kyseiset sosiaalisen mediapalveluiden tuottajat saattavat käyttää.”
”Olen kyllä kuullut paljonkin riskeistä. Henkilökohtaisesti minulle ei ole koskaan sattunut mitään tietoturvaani loukkaavaa eikä kellekään omassa ystäväpiirissäni. Varmasti käsitykseni johtuu siitä.”
”Sosiaalisen median tietoturva on mielestäni melko hyvä. Suurimmat ongelmata-

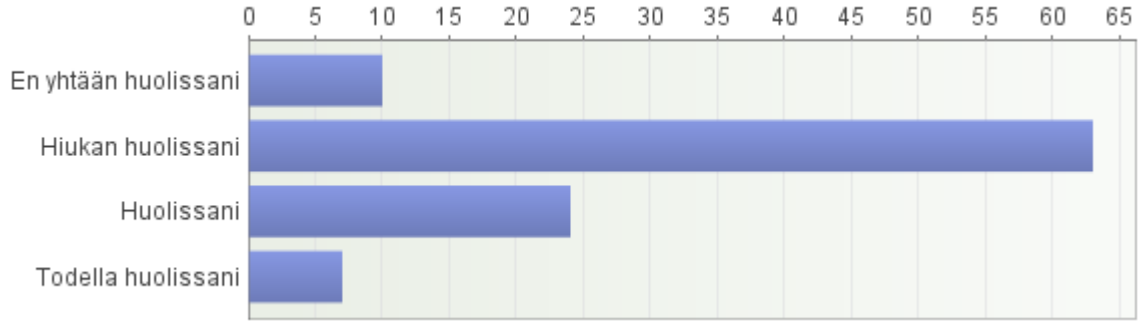
paukset ilmenevät käyttäjän tekemien virheiden vuoksi."
"Taustaani kuuluu syvempi ymmärrys ohjelmoinnista ja Internetistä."
"Hakkerit yms. ovat jatkuvasti netissä, joten taattu turvallisuus ei ole, mutta nykypäivänä ns. vaarat vähenevät kun tekniikka kehittyy."

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 tietojen kalastelu, virukset sekä hakkerit, jotka yrittävät hankkia yksityistä tietoa (LIITE 2).

Kysymykseen 6 vastattiin vapaamuotoisesti esimerkiksi seuraavasti:
"Väärille ihmisille menee tietoa asioista, joita ei haluaisi heille menevän."
"Viruksia voi tulla kaiken maailman mainosten kautta, joita esim. Facebookin sivupalkeissa pyörii."
"Tietovuotoja hakkereiden toimesta."
"Käyttäjätietojen joutumisen vääriin käsiin."
"Tiedon leviäminen vääriin käsiin tai useammalle kuin oli tarkoitettu. Yksityisyyden menetys. Facebookin ym. Uudistukset, joihin ei voi itse vaikuttaa ja jotka hyödyntävät aiempaa itsestä lisättyä materiaalia. Muut voivat kopioida kuviani koneellensa."
"Ei sinne kannata mitään kovin henkilökohtaista kirjoittaa tai kuvata. Verkosta on mahdoton poistaa mitään, jos sinne joskus jotain tallentaa."

Valtaosa vastaajista 60,6 % oli hiukan huolissaan sosiaalisen median tietoturvasta. Vain 9,6 % ei ollut yhtään huolissaan ja 6,7 % vastaajista oli todella huolissaan so-

siaalisen median tietoturvasta. Huolissaan sosiaalisen median tietoturvasta oli 23,1 % vastaajista (KUVIO 3).



KUVIO 3. Huoli sosiaalisesta mediasta

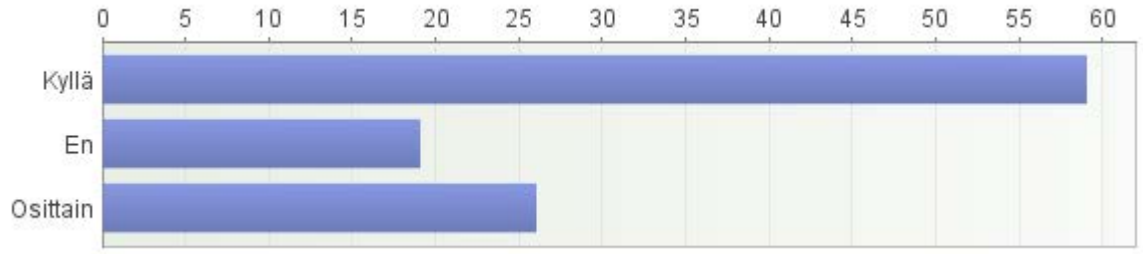
Kun tarkastellaan vastauksia koulutusohjelmittain, voidaan huomata, että enemmistö vastaajista oli hiukan huolissaan sosiaalisen median tietoturvasta, liiketaloudessa 63,9 %, tekniikan opiskelijoista tasan 50 % ja henkilökunta meni melkein samoihin lukemiin liiketalouden kanssa, heidän vastausprosenttinsa oli 63,2 %. Vähiten oltiin todella huolissaan yhteensä 6,7 % verran, kun kaikki vastanneet lasketaan yhteen.

TAULUKKO 3. Huoli sosiaalisesta mediasta

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
En huolissani	4 kpl 6,6 %	6 kpl 25 %	0 kpl 0 %	10 kpl 9,6 %
Hiukan huolissani	39 kpl 63,9 %	12 kpl 50 %	12 kpl 63,2 %	63 kpl 60,6 %
Huolissani	14 kpl 23 %	4 kpl 16,7 %	6 kpl 31,6 %	24 kpl 23,1 %
Todella huolissani	4 kpl 6,6 %	2 kpl 8,3 %	1 kpl 5,3 %	7 kpl 6,7 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 %

5.2 Tietoisuus sosiaalisen median tietoturvariskeistä

Toisen tutkimuskysymyksen sarjassa kysyttiin vastaajien tietoisuuteen sosiaalisen median tietoturvariskeistä. Tähän käytettiin kysymyksiä 8–13. Kysymyksessä 8 kysyttiin sitä, kuinka hyvin vastaajat tiesivät Facebookin käyttöehdoista löytyneestä ehdosta. Vastaajat olivat hyvin perillä kyseisestä ehdosta, sillä 56,7 % oli tietoinen kyseisestä ehdosta. Tosin 18,3 % vastaajista ei tiennyt mitään kerrotusta käyttöehdosta ja 25 % tiesi osittain kyseisestä käyttöehdosta (KUVIO 4).



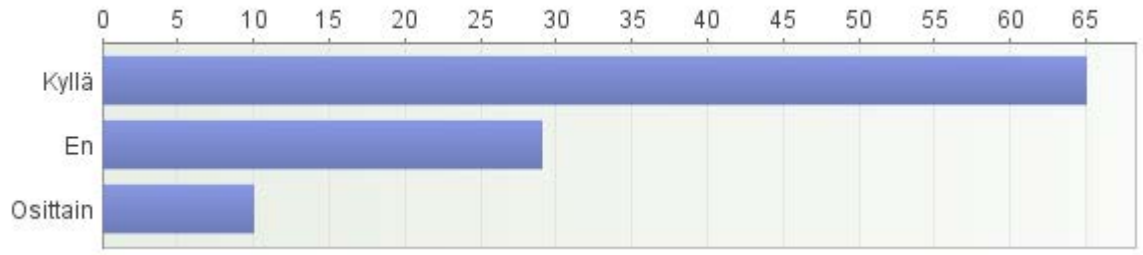
KUVIO 4. Tietoisuus Facebookin käyttöoikeuksista

Koulutusohjelmittain eroja löytyi jonkin verran. Vastanneista tekniikan opiskelijoista 75 % tiesi ehdosta, liiketalouden opiskelijoista 50,8 % ja henkilökunnasta 52,6 %. Osittain ehdosta tiesi 36,8 % henkilökunnasta, 16,7 % tekniikan opiskelijoista ja 24,6 % liiketalouden opiskelijoista (TAULUKKO 4).

TAULUKKO 4. Tietoisuus Facebookin käyttöoikeuksista

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	31 kpl 50,8 %	18 kpl 75 %	10 kpl 52,6 %	59 kpl 56,7 %
En	15 kpl 24,6 %	2 kpl 8,3 %	2 kpl 10,5 %	19 kpl 18,3 %
Osittain	15 kpl 24,6 %	4 kpl 16,7 %	7 kpl 36,8 %	26 kpl 25 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 %

Kysymyksessä 9 kysyttiin, tiesivätkö vastaajat Facebookin kolmansien osapuolien tekemien sovellusten tietojenkeruusta. 62,5 % vastaajista vastasi tietävänsä siitä (KUVIO 5).



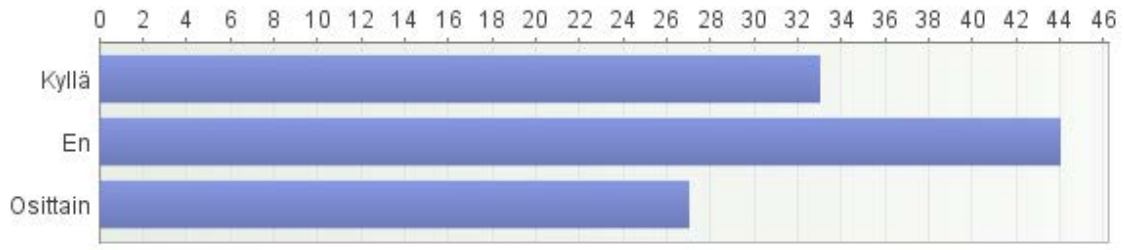
KUVIO 5. Tietoisuus henkilötietoihin pääsystä Facebookissa

Valtaosa kysymykseen vastanneista opiskelijoista koulutusohjelmasta riippumatta tiesi tietojenkeruusta vastaavasti henkilökunnasta vain vähän yli puolet (TAULUKKO 5).

TAULUKKO 5. Tietoisuus henkilötietoihin pääsystä Facebookissa

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	35 kpl	20 kpl	10 kpl	65 kpl
	57,4 %	83,3 %	52,6 %	62,5 %
En	17 kpl	4 kpl	8 kpl	29 kpl
	27,9 %	16,7 %	42,1 %	27,9 %
Osittain	9 kpl	0 kpl	1 kpl	10 kpl
	14,8 %	0 %	5,3 %	9,6 %
Yhteensä	61 kpl	24 kpl	19 kpl	104 kpl
	100 %	100 %	100 %	100 %

Kysymyksessä 10 kysyttiin Googlen yksityisyyspolitiikan ehtoja koskevasta ehdosta, jonka mukaan Google kerää tietoja myös käyttäjän tietokoneesta sekä ohjelmista, joita käyttäjä käyttää. 42,3 % vastaajista ilmoitti, ettei tiennyt kyseisistä ehdoista, 31,7 % vastaajista ilmoitti tietävänsä ja 26 % tiesi osittain asiasta. (KUVIO 6).



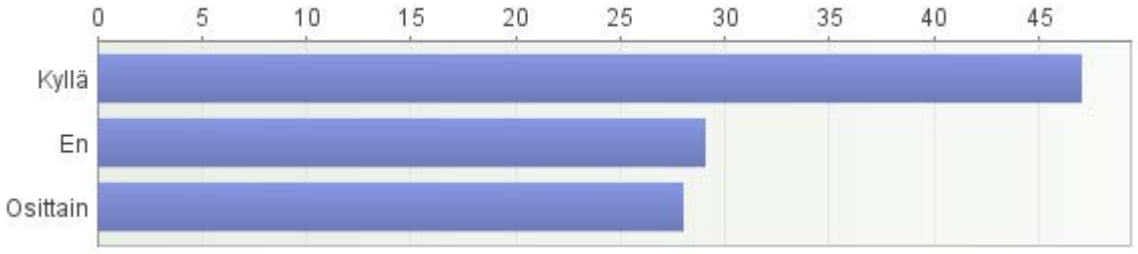
KUVIO 6. Googlen keräämät tiedot

Varmimmin asiasta ilmoitti tietävänsä tekniikan opiskelijat, joista 37,5 % ilmoitti tietävänsä ehdosta, kuitenkin 41,7 % ei tiennyt asiasta. Liiketaloudessa vastaavat tulokset olivat tietäville 27,9 % ja ei tietäneille 47,5 %. Vastaavasti henkilökunnasta asiasta tiesi 36,8 % ja ei tiennyt 42,3 % (TAULUKKO 6).

TAULUKKO 6. Googlen keräämät tiedot

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	17 kpl 27,9 %	9 kpl 37,5 %	7 kpl 36,8 %	33 kpl 31,7 %
En	29 kpl 47,5 %	10 kpl 41,7 %	5 kpl 26,3 %	44 kpl 42,3 %
Osittain	15 kpl 24,6 %	5 kpl 20,8 %	7 kpl 36,8 %	27 kpl 26 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 %

Kysymyksessä 11 kysyttiin sitä, kuinka tietoiset vastaajat olivat siitä, että palveluiden sijaitseminen ulkomailla tarkoittaa sitä, että mahdollisissa riitatilanteissa noudatetaan sen valtion lakeja, jossa palvelu sijaitsee. 45,2 % vastaajista vastasi olevansa tietoisia asiasta ja 27,9 % ilmoitti että eivät tienneet siitä (KUVIO 7).



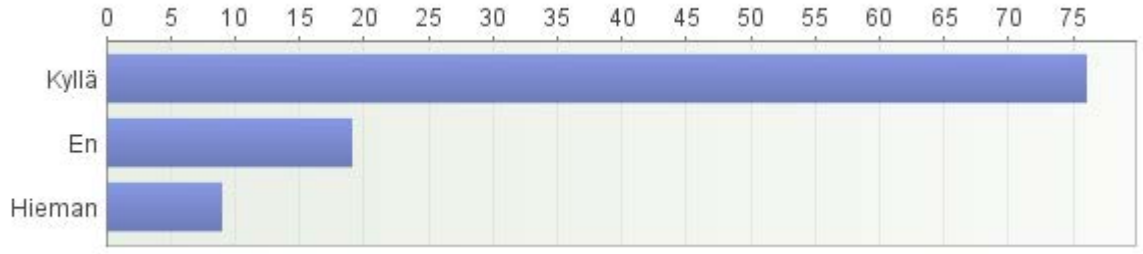
KUVIO 7. Tietoisuus lainsäädännöistä

Kun vertaillaan tuloksia keskenään, tekniikan opiskelijoista 54,2 % ilmoitti tietävänsä asiasta, liiketaloudesta 41 % ja henkilökunnasta 47,4 %. (TAULUKKO 7).

TAULUKKO 7. Tietoisuus lainsäädännöistä

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	25 kpl	13 kpl	9 kpl	47 kpl
	41 %	54,2 %	47,4 %	45,2 %
En	16 kpl	7 kpl	6 kpl	29 kpl
	26,2 %	29,2 %	31,6 %	27,9 %
Osittain	20 kpl	4 kpl	4 kpl	28 kpl
	32,8 %	16,7 %	21,1 %	26,9 %
Yhteensä	61 kpl	24 kpl	19 kpl	104 kpl
	100 %	100 %	100 %	100 %

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 73,1 % tuntui huolettavan se, että joskus heistä voisi löytyä jokin kuva/teksti/video joka antaa heistä epäedullisen kuvan sillä hetkellä. Vastaajista vain 8,7 % huoletti vain hieman sellaisen materiaalin löytyminen Internetistä joskus tulevaisuudessa (KUVIO 8).



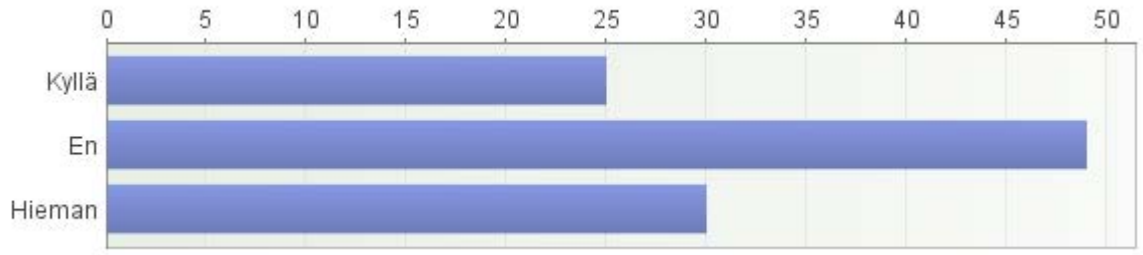
KUVIO 8. Huoli epäedullisesta aineistosta

Vastanneista tekniikan opiskelijoista asiasta ei ollut huolissaan 20,8 %, liiketalouden opiskelijoista 19,7 % ja henkilökunnasta 10,5 %. Eniten asiasta huolissaan olivat henkilökunnan jäsenet peräti 78,9 % vastanneista (TAULUKKO 8).

TAULUKKO 8. Huoli epäedullisesta aineistosta

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	46 kpl 75,4 %	15 kpl 62,5 %	15 kpl 78,9 %	76 kpl 73,1 %
En	12 kpl 19,7 %	5 kpl 20,8 %	2 kpl 10,5 %	19 kpl 18,3 %
Osittain	3 kpl 4,9 %	4 kpl 16,7 %	2 kpl 10,5 %	9 kpl 8,7 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 v

Kysymyksessä 13 kysyttiin, onko vastaaja huolissaan siitä, että voisi joutua identiteettivarkauden uhriksi. 47,1 % vastaajista ei ollut huolissaan, hieman ja kyllä vastaukset ovat lähempänä toisiaan (KUVIO 9).



KUVIO 9. Huoli identiteettivarkaudesta

Eniten huolissaan identiteettivarkauksista olivat henkilökunnan jäsenet. Vastaajista 36,8 % oli huolissaan mahdollisista identiteettivarkauksista, vastaavasti liiketalouden opiskelijoista 19,7 % oli huolissaan ja tekniikan opiskelijoista 25 %. Henkilökunnasta ei ollut huolissaan 36,8 %, tekniikan opiskelijoista 54,2 % ja liiketalouden opiskelijoista 47,5 %. (TAULUKKO 9).

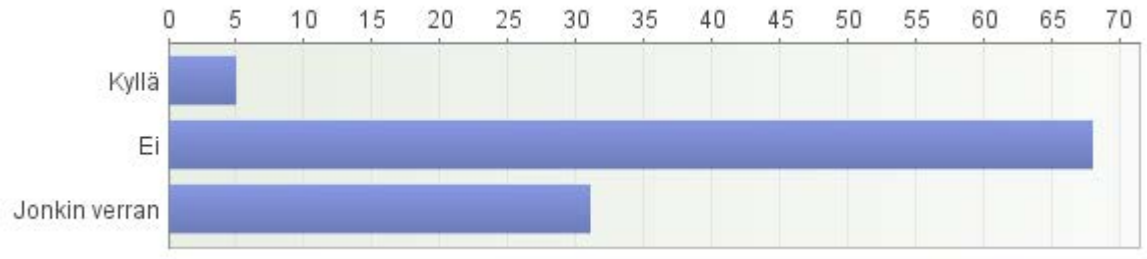
TAULUKKO 9. Huoli identiteettivarkaudesta

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	12 kpl	6 kpl	7 kpl	25 kpl
	19,7 %	25 %	36,8 %	24 %
En	29 kpl	13 kpl	7 kpl	49 kpl
	47,5 %	54,2 %	36,8 %	47,1 %
Hieman	20 kpl	5 kpl	5 kpl	30 kpl
	32,8 %	20,8 v	26,3 %	28,8 %
Yhteensä	61 kpl	24 kpl	19 kpl	104 kpl
	100 %	100 %	100 %	100 %

5.3 Suhtautuminen sosiaalisen median tietoturvaan kyselyn jälkeen

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

Kysymyksessä 14 kysyttiin, muuttuiko vastaajan käsitys sosiaalisen median tietoturvasta tämän kyselyn jälkeen. Monivalintakysymyksiin saatujen vastausten 65,4 % oli sitä mieltä että kysely ei vaikuttanut heidän suhtautumiseensa tietoturvaan sosiaalisessa mediassa (KUVIO 10).



KUVIO 10. Käsityksen muuttuminen

Vähiten kysely vaikutti tekniikan opiskelijoihin 83,3 %, liiketalouteen 60,7 % ja henkilökuntaan 57,9 % (TAULUKKO 10).

TAULUKKO 10. Käsitysten muuttuminen

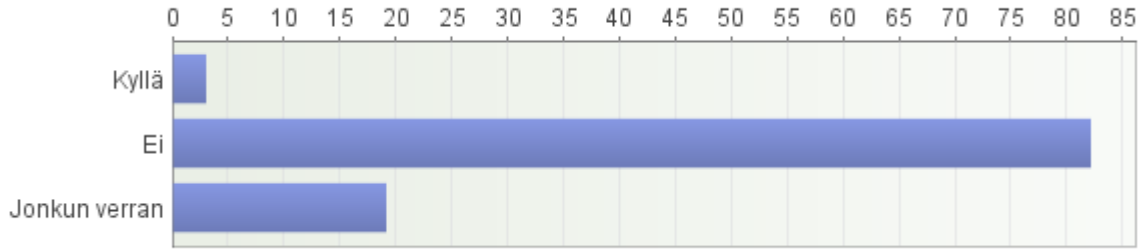
	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	3 kpl 4,9 %	1 kpl 4,2 %	1 kpl 5,3 %	5 kpl 4,8 %
Ei	37 kpl 60,7 %	20 kpl 83,3 %	11 kpl 57,9 %	68 kpl 65,4 %
Jonkin verran	21 kpl 34,4 %	3 kpl 12,5 %	7 kpl 36,8 %	31 kpl 29,8 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 %

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:

”Voisi tulevaisuudessa olla vähän tarkempi mitä Facebookissa itsestään kertoo.”
”olen ollut tietoinen riskeistä, mutta kaikkia asioista en ole tiennyt. Pitää olla edelleenkin varovainen, mitä julkaisee netissä.”
”Kiitos paljon hyvistä faktoista joita en ollut tiennyt.”
”Olen varovaisempi tästä lähtien.”
”Kyllähän tästä tietoturva-asiasta on paljon puhuttu aikaisemminkin ja ainakin omalla kohdalla voin sanoa, että en laita esim. Facebookkiin sellaista tietoa mitä en halua muiden saavan.”
”Heräsi ajattelemaan, että mitä jotkut asiat käytännössä ovat.”
”En ollut täysin tietoinen että tiedonkeruu on tosiaan noin laajaa.”
”Oma järki on käytettävissä mitä laittaa näille sivuille kuinka yksityiskohtaisesti.”

Kysymyksessä 16 kysyttiin, muuttuiko vastaajan suhtautuminen sosiaalisen median tietoturvasta tämän kyselyn jälkeen. Monivalintakysymyksiin saatujen vastausten perusteella tehdyllä kysymyksellä 78,8 % ei ollut vaikutusta sosiaalisen mediankäyttöön vastanneiden keskuudessa (KUVIO 11).



KUVIO 11. Suhtautuminen sosiaaliseen mediaan

Vastanneista tekniikan opiskelijoista 95,8 % oli sitä mieltä, että suhtautuminen sosiaalisen median tietoturvaan ei muuttunut kyselyn jälkeen, liiketaloudesta samaa mieltä oli 68,9 % ja henkilökunnasta 89,5 % (TAULUKKO 11).

TAULUKKO 11. Suhtautuminen sosiaaliseen mediaan

	Liiketalous	Tekniikka	Henkilökunta	Yhteensä
Kyllä	2 kpl 3,3 %	0 kpl 0 %	1 kpl 5,3 %	3 kpl 2,9 %
Ei	42 kpl 68,9 %	23 kpl 95,8 %	17 kpl 89,5 %	82 kpl 78,8 %
Jonkin verran	17 kpl 27,9 %	1 kpl 4,2 %	1 kpl 5,3 %	19 kpl 18,3 %
Yhteensä	61 kpl 100 %	24 kpl 100 %	19 kpl 100 %	104 kpl 100 %

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:

”En tiennyt kaikista käyttö ehdoista esim. Facebook ja Google, joten mietin nyt enemmän mitä sinne laitan itsestäni.”
”Olen varmasti hieman varovaisempi siinä mitä julkaisen esim. Facebookissa ja varoitan myös lapsiani tietoturvan vaaroista.”
”Olen aina ollut melko varovainen antamieni tietojen kanssa Facebookissa, mutta tämän kyselyn jälkeen uskon että olen vielä varovaisempi.”
”En anna kovin paljoa tietoa sosiaaliseen mediaan, enkä käytä niitä kovin paljoa. Alumiinifoliohattu tosin menee entistä syvemmälle päähän. Tietoturva ja tiedon turva ovat huolestuttavalla tolalla tämän päivän tietoyhteiskunnassa. Hyvä kysely tämä on!”

5.4 Vertaileva analyysi ammattikoreakoulujen välillä

Työssä tarkasteltiin kolmea eri kysymyskokonaisuutta, joista ensimmäinen koski Centria ammattikorkeakoulun opiskelijoiden ja henkilökunnan käsitystä tietoturvasta sosiaalisessa mediassa. Toinen kysymyskokonaisuus koski vastaajien tietoisuutta sosiaalisen median tietoturvariskeistä ja kolmas käsitystä siitä, muuttuiko vastanneiden suhtautumisensa kyselyn jälkeen sosiaalisen median tietoturvaan tai sosiaalisen median käyttämiseen.

Kysely lähetettiin 575:lle liiketalouden ja 560:lle tekniikan opiskelijalle. Lisäksi kysely lähetettiin henkilökunnalle, jota tekniikan ja liiketalouden yksikössä on 60. Yhteensä siis 1195 henkilölle. Kyselyyn vastasi yhteensä 104 henkilöä, joten vastausprosentiksi muodostui 8,7 %. Kysely toteutettiin 18.12.2012–18.1.2013. Liiketalouden opiskelijoista kyselyyn vastasi 61, tekniikan opiskelijoista 24 ja henkilökunnasta 19.

Koska lupasin neljännen luvun alussa vertailla tuloksia myös Haaga-Helian tulosten kanssa, teen sen tässä ohessa. Katariina Nuotio lähetti kyselyn 150:lle tietojenkäsittelyn opiskelijalle, 150:lle johdon assistenttityö ja journalismi opiskelijoille sekä 150:lle liiketalouden opiskelijoille. Yhteensä siis 450 opiskelijalle, joista kyselyyn vastasi 55. Haaga-Helian vastausprosenttinsa oli 12,2 %

Ensimmäiseen tutkimuskysymykseen, joka koski Centria ammattikorkeakoulun Kokkola-Pietarsaaren yksikön, Talonpojankadun kampuksen, tekniikan- ja liiketalouden opiskelijoiden ja henkilökunnan suhtautumista sosiaalisen median tietoturvaan, voisi kysymyksiin saatujen vastausten perusteella päätellä, että sosiaalisen median tietoturvaan suhtaudutaan kohtuullisesti, kun taas Haaga-Heliassa asiaan suhtaudutaan hieman varauksellisesti. Kyselyssä Centrian tekniikan opiskelijat ja Haaga-Heliassa tietojenkäsittelyä opiskelevat olivat parhaiten perillä tietoturvasta sosiaalisessa mediassa. Jokainen kyselyyn osallistuja suhtautui kuitenkin kypsästi ja suuria eroja vastaajien kesken ei ollut havaittavissa.

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. Tekniikan koulutusalan opiskelijat tuntuivat

olleen parhaiten perillä kyseisistä seikoista. Eroja Centrian ja Haaga-Helian välillä löytyi hieman. Eniten vaihtelevuutta oli kysymyksessä 10, jossa kysyttiin: *"Google ilmoittaa yksityisyyspolitiikassaan keräävänsä tietoja myös ohjelmista, joita käytät ja tietokoneestasi. Koska YouTube ja Bollerg (blogipalvelu) kuuluvat Googlelle niin nämä säännöt kuuluvat myös kyseisten palveluiden käyttäjille. Tiesitkö aikaisemmin kyseisestä tiedon keruusta?"* (TAULUKKO 12)

TAULUKKO 12. Google ja tiedon keruu

Kyllä	Centria	32 %
	Haaga-Helia	44 %
En	Centria	42 %
	Haaga-Helia	22 %

Centriassa asiasta ei tiennyt 42 % kun taas Haaga-Heliassa asiasta ei tiennyt 22 %. Asiasta tiesi Centriassa 32 % ja Haaga-Heliassa 44 %.

Vaihtelevuutta oli myös kysymyksessä 9, jossa kysyttiin: *"Jos asennat Facebookissa kolmansien osapuolien tekemiä sovelluksia, annat samalla sovelluksen tekijöille pääsyn omiin henkilötietoihisi. Oletko ollut tietoinen tästä?"* (TAULUKKO 13)

TAULUKKO 13. Facebookin henkilötiedot

Facebookin henkilötiedot

Kyllä	Centria	62,5 %
	Haaga-Helia	79 %
En	Centria	28 %
	Haaga-Helia	8 %
Osittain	Centria	9,5 %
	Haaga-Helia	14,5 %

Centriassa tietoisia oli 62,5 % kun taas Haaga-Heliassa 79 %. Asiasta ei tiennyt Centriassa 28 % ja Haaga-Heliassa 8 %. Osittain asiasta tiesi Centriassa 9,5 % ja Haaga-Heliassa 14,5 %.

Kolmanteen tutkimuskysymykseen saatujen vastausten perusteella vastaajien suhtautuminen ei muuttunut siitä johtuen, että vastaajilta kysyttiin näkemystä sosiaalisen median tietoturvasta tai sen käytöstä. Suuria 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. Tässä olimme melko lailla samoissa lukemissa Centrian ja Haaga-Helian tuloksien kanssa.

Koska vastaajajoukko oli pieni molemmissa kouluissa, tuloksiin on suhtauduttava varauksella eikä niistä pidä vetää laajempia johtopäätöksiä. Vastaajajoukosta oli kuitenkin huomattavissa, että yleisesti ottaen niin Centriassa tekniikan opiskelijat, kuin Haaga-Heliassa tietojenkäsittelyn opiskelijat, olivat paremmin perillä kysytyistä asioista ja, että he arvioivat omat tietonsa sosiaalisen median tietoturvasta keskimäärin paremmiksi kuin muut tähän kyselyyn vastanneista.

Ne opiskelijat, jotka vastasivat esitettyihin kysymyksiin, vastasivat erittäin hyvin ja perusteellisesti jopa vapaaehtoisiin kysymyksiin Tämä parantaa tulosten luotettavuutta, koska kysymykset olivat joko avoimia tai monivalintakysymyksiä. Vaikka kyselyyn vastaajien määrä on suhteellinen, saadut vastaukset osoittavat, että vastaajien käsityksissä sosiaalisen median tietoturvasta on hajontaa.

6 POHDINTA JA JOHTOPÄÄTÖKSET

Mielestäni opinnäytetyöni aihe, tietoturva sosiaalisessa mediassa, oli erittäin ajankohtainen. Kun rupesin työstämään aihetta, tuli melkein jokaisesta mediasta lisätietoa työhöni. Kun vertailin Kokkolan ja Helsingin tuloksia myös keskenään, huomasin että olisi tarpeen saada kouluille lisää kursseja tietoturvasta ja sosiaalisesta mediasta. Pääsääntöisesti vastauksemme osuivat yhteen. Työni tavoitteena oli oppia itse lisää, mutta myös antaa opiskelutovereille ja henkilökunnalle lisätietoa sosiaalisen median tietoturvasta. Tavoitteeni toteutui suunnitelmieni mukaan.

Saaduista tuloksista voidaan päätellä, että vastaajat suhtautuivat hieman varauksella sosiaalisen median tietoturvaan yleensä, mutta pitivät omaa tietämystänsä siitä suhteellisen hyvänä. Vastaajat tuntuivat kuitenkin olevan yleisesti ottaen kohtuullisen hyvin perillä myös erilaisista sosiaalisen median tietoturvan alueista. Pelkästään se, että tietää sosiaalisen median tietoturvasta, vaikuttaa suhtautumiseen sosiaaliseen mediaan ja sen käyttämiseen siten, että jatkossa vastaaja ehkä miettii tarkemmin, mitä asioita hän laittaa sosiaalisen median palveluihin. Kyselystä tuli myös kiitosta avoimissa kysymyksissä, ja olen iloinen sekä otettu kyseisistä palautteista.

Kyselyyn saatujen vastausten perusteella voi päätellä, että sosiaalisen median tietoturvaan pitäisi kiinnittää enemmän huomiota, kun sitä käyttää. Koko ajan tulee uusia muutoksia ja lisätietoa aiheesta. Sosiaalinen media sekä tietoturva kehittyvät päivä päivältä paremmiksi. Muista kuin tietojen julkisuuteen liittyvistä erilaisista tietoturvariskeistä ei myöskään tiedetä kovin hyvin. Osa opiskelijoista kertoi minulle suoraan, että ovat erittäin kiinnostuneita tästä aiheesta ja haluaisivat oppia siitä enemmän. Tätä ei kuitenkaan näy näissä tuloksissa, sillä ne ovat nimettömiä

ja osa tuli minulle suullisesti kertomaan tämän asian. Voidaan kuitenkin päätellä, että sosiaalisen median tietoturvaan, kuten muuhunkin tietoturvaan, liittyviä kysymyksiä ja riskejä olisi hyvä tuoda esille aina, kun puhutaan tietotekniikasta ja sen käyttämisestä.

Opinnäytetyöni tarkoitus oli selvittää Centria ammattikorkeakoulun, opiskelijoiden ja henkilökunnan käsitystä tietoturvasta sosiaalisessa mediassa sekä heidän suhtautumistaan siihen. Tutkimuksessa keskityin yksityisyyteen liittyviin uhkiin ja käyttäjien tietoisuuteen niistä. Tarkoituksenani oli myös selvittää eroja Haaga-Helian ja Centrian tutkimuksen välillä.

Mielestäni saavutin tavoitteeni. Keskeisten tulosten perusteella tietoturvasta sosiaalisessa mediassa tiedettiin yllättävän hyvin, mutta useampi halusi myös lisätietoa ja oli huolissaan siitä, että ei tiedä ihan kaikkea mitä sosiaalisen median tietoturva pitää sisällään. Uutisia seurataan, mutta kaikkia ohjesääntöjä ei jakseta lukea.

Rajoitteeksi minulle tuli Centrian ja Haaga-Helian tuloksia verratessa se, että opintoalat olivat erit. Centriassa lähetin kyselyn tekniikan ja liiketalouden opiskelijoille sekä henkilökunnalle, kun taas Haaga-Heliassa kysely oli eritelty liiketalouden, tietojenkäsittelyn sekä johdon assistenttityö ja journalismi opiskelijoille. Yleisesti ottaen kuitenkin Centrian tekniikan opiskelijat vastasivat samalla tavoin kuin Haaga-Helian tietojenkäsittelyn linja. Ilmeisesti opiskelijat ovat opintojensa ohessa joutuneet perehtymään asioihin tietoteknisistä syistä enemmän.

Mielestäni tuloksia voidaan hyödyntää ja soveltaa opetusta suunniteltaessa. Lisäksi jatkotutkimuksen voisi tehdä sosiaalisen median tietoturvasta yritysmaailmassa tai siitä miten sosiaalista mediaa voi hyödyntää liiketoiminnassaan, kun tietoturva on selvillä. Jäänkin mielenkiinnolla odottamaan, josko joku koulumme opiskelijoista tekisi seuraavan opinnäytetyön tästä aiheesta, sillä aihe on aika pinnalla tällä hetkellä, ja uusia sosiaalisen median palveluita syntyy tai vanhat päivittyy. Toivon myös että jatkossa sosiaalisen median ja tietoturvan opetustarjonta säilyy koulussamme, ja tarpeen tullen kasvaa. Tieto tuo turvaa ja halu oppia kasvaa.

Haluaisin lopuksi kiittää kaikkia kyselyyn osallistuneita henkilökunnan jäseniä ja opiskelijoita. Ilman teitä tämä työ ei olisi onnistunut. Haluan myös kiittää alkuperäisen kyselyn kehittäjää Katariina Nuotiota, jonka opinnäytetyöstä sain paljon lisää tietoa, jota en edes itse ollut tullut ajatelleeksi. Sain hänen työstään myös kysymykset, joiden avulla oman opinnäytetyöni tekeminen onnistui. Tästä on hyvä jatkaa matkaa eteenpäin, ja syvällisemmin sosiaaliseen mediaan tutustuen.

LÄHTEET

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

Alan.fi, 2013, Sosiaalinen media yrityksen markkinoinnissa. Www-dokumentti. Saatavissa: http://alan.fi/mita-on-sosiaalinen-media/. Luettu 14.3.2013.

Carlson, N. 2010. At Last – The Full Story of How Facebook was founded. Www-dokumentti. Saatavissa: http://www.businessinsider.com/how-facebook-was-founded-2010-3. Luettu 19.3.2013.

Cert.fi 2011. Tietoturva nyt! Omien tietojen jakaminen Facebookissa. Www-dokumentti. Saatavissa: http://www.cert.fi/tietoturvanyt/2011/01/ttn201101211318.html. Luettu 20.3.2013.

Cert.fi 2013a. Tietoturva nyt! Suomalaisia automaatiojärjestelmiä suojaamattomana verkossa. Www-dokumentti. Saatavissa: https://www.cert.fi/tietoturvanyt/2013/03/ttn201303211339.html. Luettu 28.3.2013.

Cert.fi 2013b. Tietoturva nyt! Spamhaus-palvelunestohyökkäyksessä käytetään hyväksi nimipalvelimia. Www-dokumentti. Saatavissa: https://www.cert.fi/tietoturvanyt/2013/03/ttn201303251530.html. Luettu 28.3.2013.

Cert.fi 2013. Tietoturva nyt! Twitterin tunnuksia kalastellaan verkossa. Www-dokumentti. Saatavissa: http://www.cert.fi/tietoturvanyt/2013/02/ttn201302071414.html. Luettu 20.3.2013.

Douglas, N. 2006. MySpace: The Business of Spam 2.0 (Exhaustive Edition). Www-dokumentti. Saatavissa: http://gawker.com/199924/myspace-the-business-of-spam-20-exhaustive-edition?tag=valleywagtechmyspace. Luettu 19.3.2013.

Erkkola, J-P, 2008, Sosiaalisen median käsitteistä. Pdf-dokumentti. Saatavissa: http://mlab.taik.fi/pdf/ma_final_thesis/2008_erkkola_jussi-pekka.pdf. Luettu 14.3.2013.

Finlex.fi 13.8.2004/759. Laki yksityisyyden suojasta työelämässä. 2 luku 4 §. Www-dokumentti. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L2P4. Luettu 20.3.2013.

Google 2013a. Yritys. Www-dokumentti. Saatavissa: http://www.google.com/intl/fi_fi/about/company/. Luettu 19.3.2013.

Google 2013b. Historiaa. Www-dokumentti. Saatavissa: http://www.google.com/intl/fi_fi/about/company/history/. Luettu 19.3.2013.

Google Official Blog 2012. Google's new Privacy Policy. Www-dokumentti. Saatavissa: http://googleblog.blogspot.fi/2012/02/googles-new-privacypolicy.html#!/2012/02/googles-new-privacy-policy.html. Luettu 19.3.2013.

Hachman, M. 2012. Facebook Now Totals 901 Million Users, Profits Slip. PCMag. Www-dokumentti. Saatavissa: http://www.pcmag.com/article2/0,2817,2403410,00.asp. Luettu 19.3.2013.

Heijaste, J-M. Tietoturvan perusteet. Www-dokumentti. Saatavissa: http://www.cibernarium.tamk.fi/tietoturva1/maaritelma_index.htm#. Luettu 19.3.2013.

Heikkilä, J. 2012, VTT, Teknologista liiketoimintaa. Www-dokumentti. Saatavissa: http://www.vtt.fi/sites/openrisk/index.jsp. Luettu 14.3.2013.

Hintikka, K. A. 2007. Web 2.0 – johdatus internetin uusiin liiketoimintamahdollisuuksiin. Pdf-dokumentti. Saatavissa: http://www.tieke.fi/mp/db/file_library/x/IMG/20815/file/julkaisu_28.pdf. Luettu 14.3.2013

Hopkins, J. 2006. Surprise! There's a third YouTube co-founder. USA Today. Www-dokumentti. Saatavissa: http://usatoday30.usatoday.com/tech/news/2006-10-11-youtube-karim_x.htm. Luettu 19.3.2013.

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

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

Kotilainen, S. 2011. Ikävä Facebook-viesti – Volvo antoi potkut kolmelle. Tietokone. Www-dokumentti. Saatavissa: http://www.digitoday.fi/tietoturva/2010/08/06/f-secure-antaa-7-neuvoa-facebook-turvallisuuteen/201010862/66. Luettu 20.3.2013.

La Monica, P. R. 2006. Google to buy YouTube for $1.65 billion. CNNMoney. Www-dokumentti. Saatavissa: http://money.cnn.com/2006/10/09/technology/googleyoutube_deal/index.htm?cnn=yes. Luettu 19.3.2013.

Linnake, T. 2010. Murtovarkaat iskivät Facebookin avulla. IT-viikko. Www-dokumentti. Saatavissa: http://www.itviikko.fi/uutiset/2010/09/14/murtovarkaat-iskivat-facebookin-avulla/201012699/7. Luettu 20.3.2013.

Miller, C. C. 2010. Why Twitter's C.E.O. Demoted Himself. The New York Times. Www-dokumentti. Saatavissa: http://www.nytimes.com/2010/10/31/technology/31ev.html?pagewanted=1&_r=2. Luettu 19.3.2013.

Myspace. 2012. Tietoa meistä. Www-dokumentti. Saatavissa: http://www.myspace.com/Help/AboutUs?pm_cmp=ed_footer. Luettu 19.3.2013.

Nettipoliisi. 2013. Nettirikosten pohdintaa. Virtuaalinen lähipoliisiryhmä. Pdf-dokumentti. Saatavissa: http://www.poliisi.fi/poliisi/helsinki/home.nsf/files/Nettirikosten%20pohdintaa/$file/Nettirikosten%20pohdintaa.pdf. Luettu 20.3.2013.

Nuotio, K., 2012. HAAGA-HELIA ammattikorkeakoulun opiskelijoiden käsitys sosiaalisen median tietoturvasta ja sen riskeistä. Www-dokumentti. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/45492/Nuotio_Katariina.pdf?sequence=1. Luettu 14.3.2013.

O'Reilly, T. 2005, What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software. Www-dokumentti. Saatavissa: http://oreilly.com/web2/archive/what-is-web-20.html. Luettu 14.3.2013.

Owyang, J. 2008. Social Network Stats: Facebook, MySpace, Reunion. Www-dokumentti. Saatavissa: http://www.web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/. Luettu 19.3.2013.

Sagolla, D. 2009. How Twitter Was Born. Www-dokumentti. Saatavissa: http://www.140characters.com/2009/01/30/how-twitter-was-born/. Luettu 19.3.2013.

Sanastokeskus TSK 2010a. Www-dokumentti. Saatavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&height=165&qfind=web+2.0. Luettu 14.3.2013.

Sanastokeskus TSK 2010b. Www-dokumentti. Saatavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&qfind=verkkoyhteis%C3%B6palvelu. Luettu 19.3.2013.

Sanastokeskus TSK 2012c. Www-dokumentti. Saatavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&qfind=verkkopalvelu. Luettu 19.3.2013.

Sanastokeskus TSK 40, 2010a. Www-dokumentti. Saatavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&qfind=sis%C3%A4ll%C3%B6njakopalvelu. Luettu 19.3.2013.

Sanastokeskus TSK40, 2010b. Www-dokumentti. Saatavissa: http://www.tsk.fi/tiedostot/pdf/Sosiaalisen_median_sanasto. Luettu 27.3.2013.

Sanastokeskus TSK 40, 2010c. Www-dokumentti. Saatavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&qfind=Twitter. Luettu 19.3.2013.

Stranius, L. 2012. Tietoturva sosiaalisessa mediassa. Www-dokumentti. Saatavissa: http://leostranius.fi/2012/01/tietoturva-sosiaalisessa-mediassa/. Luettu 14.3.2013.

Tietoturvaopas.fi 2008. Www-dokumentti. Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haitoiltasuojautuminen.html. Luettu 20.3.2013.

Tietoturvaopas.fi 2008. Www-dokumentti. Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html. Luettu 20.3.2013.

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

Valtiovarainministeriö 2010. VAHTI 4/2010. Sosiaalisen median tietoturvaohje. Pdf-dokumentti. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf. Luettu 19.3.2013.

Viestintätoimisto Tulus Oy. 2013. Sosiaalinen media - Uhka vai mahdollisuus. Euroopan unioni, Euroopan sosiaalirahasto, VASKE, Vipuvoimaa EU:lta. Pdf-dokumentti. Saatavissa: http://193.208.197.11/osaamisellakasvuun/some-opas.pdf . Luettu 20.3.2013.

Wikipedia.org, 2010, Social media. Www-dokumentti. Saatavissa: http://en.wikipedia.org/wiki/Social_media. Luettu 14.3.2013.

YouTube. 2013a. Tietoja YouTubesta. Www-dokumentti. Saatavissa: http://www.youtube.com/t/about_youtube. Luettu 19.3.2013.

YouTube. 2013b. Tilastot. Www-dokumentti. Saatavissa: http://www.youtube.com/yt/press/statistics.html. Luettu 19.3.2013.

LIITE 1

Tietoturva sosiaalisessa mediassa

Olen Petra Komulainen Kokkolasta ja opiskelen Centria ammattikorkeakoulussa aikuispuolella liiketaloutta. Teen opinnäytetyötäni aiheesta tietoturva sosiaalisessa mediassa, vertailen saatuja tuloksia Haaga-Helian vastaavan tutkimuksen kanssa.

Tämän kyselyn tarkoitus on selvittää Centria ammattikorkeakoulun oppilaiden ja henkilökunnan tietoisuutta sosiaalisen median tietoturvasta ja suhtautumista siihen. Kyselyn painopiste on käyttäjän yksityisyyttä uhkaavissa tietoturvauhissa. Kysely toteutetaan Kokkolan tekniikan ja liiketalouden yksikössä. Tähdellä merkittyihin kysymyksiin on pakko vastata.

1. Taustatiedot: *

☐ Nainen ☐ Mies

2. Mikä on koulutusohjelmasi vai kuulutko henkilökuntaan? *

☐ Liiketalous ☐ Tekniikka ☐ Henkilökunta

3. Käytätkö sosiaalista mediaa? Sosiaaliseksi mediaksi lasketaan tässä sellaiset palvelut kuin Facebook, Twitter, YouTube, Google+, blogit, MySpace ja muut vastaavanlaiset palvelut. *

☐ Kyllä ☐ En

4. Minkälainen käsitys sinulla on sosiaalisen median tietoturvasta? *

- ● Erinomainen
- ● Kohtuullinen
- ● Hyvä
- ● Huono

5. Perustele vastauksesi. Voit perustella edellisen kysymyksen vastauksen tähän:

LIITE 1

6. Minkälaisia tietoturvauhkia koet sosiaalisessa mediassa olevan? Voit perustella vastauksesi tähän: *

7. Kuinka huolissasi olet sosiaalisen median tietoturvasta? *

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

8. Facebookin käyttöoikeuksissa sanotaan, että niin kauan kuin materiaali on Facebookissa, Facebook omistaa materiaalin 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 Bollerg (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

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

- Kyllä
- Ei
- Jonkin verran

15. Jos muuttui niin miten? Voit perustella edellisen kysymyksen vastauksen tähän:

LIITE 1

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

- Kyllä
- Ei
- Jonkun verran

17. Jos muuttui niin miten? Voit perustella edellisen kysymyksen vastauksen tähän:

Lähetä

5. Perustele vastauksesi. Voit perustella edellisen kysymyksen vastauksen tähän:

Vastaajien määrä: 64

- Aina oppii lisää.
- Käytän ainoastaan Facebookia. Pyrin pitämään aina suoja-asetukset korkeimmalla tasolla.
- En pidä sosiaalista mediaa saati koko nettiä hirveän turvallisena, netti maailmassa liikkuu paljon hakkereita yms. muita vastaavia, aina jotain kautta pystyy murtautuu tietojärjestelmiin.
- Turvallisuus aste voi olla hyväkin, mutta yleensä sen eteen pitää tehdä töitä, itse selailla ja muuttaa asetuksia. Kuten esim. Facebookin yksityisyysasetukset, jotka olen monen mutkan kautta vasta saanut sellaisiksi kuin itse halua ja tuntu turvalliselta.
- Olen käynyt mm. Facebookin/YouTuben turvallisuus asetukset siten että tiedän mitä muuta näkevät minusta eteenpäin.
- Hakkerit yms. ovat jatkuvasti netissä, joten taattu turvallisuus ei ole, mutta nykypäivänä ns. vaarat vähenevät kun tekniikka kehittyy.
- No huonohan se on.
- Mikäli käyttäjä osaa käyttää sosiaalisen median kanavaa ja esim. laittaa asetuksensa kuntoon, on käyttö turvallista. Jos ei, tietoturva voi vaarantua. Lisäksi salasanaa olisi hyvä vaihtaa joitain kertoja vuodessa.
- Ei ainakaan vielä ole tapahtunut mitään "erikoista".
- Mediasta kuulee koko ajan uusia tietoturvaongelmia koskien sosiaalisen median tietoturvaongelmia.
- Ei missään voida luvata 100 % mihin omat tiedot menevät, loppupeleissä on aina itse vastuussa siitä mitä nettiin laittaa itsestään.
- Olen työskennellyt IT ympäristössä, joten mielestäni minulla on kohtuulliset tiedot tietoturvatekniikoista IT-ympäristössä ja esim. mitä tekniikoita kyseiset sosiaalisen mediapalveluiden tuottajat saattavat käyttää
- Tiedot ovat ostettavissa.
- En käytä lainkaan ylläolevia.?
- En uskalla.
- Olen kyllä kuullut paljonkin riskeistä. Henkilökohtaisesti minulle ei ole koskaan sattunut mitään tietoturvaani loukkaavaa eikä kellekään omassa ystäväpiirissäni. Varmasti käsitykseni johtuu siitä.
- Sosiaalisen median tietoturva on mielestäni melko hyvä. Suurimmat ongelma tapaukset ilmenevät käyttäjän tekemien virheiden vuoksi.
- Tiedän missä määrin kannattaa omia tietoja ja kasvokuvia laittaa eteenpäin, sillä loppupeleissä niistä on itse vastuussa. Ymmärrän myös lukea vieraiden sivujen pikkuprintillä kirjoitettuja ehtoja. Nämä ovat monesti estäneet menemästä epäilyttäville sivuille
- Epäilyttävät asiat tulee huomattua aika hyvin, sosiaalisessa mediassa.
- Osaan käyttää konetta ja minulla on tietoturva kunnossa. Osaan säätää eri sivustojen tietoturva-asetukset kohdilleen.
- Mielestäni ei kannata luottaa sosiaalisen median tietoturvaan, koska netistä kaikki voi kopioida eikä tekijänoikeuksista sun muista säännöistä välitetä. Kaikkea mitä julkaiset netissä voidaan käyttää melkeinpä miten vain eteenpäin.
- Sosiaalisen median tietoturvan taso riippuu myös käyttäjästä itsestään. Esim. säätämällä tietoturva-asetukset käyttäjät itse voivat vaikuttaa sen tasoon.
- Huonosti on tietoa tietoturvasta.
- Uskoisin tietoturvan olevan kohtuullinen, mutta eri sovellukset keräävät käyttäjistä varmaankin erilaista tietoa, jota sitten käytetään esim. mainonnassa hyväksi.
- Ei ole tullut mitään ongelmia vaikka olen useita vuosia käyttänyt.
- Taustaani kuuluu syvempi ymmärrys ohjelmoinnista ja internetistä.
- En ole oikeastaan varma siitä, kuinka turvallista on laittaa omia tietoja tai rekisteröityä sosiaaliseen mediaan. Ei voi tietää kuinka helposti voi käyttäjätilille hakkeroitua, tai ketkä kaikki (ylläpito) tietoja lukevat.
- Käytän Facebookia vain yhteydenpitoon opiskelijoiden kanssa ja suljetussa ryhmässä. En luota siihen muuten enkä koe tarpeelliseksi.

LIITE 2

- Olen lukenut uutisia ja tiedotteita esim. Facebookin tietoturvariskeistä ja muista vastaavista.
- Kyllä Facebookin asetuksissa jotain siitä lukee.
- Tuntuu siltä että sosiaalinen media jakaa henkilökohtaisia tietoja suoramarkkinointiin ja esim. Facebookissa mainokset tulevat sen mukaan, mitä sivuhistoriasta löytyy.
- Mitä olen lukenut lehdistä. Ei ole omaa kokemusta.
- Melko huoleti voi jakaa tietoa suljetussa ryhmässä Facebookissa. On myös itsestä kiinni mitä kaikkea siellä julkaisee, Facebook:in tietojenkäyttökäytännöt ovat helposti saatavilla ja luettavissa.
- Minun tietoni yms. näkee vain minun kaverini.
- Aina ei voi tietää pysyvätkö tiedot salassa, mutta pääsääntöisesti luotan siihen, että kaikki tieto ei ainakaan suoraan mene kaikkien käyttäjien saataville.
- Missään ei kannata julkaista mitään sellaista, mitä ei tahdo jonkun joskus tietävän. Sosiaalisen median tietoturva ei ole niin korkeatasoinen ettei sitä hakkeri, ei ammattimainen, saisi murrettua.
- Suhtaudun kriittisesti tietojen (pitkäaikaiseen) säilyttämiseen ja tietojen keräämiseen markkinointi mielessä.
- Kohtuullinen siksi, että tiedän perusasiat sosiaalisen median tietoturvasta, mutta perusteellisempi perehtyminen aiheeseen voisi olla paikallaan.
- Käytän aika vähän somea ja vastaukseni perustuu pelkästään mielikuvaan sekä muuhun mediaan. Somessa kuitenkin liikkuu paljon tietoa, joten kuvittelisin, että siellä on helppo myös käyttää tietoja väärin, esim. kaapata toisen kuvia.
- Olen ottanut asiasta selvää ja seuraan tarkasti alan tapahtumia.
- Työnkuvani (IT-osasto) puolesta minun täytyy olla perehtynyt myös sosiaalisen median tietoturvaan.
- Tiedän että aika monella palvelulla on oikeudet tiedostoihin mitä heidän sivulle lisään, mutta esimerkiksi en tiedä mitä heillä on oikeus tehdä niillä.
- Tiedän, että esim. Facebook ei ole mikään tietoturvallisin paikka. En kuitenkaan tiedä mitä kaikkea sieltä voi levitä muualle.
- Kun tili on luotu, niin alussa tuli katsottua tarkastikin tietoturva-asiat, mutta käytön jälkeen asia on päässyt lipsumaan. Siihen ei tule enää kiinnitettyä niin tarkasti huomiota ja "rajaus" saattaa olla liiankin löysä, jolloin tiliä päästään katsomaan.
- Sosiaalisessa mediassa tietoa voi saada melkein kuka vain. Käyttäjä ei voi koskaan tietää kenelle tietoja menee eteenpäin.
- Kuvia voi kopioida. Sivuja voi tehdä väärällä nimellä. Omat kommentit voi levitä kavereiden sivujen kautta tuntemattomille.
- Osaan varoa julkaisemasta asioita, joita en halua jakaa kaikille.
- Yleisen tiedotuksen perusteella pidän sosiaalisen median tietoturvaa huonona. Itselläni ei ole huonoja kokemuksia, mutta olenkin varovainen mitä sosiaalisen median kautta jaan.
- Ensinnäkin yksityisyysasetukset - kuka vaan voi napata kuviasi koneelle, identiteettivarkaudet ym.
- Olen alalla.
- Työskentelen IT tehtävissä. painopisteenä mobiili ja langattomat järjestelmät, Cloud Computing sovelluskehitys yms.
- No ns. mitään minkä internetiin laittaa, ei voi sieltä koskaan kokonaan poistaa. Oli se sitten kuva tai tekstiä. Esim. jos Facebookista jonkin oman kuvansa poistaa, voi se silti olla internetissä jo jossain sivustolla tai Facebookinkin palvelimella.
- Käytän ainoastaan YouTubea, enkä ole edes miettinyt niin paljoa tietoturvapuolta :(
- Helppo päästä käsiksi toisten ihmisten tietoihin heidän sitä tietämättä.
- Tiedän, ettei tietoturvan taso ole aina kovinkaan hyvä sosiaalisissa medioissa.
- Olen kuullut esim. Facebookin kautta saaduista viruksista ja siellä tapahtuneista identiteettivarkauksista.
- Ei ole minulle aiheuttanut mitään ongelmia.
- Ei huonoja kokemuksia, pienellä perehtymisellä saa kohtuullisesti rajattua tiedonjakoaan.
- No Google lupaa käsitellä tietonsa luottamuksella, mutta suhtaudun hyvin skeptisesti tähän lupaukseen.
- Seuraan aikaani.
- Sosiaalisen median ajatus perustuu tiettyyn avoimuuteen ja tiedon jakamiseen. Käyttäjien tulisi toimia niin, että ei koskaan jaa itselleen haitallista tietoa palveluihin.
- Riippuu aika paljon siitä mitä tietoja itsestään antaa ja kuinka tarkkaan lukee ohjeet oman turvallisuuden parantamisesta. Ne jotka eivät oikein osaa/viitsi ohjeita lukea (monet englanniksi) antavat

turhan paljon itsestään tietoja kaikille jaettavaksi.
- Asiasta on puhuttu niin paljon ja omat vanhemmat on toitottanut asiaa yläasteesta lähtien. Ja lukemalla kaikki kaikki jutut joita on kirjoitettu iltalehessä.
- En ole juuri perehtynyt asiaan.

6. Minkälaisia tietoturvauhkia koet sosiaalisessa mediassa olevan? Voit perustella vastauksesi tähän:

Vastaajien määrä: 104

- Väärille ihmisille menee tietoa asioista, joita ei haluaisi heille menevän.
- Viiruksia voi tulla kaiken maailman mainosten kautta, joita esim. Facebookin sivupalkeissa pyörii.
- Tiedon leviäminen vääriin käsiin tai useammalle kuin oli tarkoitettu. Yksityisyyden menetys. Facebookin ym. Uudistukset, joihin ei voi itse vaikuttaa ja jotka hyödyntävät aiempaa itsestä lisättyä materiaalia. Muut voivat kopioida kuviani koneellensa.
- Tietovuotoja hakkeriden toimesta.
- Ei sinne kannata mitään kovin henkilökohtaista kirjoittaa tai kuvata. Verkosta on mahdoton poistaa mitään, jos sinne joskus jotain tallentaa.
- Mielipiteet ymmärretään väärin tai kuvia, mielipiteitä vääristellään ja käytetään väärin.Kopiointia on paljon.Kaikki kuvat yms. tallentuvat jonnekkin bitteihin,ja kymmenen vuoden kuluttua joku voi käyttää niit vaik itse olisi poistanut esim.kyseisen kuvan
- Kuvien varastaminen ja väärin käyttö. Oman sanan hyväksikäyttö toisessa yhteydessä, niin että se laitetaan tarkoittamaan jotain aivan muuta. Suomeksi siis eriasteiset plagioinnit.
- Tieto minusta voi silti levitä eteenpäin toisten esim. kaverieni kautta.
- Henkilökohtaiset tietoni päätyvät vääriin käsiin ja niitä käytetään vääriin tarkoituksiin.
- Hakkerit,ammattilaiset varkaat,identiteettien väärentäjät jne
- Kaikenlaisia mahdollisia..
- Jos on huolimaton, tietoja voi päästä sellaisten ihmisten käsiin, joille ei olisi tarvetta tietoja jakaa. Jos tunnukset joutuvat vääriin käsiin, voi toinen henkilö saada selville kovinkin henkilökohtaisia asioita esim. lukemalla toisten viestejä/keskustel
- Yleensä on pelkona, että omat asiat julkaistaan jossain missä ei pitäisi ja vielä liioiteltuna tai kokonaan erilaisena tietona itsestä.
- Itselläni on omat epäilykseni koskien jaettavien tietojen kontrolloinnista.
- Virukset leviää Facebookissa helposti erilaisten sovellusten kautta. Niiden kautta on helppo onkia tietoa henkilöstä.
- Olen aika välinpitämätön tietoturvan suhteen. Toisaalta jos esimerkiksi facebookissa ei itse julkaise mitään arkaluontoista, ongelmia ei pitäisi syntyä.
- Tiedot voivat levitä sellaisille ihmisille kelle ne eivät kuulu, sekä muutenkin sosiaaliseen mediaan.
- -aika helppo kalastaa ihmisten tietoja jos sellaista haluaa tehdä?
  -sitäpaitsi koko sos. media perustuu tietojen antamiseen itsestään, joko enemmän tai vähemmän?
  -ainoa varma keino tiedon leviämisen estämiseksi on olla pistämättä sitä sos. mediaan ollenkaan
- Sivustot keräävät tietoja kaikesta, mitä teet internetissä.
- Tiedot ja kuvat päätyvät vieraille tahoille.
- Kaikki tietää kaiken minusta,jos lähden tähän.
- Henk.koht. en ymmärrä, mitä riskejä siellä voi olla. Käyttäjien pitää itse tajuta riskien olemassaolo ja käyttää sos. mediaa niin, ettei liian henk.koht. asiat vuoda sitä kautta julkisiksi. Pitää kantaa vastuu omasta käyttäytymisestään sos. mediassa.
- Kolmannen osapuolen henkilö (esim. automaattinen botti) on saanut pääsyn tunnuksiin, jolloin haittaohjelmia voidaan levittää tilapäivitysten / liitteiden kautta.
- Henkilökohtaiset tiedot voivat levitä,yksityisyysasetukset täytyy olla kohdillaan. Liian selvät naamakuvat ovat helposti kaapattavissa.
- En koe että niitä on.
- Tunnusluvut menee vääriin käsiin.

LIITE 2

- Kuvien kopiointi. Identiteettivarkaudet.
- Aika suuri, koska monen on varmasti vaikea tulkita kaikki epäilyttävä mm. facebookissa ja muualla... Varsinkin alaikäiset.
- Tiedonkaappaukset, hakkerointi jne.
- edellisessä kohdassa on vastaus tähänkin.
- Tietojeni leviäminen ulkopuolisille
- henkilökohtaisten tietojen ja kuvien käyttö ilman lupaa, profiilien tutkiminen mainonnan tähtäämiseksi.
- en oikein tiedä
- Tietojen anastus ja väärinkäyttö
- Identiteettikaappaus
- Käyttäjätietojen joutumisen vääriin käsiin.
- Suurin uhka on varmaan ettei kaikki ajattele mitä kirjoittavat. Kaikkia pankkisalaisuuksia, sosiaaliturva tunnuksia tai toisen luottamuksellisesti antamia tietoja ei pitäis levitää eteenpäin verkossa pienellekään piirille. koska tieto jää bittiavaruuteen.
- Jos laittaa liian henkilökogtaisia tietoja tai kuvia järjestelmiin
- Erialaiset identiteettivarkaudet, toisen nimissä puhumisen ja omaisuuteen liittyvät petokset.
- Joku voi varastaa oman käyttäjätilin tai tutkia salaisia tietoja. Kooneelle murtautuminen tai virusten asettaminen pelottaa myös.
- tiedot vuotavat jonnekin, niitä voidaan väärinkäyttää, ihmiset ovat liian "sinisilmäisiä" esim Facebookissa ja paljastvat/kertovat itsestään liikaa ja julkaisevat turhia valokuvia siellä
- yksityisyyssuojane menettäminen
- Yleisin on varmaan se että, face jää koneelle auki ja joku käyttää tilaisuuden hyväkseen. Ja onhan näistä facebookin tietoturva ongelmista uutisoitu...
- En oikeastaan minkäänlaisia, koska en jaa sinne paljon itsestäni tietoa.
- Yksityisten tietojen leviäminen suoramarkkinointiin.
- Murtautuminen facebookiin on helppoa ja sujuvaa perus hakkereilta.
- esimerkiksi murtautuminen suojaamattomalle tai suojatulle tietokoneelle ja sen käyttäminen luvatta ja itse sosiaalisen median käyttäjä on uhkana, jos esim säilyttää salasanaa väärässä paikassa.
- Vaikka ja mitä.
- Henkilökohtaisia tietoja voidaan väärinkäyttää.
- Henkilökohtaisen tietojen myyminen eteenpäin.
- Erilaiset sovellukset voivat tuoda viruksia koneelle. Ihmisistä saadaan urkittua paljon tietoa esim. Facebookin kautta.
- En käytä muuta sosiaalista mediaa kuin YouTube, niin en koe että minulle on tullut kovinkaan paljon tietoturvauhkia.
- Kaikki tienoni ovat kaikkien nähtävillä
- Facebook esimerkiksi muuttaa välillä ihan itsestään tietoturva-asetuksia.? Julkisuudessa on ollut myös paljon juttuja sähköpostien tunnuksien ja salasanojen kaappauksista.
- Joku kaappaa sun tilin, tietosi päätyvät kolmannille osapuolille
- eniten itseäni häiritsevät ohjelmat, jotka päivittävät olinpaikkasi joskus jopa haluamattasi...mielestäni se ei ole oikeutettua ja ainakin omalla kohdalla haluan edes sen verran yksityisyyttä. Toki on oma valilnta käyttääkö esim. facebookkia
- Tileihin on helppo päästä käsiksi, sillä netistä löytyy monia ohjeita ja ohjelmia hakkeroimiseen. Näillä tiedoilla melkein tavallinen tallaajakin voi onnistua.
- Tiedot menee vääriin käsiin.
- Hakkerit ovat aivan eri tasolla kuin parikymmentä vuotta sitten, palveluntarjoaja ei pysty pelaamaan niitä vastaan.
- salassa pidettävät asiat
- Identiteetti varkaus...
- Identiteettivarkaus on ehkä se pahin uhka, jonka voin kuvitella esiintyvän sosiaalisessa mediassa.
- Yksityisyyden menetys, henkilöllisyyden tai henkilötietojen kaappaus, yksityisten tietojen ajautuminen vääriin käsiin
- Tietovuodot ja se, että kun antaa tietojaan jollekin sivustolle, ei enää tiedä mihin niitä levitetään ja mistä ne seuraavaksi tulevat vastaan
- Esim. kuvien ja jopa identiteetin varkauksia.

LIITE 2

- Yksityisiin tietoihin käsiksi pääsemisen. joka paikkaan vaaditaan rekisteröityminen ja henkilötiedot.
- henkilökohtaiset tiedot joutuvat väärille henkilöille
- identttiteettivarkaudet, tietojen leviä (kuvia ei saa koskaan pois)
- Joissakin palveluissa voit lähes vahingossa antaa oikeudet myös omaan sähköpostin osoiterekisteriin, kännykän tietoihin jne.?
  Aiheuttaa uhkaa tietoturvan suhteen melkoisesti ja ainakin roskaposti tulva lisääntyy kun tietoja leviää ulkopuolisille.
- Luottamuksellisten tietojen vuotaminen tahattomasti tarkoitettua kohderyhmää laajemmalle teknisin keinoin, jotka eivät ole peruskäyttäjälle selviä. Harva ihminen oikeasti lukee käyttöoikeussopimuksen, minkä hyväksyy.
- Jos tiedot joutuvat vääriin käsiin, esimerkiksi hakkereiden kautta.
- yksityisasioiden leviäminen
- Aina ei voi välttämättä olla varma siitä, että käytetäänkö mediaan lisättyä materiaalia vääri. Siksi olen aika kriittinen siinä mitä lisään sinne.
- -Use security tools from supplier?
  -Reduce individual information
- Epäilen, että sosiaalisessa mediassa seurataan mitä muita sivustoja käytän ja ehkä kuvani ja tekstini menevät muualle jakeluun tietämättäni.
- Tietojen leviämistä, identiteettivarkauksia
- Hakkerit, ahdistelijat, virukset, tunkeilijat, tiedon kaappaajat/kaappaajat, onnen onkijat ym.
- Tietoja käytetään vääriin tarkoituksiin
- Joku voi luoda epäedullisen kuvan väärällä nimellä toisesta.?
  Ylläpitäjät levittävät tietojani markinointi tarkoituksiin yrityksille. =>Roskaposti, jne..
- kuvien kopiointioikeus, hakkerointi
- Oman verkkoidentiteetin menettäminen, niin että joku toinen käyttää henkilöllisyyttäni hyväkseen lähinnä taloudellisesti mutta myös muuten.
- Jos ei käytä uhkaa ei ole.
- eli omien tietojen nappaaminen, identiteettivarkaus että joku esiintyy minuna ym.
- Normaaleja tietoihin liittyviä. En koe että ne ovat pahoja jos käyttää maalaisjärkeä. (vrt. puhelinluettelo)
- hakkerit
- Identiteetin varastaminen, liiaksi sirpaloituneet päätelaitteet & niiden tietoturva ko. asioissa, kyber rikollisten murrot suurimpien toimijoiden palvelimiin.
- Esim chatviestit jotka kaverisi näkevät sinun kirjoittaneen mutta itse et ole niistä ollenkaan tietoinen. Julkaisut jotka muut näkevät sivullasi mutta et itse näe etkä tiedä niistä mitään. Huijausohjelmat, peliksi tai muuksi naamioidut tietojenkalastukset
- Koen uhkana sen, että henkilötietoni joutuisivat vääriin käsiin.
- En osaa sanoa...tiedot joutuvat vääriin käsiin.
- Helppo päästä käsiksi toisten ihmisten tietoihin heidän sitä tietämättä.
- Joku varastaa henkilötietoja.
- Edellä mainitut.
- Henkilöllisyys ,yksityiset asiat
- Yhteystietojen ym. leviäminen vääriin käsiin, valokuvien väärinkäyttö nyt tulee ensimmäisenä mieleen.
- Sivustojen kaappaukset, hakkeroinnit. Väärinkäsityksistä johtuvat salaiseksi tarkoitetun tiedon julkistaminen. Tulevaisuudessa sivuston lopettamisen yhteydessä tapahtuvat vuodot.
- Ensimmäisenä tulee mieleen henkilötietojen varastaminen ja hyödyntäminen.(urkinta ohjelmien avulla) Sekä tietämättömien tai muuten vain naiivien ihmisten avoin tietojen jakaminen sosiaalisessa mediassa.
- huonon
- Tunnuksien kalastelua (salasanat, pankkitunnukset jne.)?
- Tietojen keräämistä ja niiden hyödyntämistä ilman lupaa?
- Käyttäjien tulisi kriittisesti arvioida millaista tietoa itsestään ja muista ihmisistä verkossa jakaa, sillä niitä voidaan jakaa eteenpäin.
- Jos vaikka kerrot olevasi lähdössä lomalle etkä ole rajannut omaa näkyvyyttäsi voi murtovarkaat käyttää tietoa hyväkseen.

- tietojen 'luvaton' julkaiseminen
- Tekijänoikeusproblematiikka, henkilötietojen varastaminen ja väärinkäyttö, toisen identiteetillä esiintyminen ym...

15. Jos muuttui niin miten? Voit perustella edellisen kysymyksen vastauksen tähän:

Vastaajien määrä: 28

- Olen varovaisempi.
- Joistakin säännöistä en tiennyt liittyen facebookin käyttämiseen.
- Turvattomampaa kuin edes ajattelin.
- Voisi tulevaisuudessa olla vähän tarkempi mitä Facebookissa itsestään kertoo.
- olen ollut tietoinen riskeistä, mutta kaikkia asioista en ole tiennyt. pitää olla edelleenkin varovainen, mitä julkaisee netissä.
- Henkilätietoni ja käyttäytymiseni internetissä onkin paljon avoimempana, kun olen tiennyt. Huolestuttaa oma tietoturvallisuus.
- Olen tietoisempi näistä riskeistä jotka liittyvät sosiaaliseen mediaan
- En osaa sanoa.
- Kiitos paljjon hyvistä faktoista joita en ollut tiennyt :)
- Olen varovaisempi tästä lähtien.
- kyllähän tästä tietoturva-asiasta on paljon puhuttu aikaisemminkin ja ainakin omalla kohdalla voin sanoa, että en laita esim facebookkiin sellaista tietoa mitä en halua muiden saavan.
- Heräsi ajattelemaan, että mitä jotkut asiat käytännössä ovat
- En ollut täysin tietoinen että tiedonkeruu on tosiaan noin laajaa.
- Olen tietoinen mm. sosiaalisen median riskeistä (ovat tietysti myös suuria mahdollisuuksia). Peruskäyttäjälle tulisi jollain tavalla tiedottaa riskit ja suomennetut (lue: kansankielistetyt) sopimukset mitkä he hyväksyvät. EFFI voisi olla hyvä tiedonlähde.
- Tuli hieman epävarmempi olo sosiaalisesta mediasta.
- Now I know that social media is not safe as what I thought, minun pitaisin valvoa toimiani.
- Muistutti ehkä taas miettimään, että mitä kaikkea kannattaa jakaa sosiaalisiin medioihin ja mitä tietoja itsestään sinne lataa
- Sain paljon sellaista tietoa, mitä en ole tullut ajatelleeksikaan tai olet tullut edes mieleeni. :) Kiitos Petra. :)
- Täytyy miettiä yhä tarkemmin, mitä julkaisee omassa tai yritykseni facebookissa
- ehkä vielä tietoisempi siitä ettei jaa tietoja ulkopuolisten yksityishenkilöiden kanssa (en koe niin pahaksi uhaksi esim. googlea ja facebookkia, vaan ns. yksityisiä henkilöitä)
- Nyt aloin huolestua....
- Kys. 12 kommentti: En ole laittanut sosiaaliseen mediaan kuvia, mitkä antaisivat minusta epäedullisen vaikutelman, mutta olen tietoinen kuvien säilymisestä poistamisesta huolimatta.
- Täytyy tarkkailla enemmän että mitä tietoja itsestään luovuttaa sosiaaliseen mediaan.
- Oma järki on käytettävissä mitä laittaa näille sivuille kuinka yksityiskohtaisesti.
- osa asioista on jo unohtunut
- miettii entistä tarkemmin mitä sinne laittaa.
- Tietoturvakysymyksiin tulisi kiinnittää huomiota entistä enemmän.

17. Jos muuttui niin miten? Voit perustella edellisen kysymyksen vastauksen tähän:

Vastaajien määrä: 18

- Olen varovaisempi.
- Ei muutu, olen ollut tietoinen tästä jo valmiiksi. Sosiaalisen mediaan ei ole hirveästi luottamista. itse olen ainakin aika varovainen sen suhteen.
- Varovaisuutta Facebookin käytössä enemmän.
- Käytän SoMea muutenkin niin vähän.

LIITE 2

- Ehkä mietin tarkemmin, mille sivuille internetissä' menen. Olen myös ajatellut facebook-tilin poistamista, vaikka tiedot voivatkin jäädä tallennuksiin.
- en käytä niitä muuta kuin työn takia
- En tiennyt kaikista käyttö ehdoista esim facebook ja google, joten mietin nyt enemmän mitä sinne laitan itsestäni.
- Aion entistäkin tarkemmin miettiä mitä julkaisen Facebookissa.
- Olen aina ollut melko varovainen antamieni tietojen kanssa facebookissa, mutta tämän kyselyn jälkeen uskon että olen vielä varovaisempi.
- En anna kovin paljoa tietoa sosiaaliseen mediaan, enkä käytä niitä kovin paljoa. Alumiinifoliohattu tosin menee entistä syvemmälle päähän. Tietoturva ja tiedon turva ovat huolestuttavalla tolalla tämän päivän tietoyhteiskunnassa. Hyvä kysely tämä on!
- Mietin tarkemmin, mitä kuvia/videoita julkaisen internettiin ja yleensäkin se, mitä tietoja julkaisen itsestäni ja missä muodossa.
- Haluan ettei kukaan ns." itselle tuntematon" näe omia facebook tietoja.
- Olen aina sanonut etten laita itselleni Facebookia ja tämän jälkeen olen vakuuttunut että olen oikeilla raiteilla.
- En aio luovuttaa tietojani muihin sos. medioihin kuin facebookiin.
- Edelleenkin mitä laittaa ja kunka ysksityiskohtaisesti
- Olen varmasti hieman varovaisempi siinä mitä julkaisen esim Facebookissa ja varoitan myös lapsiani tietoturvan vaaroista.
- miettii entistä tarkemmin mitä sinne laittaa.