HAAGA-HELIA
ammattikorkeakoulu

HAAGA-HELIAN tietojenkäsittelyn ja liiketalouden koulutusohjelmien aloittelevien ja lopettelevien opiskelijoiden suhtautuminen tietoturvaan internetin sosiaalisessa kanssakäymisessä

Juha Hirvonen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
Kevät 2009

Tiivistelmä
27.5.2009

HAAGA-HELIA
Tietojenkäsittelyn koulutusohjelma

Tekijät Juha Hirvonen	**Ryhmä** TIKO04
Opinnäytetyön nimi HAAGA-HELIAN tietojenkäsittelyn ja liiketalouden koulutusohjelmien aloittelevien ja lopettelevien opiskelijoiden suhtautuminen tietoturvaan internetin sosiaalisessa kanssakäymisessä	**Sivu- ja liitesivumäärä** 65 + 27
Ohjaajat Titta Ahlberg	

Tietoturvasta puhutaan eri medioissa ja kehotetaan varomaan erilaisia vaaroja, huolehtien tietoturvasta. Tämä on ymmärrettävää, koska ihmisillä on henkilökohtaisia tietoja tietokoneella ja ihmisten viettämä aika internetissä on kasvanut, erilaisten sosiaaliseen kanssakäymiseen tarkoitettujen verkkopalvelujen myötä, joista Facebook viimeisimpänä

Tutkimuksessa selvitettiin kuinka HAAGA-HELIASSA Pasilan toimipisteessä tietojenkäsittelyn ja liiketalouden koulutusohjelmassa aloittelevat ja lopettelevat opiskelijat (1) huolehtivat ja kiinnittävät huomiota tietokoneen tietoturvaan, (2) käyttäjätietoihin internetissä ja (3) Facebookin yksityisyyteen. Vastaavaa opiskelijatutkimusta ei ollut käsityksen mukaan tehty. Lisäksi lähdeaineiston perusteella selvitettiin sosiaaliseen kanssakäymiseen mahdollisesti liittyviä yleisiä tietoturvauhkia sekä Facebookin yksityisyyteen liittyviä uhkia. Tutkimuksessa käytiin myös läpi suojautumis- ja ennaltaehkäisymenetelmiä, joilla voidaan suojautua uhilta.

Tutkimusmenetelminä käytettiin lähdeaineistoja ja WEBROPOL palvelua, jolla tehtiin kyselylomake. Valmis kyselylomake ohjattiin HAAGA-HELIAN edustajan avustuksella WINHAPRON kautta ennalta määritellyille opiskelijoille, sähköpostitse. Opiskelijoiden vastaukset analysoitiin ja kirjattiin tutkimukseen.

Tutkimuksessa selvisi, että HAAGA-HELIAN opiskelijat näyttäisivät huolehtivan tietokoneen tietoturvasta, käyttäen tietoturvaratkaisuja ja seuraten tietoturvavaroituksia sekä reagoiden niihin. Liiketalouden opiskelijat näyttäisivät huolehtivan suhteellisesti enemmän tietokoneen tietoturvasta, vertailtaessa aloittelevia opiskelijoita keskenään. Tietojenkäsittelyn opiskelijat näyttäisivät puolestaan huolehtivan suhteellisesti enemmän tietokoneen tietoturvasta, vertailtaessa lopettelevia opiskelijoita keskenään. Lisäksi selvisi, että HAAGA-HELIAN opiskelijat näyttäisivät kiinnittävän pääsääntöisesti huomiota käyttäjätietoihin internetissä (salasanojen -sisältöön, -pituuteen, -vaihtoväliin, -vaihtelevuuteen eri palveluissa sekä tietojen jakamiseen) ja näyttäisivät huolehtivan pääsääntöisesti Facebookin yksityisyydestä (tietoisuus käyttäjäehtojen muutoksista, tietojen jakaminen, kavereiksi hyväksyminen, virtuaalisovellusten käyttöönottokriteerit ja kiertoviesteihin reagoiminen), hieman vaihdellen, riippuen asiasta. Tavoitekohtiin 2. ja 3. ei löytynyt sellaisia eroavaisuuksia, jotta voisi eroja olevan koulutusohjelmien välillä, koska erot jakaantuivat liikaa kysymysten välillä.

Yleisesti sosiaalisessa kanssakäymisessä haittaa aiheuttavat erilaiset madot, virukset, hakkerit, vakoiluohjelmat, haittaohjelmat, huijaukset, roskaposti ja tietojen katoamiset. Facebookin käyttäjän yksityisyyttä uhkaavat pääsääntöisesti ihmisten sinisilmäisyys profiilia, virtuaalisovelluksia ja kiertoviestejä kohtaan sekä erilaiset virukset ja vakoiluohjelmat. Koulutusohjelmalla ei ollut niin suurta vaikutusta tutkimuksen tuloksiin kuin odotettiin.

Asiasanat Tietokone, Tietoturva, Internet, Virus, Tietoturvauhka, Sosiaalinen kanssakäyminen, Yksityisyys, HAAGA-HELIA, Facebook, Opiskelija, Tietojenkäsittely, Liiketalous ja Koulutusohjelma.

Abstract
27 May 2009

HAAGA-HELIA
Degree Programme in Business Information Technology

Authors	**Group**
Juha Hirvonen	TIKO04
The title of thesis First and last year students' attitude to the information security regarding the social media of the Internet. Case: HAAGA-HELIA University of Applied Sciences, Degree Programmes in Business Information Technology and Business Management	**Number of pages and appendices** 65 + 27
Supervisors Titta Ahlberg	

Information security is one of the most frequently discussed topics in the media today. Taking care of the information security issues is highly recommended because of the many threats involved in the internet usage. This is understandable because people have their personal information on their computers and the time spent on the Internet has increased partly due to the emerging of various, new network services included in the social media, of which Facebook is one of the latest ones.

The purpose of this study was to determine how the first and last year students at HAAGA-HELIA Pasila Campus's Information Technology and Business Management Programmes take care and pay attention to the computer information security, to user information on the Internet and to the Facebook privacy. In addition, the objective of this study was to clarify what kind of common information security threats and Facebook specific threats related to user privacy are included in the social media. Furthermore, the study looked into protection and prevention methods, which protect the users from the above-mentioned security threats.

The study was carried out by investigating source material and conducting a WEBROPOL network survey sent by e-mail to specified HAAGA-HELIA students.

The study showed that HAAGA-HELIA students seem to take care of the computer information security by using security solutions and following the information security announcements. Business students seem to care more about their computer information security than IT students when comparing the first year students. The situation was reversed when comparing the last year students in these two programmes.

In addition, the study indicated that HAAGA-HELIA students seem to pay attention to the user information on the Internet i.e. to the concepts related to the contents, length and changing of the passwords, and also to the variation of the passwords in different services. They also seem to take care of Facebook privacy i.e. user requirement adjustment knowledge, information sharing, friend requests, virtual apps deployment criterions and response to circular message with minor alterations depending on the issue.

The study concludes that the biggest problems and threats in social media are caused by different kind of worms, viruses, hackers, spyware apps, malware apps, cheats, spam and the disappearing of the information. The Facebook user's identity may be in danger because people are rather blue-eyed regarding issues related to profile, virtual apps and circular messages and also various viruses and spyware apps. The Degree Programme did not have as significant a role as was expected.

Key words Computer, Information Security, Internet, Virus, Information Security Threat, Social Communication, Privacy, HAAGA-HELIA, Facebook, Student, Information Technology, Business Management and Programme

Sisällys

Liite 3. Liiketalouden koulutusohjelman aloittelevien opiskelijoiden kyselytulokset
Liite 4. Liiketalouden koulutusohjelman lopettelevien opiskelijoiden kyselytulokset
Liite 5. Kyselylomake tietoturvaan suhtautumisesta sosiaalisessa kanssakäymisessä
Liite 6. Tutkimuksen loppuraportti

1 Johdanto

Tutkimuksella selvitän, kuinka HAAGA-HELIAN Pasilan toimipisteen tietojenkäsittelyn ja liiketalouden koulutusohjelman aloittelevat ja lopettelevat opiskelijat suhtautuvat tietoturvaan eli kiinnittävätkö siihen huomiota käyttäessään internetiä sosiaalisessa kanssakäymisessä. Lisäksi selvitän mitä yleisiä tietoturvauhkia sosiaaliseen kanssakäymiseen voi liittyä ja mitkä uhkatekijät voivat mahdollisesti uhata Facebookin käyttäjän yksityisyyttä, jos tietoturvasta ei huolehdita. Käyn myös läpi suojautumis- ja ennaltaehkäisymenetelmiä, joilla suojaudutaan edellä mainituilta uhkatekijöiltä.

Tietoturvasta puhutaan erilaisissa tiedotusvälineissä mm. radiossa, televisiossa, internetissä, lehdissä jne. lähes päivittäin ja kehotetaan varomaan mitä erilaisimpia vaaroja, huolehtimalla tietoturvasta. Aiheen valinta oli helppoa, koska tietoturvasta löytyy jo itsessään paljon tietoa, mutta laajuudesta johtuen se oli jotenkin rajattava tähän tutkimukseen. Opiskelijoiden suhtautuminen tietoturvaan sosiaalisessa kanssakäymisessä on hyvä valinta, koska sosiaalinen kanssakäyminen on entistä suositumpaa internetissä, johtuen uusien sosiaalisten verkkopalvelujen suosiosta, kuten Facebook. Lisäksi aiemmin ei ole tehty vastaavia tutkimuksia, joten tuloksena saadaan arvokasta tietoa opiskelijoiden suhtautumisesta tietoturvaan sekä mahdollisista eroavaisuuksista koulutusohjelmien aloittelevien ja lopettelevien keskuudessa.

Tutkimusmenetelminä käytän erilaisia lähdeaineistoja, joilla selvitän ”mitä tietoturvauhkia yleisesti sosiaaliseen kanssakäymiseen liittyy” ja ”mitkä uhkatekijät mahdollisesti uhkaavat Facebookin käyttäjän yksityisyyttä” sekä miten suojaudutaan näiltä uhkatekijöiltä eli suojaus- ja ennaltaehkäisymenetelmät.

Projektin pääselvitykseen eli kyselyyn ”kuinka HAAGA-HELIAN Pasilan toimipisteen (tietojenkäsittelyn) ja (liiketalouden) koulutusohjelmien aloittelevat ja lopettelevat opiskelijat suhtautuvat tietoturvaan käyttäessään internetiä sosiaalisessa kanssakäymisessä (Facebook)” käytän HAAGA-HELIASSA suosittua WEBROPOL verkkokyselylomakepalvelua. Kun kyselylomake on valmis, se ohjataan WINHAPRO:n kautta HAAGA-HELIAN määritellyn koulutusohjelman opiskelijoille sähköpostitse. Kaikki opiskelijoiden vastaukset tulevat

suoraan WEBROPOL -verkkopalveluun, josta ne analysoidaan, tarvittaessa tarkemmin tavallista paperia ja Microsoft Excel-ohjelmaa apuna käyttäen. Lopuksi tulokset kirjataan tutkimukseen.

Pyrin tutkimaan ja selvittämään asioita käyttäjäystävällisesti, jotta tästä opinnäytetyöstä olisi hyötyä jatkossa niin opiskelijoille kuin myös muille asiasta kiinnostuneille.

2 Tutkimuksen taustaa

2.1 Sosiaalinen kanssakäyminen

Sosiaalisella kanssakäymisellä tarkoitetaan ihmisten välistä yhteydenpitoa ja kommunikointia ajasta ja paikasta riippumatta. Internetissä sosiaalinen kanssakäyminen on kasvattanut suosiotaan entisestään erilaisten sosiaalisten verkkopalvelujen lisääntymisen myötä, jotka ovat tulleet perinteisen sähköpostin tueksi. Tämän lisäksi on olemassa erilaisia pikaviestimiä (MSN-/Yahoo Messenger, ICQ jne.), joiden avulla ihmiset pitävät paljon yhteyttä ja kommunikoivat toisilleen. Tässä opinnäytetyössä sosiaalisella kanssakäymisellä tarkoitetaan yhteydenpitoa ihmisiin pääasiassa Facebookin erilaisten yhteydenpito toimintojen avulla sekä sähköpostilla ”sähköpostiviestein”.

2.2 Yksityisyys

Yksityisyys kuuluu ihmisen perustarpeisiin, jota varten on kehitelty yksityisyydensuoja. Lähtökohta on, että jokaisella ihmisellä olisi oikeus omien henkilötietojen pysymiseen turvattuna ulkopuolisilta, jota säätelee henkilötietolaki. Yksityisyys on noussut ajankohtaiseksi internetissä erilaisten sosiaalisten verkkopalvelujen yleistymisen ja sitä kautta suosion myötä. Ongelmaksi on muodostumassa se, etteivät läheskään kaikki palveluja käyttävät ihmiset tiedosta riittävästi sitä, mitä tietoja oikeasti ihmisestä tallentuu ylös ja millaista tietoa on turvallista jakaa muiden palvelua käyttävien nähtäville.

Tässä opinnäytetyössä yksityisyyttä käsittelevät asiat pohjautuvat siihen, mitä tietoja ihmisistä oikeasti kerätään ylös, kun käyttävät erilaisia palveluja internetissä liikkuessaan. Pelkästään internetissä liikkuessa ihmisistä tallentuu tietoja, kuten IP – osoite ja evästeitä, jonka lisäksi tietokoneelle tallentuu sivuhistoria ja mahdollisesti tallennettuja lomaketietoja, käyttäjätunnuksia ja salasanoja.

Tämän lisäksi rekisteröitymisvaiheessa eri palveluissa kysytään tietoja, jolloin tulisi selkeästi mainita, mitä tietoja tarvitaan rekisteröityvältä ihmiseltä, mihin tietoja käytetään sekä miten näitä tietoja käsitellään esim. henkilötietolakiin nojautuen. Jos tietoja halutaan luovuttaa kolmannelle osapuolelle, tulisi siihen pyytää suostumus palveluun rekisteröityvältä ihmiseltä.

3 Keskeiset käsitteet

3.1 Tietoturva yleisesti

Tietoturvan tarkoituksena on suojata jotakin, esimerkiksi tärkeiden tietojen leviäminen ulkopuolisille, johon tarvitaan erilaisia suojaustoimenpiteitä. Tietoturvan tulee täyttää erilaisia kriteerejä, kuten luottamuksellisuus, eheys, todennus, kiistämättömyys, pääsynvalvonta ja käytettävyys. (Opasmedia 2006)

Luottamuksellisuudella pyritään varmistamaan, että tiedot ovat vain sellaisten henkilöiden käytettävissä, joilla on oikeus tietoihin. Suojaa tietojen yksityisyyttä ja omistusoikeutta, koska ulkopuoliset eivät näe tietoja. (T. Mikkola, O. Virkki 2006)

Eheydellä varmistetaan tiedon muuttumattomuus luomis-, käsittely-, ja siirtotilanteissa, joista siirtotilanteeseen kuuluu myös (lähetys ja vastaanotto). Eheys toimii vain, jos viestin lähettäjä pystytään tavalla tai toisella todentamaan, koska toimii yhteistyössä todennuksen kanssa. (T. Mikkola, O. Virkki 2006)

Todennuksella varmistetaan, että vastapuolen osapuoli on se henkilö, joka väittää olevansa. Todennuksen rooli korostuu erityisesti viranomaispalveluiden ja verkkokauppojen yhteydessä. (T. Mikkola, O. Virkki 2006)

Kiistämättömyydellä pyritään siihen, että saadaan konkreettinen tapahtumamerkintä ylös tapahtuneesta, jotta henkilö ei voi jälkikäteen kiistää tekemisiään. Toteutetaan esimerkiksi sähköisellä allekirjoituksella. (T. Mikkola, O. Virkki 2006)

Pääsynvalvonnalla varmistetaan, ettei kukaan ulkopuolinen pääsisi käsiksi järjestelmässä oleviin tietoihin ja palveluihin. Toteutetaan rajoittamalla ja valvomalla sitä, kenellä on oikeus päästä järjestelmässä oleviin tietoihin käsiksi. (T. Mikkola, O. Virkki 2006)

Käytettävyydellä varmistetaan, että järjestelmässä olevat tiedot ovat aina niiden henkilöiden saatavissa, joilla on oikeudet tietoihin. (T. Mikkola, O. Virkki 2006)

3.1.1 Tietoturvan suojausmenetelmien jaottelu

Teknisellä tietoturvalla pyritään estämään järjestelmään kohdistuvat väärinkäytöt erilaisten laitteiden, ohjelmistojen ja tekniikoiden avulla. Suojaus toteutetaan usein salasanojen ja käyttäjätunnusten avulla, jonka pitävyyttä voidaan parantaa esimerkiksi mahdollisimman pitkillä salasanoilla. Vielä turvallisempia keinoja ovat erilaiset palomuurit sekä käsiteltävän tiedon kryptaaminen sellaiseen muotoon, jota ei voida lukea. (Opasmedia 2006)

Hallinnollinen tietoturva koostuu ohjeistuksista, määräyksistä ja järjestelmään liittyvistä dokumentaatioista, joiden tarkoituksena on vähentää sisään pääsyä yrityksen tietoturvajärjestelmään ja sitä kautta mahdollisia tietovuotoja. (Opasmedia 2006)

Fyysinen tietoturva pyrkii estämään palvelimiin/tietokoneisiin ja niiden tietoihin käsiksi pääsemisen. (Opasmedia 2006)

3.2 Tietoturvauhkat

Tietoturvauhilla ei ole maantieteellisiä rajoja internetissä ja siihen kytkettyjen tietojärjestelmien kesken. Uhat voivat kohdistua kenen tahansa tietokoneeseen, päivästä ja kellonajasta riippumatta. Uhat leviävät erittäin nopeasti yli maapallon, esimerkiksi tietokoneisiin kohdistetut virukset ja muut haitalliset ohjelmat leviävät jopa muutamissa tunneissa. Harmillisinta tietokonetta käyttävän kannalta on se, että kone voi olla jo hyökkääjän hallussa ilman, että käyttäjä havaitsee tietokoneessa mitään vikaa ja jatkaa työskentelyä tietokoneella täysin normaalisti. (Saarijärvi 2004, 9)

Suurin uhka tietoturvan suhteen on se, etteivät ihmiset aina tiedosta tietoturvaan liittyviä riskejä ja suhtaudu niihin riittävällä vakavuudella. On myös muistettava, että tietokonelaitteet ja internet kehittyy, joka itsessään tuo paljon uusia haasteita tietoturvauhkien suhteen. (Saarijärvi 2004, 10)

Seuraavassa on käyty läpi tietoturvauhkia, jotka voivat uhata tietokoneen käyttäjää, jos ei tietoturvasta ole huolehdittu.

3.2.1 Virukset ja madot

Mitä virukset ovat?

Verkossa on lähes jatkuvasti liikkeellä monenlaisia viruksia, jotka aiheuttavat haittaa tietokoneen toiminnalle tai pahimmassa tapauksessa tuhoavat/muuttavat tietokoneessa

olevia tietoja. Viruksia kutsutaan ”tuholaisohjelmiksi”, koska ovat tietokoneelle päästyään usein käyttäjälle täysin huomaamattomia, kunnes tietokone alkaa toimia epänormaalisti (Korpela 2005, 63)

Virukset ovat pieni osa jotain ohjelmaa ja käynnistyvät tietyn ajan kuluessa tai, kun jokin muu ehto toteutuu. Viruksia on olemassa erittäin vaarallisia, haitallisia sekä vaarattomia, jotka on helppo tunnistaa tiedostopäätteestä mm. .exe, .com, .dll. (Kuivanen 2005)

Miten virukset leviävät?

Leviäminen tapahtuu pääsääntöisesti internet linkkien- ja tiedostoliitteiden, sähköpostin liitetiedostojen, levykkeiden, cd- /dvd -levyjen, USB - muistitikkujen, ulkoisten kovalevyjen sekä muiden siirrettävien oheislaitteiden avulla. Virukset eivät koskaan leviä itsestään, vaan vaativat aina viruksen sisältävän liitteen tai tiedoston avaamisen. (Korpela 2005, 64)

Viruksien kolmijaottelu

Tiedostovirukset tarttuvat käynnistystiedostoihin, jotka pystyvät suorittamaan ohjelman käynnistyksen. (Kuivanen 2005)

Levykevirukset tarttuvat levykkeitä siirrettäessä tietokoneesta toiseen ja suoritettaessa käynnistys kyseiseltä levykkeeltä ”avaamalla”. (Kuivanen 2005)

Makrovirukset ovat dokumenttiin erillisellä sovellusohjelman makrokielellä kirjoitettua ”koodia”. Kun dokumentin avaa, makrovirus käynnistyy ja aiheuttaa välittömän haitan tietokoneelle. (Kuivanen 2005)

Mitä haittoja virukset aiheuttavat?

Virukset voivat liittää itseään tietokoneessa oleviin muihin tiedostoihin tai samaan verkkoon kuuluviin muihin tietokoneisiin. Avatessa internet-selaimen voi huomata aloitussivun muuttuneen tai näytölle ilmestyneen ”viestikehotteen” tai pahimmassa tapauksessa virus on sekoittanut näytön toiminnan kokonaan. Virukset tuhoavat tiedostoja yksitellen, tai isommissa ryhmissä ja aiheuttavat tuhoa tietokoneessa oleville tiedostoille. (Korpela 2005, 63)

Yksi viruksien ikävimmistä piirteistä on, kun esimerkiksi henkilö x kirjautuu sähköpostiin, syöttäen ”käyttäjätunnuksen” ja ”salasanan”, niin samanaikaisesti tietokoneessa oleva virus tallentaa syötteet ylös muistiin, jotka näin viruksen laatija/tekijä saa haltuunsa. Toinen ikävä viruksien piirre on, kun lähettävät roskapostia sähköpostitse tietokoneen omistajan nimellä. (Korpela 2005, 63)

Ongelmia aiheuttaa myös se, että virukset kopioivat itseään tietokoneen muistiin, jolloin rasittavat tietokonetta täysin resurssein, joka jumiuttaa tietokoneen täysin. Virukset voivat sekoittaa tietokoneessa olevan tietojärjestelmän niin pahasti, että kone ei välttämättä enää käynnisty ollenkaan tai, jos käynnistyy, niin hyvin hitaasti. Yksi todella ikävä piirre on myös se, kun ollaan internet yhteydessä, voi ulkopuolinen henkilö saada tietokoneen haltuunsa esim. tietoturva-aukkoja hyödyntämällä ilman, että käyttäjä huomaa mitään. Useimmiten koneen hidastuminen on selvä signaali siihen, että kaikki ei ole hyvin ja olisi syytä havahtua selvittämään ongelmaa. (Korpela 2005, 63-64)

Mitä madot ovat?

Madot ovat ohjelmia, jotka pyrkivät leviämään tietokoneesta toiseen tai aiheuttamaan tuhoa ”kopioimalla” itseään mahdollisimman moneen paikkaan kyseiselle tietokoneelle. Toisin kuin virukset, madot eivät piiloudu tiedoston tai dokumentin sisään. (Kuivanen 2005)

Miten madot leviävät?

Leviävät verkon välityksellä, käyttäen hyväkseen järjestelmän tietoturva-aukkoja, ohjelmistovirheitä ja sähköpostin liitetiedostoja. Voivat myös käyttää hyväkseen internet-selaimen tai tietokoneella käynnissä olevan ohjelman tietoturva-aukkoa, levitäkseen. (Kuivanen 2005)

Mitä haittoja madot aiheuttavat?

Häiritsevät tietojärjestelmien toimivuutta, tukkimalla muistialueita. Madot pyrkivät usein pääsemään tietokoneeseen, käyttämällä järjestelmän tietoturva-aukkoja hyväksi ja asentamalla takaporttiohjelman, jolloin ulkopuolinen saa koneen hallintaan. (Kuivanen 2005)

3.2.2 Hakkerit

Mitä hakkerit ovat?

Hakkerit eli tietomurtajat etsivät suojaamattomia tietoturva-aukkoja sisältäviä tietokoneita verkosta ja löydettyään sellaisen, asentavat sinne ns. takaporttiohjelman. Ohjelman avulla hakkerit pystyvät hallitsemaan konetta ikään kuin se olisi heidän omaisuutta. (Tietoturvaopas 2008 1)

Mitä haittoja hakkerit aiheuttavat?

Voivat saada haltuunsa tiedostoja, luottokorttinumeroita, salasanoja ja muita henkilökohtaisia tietoja, jos saavat tietokoneen hallintaan takaportti-ohjelman avulla. (Tietoturvaopas 2008 1)

3.2.3 Vakoiluohjelmat

Mitä vakoiluohjelmat ovat?

Ohjelmia, jotka tarkkailevat käyttäjän internet-surffailua ja keräävät tietoa mm. siitä, millä sivustoilla käyttäjä kulloinkin vierailee ja mitä näppäinpainalluksia painaa.

Miten vakoiluohjelmat leviävät?

Voivat levitä ja tarttua tietokoneeseen ohjelmiston ”asennuksessa” tai internet surffailun aikana. Hyvänä signaalina vakoiluohjelman pesiytymisestä tietokoneelle voidaan pitää sitä, jos tietokoneen näytölle alkaa tulla erilaisia mainoksia, kesken internetissä surffailemisen. (Järvinen 2006, 99–100)

Mitä haittoja vakoiluohjelmat aiheuttavat?

Voivat saada haltuunsa käyttäjätunnuksia, salasanoja, henkilötietoja, luottokorttitietoja ja kovalevyllä olevia tietoja, jotka vakoiluohjelma ohjaa eteenpäin ulkopuoliselle taholle. (Järvinen 2006, 99–100)

3.2.4 Haittaohjelmat

Mitä haittaohjelmat ovat?

Ohjelmia, joiden tarkoituksena on aiheuttaa haittaa ja vahinkoa tietokoneelle. Haittaohjelmia ovat mm. verkkomadot, rootkitit, botit, näppäimistökaapparit, modeemikaapparit, troijalaiset, takaportit sekä mainosohjelmat.

Miten haittaohjelmat leviävät?

Leviävät tietokoneelle pääsääntöisesti sähköpostin liitetiedostojen, käyttöjärjestelmässä tai internet-selaimessa olevien tietoturva-aukkojen, internet-sivuilla esiintyvien ActiveX – komponenttien tai muiden verkosta ladattavien ohjelmien mukana. Usein ohjelmat etsivät tietoturva-aukollisia eli suojaamattomia tietokoneita verkosta ja löydettyään sellaisen, asentavat takaporttiohjelman tietokoneelle. (Järvinen 2006, 79 – 81, 88)

Mitä haittoja haittaohjelmat aiheuttavat?

Suurin osa haittaohjelmista, kuten verkkomadot, botit, troijalaiset ja takaporttiohjelmat pystyvät hallitsemaan tietokonetta kuin omaansa ja samaan haltuunsa arkaluontoisia henkilötietoja. (Järvinen 2006, 88)

Troijalaiset voivat naamioitua myös normaalia ohjelmaa muistuttaviksi, sisältäen mitä tahansa. Tietokoneen kiintolevy voi olla pahimmassa tapauksessa mennyttä. (Tietoturvaopas 2008 2)

Mainosohjelmien tarkoituksena on puolestaan houkutella käyttäjä tietylle sivustolle. Mainosohjelmien luokittelu on vaikeaa, koska tulevat usein ilmaisohjelmien kylkiäisenä. (Tietoturvaopas 2008 2)

Haittaohjelmiin kuuluvat myös rootkitit, joiden havaitseminen on vaikeaa virustorjuntaohjelmille sekä tietokoneen käyttäjälle. Ohjelmia on havaittu mm. laillisten kopiosuojausten toteuttamisvälineenä sekä bot – ohjelmien piilotusvälineenä. (Tietoturvaopas 2008 2)

Mistä tunnistaa haittaohjelman?

Signaalina voi pitää mm. koneen hidastumista, internet-sivujen vaihtumista tai mainosten avautumista selaimessa itsekseen tai selaimen kaatumista. Lisäksi hyvänä signaalina voi pitää tietokoneen täyttä kuormitusta 100 %:sesti tai tietokoneen epänormaalia toimintaa. (Järvinen 2006, 77-78)

3.2.5 Roskaposti

Sähköpostia, jonka lähettää ei tunneta ja viestin sisältö on hyvin epämääräistä sekä alkaa usein otsikolla RE: jotain. Roskaposti on massasähköpostia, jota ei ole kenellekään

erityisesti kohdennettu, vaan pyrkii täyttämään ihmisten sähköpostin ja tukkimaan sitä kautta sähköpostijärjestelmiä. (Oulun Yliopisto 2009)

3.2.6 Huijaukset

Mitä huijaukset ovat?

Huijaukset ovat järjestelmällistä rikollistoimintaa eli tietojen kalastelua (phishing).

Miten huijaukset toteutetaan?

Toteutetaan lähettämällä massasähköpostia ihmisille maakohtaisen ”maakoodin” perusteella tai väärentämällä aidonnäköiset verkkosivustot. (Järvinen 2006, 274)

Mitä haittoja huijaukset aiheuttavat?

Huijauksilla pyritään keräämään verkossa liikkuvien ihmisten verkkopankkiin ja erilaisiin muihin verkkopalveluihin liittyviä käyttäjätunnuksia, salasanoja ja muita henkilökohtaisia tietoja.

Nigerialaiskirjeet yrittävät saada huijattua ihmisiltä suuria rahasummia esim. sähköpostitse. Kirjeissä luvataan suurta rahasummaa ihmiselle, jos toimii ohjeiden mukaan ja maksaa tietyn rahasumman tiettyyn päivämäärään mennessä.

Ketjukirjeissä puolestaan luvataan jotakin tapahtuvan ihmiselle tietynajan kuluessa (onnea tai menestystä tai mainetta jne.), jos laittaa kirjeen eteenpäin esim. 10 tuntemalleen henkilölle. Todellisuudessa tästä aiheutuu suurta haittaa.

3.2.7 Tietojen katoaminen

Tietojen katoaminen on hyvin yleinen uhka, koska tietokoneen kiintolevy ei ole ikuinen, vaan voi yhtäkkiä hajota monesta syystä. Kiintolevyllä olevat tärkeät tiedostot voivat hävitä/tuhoutua oman huolimattomuuden seurauksena. On myös mahdollista, että tietokone varastetaan, jolloin tiedot ovat mennyttä sekä väärissä käsissä. (Tietoturvaopas 2008 3)

3.3 Suojautuminen tietoturvauhkia vastaan

Seuraavassa on käyty aiheittain läpi asioita, joiden pitäisi olla kunnossa, jotta edellä mainituilta tietoturvauhkilta voidaan pysyä suojassa.

3.3.1 Käyttöjärjestelmä ja tietoturvapäivitykset

Tietokoneen ydin eli järjestelmä, jonka päällä kaikki muut ohjelmat toimivat. Käyttöjärjestelmiä on useita erilaisia, jopa eri versioita käyttöjärjestelmien sisällä, kuten esimerkkinä Windows, johon tässä keskitytään.

Kun uusi käyttöjärjestelmä on asennettu tietokoneeseen, tulisi huolehtia, ettei tietokone ole liitetty verkkoon eli ”verkkojohto irti”. Jos löytyy useampia tietokoneita, voi hakea toisella tietokoneella tarvittavat tietoturvapäivitykset internetistä esimerkiksi cd-, dvd- levylle tai USB - muistitikulle, josta sitten asentaa tietokoneeseen, joka ei ole verkkoon kytkettynä.

Windows XP:ssä tai Vistassa voi käyttää mukana tulevaa palomuuria sillä aikaa, kun lataa internetistä uusimmat tietoturvapäivitykset käyttöjärjestelmään liittyen. Tietoturvapäivitysten automaattipäivitys on oletuksena päällä, jolloin järjestelmä ilmoittaa uusista tietoturvapäivityksistä, kun ovat saatavilla ja mahdollisesti asentaa ne. Tietoturvapäivitykset tulisi kuitenkin ladata aina itse ”manuaalisesti”, jolloin varmistuu siitä, ettei päivityksen mukana tule mitään haitallista/ylimääräistä, tietokoneelle.

Tietoturvapäivitykset on syytä pitää ajan tasalla eli ladata aina uusimmat päivitykset kun on saatavilla, koska tukkivat käyttöjärjestelmästä löytyneet tietoturva-aukot ja näin parantavat käyttöjärjestelmän turvallisuutta.

Vähemmällä vaivalla pääsee, jos on mahdollisuus siirtyä toisen käyttöjärjestelmän käyttöön, (Linux tai Macintosh), koska ovat huomattavasti turvallisempia jo oletuksena.

3.3.2 Virustorjunta

Ohjelma, joka suojaa erilaisilta viruksilta ja madoilta. Toimii tietokoneen taustalla ”estäen” viruksien pääsyn tietokoneeseen, kun tietokone on verkkoyhteydessä.

Käyttäjälle ohjelman toiminta ilmenee tilanteissa, kun virus on löytynyt joltain www-sivulta tai tiedostosta, jolloin näyttöruudulle ponnahtaa ”varoitusikkuna”, jossa virustorjuntaohjelma kysyy käyttäjältä mitä virukselle tehdään eli tuhotaanko, siirretäänkö karanteeniin vai tuhotaanko myöhemmin seuraavan tietokoneen käynnistyksen yhteydessä. Jos virus on löytynyt www-sivulta, niin ohjelma kehottaa käyttäjää lopettamaan yhteyden kyseiseen www-sivuun välittömästi. (Korpela 2005, 65)

Hankinta ja asentaminen

Hankkiessa virustorjuntaa, tulisi vertailla tunnettujen ja muiden käyttäjien keskuudessa hyväksi havaittuja ohjelmia, jotta varmasti löytää itselleen parhaiten toimivan ohjelman. Ohjelman keveyteen tulisi panostaa, jotta ohjelma ei häiritse varsinaista tietokoneella työskentelyä. Virustorjuntaohjelma voidaan ostaa joko kaupasta tai internetin verkkokaupasta. Lisäksi on tarjolla ilmaisia virustorjuntaohjelmia, joita voidaan ladata internetistä.. Usein uuden tietokonepaketin mukana saattaa tulla virustorjuntaohjelmisto. (Korpela 2005, 65 - 66) Ilmainen ohjelma riittää aivan mainiosti erityisesti koti – ja opiskelukäyttöön.

Kun ohjelma on hankittu, se täytyy asentaa. Asennuksen loppuvaiheessa ohjelma ehdottaa virustietokannan päivitystä, jolloin tulisi ladata uusimmat päivitykset ohjelmaan. Tämän jälkeen tulee laittaa ohjelman asetukset kuntoon ennen varsinaista käyttöä, johon apua löytyy ohjelman manuaalista, joka on tullut ostopakkauksessa ja on myös katsottavissa/ladattavissa ohjelman WWW-sivuilta.

Milloin kannattaa suorittaa virustarkistus?

Virustorjuntaohjelma kannattaa ajaa säännöllisin väliajoin (viikoittain), jolloin varmistuu tietokoneen puhtaana pysymisestä. Ohjelman toimintakunto kannattaa myös tarkistaa, jos ei ole varmuutta sen toimivuudesta. Internetistä on ladattavissa viruksen kaltaisia vaarattomia testitiedostoja, joihin ohjelman tulisi reagoida, jos ohjelma toimii oikein.

3.3.3 Palomuuri

Ohjelma tai rautaratkaisu, joka tulee olla virustorjunnan ohella, koska toimivat ikään kuin yhteistyössä. Tässä keskitytään ohjelmistopohjaiseen ratkaisuun. Palomuuri pitää huolen siitä, että verkon kautta tulevat tietomurtoyritykset ja hyökkäykset tulevat estetyksi. Valvoo koneen sovelluksien ja porttien tietoliikennettä verkosta ulos- ja sisäänpäin sekä pitää koneen sovellukset toiminnassa estäen ulkopuoliset kuormitusyritykset. (Järvinen 2006, 105 -107)

Käyttäjälle palomuurin toiminta näkyy selkeimmin silloin, kun joku on yrittänyt skannata tietokonetta verkosta käsin, jolloin palomuuri antaa ilmoituksen, jossa kerrotaan mitä portteja on skannattu ja milloin sekä sen, että tunkeutumisyritys on estetty.

Hankinta ja asentaminen

Palomuuriohjelman voi joko ostaa kaupasta tai internetin verkkokaupasta tai ladata internetistä ilmaisohjelman. Palomuuri voi tulla myös tietokonepaketin mukana. Jos omistaa Windows Xp:n tai Vistan, voi käyttää toki käyttöjärjestelmän mukana tulevaa palomuuria, mutta rajallista konfigurointi mahdollisuuksista johtuen tässä keskitytään erilliseen palomuuriohjelmaan. (Järvinen 2006, 116)

Kun ohjelma on hankittu, tulee se ensitilassa asentaa koneelle. Tämän jälkeen on hyvä tarkistaa ohjelman oletusasetukset, ovatko ne omaan tietokoneen käyttötarkoitukseen sopivat eli sen mukaan, mitä yleensä tietokoneella tekee. Yleensä määritellään mitkä ohjelmat saavat mennä internetiin (ulospäin) ja mitkä saavat toimia tietokoneelle verkosta/internetistä (sisäänpäin). Asetuksien muokkaamiseen löytyy apua ohjelman manuaalista, joka löytyy joko ostopakkauksesta tai on katsottavissa/ladattavissa ohjelman WWW-sivuilta.

Päivitykset kuntoon

Palomuuri olisi hyvä pitää ajan tasalla eli päivittää aina, kun virallinen uusi versio on saatavilla. Korjaa usein palomuurista löydettyjä virheitä, parantaen suojaavuutta tai käytettävyyttä. Uudesta versiosta palomuuri ilmoittaa, kun sellainen on saatavilla, jos asetuksiin on merkitty ”ruksilla” kyseinen kohta.

Palomuurin pitävyyden testaaminen

Palomuurin pitävyys tulisi tarkistaa aina muutoksien jälkeen. Internetistä löytyy paljon testaukseen erikoistuneita sivustoja, jossa voidaan tarkistaa palomuurin pitävyys, jonka tuloksista saadaan raportti. (Järvinen 2006, 113–115)

Rautapalomuuri vs. ohjelmistopalomuuri

Palomuureja on sekä ohjelmistopohjaisia, että rautapohjaisia, jotka molemmat ovat toimivia ratkaisuja. Rautapuolen palomuureissa on se etu, että ne ovat heti tietokoneen käynnistysvaiheessa toiminnassa, kun taas ohjelmistopohjainen käynnistyy ohjelmien mukana, jolloin tietokone on periaatteessa muutaman minuutin suojaamattomassa tilassa, toki ohjelmistopalomuuria voi muokata käynnistymään ennen kuin tietokone yhdistyy verkkoon. (Järvinen 2006, 109–111) Ohjelmistopohjaiset ovat täysin riittäviä koti- ja

yksityiskäyttöön. Yksinkertaisin rautapalomuuriratkaisu on useimmissa WLAN – verkkobokseissa.

3.3.4 Muut ohjelmistot

Virustorjunta ja palomuuri eivät yksinään riitä suojaamaan erilaisilta verkossa pyöriviltä haitta- ja vakoiluohjelmilta. Tarvitaan lisäksi ohjelma, jonka toimintaperiaatteena on pitää kone puhtaana erilaisilta haitta- ja vakoiluohjelmilta.

Ohjelman hankinta ja asennus (maksullinen vs. ilmainen)

Ilmaisversioissa ei ole reaaliaikaista taustasuojausta suojaamassa tietokonetta aktiivisesti kokoajan, kuten maksullisessa versiossa. Jos taustasuojaus löytyy, niin se on rajoitettu toimimaan vain esimerkiksi 30 päivää, jonka jälkeen siirtyy rajoitettuun tilaan, jos lisenssiä ei osteta. Molempia versioita, ilmaisia ja maksullisia löytyy internetistä.

Kun ohjelma on ladattu, se asennetaan, jonka jälkeen ehdottaa uusimpien päivitysten asentamista, jotka tulisi ladata ja asentaa.

Milloin kannattaa suorittaa tarkistus?

Asennuksen jälkeen tulisi suorittaa täydellinen tietokoneen tarkistus, muulloin nopeampi tarkistus riittää, edellyttäen ettei tietokoneella ole ongelmia.

3.3.5 Internet-selain

Ohjelma, jonka avulla pystyy liikkumaan internetissä ja näkemään sivut graafisessa muodossa tietokoneen näyttöruudulla. Selaimista tunnetuin on Internet Explorer, jota ei kuitenkaan suositella käytettävän, selaimen heikon tietoturvan vuoksi. Tulisi käyttää turvallisempia selaimia, joita ovat mm. Mozilla Firefox ja Opera. Selaimia löytyy internetistä ohjelmien WWW - sivuilta. On suositeltavaa asentaa selaimen uusin ohjelmaversio aina, kun on saatavilla, koska korjaa mahdollisia puutteita ja parantaa selaimen tietoturvaa.

Asetuksien määrittäminen

Selaimen asetuksiin tulisi kiinnittää huomiota ainakin seuraavasti. Evästeiden kohdalla tulisi miettiä, mille sivustoille on tarve sallia evästeet ja evätä sen mukaan kaikilta muilta osin evästeet. Sivustot voidaan myös jakaa ryhmiin ”luotettavat sivustot” sekä ”rajoitetut sivustot”. (Korpela 2005, 49-52).

Javan sekä Javascriptin käytön salliminen ja estäminen, on syytä määritellä sivustokohtaisesti aina tarpeen mukaan. Tähän voidaan käyttää myös javascriptin kontrollointiin kehiteltyjä lisäosaohjelmia, ainakin Mozilla Firefox selaimeen löytyy. Lomakkeisiin, hakupalkkeihin sekä sivustoille kirjautumiseen kirjoitettujen salasanojen ja tietojen tallennusta ei tulisi pitää päällä. On suositeltavaa estää ponnahdusikkunat ”pop-up” ja sallia ne aina sivustokohtaisesti, aina tarpeen mukaan, jolla estetään valemainokset sekä virheilmoitukset, joihin törmätessä voisi olla tuhoisat seuraukset.

Lisäksi on suositeltavaa määritellä yksityisyystietojen asetukset niin, että pyyhkiytyvät aina automaattisesti internet-selaimen sulkeutuessa, mm. sivuhistoria, latauslista, tallennetut lomaketiedot, väliaikaistiedostot, evästeet, tallennetut salasanat ja todennetut istunnot. Näin parannetaan selaimen turvallisuutta, kun ei tietokoneelle tallennu internet-surffailun jälkiä, joka on tärkeää etenkin julkisissa paikoissa, tietokoneilla asioitaessa.

3.3.6 Sähköposti

Sähköposti on perinteinen sosiaalisen kanssakäymisen kommunikointiväline, johon suurimpana uhkana liittyy roskaposti, josta tarkemmin luvussa 3.2.5.

Miten roskaposti voidaan estää?

Roskapostia välttääkseen tulisi kytkeä sähköpostipalvelusta suodattimet päälle. Suodatin olisi turvallisinta määritellä niin, että sallii vain yhteyshenkilöluettelossa olevilta henkilöiltä sähköpostin vastaanottamisen. Sähköpostin asetuksia kannattaa muutenkin muuttaa turvallisemmaksi eli on mietittävä, mitä tietoja halutaan sähköpostiviestin vastaanottajan näkevän, sähköpostiviestin saadessaan. Omaa sähköpostiosoitetta ei tulisi koskaan laittaa julkisesti muiden nähtäville internetissä. (Korpela 2005, 155)

Sähköpostiviestissä olevia linkkejä, jotka sisältävät liitetiedostoja, ei tulisi avata missään tapauksessa. On suositeltavaa olla vastaamatta ketjuviesteihin, kiertokirjeisiin ja huijausviesteihin, vaikka näyttävät usein aidoilta, mutta todellisuudessa aiheuttavat vain suurta haittaa.

Kannattaa myös olla epäileväinen kaikenlaisia sähköpostiviestejä kohtaan, jolloin välttyy monelta murheelta. Jos lähettäjää ei ole mainittu, tulee viestiin suhtautua varauksella. On suositeltavaa olla avaamatta viestejä, joissa on ohjelmiin viittaavia liitetiedostoja esim. COM, EXE, SHS, PIF, VBS, DLL tai liitetiedosto koostuu kaksiosaisesta

tiedostopäätteestä (joku.JPG.VBS tai jotain.DOC.EXE), koska sisältävät useimmiten viruksen.

3.3.7 Käyttäjäoikeudet

Käyttäjäoikeudet suojaavat sitä, mitä kaikkea käyttäjä voi tehdä tietokoneellaan. Oletuksena asennetussa käyttöjärjestelmässä on pääkäyttäjän (administrator) oikeudet ja ”käytöstä poistetut” vieraan (guest) oikeudet. Käyttäjäoikeudet jaotellaan ryhmiin, jotta jokaiselle käyttäjälle ei tarvitsisi erikseen määritellä oikeuksia. Muita ryhmiä ovat mm. tehokäyttäjät (power users) ja rajoitetut käyttäjät (users). (Järvinen 2006, 196)

Pääkäyttäjät ryhmään kuuluvalla käyttäjällä on täydet oikeudet tietokoneeseensa ja käyttöjärjestelmän käyttöön, kun taas rajoitetulla käyttäjällä on vain oikeus käyttää ohjelmia ja tallentaa tuotoksiaan, mutta ei ole oikeutta asentaa, eikä tallentaa mitään käyttöjärjestelmän juureen tai muihin kriittisiin paikkoihin. Tämä rajoitus estää mm. sen, jos käyttäjä erehtyy käynnistämään viruksen tai haittaohjelman, niin tästä ei voi aiheutua rajoitetuin käyttöoikeuksin käynnissä olevalle järjestelmälle ja sitä kautta tietokoneelle ongelmia. (Järvinen 2006, 196)

Turvallisinta olisi luoda pääkäyttäjätilin rinnalle rajoitettu käyttäjätili, jota käyttää arkipäiväiseen työskentelyyn ja pääkäyttäjätiliä vain silloin, kun tarvitsee asentaa ohjelmia. Ohjelmia voidaan asentaa myös rajoitetuin oikeuksin, kun tiedetään pääkäyttäjän tunnus ja salasana. Käyttäjäoikeuksien turvallinen määrittely parantaa tietokoneen tietoturvaa merkittävästi.

3.3.8 Salasana

Salasana suojaa tietokoneelle kirjautumista ja internetin palveluja, kuten Facebookin ja sähköpostin henkilökohtaisia tilejä, joita käyttääkseen on tiedettävä käyttäjätunnuksen lisäksi salasana. Salasana on syytä määritellä hyvin tarkkaan, jotta siitä saadaan riittävän turvallinen. (Microsoft 2006)

Millainen on hyvä salasana?

Hyvä salasana on riittävän pitkä eli vähintään 8 merkkiä pitkä, mutta suositeltu on 14 merkkiä tai sitä pidempi. Salasanassa tulisi esiintyä numeroita kirjaimien lisäksi. Pitkä lause ”välilyönnein” eroteltuna on hyvä salasana, koska on helppo muistaa ja, jota on hyvin vaikea ulkopuolisen saada selville. Hyvä tapa on myös käyttää erilaisia sallittuja symboleja

sekä isoja ja pieniä kirjaimia sekaisin numeroiden kanssa. On hyvä selvittää aina internetissä palveluun rekisteröityessä millaiset ehdot rajoittavat salasanan muotoa ja sen mukaan tehdä mahdollisimman turvallinen salasana. (Microsoft 2006)

Milloin salasanaa tulisi vaihtaa?

Salasana on suositeltavaa vaihtaa vähintään pari kertaa vuodessa. Vaihtovälin tarpeellisuus korostuu, jos on päivittäin käytössä olevia palveluita tai käytetään palveluja paljon julkisilta tietokoneilta käsin (kirjasto, koulu, työpaikka jne.). Riittävä salasanan vaihtoväli luo turvallisuutta salasanalle, koska vaikeuttaa salasanan selvitystä. (Microsoft 2006)

Salasanat palvelukohtaisesti?

Turvallisuuden maksimoimiseksi tulisi jokaiseen palveluun olla aina oma erillinen salasana. Tämä turvaa sen, jos ulkopuolinen henkilö saa tietää yhden salasanan, niin se ei käy kuin vain yhteen palveluun. Kun taas, jos on yksi ja sama salasana kaikkiin käytettäviin palveluihin, niin seuraukset ovat paljon mittavammat, koska yhdellä salasanalla pystyy ulkopuolinen henkilö hallitsemaan kaikkia palveluita.

3.3.9 Yksityisyyden parantaminen

Kannattaa seurata tietoturvaan liittyviä uutisia internetistä, televisiosta, radiosta ja muista tiedotusvälineistä. Erityisesti tulisi olla hereillä uutisien suhteen, jotka koskevat tietoturvauhkia ja toimia niissä suositeltujen ohjeiden mukaisesti. Jos jotain ei tiedä, niin aina kannattaa kysyä paremmin asiasta tietäviltä esim. ystäviltä/kavereilta ja tutuilta.

Internetissä surffaillessa ei kannata mennä epäilyttäville sivustoille, eikä varsinkaan avata jokaista eteen tulevaa linkkiä. Tietynlainen terve maalaisjärki ja epäileväisyys kannattaa pitää mielessä internetissäkin eli tulisi suhtautua epäilevästi sivustoihin, jotka houkuttelevat, mutta ovat kuitenkin tietyllä tapaa epäilyttäviä ja normaalista poikkeavia, tällöin tulisi siirtyä välittömästi toiselle internet-sivustolle, vahinkojen ehkäisemiseksi.

Erityisen tarkkana tulisi olla paikoissa, joissa käsitellään luottamuksellisia henkilötietoja, joista esimerkkinä verkkopankki. Kyseisissä paikoissa varoitetaan mahdollisista huijauksista palvelun pääsivulla ja kerrotaan millaiselta sivun tulisi näyttää, mutta koskaan ei voi olla 100 % varma sivun luotettavuudesta. Esimerkiksi verkkopankkipalvelun luottamuksellisuutta/aitoutta kuvaa ”lukossa” olevan lukon kuva, sivuston oikeassa alakulmassa, jolloin sivuston pitäisi olla turvallinen. Jos haluaa kuitenkin täysin varmistua

sivuston turvallisuudesta, voi lukon avata hiirellä, jolloin näkee onko sivusto oikeasti varmennettu ja suojattu eli turvallinen. Toimenpiteet vievät aikaa, mutta parempi varmistaa, kuin katua jälkeenpäin joutuneensa ulkopuolisen tahon uhriksi arkaluontoisten tietojen suhteen.

Huijaukset, kuten nigerialaiskirjeet ja kiertokirjeet tulisi tuhota saman tien, jolla estetään vahinkojen syntyminen.

Internetissä liikkuessa tulisi miettiä hyvin tarkkaan, mitä tietoa on turvallista jakaa muiden nähtäville. Erilaiset palvelut, kuten sähköposti, Facebook, verkkokaupat jne. keräävät jokaisesta käyttäjästään henkilötietoja jo palveluun rekisteröityessä, jonka takia on suositeltavaa lukea palvelua tarjoavan www-sivulta käyttäjän tietosuojaa käsittelevät ehdot, jotka löytyvät käyttäjä- tai sopimusehdoista, palvelusta riippuen. Ehtoihin tulisi tutustua ennen palveluun rekisteröitymistä, joista selviää mitä tietoja palvelu tarvitsee rekisteröityvältä käyttäjältä ja mihin niitä käytetään sekä millä perusteella tietoja mahdollisesti luovutetaan muille osapuolille. Jos ehdot eivät miellytä, ei palveluun tulisi rekisteröityä, palvelun käytöstä puhumattakaan. (MBnet 2005)

Lisäksi suositut blogit ja keskustelualueet ovat riskialttiita paikkoja, koska niissä on kävijöitä päivittäin. On suositeltavaa, ettei henkilötietoja laiteta muiden nähtäville (nimi, sähköposti, osoite, puhelinnumero ja muut arkaluontoiset tiedot). Sähköpostitse tapahtuviin tietojen kyselyihin ei tulisi vastata, eikä luovuttaa tietoja, koska mikään viranomainen tai julkinen palvelu ei kysele henkilötietojen päivitystä, käyttäjätunnuksia tai salasanoja sähköpostitse. Internetissä liikkumisen jälkeen, selaimen suljettua tulisi poistaa väliaikaiset tiedostot, josta tarkemmin kohdassa 3.3.5.

3.3.10 Varmuuskopiointi

Varmuuskopioinnilla varmistetaan, että tärkeät tiedot ovat tallessa erilaisten uhkien/ongelmatilanteiden varalta esim. tiedostojen katoamiset. Ihmiset ajattelevat helposti, että ei sitä omat tiedot voi mihinkään kadota/joutua, mutta todellisuus on juuri toisenlainen. Tietokoneita käytetään päivittäin ja erilaiset komponentit, kuten ”tietojen tallennuspaikka” eli kiintolevy joutuu päivittäiseen rasitukseen. Kiintolevy ei ole ikuinen ja voi hajota vuosien saatossa vanhuuteen tai muuten vaan esimerkiksi ulkoisesta virtapiikistä ”ukkonen”. Usein rikkoutuminen tapahtuu juuri silloin, kuin sitä vähiten odottaa. Tällöin on myöhäistä toimia, jos varmuuskopiota ei ole.

Tietokone voi joutua myös varkaustilanteisiin, tulipaloon jne., jolloin tiedot ovat menetetty ainakin osittain. Rikkoutuneelta tai epänormaalisti toimivalta kiintolevyltä voi saada jälkeenpäin luultavammin osan tiedoista pelastettua asiantuntevan huollon toimesta, joka vaatii taloudellisia investointeja. Yksi yleisimmistä ongelmista on, kun käyttöjärjestelmä menee jumiin ja ei tahdo käynnistyä. Tässä tilanteessa joutuu kaikki asentamaan uudelleen, joka vie paljon aikaa. Jos varmuuskopio käyttöjärjestelmästä löytyy, säästytään tältä. (Korpela 2005, 95-96)

Mihin varmuuskopiot voidaan tehdä?

Varmuuskopiointi voidaan suorittaa kopioimalla tietoja toiselle sisäiselle IDE, SCSI tai SATA - kiintolevylle, USB -muistille, ulkoiselle USB -kiintolevylle, polttamalla CD tai DVD – levylle tai hieman ajasta jääneelle nauhavarmistukselle. Näistä CD ja DVD -levyt ovat suosittuja ja nykyään etenkin USB - muisti, joka on keveyden ja liikuteltavuuden ansioista aivan omaa luokkaansa ja suurempien muistikapasiteettien ansioista soveltuu erinomaisesti varmuuskopiointiin, 1Gb aina 16 Gb asti. (Korpela 2005, 97)

Toinen kiintolevy tarjoaa kuitenkin enemmän tallennustilaa (sisäinen tai ulkoinen). Sisäinen kiintolevy on kiinni tietokoneessa, jolloin tiedon kopioiminen onnistuu toiselta kiintolevyltä toiselle tai jollain järjestelmällä esim. RAID. Ulkoisen ”USB” kiintolevyn etuja on ehdottomasti sen liikuteltavuus ja, että se voidaan liittää tietokoneeseen ns. lennossa eli tietokoneen ollessa päällä. USB – kiintolevyjen hinnat alkavat olemaan edullisia, joten USB – kiintolevy on suositeltava sijoitus varmuuskopiointiin. Nauhavarmistuksia käytetään lähinnä yrityksissä, koska varmistusohjelmisto sekä nauhat ja laitteet maksavat paljon.

Varmuuskopiointiin on olemassa erilaisia ohjelmia/järjestelmiä, joiden avulla voidaan helposti määritellä esim. viikoittain otettavat varmuuskopiot tärkeistä tiedoista/tiedostoista. Yksi järjestelmä on RAID, joka on käytettävissä tietokoneissa, joissa on emolevyllä RAID-piiri sekä vähintään 2 kiintolevyä. RAIDissa kiintolevyjen tulisi olla mieluiten samanlaisia merkiltään/malliltaan sekä kooltaan. RAIDissa on 5 eri tasoa, joista jokainen toimii hiukan eri tavoin. Esimerkkinä yksi näistä tasoista toimii niin, että toinen kiintolevy peilaa toista kiintolevyä jatkuvasti varmistaakseen, että molemmilla kiintolevyillä on samat tiedot kokoajan. Ohjelmat joilla voidaan ajastaa ja ottaa varmuuskopiointeja on markkinoilla useampia, mutta hinnatkin ovat sen mukaiset. Yksityiskäyttöön riittää mahdollisimman helppokäyttöinen ja edullisella hinnalla varustettu ohjelmisto esim. Norton Ghost.

Milloin varmuuskopiointi kannattaa?

Jos tietokoneella on paljon omia tärkeitä tiedostoja/tietoja (dokumentteja, kuvia, jne.) kannattaa varmuuskopioita ottaa säännöllisesti esim. USB – muistitikulle. On myös suositeltavaa ottaa varmuuskopio koko järjestelmästä, kun on asentanut käyttöjärjestelmän ja siihen tarvittavat tietoturvapäivitykset, palomuurin, virustorjunnan sekä muut päivittäiseen käyttöön tarvittavat ohjelmat ja on käyttänyt konetta muutama päivän, kunnes tuntee kaiken toimivan normaalisti.

Mihin varmuuskopio auttaa?

Varmuuskopio auttaa ongelmatilanteisiin, esimerkiksi, kun käyttöjärjestelmä ei käynnisty tai toimii muuten epänormaalisti ja antaa erilaisia virheilmoituksia, jolloin normaalisti pitäisi formatoida/tyhjentää koko kiintolevyn osio sekä asentaa kaikki alusta alkaen, joka vie aikaa paljon. Jos on olemassa varmuuskopio käyttöjärjestelmästä, pystyy koko käyttöjärjestelmän palauttamaan toimivaan ajankohtaan 20 – 45 minuutissa.

3.4 Facebook

3.4.1 Historia

Facebookin historia ulottuu vuoden 2004 helmikuuhun, jolloin Harvardin yliopistossa pääsuunnittelija Mark Zuckerberg yhdessä Dustin Moskovitzin, Chris Hughesin ja Eduardo Saverin avustuksella laittoi palvelun alulle. (Facebook 2009)

Alkujaan Facebook oli tarkoitettu ainoastaan yliopiston sisäiseen käyttöön, mutta suosiosta johtuen, käyttöä päätettiin laajentaa Stanfordin, Columbian ja Yalen yliopistoihin. Vuoden 2004 lopussa käyttäjämäärä lähenteli jo miljoonaa. Elokuussa 2005 sosiaalipalvelun nimi muuttui thefacebook.com nimestä Facebook nimeen ja jatkoi samalla laajentumistaan eri yliopistoihin ja korkeakouluihin Yhdysvalloissa, päätyen lopulta myös ulkomaisiin kouluihin. Facebookin käyttäjämäärä oli 5,5 miljoonaa vuoden 2005 lopussa. (Facebook 2009)

Vuonna 2006 käyttäjäkohderyhmää laajennettiin ensin työyhteisöille ja myöhemmin kaikille avoimeksi, jonka seurauksena käyttäjämäärä kasvoi entisestään, ollen yli 12 miljoonaa vuoden lopussa. (Facebook 2009) Suomessa Facebookin käyttö alkoi vuoden 2007 lokakuussa ja oma suomennos saatiin vuonna 2008. (Facebook 2009)

Facebookin suosio on vain jatkanut kasvua ja käyttäjämäärä on nykypäivänä yli 150 miljoonaa, kun mukaan lasketaan viimeisen 30 päivän aikana sosiaalipalvelussa käyneet. (Facebook 2009 -1)

3.4.2 Yleisesti ja toimintaperiaate

Facebook on suosittu sosiaaliverkkopalvelu, jota miljoonat ihmiset käyttävät päivittäin, lähinnä pitääkseen yhteyttä kavereihinsa ja tuttaviinsa.

Palveluun rekisteröityminen on täysin ilmaista, tarvitaan vain voimassa oleva sähköpostiosoite. Rekisteröitymisen jälkeen palvelu toimii hyvin yksinkertaisesti eli kirjaudutaan rekisteröidyllä sähköpostiosoitteella ja siihen määritellyllä salasanalla www.facebook.com sivustolla, jonka jälkeen pääsee luomaan profiilia.

Henkilökohtaiset tiedot eivät näy kuin vain käyttäjälle ja lisäksi voidaan määritellä kenelle mitäkin tietoja näkyy eli itselle, ystäville ja muille käyttäjille.

Profiilin luonnin jälkeen voidaan tehdä palvelussa kaikkia seuraavia asioita.
Voidaan pitää yhteyttä ystäviin yksityisin pikaviestein tai jättämällä viestejä kirjoitustauluihin tai Javaan pohjautuvan Chat – keskusteluikkunan avulla.

Facebook mahdollistaa liittymisen erilaisiin ryhmiin (esim. tietyn asian puolesta), erilaisten tapahtumien selailemisen ja liittymisen niihin. Palvelussa voidaan lisäillä erilaisia virtuaalisovelluksia, haastaa kavereita erilaisissa kysymysvisailuissa, peleissä ja nähdä kuinka sijoitutaan suhteessa kavereihin sekä muihin Facebook käyttäjiin, jotka ovat osallistuneet kyseiseen visailuun/peliin. Lisäksi kavereiden kesken on mahdollista jakaa kuvia, videoita, youtube – videolinkkejä sekä virtuaalilahjoja, kuten halauksia, onnitteluja, kukkia ja nalleja. Facebookin mahdollisuudet ovat hyvin laajat, jossa voi tehdä asioita, kuten reaalimaailmassakin.

3.4.3 Yksityisyyden tietoturvauhat

Facebook on vahvassa roolissa internetin sosiaalisessa kanssakäymisessä, jolloin siihen liittyy valitettavasti yleisten tietoturvauhkien lisäksi myös ihmisten yksityisyyttä uhkaavia tietoturvauhkia. Yksityisyysuhat ovat tulleet jäädäkseen. (C. Abram, L. Pearlman 2008, 53)

Facebookin suurin uhka yksityisyyden suhteen on se, että ihmiset eivät kiinnitä riittävästi huomiota profiilia luodessa siihen, mitä tietoja on turvallista laittaa muiden näkyville. Ei mietitä kenelle tiedot oikeasti näkyvät, etenkin jos profiili on luokiteltu julkiseksi eli avoimena kaikille näkyväksi.

Toinen suuri uhka on se, kun hyväksytään kavereiksi sellaisia ihmisiä, joita ei oikeasti tunneta eli luotetaan sinisilmäisesti ihmisten olevan kunnollisia, kun halutaan välttämättä kasvattaa kaverilistaa mahdollisimman suureksi, mutta kaveri saattaa myöhemmin paljastua yksityisyyttä loukkaavaksi. Ei rajata profiilin näkyvyyttä riittävästi esim. ”rajatulla profiililla” eli ns. ei oikeiden kavereiden tai muiden tuntemattomien ihmisten osalta. Tämä on suuri uhka käyttäjän yksityisyydelle, koska tällöin kuka tahansa palvelua käyttävä ihminen voi saada kaikki käyttäjän jakamat tiedot haltuunsa.

Uhkana pidetään myös erilaisia houkuttelevia virtuaalisovelluksia, pelejä jne., joita käyttäjät lisäilevät joko itse tai kavereiden pyynnöistä/kehotuksista ja usein tiedostamatta sovelluksen tai pelin todellista tarkoitusperää ja turvallisuutta.

Uhkia aiheuttavat myös muutamat virukset (mm. koobface), jossa ongelmalliseksi tilanteen tekee se, että virukset tuntuvat vaihtelevan toimintatavoiltaan. (Iltasanomat, 2009) Tämän lisäksi on vielä kiertoviestit, joilla uhataan käyttäjän profiilin poistoa, jos ei lähetetä saatua viestiä eteenpäin 15 kaverille.

Lisäksi uhkia aiheuttavat myös vakoiluohjelmat, kuten ”Error Check System -ohjelma”, joka väittää korjaavansa profiilin katseluongelmaa kaverin osalta, jos käyttäjä asentaa ohjelman. Todellisuudessa ohjelma kerää vain tietoa käyttäjästä ja lähettää viestin käyttäjän kaikille kavereille. Toinen vakoiluohjelma puolestaan väittää viestissään, että käyttäjä on ilmiannettu Facebookin ylläpitäjille käyttäjäehtojen rikkomisesta, pyrkimyksenä saada käyttäjän tiedot haltuunsa. Jos käyttäjä asentaa viestissä olevan linkin kautta "My Account"- tai "Reported for Rule Breaking"-sovelluksen, niin ohjelma lähettää viestiä kaikille käyttäjän kavereille. (Digitoday 2009)

Viimeisimpänä on havaittu koobface viruksen uusi ja vakavampi aste. Käyttäjälle tulleessa viestissä on aidonnäköinen kaverin kuva ja nimi sekä linkki videoon. Tarkoituksena on houkutella käyttäjä avaamaan videon linkki, joka ohjaa käyttäjän suosittuun YouTube –

palveluun, jonka videoruudulla pyörii ”viesti”, kehottaen asentamaan Adobe Flash Player – päivityksen. Jos käyttäjä klikkaa install – valintaa, niin uusin Koobface – virus asentuu koneelle. Youtube – palvelun sivusto ei ole aito vaan tekaistu. (Digitoday 2009 -1)

Facebookin suurimmaksi ongelmaksi on muodostumassa valvonnan puute, joka näkyy auttamatta viruksien ja muiden huijauksien leviämisessä. Tämä on huomattu myös viruksia valmistelevien tahojen keskuudessa, jotka ovat selvittäneet keinot, joilla sosiaaliverkkopalveluissa voidaan viruksia ja haittaohjelmia levittää. Ongelma ydin on siinä, että Facebookin ylläpitäjät eivät tarkista riittävästi etukäteen palvelussa julkaistavia sovelluksia, johon ei auta Facebookin lanseeraama vapaaehtoinen ja maksullinen sovelluksien tarkistuspalvelu. (Digitoday 2009 -1)

Facebookin onneksi uhat näyttäisivät olevan vielä vain liikkeellä leviämistarkoituksessa, mutta tulevaisuudessa voidaan mitä suurimmalla todennäköisyydellä odottaa konkreettista haittaa aiheuttavia uhkia, jos Facebook ei kiinnitä paremmin huomiota sovelluksien tarkistuksiin. (Digitoday 2009 -1)

3.4.4 Suojautuminen yksityisyyden tietoturvauhilta

Facebookin yksityisyyden tietoturvauhilta suojautuminen alkaa tietokoneen perustietoturvasta huolehtimisella, josta on kerrottu tarkemmin luvussa 3.3. Tämä ei kuitenkaan itsessään välttämättä riitä, joten seuraavassa käydään läpi Facebookin yksityisyyden turvaamiseksi, parantavia asetuksia ja ohjeita.

Profiili (Profile)

Tällä kontrolloidaan sitä, kuka näkee profiilissa olevat tiedot (tilapäivityksen, videot, kuvat, yhteystilan (=offline/online), kaverit, kirjoitusseinän, yhteystiedot ja lisätyt ohjelmat. Tässä tulisi miettiä hyvin tarkkaan mitä tietoja halutaan profiilista näkyvän ja kenelle.
(C. Abram, L. Pearlman 2008, 55)

Haku (Search)

Tällä kontrolloidaan sitä, miten muut ihmiset näkevät profiilin, kun etsivät profiilia Facebookin hakutoiminnolla. Tulisi määritellä niin, että näkevät vain profiilin kuvan ja voivat lähettää vain kaveripyynnön. (C. Abram, L. Pearlman 2008, 55)

Uutis – ja mini-ikkuna (News feed ja Mini feed)

Tässä voidaan määritellä mitkä tapahtumat (kirjoitukset, kaverinlisäykset jne.) näkyvät profiilin seinässä ja mitkä vastaavasti kavereiden seinällä. On syytä miettiä, onko tapahtumatietojen näkyminen tarpeellista. (C. Abram, L. Pearlman 2008, 55)

Tökkäys, viesti ja kaveripyyntö (Poke, message ja friend request)

Tökkäys, viesti ja kaveripyyntö asetuksissa tulisi miettiä sitä, mitä tietoja haluaa näkyvän profiilista sellaisille ihmisille, jotka eivät ole kavereita tai eivät kuulu edes samaan verkkoon. Suositeltavaa olisi käyttää asetuksia, joilla rajoitetaan profiilin näkyvyys minimiin. (C. Abram, L. Pearlman 2008, 56)

Ohjelmat / virtuaalisovellukset (Applications)

Voidaan katsella ja kontrolloida sitä, miten kukin sovellus on yhteydessä profiilin tietoihin ja millaisia tietoja vaativat toimiakseen. Tulisi miettiä tarkkaan, mitkä sovellukset ovat varmasti luotettavia ja rajata sovellukselle luovutettavat tiedot mahdollisimman minimiin. (C. Abram, L. Pearlman 2008, 56)

Facebookin yksityisyyden parantaminen

Facebookissa kannattaa liittyä vain sellaisiin verkkoihin, joihin on itse yhteydessä ja joihin tuntee kuuluvansa (mm. koulu – ja työpaikkaverkot). Lisäksi tulisi määritellä profiilin tietojen näkyvyys vain samaan verkkoon kuuluville sekä kavereille, joka on jo oletuksena. (C. Abram, L. Pearlman 2008, 56–57)

Kannattaa ottaa käyttöön ”rajoitettu profiili / limited profile” ja määritellä sen asetukset kuntoon, jolla kontrolloidaan mitä tietoja rajoitetussa profiilista näkyy ”rajoitetusti” ja ketkä kaverit (kaverilistasta) kuuluvat rajoitetun profiilin piiriin. Rajoitetun profiilin asetuksia pääsee muokkaamaan ”profiili / profile” – asetuskohdasta. (C. Abram, L. Pearlman 2008, 57 - 58)

Facebookin yksityisyyden turvaamisen ydinajatuksena on se, että ei tulisi lisätä kavereiksi sellaisia ihmisiä, joita ei tunne ja joiden aikeista ei ole täysin varma. Kaverilistalta voidaan poistaa ihmisiä jälkikäteen, joka on suositeltavaa, jos vähääkään arveluttaa jonkun ihmisen aikeet. (C. Abram, L. Pearlman 2008, 57)

Lisäksi tulisi miettiä hyvin tarkkaan, mitä tietoja on turvallista laittaa itsestään näkyville ja kenelle nämä tiedot haluaa näkyvän. Tulisi ottaa selvää ja kiinnittää huomiota siihen, mitä tietoja virtuaalisovellukset todellisuudessa keräävät profiilista ja olisi syytä olla varma sovelluksien toimintatarkoituksista, ennen kuin lisäilee mitään. Kiertoviestejä ei tulisi lähettää eteenpäin, koska ovat useimmiten pelkkää huijausta, kehotuksista huolimatta.

Tulisi suhtautua epäilevästi sovelluksien lähettämiin viesteihin ns. vakoiluohjelmat, jotka väittävät, että käyttäjä olisi rikkonut Facebookin käyttäjäehtoja, koska tulee muistaa, että profiilin asioista tiedottaa vain Facebookin ylläpito henkilökohtaisella viestillä jokaiselle käyttäjälle erikseen. (Digitoday 2009)

Lisäksi tulisi suhtautua epäilevästi sovelluksien lähettämiin viesteihin, joissa väitetään, että kaverilla on ongelmia nähdä profiilia ja kehotetaan asentamaan jokin sovellus. Ei ole suositeltavaa asentaa mitään mitä kehotetaan, jos kehotus ei tule Facebookin ylläpidon suunnalta. Jos vakoilusovellus on kuitenkin tullut asennettua, tulisi ensitilassa vaihtaa profiilin salasana, sekä poistaa sovellus profiilin etusivun Applications/Sovellukset-valikon Edit/Muokkaa-linkin avulla. (Digitoday 2009)

Lyhyesti yhteenvetona, yksityisyyttä parantavaa paljon jo se, että asettaa yksityisyysasetukset Facebookissa mahdollisimman tiukalle ja jättää avaamatta epäilyttävät viestit. (Digitoday 2009 -1)

4 Tutkimuksen tavoitteet

Selvitetään, kuinka HAAGA-HELIASSA Pasilan toimipisteessä tietojenkäsittelyn ja liiketalouden koulutusohjelmassa aloittelevat ja lopettelevat opiskelijat suhtautuvat tietoturvaan eli kiinnittävätkö siihen huomiota käyttäessään internetiä sosiaaliseen kanssakäymiseen. Alikysymykset tässä tutkimustavoitteessa ovat

1. Miten opiskelijat huolehtivat oman tietokoneensa tietoturvasta?
2. Miten opiskelijat kiinnittävät huomiota omiin käyttäjätietoihin internetissä liikkuessaan?
3. Miten opiskelijat huolehtivat Facebookin yksityisyydestä?

Näitä kolmea alikysymystä tutkittiin seuraavista kahdesta näkökulmasta:
Onko eroavaisuuksia tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välillä? Onko eroavaisuuksia tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden välillä?

Tutkimuksessa ei oteta kantaa koulutusohjelmien sisällä oleviin eroihin aloittelevien ja lopettelevien opiskelijoiden välillä, koska odotusarvoisesti tästä ei luultavasti saataisi mitään uutta tietoa, koska koulutuksen edetessä opiskelijoiden suhtautumisen voidaan olettaa muuttuvan paremmaksi. Tästä johtuen tutkimuksessa selvitetään vain mahdollisia koulutusohjelmien välisiä eroavaisuuksia, vertailtaessa aloittelevia opiskelijoita keskenään ja lopettelevia opiskelijoita keskenään, jolla odotusarvoisesti saadaan konkreettista uutta tietoa. Perusoletuksena lähdetään siitä, että tietojenkäsittelyn opiskelijat suhtautuvat paremmin tietoturvaan liiketalouden opiskelijoihin nähden, erityisesti lopettelevien opiskelijoiden keskuudessa.

Lisäksi selvitetään mitä yleisiä tietoturvauhkia sosiaaliseen kanssakäymiseen voi liittyä ja mitkä uhkatekijät voivat mahdollisesti uhata Facebookin käyttäjän yksityisyyttä, jos tietoturvasta ei huolehdita. Tämän lisäksi käytiin läpi tarvittavia suojautumis- ja ennaltaehkäisymenetelmiä, joilla voidaan suojautua uhkatekijöiltä.

Tutkimuksessa selvisi, että yleisesti tietoturvauhkia aiheuttavat sosiaalisessa kanssakäymisessä erilaiset madot, virukset, hakkerit, vakoiluohjelmat, haittaohjelmat,

huijaukset, roskaposti sekä joissakin tapauksissa näiden seurauksena tietojen katoamiset. Suojautumismenetelmät yleisiltä tietoturvauhilta suojautumiseen, on kerrottu luvussa 3.3.

Tutkimuksessa selvisi myös, että Facebookin yksityisyyttä uhkaavat, ihmisten sinisilmäisyys profiilia kohtaan ja siihen liittyvien tietojen suhteen. Ei kiinnitetä huomiota siihen, millaista tietoa on turvallista laittaa profiiliin, eikä määritellä tarkasti kenelle nämä tiedot näkyvät, pahimmassa tapauksessa julkisesti. Hyväksytään kavereiksi ketä tahansa, tuntematta ihmisiä entuudestaan millään tavoin. Otetaan virtuaalisovelluksia (sovellukset, pelit jne.) käyttöön tiedostamatta virtuaalisovellusten käyttötarkoituksia ja mitä tietoja keräävät käyttäjästä toimiakseen. Luotetaan kiertokirjeviesteihin liian sinisilmäisesti. Näiden lisäksi uhkia aiheuttavat myös yleiset tietoturvauhkat, joista ainakin viruksia ja vakoiluohjelmia on löydetty Facebookista. Suojautumismenetelmät Facebookin yksityisyyden uhilta suojautumiseen, on kerrottu luvussa 3.4.4.

5 Tutkimusmenetelmät

Käytin erilaisia lähdeaineistoja selvittääkseni ”mitä yleisiä tietoturvauhkia sosiaaliseen kanssakäymiseen liittyy ja mitkä uhkatekijät voivat mahdollisesti uhata Facebookin käyttäjän yksityisyyttä” sekä millä suojautumis- ja ennaltaehkäisymenetelmillä voidaan suojautua näiltä uhilta.

Tutkimuksen pääselvityksen tein HAAGA-HELIAN tietojenkäsittelyn ja liiketalouden koulutusohjelmien aloittelevien ja lopettelevien opiskelijoiden suhtautumisesta tietoturvaan internetin sosiaalisessa kanssakäymisessä WEBROPOL – verkkolomakepalvelun avulla.

Mietin kysymyksiä pohjautuen tutkimuksen päätavoitteisiin (luku 4) niin, että kysymysten pohjalta saisin vastaukset päätavoitteeseen alikysymyksineen. Seuraavassa on valitsemani kysymykset kyselyyn (liite 5), joilla tutkimuksen päätavoitteiden alikysymyksiin vastauksia hain.

1) Miten opiskelijat huolehtivat oman tietokoneensa tietoturvasta?
(Mitä tietoturvaratkaisuja käytät säännöllisesti?, Miten suhtaudut tietoturvavaroituksiin?)

2) Miten opiskelijat kiinnittävät huomiota omiin käyttäjätietoihin internetissä liikkuessaan?
(Liittyykö mielestäsi sosiaaliseen kanssakäymiseen uhkia?, Millaisia merkkejä salasanasi sisältävät?, Kuinka pitkiä salasanasi ovat?, Kuinka usein vaihdat salasanan?, Vaihtelevatko salasanasi eri palvelujen kesken?, Mitä tietoja jaat internetissä kotisivut/blogit/keskustelut jne.?)

3) Miten opiskelijat huolehtivat Facebookin yksityisyydestä?
(Oletko lukenut ja tietoinen Facebookin käyttäjäehtojen muutoksesta?, Mitä tietoja jaat Facebookissa?, Ketä ihmisiä hyväksyt kavereiksi?, Millä perusteella otat käyttöön virtuaalisovelluksia? Miten toimit, jos saat kiertoviestin?)

Kysymyksistä tein lomakkeen WEBROPOL – palvelussa. Valmiista lomakkeesta tein 3 kopiota (1. tietojenkäsittely aloittelevat, 2. tietojenkäsittely lopettelevat, 3. liiketalouden aloittelevat, 4. liiketalouden lopettelevat), jotta analysointi olisi helpompaa suhteellisten

erojen selvittämiseksi tietojenkäsittelyn ja liiketalouden aloittelevien välillä, sekä lopettelevien välillä.

Kun kysymyslomake (kopioineen) oli valmis, laadin saatteen, joka sisälsi tutkimuksen varsinaisen saatteen lisäksi WEBROPOL kyselylomakelinkit jaoteltuna opiskelijaryhmittäin (tietojenkäsittely aloittelevat, tietojenkäsittely lopettelevat, liiketalouden aloittelevat ja liiketalouden lopettelevat). Tämän jälkeen lähetin saatteen HAAGA-HELIAN edustajalle, joka ohjasi ne WINHAPRON kautta kurssikoodien perusteella HAAGA-HELIAN opiskelijoille sähköpostitse. Opiskelijoiden vastaukset kaavioineen tulivat suoraan WEBROPOL -palveluun, josta otin ne tutkittavaksi sekä analysoitavaksi tietokoneelle. Osan vastauksina tulleista kaavioista jouduin tarkentamaan tavallista paperia ja Microsoft Exceliä apuna käyttäen, jotta sain riittävän tarkat tulokset erojen selventämiseksi. Tämän jälkeen kirjoitin tuloksista opinnäytetyön tuloksiin. Lopuksi tein johtopäätökset sekä yhteenvedon ja tiivistelmät.

6 Tulokset

Seuraavassa käydään läpi HAAGA–HELIAN tietojenkäsittelyn ja liiketalouden aloitteleville ja lopetteleville opiskelijoille suunnatun kyselyn tuloksia (Liite 5)

Kyselyyn vastasi kaikkiaan 103 henkilöä, joista (37,3 %, kuva 1) 38 kpl oli miehiä ja (62,7 %) 64 kpl naisia. Yksi kyselyyn vastannut henkilö ei ollut maininnut sukupuoltaan.

Koulutusohjelma ja ryhmä	Mies		Nainen	
	kpl	%	kpl	%
TIETOJENKÄSITTELY				
* aloittelevat	14	60,9	9	39,1
* lopettelevat	13	68,4	6	31,6
// Kaikki	**27**	**64,3**	**15**	**35,7**
LIIKETALOUS				
* aloittelevat	6	20,0	24	80,0
* lopettelevat	5	16,7	25	83,3
// Kaikki	**11**	**18,3**	**49**	**81,7**
KAIKKI YHTEENSÄ	**38**	**37,3**	**64**	**62,7**

Kuva 1. Sukupuolen jakautuminen kyselyssä koulutusohjelmittain

Kyselyn kokonaisvastausprosentiksi muodostui (38,6 %, kuva 2), josta tietojenkäsittelyn koulutusohjelman opiskelijoiden vastausosuus oli (35 %), kun taas liiketalouden opiskelijoiden vastausprosentti oli hieman suurempi (41,5 %,).

Koulutusohjelma ja ryhmä	Osallistujamäärä (kpl)	Kyselyyn vastaajat (kpl)	Vastaus %
TIETOJENKÄSITTELY			
* aloittelevat	71	23	32,4 %
* lopettelevat	49	19	38,8 %
// Kaikki	**120**	**42**	**35,0 %**
LIIKETALOUS			
* aloittelevat	107	30	28,0 %
* lopettelevat	40	31	77,5 %
// Kaikki	**147**	**61**	**41,5 %**
KAIKKI YHTEENSÄ	**267**	**103**	**38,6 %**

Kuva 2. Vastausten jakautuminen kyselyssä koulutusohjelmittain

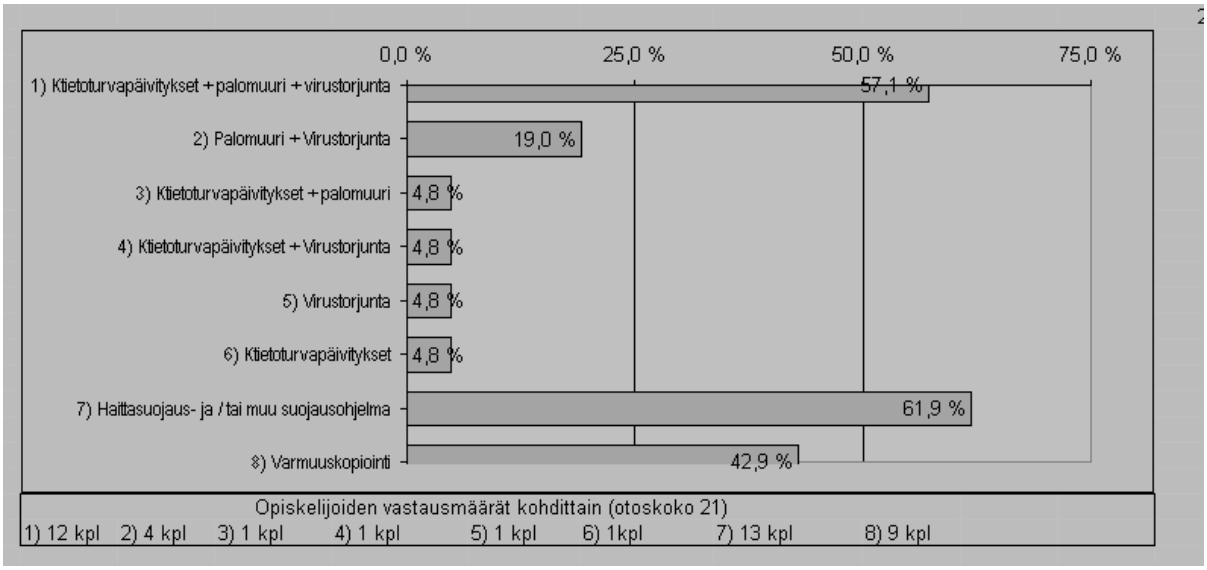
6.1 Miten opiskelijat huolehtivat tietokoneensa tietoturvasta?

Tietoturvaratkaisujen käyttö

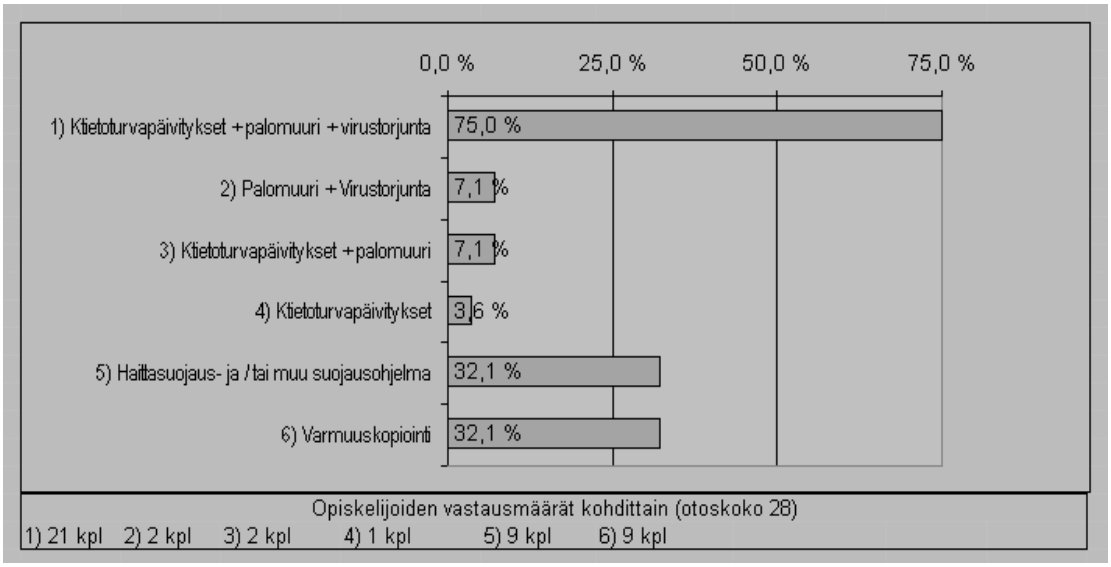
Aloittelevat opiskelijat

Tarkasteltaessa aloittelevien opiskelijoiden tietoturvaratkaisujen käyttöä, eroja löytyi lähinnä käyttöjärjestelmän tietoturvapäivitysten, palomuurin, virustorjunnan ja varmuuskopioinnin käytönsuhteen.

Erojen selventämiseksi on koostettu kaksi tarkempaa kuvaa. Liiketalouden opiskelijat (kuva 4) käyttävät suhteellisesti hieman enemmän käyttöjärjestelmän tietoturvapäivityksiä yhdessä palomuurin ja virustorjunnan kanssa kuin tietojenkäsittelyn opiskelijat (kuva 3). Tietojenkäsittelyn opiskelijat (kuva 3) puolestaan käyttävät suhteellisesti hieman enemmän palomuuria ja virustorjuntaa yhdessä ilman käyttöjärjestelmän tietoturvapäivityksiä kuin liiketalouden opiskelijat (kuva 4). Lisäksi tietojenkäsittelyn opiskelijat (kuva 3) käyttävät suhteellisesti enemmän haittasuojaus-, muita suojausohjelmia ja varmuuskopiointia kuin liiketalouden opiskelijat (kuva 4).



Kuva 3. Tietojenkäsittelyn aloittelevien opiskelijoiden tietoturvaratkaisujen tarkennettu käyttö (alkuperäisestä otoskoosta 23 on vähennetty 2 opiskelijaa, jotka eivät käytä tietoturvaratkaisuja) (Liite 1, kuva 17)



Kuva 4. Liiketalouden aloittelevien opiskelijoiden tietoturvaratkaisujen tarkennettu käyttö (alkuperäisestä otoskoosta 30 on vähennetty 2 opiskelijaa, jotka eivät käytä tietoturvaratkaisuja) (Liite 3, kuva 43)

Lopettelevat opiskelijat

Tarkasteltaessa lopettelevien opiskelijoiden tietoturvaratkaisujen käyttöä, pohjaudutaan pelkästään kyselystä saatuihin tuloksiin, koska erot ovat vähäisiä. Virustorjuntaa käyttävät kaikki opiskelijat ja palomuuria kaikki tietojenkäsittelyn opiskelijat. Tietojenkäsittelyn opiskelijat (taulukko 1) käyttävät suhteellisesti hieman enemmän palomuuria, käyttöjärjestelmän tietoturvapäivityksiä ja haittasuojausohjelmia kuin liiketalouden opiskelijat. Lisäksi tietojenkäsittelyn opiskelijat käyttävät suhteellisesti enemmän varmuuskopiointia.

Taulukko 1. Tietoturvaratkaisujen käyttö tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 30) (Liite 4, kuva 56)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Käyttöjärjestelmän tietoturvapäivitykset	84 %	77 %
Palomuuri	100 %	94 %
Virustorjunta	100 %	100 %
Haittasuojausohjelmat	37 %	29 %
Varmuuskopiointi	53 %	36 %

Tietoturvavaroituksiin suhtautuminen

Aloittelevat opiskelijat

Tarkasteltaessa aloittelevien opiskelijoiden suhtautumista tietoturvavaroituksiin, nähdään, että liiketalouden opiskelijat (taulukko 2) suhtautuvat suhteellisesti vakavammin tietoturvavaroituksiin kuin tietojenkäsittelyn opiskelijat.

Taulukko 2. Tietoturvavaroituksiin suhtautuminen tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 18) (Liite 3, kuva 44)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Vakavasti	39 %	60 %
Vähän niin ja näin	57 %	37 %
Ei kiinnitä huomiota	4 %	3 %

Lopettelevat opiskelijat

Tarkasteltaessa lopettelevien opiskelijoiden suhtautumista tietoturvavaroituksiin, nähdään, että tietojenkäsittelyn opiskelijat (taulukko 3) suhtautuvat suhteellisesti hieman vakavammin tietoturvavaroituksiin kuin liiketalouden opiskelijat. Erot ovat kuitenkin pieniä.

Taulukko 3. Tietoturvavaroituksiin suhtautuminen tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 31) (Liite 4, kuva 57)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Vakavasti	74 %	61 %
Vähän niin ja näin	26 %	36 %
Ei kiinnitä huomiota	0 %	3 %

Yhteenveto

Tuloksissa oli yllättävää se, että miten hyvin liiketalouden opiskelijat kokonaisuudessaan (aloittelevat ja (lopettelevat) huolehtivat tietokoneensa tietoturvasta suhteessa tietojenkäsittelyn opiskelijoihin. Liiketalouden aloittelevat opiskelijat huolehtivat suhteellisesti enemmän tietokoneensa tietoturvasta, käyttäen tietoturvaratkaisuja ja reagoiden tietoturvavaroituksiin kuin tietojenkäsittelyn aloittelevat opiskelijat.

Tietojenkäsittelyn aloittelevat opiskelijat käyttävät suhteellisesti enemmän varmuuskopiointia ja haittasuojausohjelmia.

Tietojenkäsittelyn lopettelevat opiskelijat huolehtivat suhteellisesti enemmän tietokoneensa tietoturvasta, käyttäen tietoturvaratkaisuja ja reagoiden tietoturvavaroituksiin kuin liiketalouden lopettelevat opiskelijat.

6.2 Miten opiskelijat kiinnittävät huomiota omiin käyttäjätietoihin internetissä?

Tietoisuus sosiaalisen kanssakäymisen uhista

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 4) tietoisuutta sosiaalisen kanssakäymisen uhista, nähdään, että lähes kaikki opiskelijat tiedostavat sosiaaliseen kanssakäymiseen liittyvän uhkia. Tulosten perusteella nähdään, että liiketalouden opiskelijat tiedostavat suhteellisesti hieman enemmän uhkien olemassa olon. Erot ovat kuitenkin pieniä.

Taulukko 4. Tietoisuus sosiaalisen kanssakäymisen uhista tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 19) (Liite 3, kuva 45)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Kyllä	91 %	97 %
Ei	9 %	3 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden (taulukko 5) tietoisuutta sosiaalisen kanssakäymisen uhista, nähdään pieniä eroja olevan. Kaikki liiketalouden opiskelijat tiedostavat sosiaaliseen kanssakäymiseen liittyvän uhkia, kun taas tietojenkäsittelyn opiskelijoista lähes kaikki (=yhdeksän kymmenestä). Tulosten perusteella nähdään, että liiketalouden opiskelijat tiedostavat suhteellisesti hieman enemmän uhkien olemassa olon, mutta erot ovat pieniä.

Taulukko 5. Tietoisuus sosiaalisen kanssakäymisen uhista tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 32) (Liite 4, kuva 58)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Kyllä	90 %	100 %
Ei	11 %	0 %

Salasanojen sisältö

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 6) salasanojen sisältöä, nähdään, ettei huomattavia eroavaisuuksia ole. Tulosten perusteella nähdään, että molempien koulutusohjelmien opiskelijat kiinnittävät huomiota suhteellisen samantyylisesti salasanojen sisältöön (kirjainten, numeroiden ja erikoismerkkien) osalta.

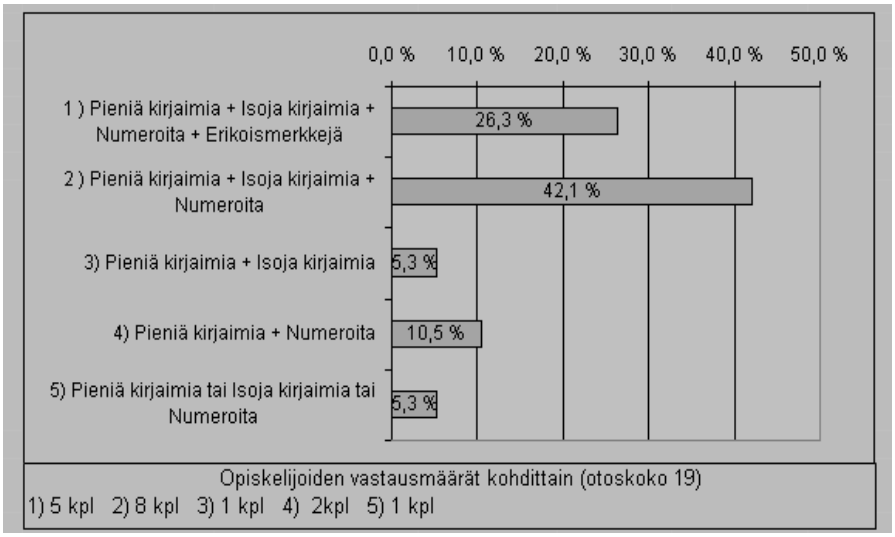
Taulukko 6. Salasanojen sisältö tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 20) (Liite 3, kuva 46)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Pieniä kirjaimia	96 %	97 %
Isoja kirjaimia	52 %	50 %
Numeroita	91 %	93 %
Erikoismerkkejä	13 %	13 %

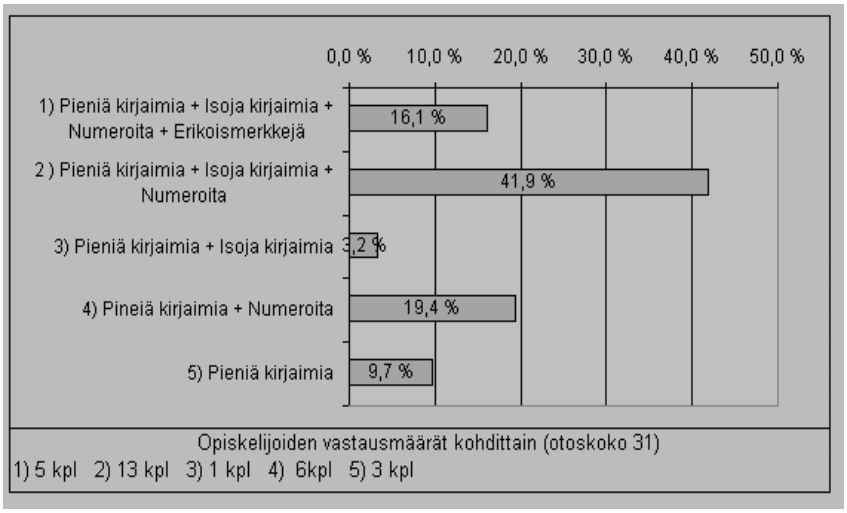
Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden salasanojen sisältöä, nähdään eroavaisuuksia olevan hieman. Erojen selventämiseksi on koostettu kaksi tarkempaa kuvaa (kirjainten, numeroiden ja erikoismerkkien) osalta.

Tietojenkäsittelyn opiskelijat (kuva 5) käyttävät suhteellisesti hieman enemmän (pieni kirjain + iso kirjain + numero + erikoismerkki- yhdistelmiä) salasanoissaan kuin liiketalouden opiskelijat (kuva 6). Liiketalouden opiskelijat puolestaan käyttävät suhteellisesti hieman enemmän (pieni kirjain + numeroyhdistelmiä) salasanoissaan. Tarkennettujen tulosten perusteella nähdään, että erot ovat pieniä, mutta hieman tietojenkäsittelyn lopettelevien opiskelijoiden hyväksi.



Kuva 5. Tietojenkäsittelyn lopettelevien opiskelijoiden salasanojen sisältö (Liite 2, kuva 33)



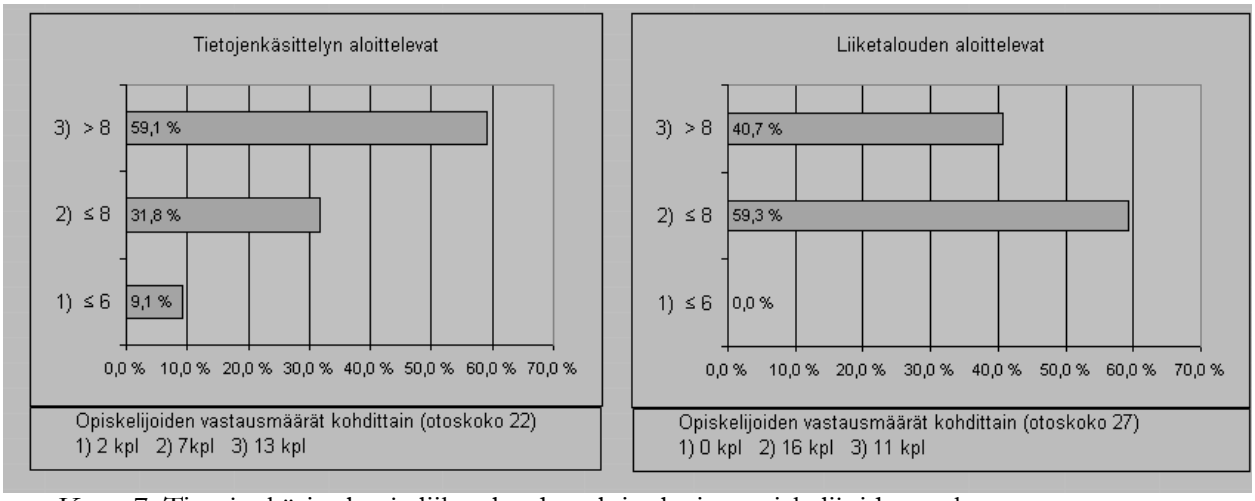
Kuva 6. Liiketalouden lopettelevien opiskelijoiden salasanojen sisältö (Liite 4, kuva 59)

Salasanojen pituudet

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välisiä salasanojen pituuksia, nähdään, että osa opiskelijoista käyttää riittävän pitkiä salasanoja ja osa ei. Tietojenkäsittelyn opiskelijat (kuva 7) käyttävät suhteellisesti enemmän yli 8 merkkiä pitkiä salasanoja kuin liiketalouden opiskelijat (kuva 7). Liiketalouden opiskelijat puolestaan käyttävät suhteellisesti enemmän 8 merkkiä tai sitä lyhyempiä salasanoja kuin tietojenkäsittelyn opiskelijat. Lisäksi muutama tietojenkäsittelyn opiskelija käyttää 6 merkkiä pitkiä tai sitä lyhyempiä salasanoja.

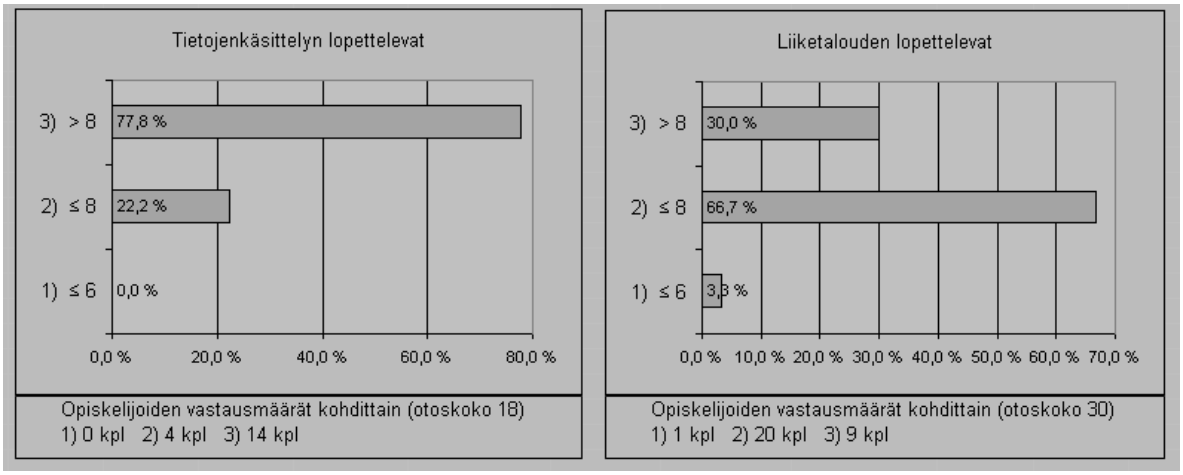
Tietojenkäsittelyn aloittelevat opiskelijat käyttävät suhteellisesti hieman pidempiä salasanoja kuin liiketalouden aloittelevat opiskelijat. Jos opiskelijan ilmoittama pituus oli vaihtelevamittainen esimerkiksi 5 – 10 merkkiä, tällöin pituudesta on otettu keskikohta tarkennettuun kuvaan (kuva 7). Kuvassa ei ole huomioitu yhden tietojenkäsittelyn opiskelijan vastausta ”riippuu palvelusta”, koska oli epämääräinen. Tästä syystä otoskoko on 22 eikä 23.



Kuva 7. Tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden tarkennetut salasanojen pituuksien jakaumat (Liite 1, kuva 21) (Liite 3, kuva 47)

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden välisiä salasanojen pituuksia, nähdään eroja olevan. Tietojenkäsittelyn opiskelijat (kuva 8) käyttävät suhteellisesti enemmän yli 8 merkkiä pitkiä salasanoja kuin liiketalouden opiskelijat (kuva 8). Liiketalouden opiskelijat puolestaan käyttävät 8 merkkiä tai sitä lyhyempiä salasanoja suhteellisesti enemmän kuin tietojenkäsittelyn opiskelijat. Yksi liiketalouden lopetteleva opiskelija käyttää vain 6 merkkiä tai sitä lyhyempiä salasanoja. Tämän lisäksi yhden tietojenkäsittelyn lopettelevan opiskelijan vastausta ”riittävän lyhyitä”, ei huomioitu, koska oli epämääräinen. Tulosten perusteella nähdään, että tietojenkäsittelyn lopettelevat opiskelijat käyttävät suhteellisesti pidempiä salasanoja kuin liiketalouden lopettelevat opiskelijat.



Kuva 8. Tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden tarkennetut salasanojen pituuksien jakaumat (Liite 2, kuva 34) (Liite 4, kuva 60)

Salasanojen vaihtoväli

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välisiä eroja salasanojen vaihtovälien suhteen, nähdään, että molempien koulutusohjelmien opiskelijat (taulukko 7) vaihtavat salasanojaan, lähinnä ”puolen vuoden välein tai harvemmin”. Eroavaisuuksia on siinä, että liiketalouden opiskelijat vaihtavat suhteellisesti hieman enemmän salasanojaan ”kuukausittain tai harvemmin”. Tulosten perusteella nähdään, että liiketalouden aloittelevat opiskelijat vaihtavat salasanojaan suhteellisesti hieman useammin kuin tietojenkäsittelyn aloittelevat opiskelijat.

Taulukko 7. Salasanojen vaihtoväli tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 22) (Liite 3, kuva 48)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Puolen vuoden välein tai harvemmin	57 %	50 %
Kuukausittain tai harvemmin	13 %	30 %
Ei koskaan	30 %	20 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden välisiä eroja salasanojen vaihtovälien suhteen, nähdään eroavaisuuksia olevan. Tietojenkäsittelyn opiskelijat (taulukko 8) vaihtavat suhteellisesti hieman enemmän salasanoja ”puolen vuoden välein tai harvemmin” kuin liiketalouden opiskelijat. Liiketalouden opiskelijat puolestaan vaihtavat suhteellisesti hieman enemmän salasanoja ”kuukausittain tai harvemmin” kuin tietojenkäsittelyn opiskelijat. Tulosten perusteella nähdään, että liiketalouden lopettelevat opiskelijat vaihtavat salasanojaan suhteellisesti hieman useammin kuin tietojenkäsittelyn lopettelevat opiskelijat.

Taulukko 8. Salasanojen vaihtoväli tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 35) (Liite 4, kuva 61)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Puolen vuoden välein tai harvemmin	47 %	37 %
Kuukausittain tai harvemmin	26 %	33 %
Ei koskaan	26 %	30 %

Salasanojen vaihtelevuus palveluittain

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 9) salasanojen vaihtelevuutta eri palvelujen kesken, nähdään, että molempien koulutusohjelmien opiskelijat käyttävät pääsiassa vain ”muutamia salasanoja” erilaisten palvelujen kesken. Eroavaisuuksia on lähinnä siinä, että tietojenkäsittelyn opiskelijat käyttävät suhteellisesti hieman enemmän ”jokaisessa palvelussa eri salasanaa” kuin liiketalouden opiskelijat. Tulosten perusteella nähdään, että tietojenkäsittelyn aloittelevat opiskelijat kiinnittävät suhteellisesti hieman enemmän huomiota salasanojen vaihtelevuuteen.

Taulukko 9. Salasanojen vaihtelevuus palveluittain tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 23) (Liite 3, kuva 49)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Jokaiseen palveluun eri salasana	22 %	17 %
Muutama salasana, jotka käytössä eri palvelujen kesken	70 %	77 %
Yksi ja sama salasana	9 %	7 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden (taulukko 10) salasanojen vaihtelevuutta eri palvelujen kesken, nähdään, että molempien koulutusohjelmien opiskelijat käyttävät vain ”muutamia salasanoja” erilaisten palvelujen kesken. Eroavaisuuksia on lähinnä siinä, että liiketalouden opiskelijat käyttävät suhteellisesti enemmän ”jokaisessa palvelussa eri salasanaa”, kuin tietojenkäsittelyn opiskelijat. Tulosten perusteella nähdään, että liiketalouden lopettelevat opiskelijat kiinnittävät suhteellisesti hieman enemmän huomiota salasanojen vaihtelevuuteen.

Taulukko 10. Salasanojen vaihtelevuus palveluittain tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, 36) (Liite 4, 62)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Jokaiseen palveluun eri salasana	5 %	19 %
Muutama salasana, jotka käytössä eri palvelujen kesken	90 %	74 %
Yksi ja sama salasana	5 %	7 %

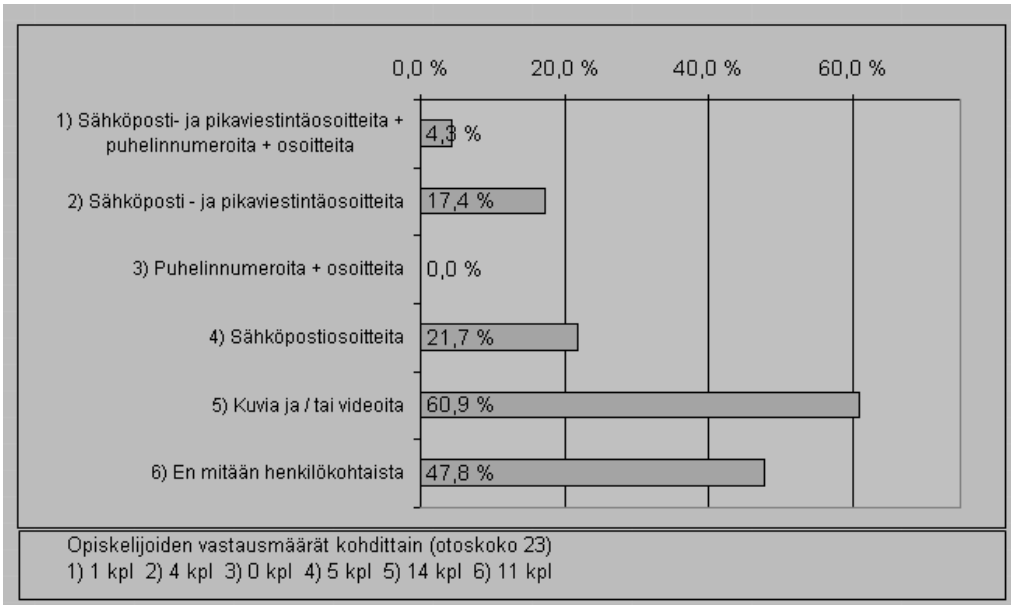
Tietojen jakaminen internetissä (kotisivut/blogit/keskustelut jne.)

Aloittelevat opiskelijat

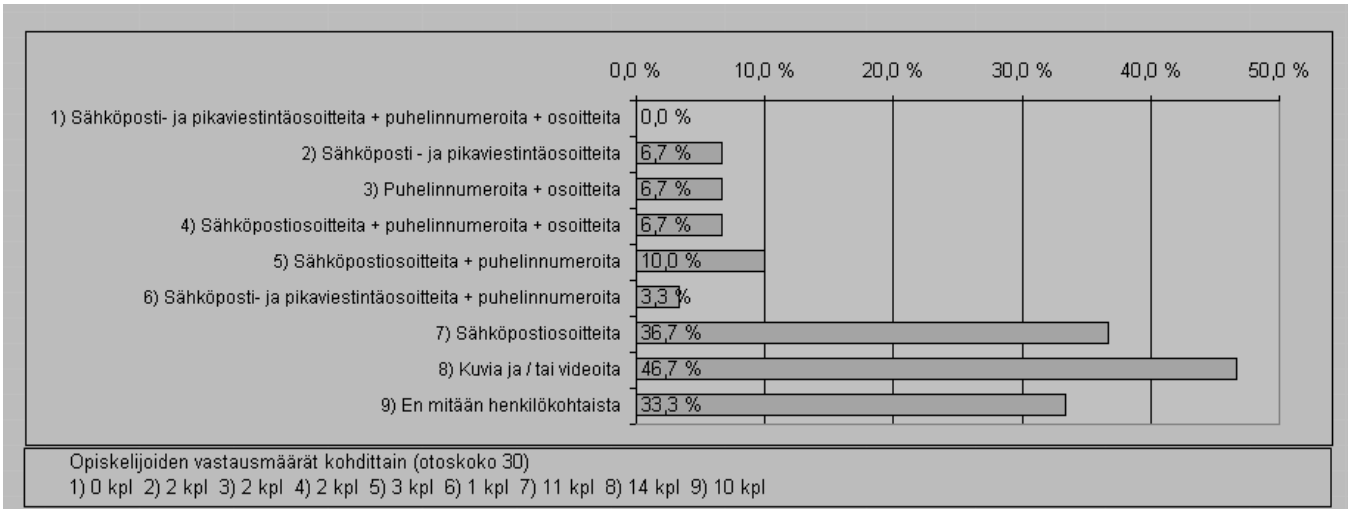
Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välisiä eroja tiedon jakamisen suhteen internetissä, nähdään eroavaisuuksia olevan. Liiketalouden

opiskelijat (kuva 10) jakavat sähköposti- ja pikaviestintäosoitteita sekä muita henkilökohtaisia tietoja (puhelinnumeroita ja osoitteita) suhteellisesti hieman enemmän kuin tietojenkäsittelyn opiskelijat (kuva 9). Tietojenkäsittelyn opiskelijat puolestaan jakavat kuvia ja videoita suhteellisesti enemmän kuin liiketalouden opiskelijat.

Tulosten perusteella nähdään, että tietojenkäsittelyn aloittelevat opiskelijat kiinnittävät suhteellisesti enemmän huomiota siihen, mitä tietoja on turvallista jakaa internetissä, koska jakavat suhteellisesti vähemmän henkilökohtaisia tietoja kuin liiketalouden aloittelevat opiskelijat.



Kuva 9. Tietojenkäsittelyn aloittelevien opiskelijoiden tarkennettu tietojen jakaminen internetissä (Liite 1, kuva 24)

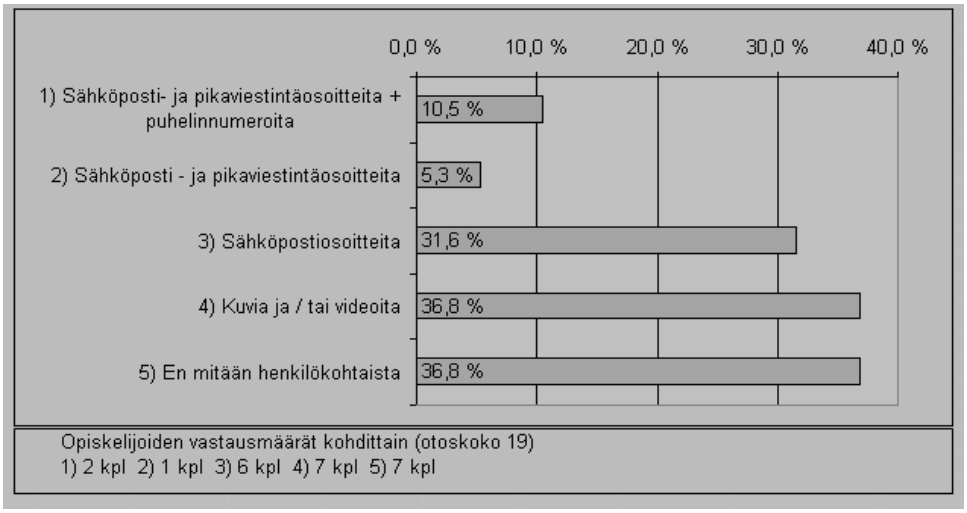


Kuva 10. Liiketalouden aloittelevien opiskelijoiden tarkennettu tietojen jakaminen internetissä (Liite 3, kuva 50)

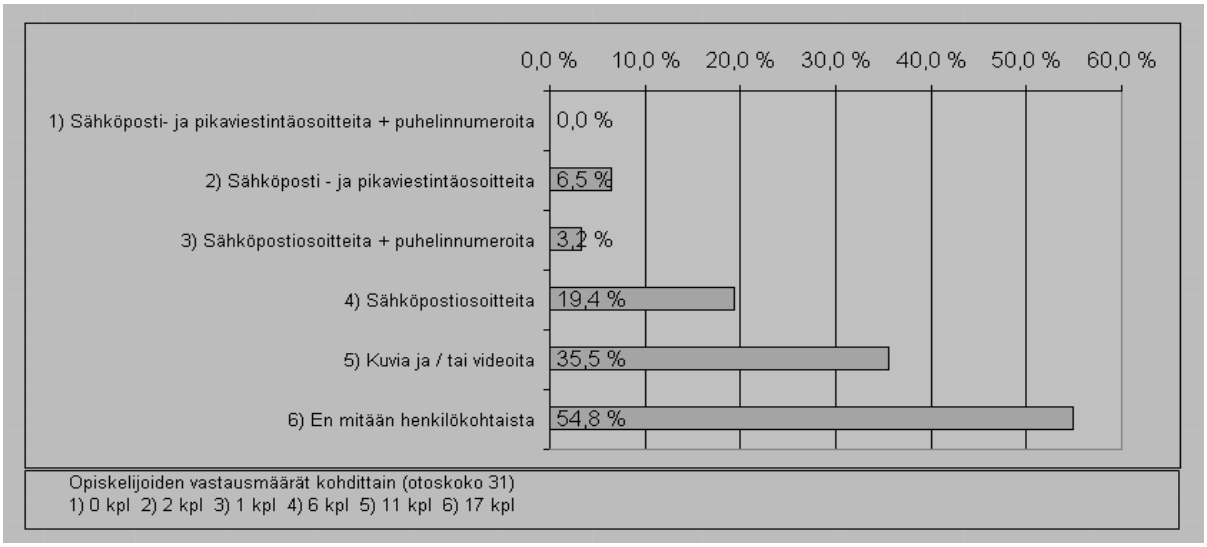
Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden välisiä eroja tiedon jakamisen suhteen internetissä, nähdään pieniä eroavaisuuksia olevan. Tietojenkäsittelyn opiskelijat (kuva 11) jakavat sähköposti- ja pikaviestintäosoitteita suhteellisesti hieman enemmän kuin liiketalouden opiskelijat (kuva 12). Kuvia ja videoita molempien koulutusohjelmien opiskelijat jakavat lähes samassa suhteessa.

Tulosten perusteella nähdään, että liiketalouden lopettelevat opiskelijat kiinnittävät suhteellisesti enemmän huomiota siihen, mitä tietoja on turvallista jakaa internetissä, koska jakavat suhteellisesti vähemmän henkilökohtaisia tietoja kuin tietojenkäsittelyn opiskelijat.



Kuva 11. Tietojenkäsittelyn lopettelevien opiskelijoiden tarkennettu tietojen jakaminen internetissä (Liite 2, 37)



Kuva 12. Liiketalouden lopettelevien opiskelijoiden tarkennettu tietojen jakaminen internetissä (Liite 4, 63)

Yhteenveto

Tuloksissa oli hieman yllättävää se, että miten paljon vastaukset jakaantuivat kysymyksien välillä. Liiketalouden aloittelevat opiskelijat tiedostavat suhteellisesti hieman enemmän sen, että sosiaaliseen kanssakäymiseen liittyy uhkia ja vaihtavat salasanojaan suhteellisesti useammin kuin tietojenkäsittelyn aloittelevat opiskelijat, jota voidaan pitää yllättävänä oletuksiin nähden. Tietojenkäsittelyn aloittelevat opiskelijat puolestaan käyttävät suhteellisesti hieman pidempiä ja enemmän vaihtelevia salasanoja eri palvelujen kesken sekä jakavat vähemmän henkilökohtaista tietoa internetissä kuin liiketalouden aloittelevat opiskelijat. Salasanojen sisällön (merkistön) suhteen ei ollut mainittavia eroja, aloittelevien opiskelijoiden kesken.

Liiketalouden lopettelevat opiskelijat tiedostavat suhteellisesti enemmän sosiaaliseen kanssakäymiseen liittyvät uhkat ja vaihtavat salasanojaan hieman useammin kuin tietojenkäsittelyn lopettelevat opiskelijat. Tämän lisäksi liiketalouden lopettelevat opiskelijat käyttävät suhteellisesti enemmän vaihtelevia salasanoja eri palvelujen kesken ja jakavat vähemmän henkilökohtaista tietoa, jota voidaan pitää yllättävänä oletuksiin nähden. Tietojenkäsittelyn lopettelevat opiskelijat puolestaan käyttävät suhteellisesti pidempiä ja sisällöltään turvallisempia salasanoja kuin liiketalouden lopettelevat opiskelijat.

6.3 Miten opiskelijat huolehtivat Facebookin yksityisyydestä?

Tietoisuus Facebookin käyttäjäehtojen muutoksista

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 11) tietoisuutta Facebookin käyttäjäehtojen muutoksista, nähdään, että liiketalouden opiskelijat ovat suhteellisesti hieman enemmän tietoisia Facebookin käyttäjäehtojen muutoksista kuin tietojenkäsittelyn opiskelijat. Tulosten perusteella nähdään erojen olevan kuitenkin pieniä.

Taulukko 11. Tietoisuus Facebookin käyttäjäehtojen muutoksesta tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 25) (Liite 3, kuva 51)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Kyllä	59 %	64 %
En	41 %	36 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden (taulukko 12) tietoisuutta Facebookin käyttäjäehtojen muutoksista, nähdään, että tietojenkäsittelyn opiskelijat ovat suhteellisesti hieman enemmän tietoisia käyttäjäehtojen muutoksista kuin liiketalouden opiskelijat. Tulosten perusteella erot ovat kuitenkin pieniä.

Taulukko 12. Tietoisuus Facebookin käyttäjäehtojen muutoksesta tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 38) (Liite 4, kuva 64)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Kyllä	80 %	70 %
En	20 %	30 %

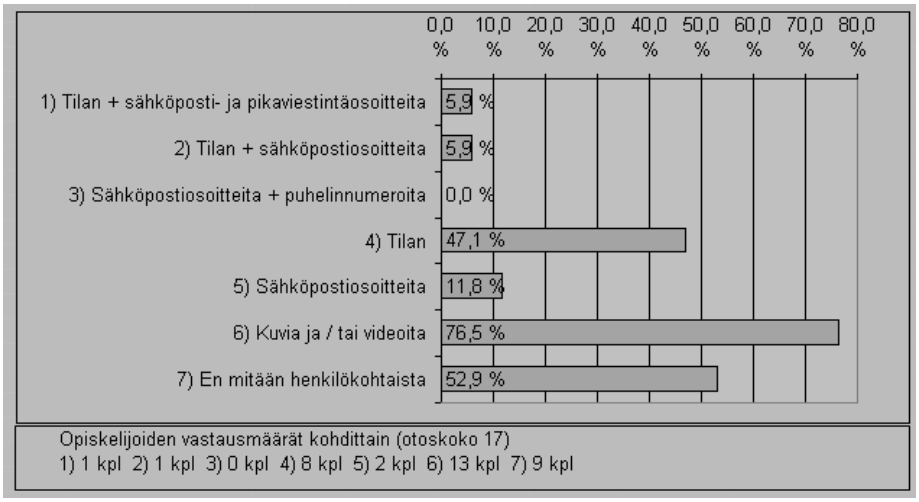
Tietojen jakaminen Facebookissa

Aloittelevat opiskelijat

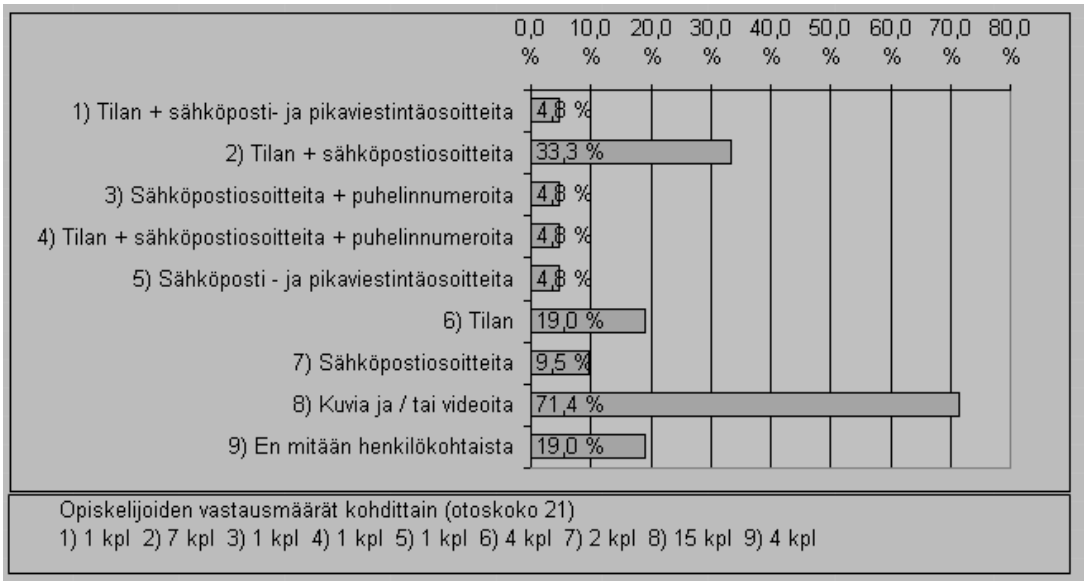
Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välisiä eroja tiedon jakamisen suhteen Facebookissa, nähdään eroavaisuuksia olevan hieman.

Molempien koulutusohjelmien opiskelijat päivittävät suhteellisen aktiivisesti omaa tilaansa Facebookissa. Liiketalouden opiskelijat (kuva 14) jakavat henkilökohtaisia tietoja (erityisesti sähköpostiosoitteita) suhteellisesti enemmän kuin tietojenkäsittelyn opiskelijat (kuva 13).

Tietojenkäsittelyn opiskelijat puolestaan jakavat kuvia ja/tai videoita suhteellisesti hieman enemmän kuin liiketalouden opiskelijat. Tulosten perusteella nähdään, että tietojenkäsittelyn aloittelevat opiskelijat kiinnittävät suhteellisesti enemmän huomiota siihen, mitä tietoja Facebookissa on turvallista jakaa, kuin liiketalouden aloittelevat opiskelijat.



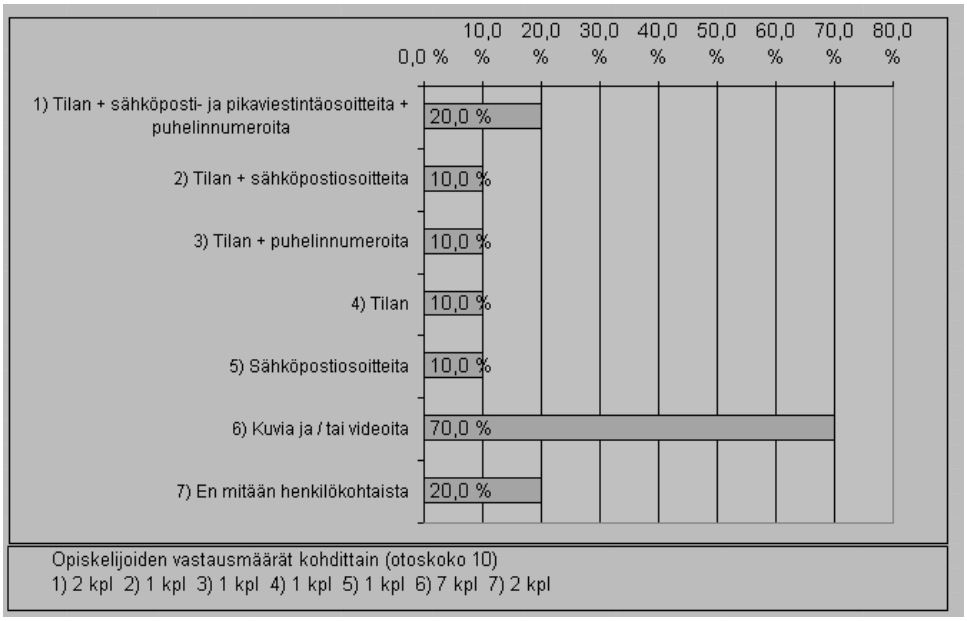
Kuva 13. Tietojenkäsittelyn aloittelevien opiskelijoiden tarkennettu tietojen jakaminen Facebookissa (Liite 1, kuva 26)



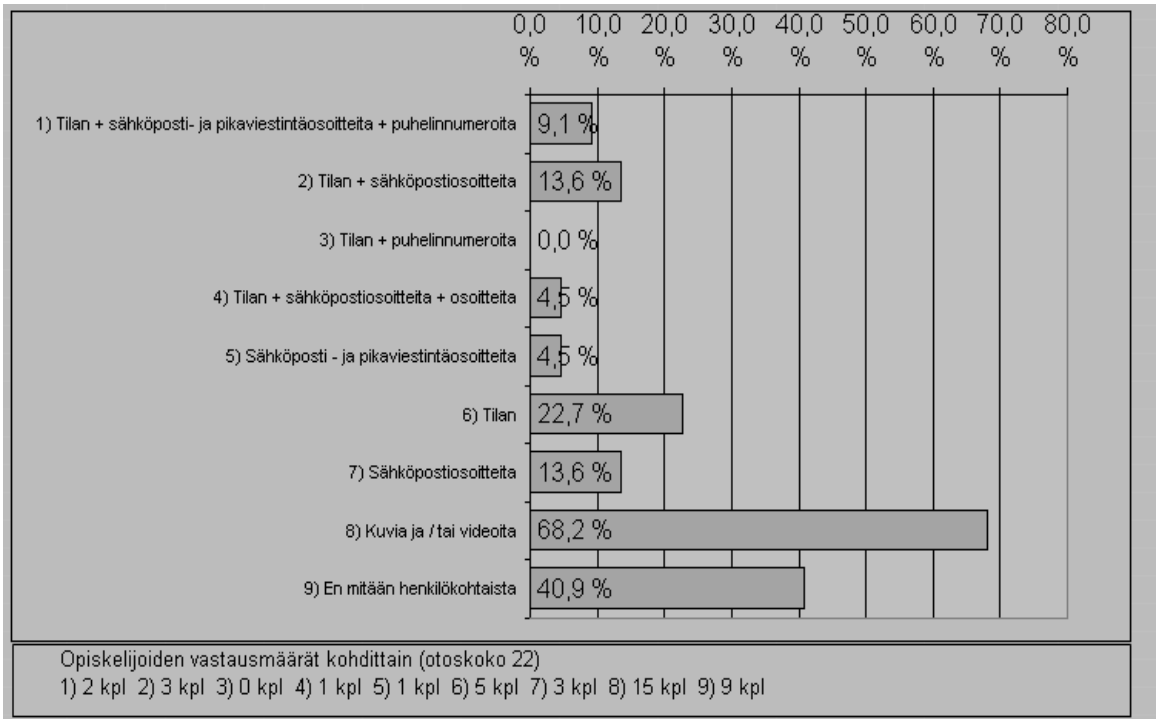
Kuva 14. Liiketalouden aloittelevien opiskelijoiden tarkennettu tietojen jakaminen Facebookissa (Liite 3, kuva 52)

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn (kuva 15) ja liiketalouden lopettelevien opiskelijoiden välisiä eroja tiedon jakamisen suhteen Facebookissa, nähdään eroavaisuuksia olevan hieman. Molempien koulutusohjelmien opiskelijat päivittävät Facebookin tilaansa suhteellisen aktiivisesti ja jakavat sähköpostiosoitteita, kuvia ja/tai videoita suurin piirtein samalla tavalla. Tulosten perusteella nähdään, että liiketalouden lopettelevat opiskelijat (kuva 16) kiinnittävät suhteellisesti hieman enemmän huomiota siihen, että mitä tietoja Facebookissa on turvallista jakaa, kuin tietojenkäsittelyn lopettelevat opiskelijat.



Kuva 15. Tietojenkäsittelyn lopettelevien opiskelijoiden tarkennettu tietojen jakaminen Facebookissa (Liite 2, kuva 39)



Kuva 16. Liiketalouden lopettelevien opiskelijoiden tarkennettu tietojen jakaminen Facebookissa (Liite 4, kuva 65)

Kavereiksi hyväksymiskriteerit Facebookissa

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 13) kavereiksi hyväksymiskriteerejä Facebookissa, nähdään, että tietojenkäsittelyn opiskelijat hyväksyvät kavereiksi vain ihmisiä, jotka oikeasti tuntevat, kuten lähes kaikki liiketalouden opiskelijoistakin. Liiketalouden opiskelijoista puolestaan pieni osa hyväksyy kavereiksi, ketä tahansa. Tulosten perusteella nähdään, että tietojenkäsittelyn aloittelevat opiskelijat kiinnittävät suhteellisesti hieman enemmän huomiota siihen, ketä hyväksyvät kavereiksi Facebookissa, kuin liiketalouden aloittelevat opiskelijat. Erot ovat kuitenkin todella pieniä.

Taulukko 13. Kavereiksi hyväksymiskriteerit tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 27) (Liite 3, kuva 53)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Vain ihmisiä, jotka tunnen	94 %	91 %
Ketä tahansa	0 %	5 %
En ketään	6 %	5 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden (taulukko 14) kavereiksi hyväksymiskriteerejä Facebookissa, nähdään, että tietojenkäsittelyn opiskelijat hyväksyvät kavereiksi vain ihmisiä, jotka oikeasti tuntevat, kuten liiketalouden opiskelijoistakin lähes kaikki. Liiketalouden opiskelijoista puolestaan todella pieni osa hyväksyy kavereiksi, ketä tahansa. Tuloksien perusteella näyttää, että tietojenkäsittelyn lopettelevat opiskelijat kiinnittävät suhteellisesti hieman enemmän huomiota siihen, ketä hyväksyvät kavereiksi Facebookissa, kuin liiketalouden lopettelevat opiskelijat. Erot ovat kuitenkin pieniä.

Taulukko 14. Kavereiksi hyväksymiskriteerit tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 40) (Liite 4, kuva 66)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Vain ihmisiä, jotka tunnen	100 %	96 %
Ketä tahansa	0 %	5 %
En ketään	0 %	0 %

Virtuaalisovellusten käyttöönottokriteerit Facebookissa

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 15) virtuaalisovellusten käyttöönottokriteerejä Facebookissa, nähdään, että molempien koulutusohjelmien opiskelijat suhtautuvat suhteellisen samantyylisesti virtuaalisovellusten käyttöönottoon, koska erot ovat lähes olemattomat. Tulosten perusteella nähdään, että suurin osa tietojenkäsittelyn ja liiketalouden aloittelevista opiskelijoista kokee virtuaalisovelluksen käyttöönoton tärkeimmäksi kriteeriksi sovelluksen ”käyttötarkoituksen ja turvallisuuden”. Moni opiskelija ei ota käyttöön virtuaalisovelluksia ollenkaan.

Taulukko 15. Virtuaalisovellusten käyttöönottokriteerit tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 28) (Liite 3, kuva 54)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Käyttötarkoitus ja turvallisuus	44 %	46 %
Mielenkiintoinen	28 %	27 %
Eivät ota käyttöön	28 %	27 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden (taulukko 16) virtuaalisovellusten käyttöönottokriteerejä Facebookissa, nähdään eroavaisuuksia olevan. Tietojenkäsittelyn opiskelijat kokevat virtuaalisovellusten käyttöönoton tärkeimmäksi kriteeriksi sovelluksen ”käyttötarkoituksen ja turvallisuuden”. Liiketalouden opiskelijat puolestaan kokevat virtuaalisovellusten käyttöönoton tärkeimmäksi kriteeriksi sovelluksen ”mielenkiintoisuuden”. Lisäksi tietojenkäsittelyn opiskelijoista näyttäisi suurempi enemmistö olevan kielteisellä kannalla virtuaalisovellusten käyttöönottamiseen verraten liiketalouden opiskelijoihin. Tulosten perusteella nähdään, että tietojenkäsittelyn lopettelevat opiskelijat kiinnittävät suhteellisesti enemmän huomiota virtuaalisovellusten käyttöönottoon kriteerit huomioiden, kuin liiketalouden lopettelevat opiskelijat.

Taulukko 16. Virtuaalisovellusten käyttöönottokriteerit tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 41) (Liite 4, kuva 67)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Käyttötarkoitus ja turvallisuus	40 %	22 %
Mielenkiintoinen	10 %	52 %
Eivät ota käyttöön	50 %	26 %

Kiertoviesteihin reagointi Facebookissa

Aloittelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden (taulukko 17) kiertoviesteihin reagointia Facebookissa, nähdään, että molempien koulutusohjelmien opiskelijat reagoivat suhteellisen samantyylisesti kiertoviesteihin Facebookissa, koska erot

ovat lähes olemattomat. Tulosten perusteella nähdään, että tietojenkäsittelyn ja liiketalouden aloittelevista opiskelijoista lähes kaikki reagoivat kiertoviesteihin Facebookissa, joko poistamalla viestin saman tien tai suhtautumalla epäilevästi eli jättämällä viestin omaan arvoonsa. Yksi tietojenkäsittelyn opiskelija toimii kiertoviestin ohjeistuksen mukaan.

Taulukko 17. Kiertoviesteihin reagointi tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden keskuudessa (Liite 1, kuva 29) (Liite 3, kuva 55)

	Tietojenkäsittely aloittelevat	Liiketalous aloittelevat
Poistan viestin saman tien	44 %	46 %
Suhtaudun epäilevästi, koskematta viestiin	50 %	55 %
Toimin viestin ohjeistuksen mukaan, lähettämällä eteenpäin	6 %	0 %

Lopettelevat opiskelijat

Tarkasteltaessa tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden (taulukko 18) kiertoviesteihin reagointia Facebookissa, nähdään eroavaisuuksia olevan. Tulosten perusteella nähdään, että tietojenkäsittelyn ja liiketalouden opiskelijoista lähes kaikki reagoivat kiertoviesteihin Facebookissa, joko poistamalla viestin saman tien tai suhtautumalla epäilevästi viestiin eli jättämällä viestin omaan arvoonsa. Liiketalouden lopettelevat opiskelijat reagoivat suhteellisesti hieman enemmän kiertoviesteihin (poistamalla kiertoviestin saman tien) kuin tietojenkäsittelyn lopettelevat opiskelijat. Tätä tukee myös se, että muutama tietojenkäsittelyn opiskelija toimii kiertoviestin ohjeistuksen mukaan.

Taulukko 18. Kiertoviesteihin reagointi tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden keskuudessa (Liite 2, kuva 42) (Liite 4, kuva 68)

	Tietojenkäsittely lopettelevat	Liiketalous lopettelevat
Poistan viestin saman tien	30 %	48 %
Suhtaudun epäilevästi, koskematta viestiin	60 %	52 %
Toimin viestin ohjeistuksen mukaan, lähettämällä eteenpäin	10 %	0 %

Yhteenveto

Tuloksissa oli hieman yllättävää se, että miten paljon vastaukset jakaantuivat kysymyksien välillä. Liiketalouden aloittelevat opiskelijat ovat suhteellisesti enemmän tietoisia Facebookin käyttäjäehtojen muutoksista kuin tietojenkäsittelyn aloittelevat opiskelija, jota voidaan pitää yllätyksenä odotusarvoihin nähden. Tietojenkäsittelyn aloittelevat opiskelijat puolestaan jakavat suhteellisesti vähemmän henkilökohtaista tietoa Facebookissa ja kiinnittävät suhteellisesti enemmän huomiota siihen, ketä ihmisiä hyväksyvät kavereiksi Facebookissa kuin liiketalouden aloittelevat opiskelijat. Facebookin virtuaalisovellusten käyttöönotossa (kriteerit huomioiden) ja kiertoviesteihin reagoinnissa ei ollut huomattavia eroja aloittelevien opiskelijoiden välillä.

Liiketalouden lopettelevat opiskelijat reagoivat suhteellisesti hieman enemmän Facebookin kiertoviesteihin ja jakavat suhteellisesti hieman vähemmän henkilökohtaista tietoa Facebookissa kuin tietojenkäsittelyn lopettelevat opiskelijat, jota voidaan pitää yllätyksenä odotusarvoihin nähden. Tietojenkäsittelyn lopettelevat opiskelijat puolestaan ovat suhteellisesti hieman enemmän tietoisia Facebookin käyttäjäehtojen muutoksista ja kiinnittivät suhteellisesti hieman enemmän huomiota siihen, ketä ihmisiä hyväksyvät kavereiksi Facebookissa sekä kiinnittävät suhteellisesti enemmän huomiota virtuaalisovellusten käyttöönottoon (kriteerit huomioiden), kuin liiketalouden lopettelevat opiskelijat.

7 Johtopäätökset

Tietoturva-asioihin on tullut kiinnitettyä itse aina huomiota internetissä liikkuessa, mutta kuinka tietoturvaan suhtautuvat HAAGA – HELIAn tietojenkäsittelyn ja liiketalouden aloittelevat sekä lopettelevat opiskelijat, käyttäessään internetiä sosiaalisessa kanssakäymisessä. Aluksi oli kuitenkin tutkittava lähdeaineistoja hyväksikäyttäen mitä yleisiä uhkia internetin sosiaaliseen kanssakäymiseen liittyy ja mitä uhkia Facebookin yksityisyyteen liittyy sekä miten näiltä uhkilta voidaan suojautua.

Yleiset tietoturvauhkat

Yleisesti tietoturvauhkia aiheuttavat sosiaalisessa kanssakäymisessä erilaiset madot, virukset, hakkerit, vakoiluohjelmat, haittaohjelmat, huijaukset, roskaposti sekä joissakin tapauksissa näiden seurauksena tietojen katoamiset. Yleisiltä tietoturvauhilta suojautuminen on kerrottu luvussa 3.3.

Tuloksien perusteella voidaan päätellä, että todellisia uhkia internetin sosiaaliseen kanssakäymiseen liittyy, joka oli odotettua. Huolestuttavana voidaan pitää sitä, että läheskään kaikkia uhkia ei ole mahdollista havaita riittävän ajoissa eli pahimmassa tapauksessa vaaratilanne voi päästä syntymään ennen kuin uhkaan ehditään reagoida. Tämä voi johtua tietoturvauhkien erilaisista ja poikkeavista käyttäytymistavoista/ ilmenemismuodoista.

Facebookin yksityisyyden uhat

Facebookin yksityisyyttä uhkaavat ihmisten sinisilmäisyys profiilia kohtaan ja siihen liittyvien tietojen suhteen. Ei kiinnitetä huomiota siihen, millaista tietoa on turvallista laittaa profiiliin, eikä määritellä tarkasti kenelle nämä tiedot näkyvät, pahimmassa tapauksessa julkisesti. Hyväksytään kavereiksi ketä tahansa, tuntematta ihmisiä entuudestaan millään tavoin. Otetaan virtuaalisovelluksia (sovellukset, pelit jne.) käyttöön tiedostamatta virtuaalisovellusten käyttötarkoituksia ja mitä tietoja keräävät käyttäjästä toimiakseen. Luotetaan kiertokirjeviesteihin liian sinisilmäisesti. Näiden lisäksi uhkia aiheuttavat myös yleiset tietoturvauhkat, joista ainakin viruksia ja vakoiluohjelmia on löydetty Facebookista. Facebookin yksityisyyden uhilta suojautuminen on kerrottu luvussa 3.4.4.

Tuloksien perusteella voidaan päätellä, että todellisia uhkia Facebookin yksityisyyteen liittyy, joita on suhteellisesti enemmän odotuksiin nähden. Tämä voi johtua siitä, kun Facebook on palveluna vielä suhteellisen uusi ja kokoajan mahdollisesti uusia käyttäjiä rekisteröityy palvelun käyttäjiksi. On myös mahdollista, että ihmiset eivät välttämättä tiedosta Facebookiin liittyvän uhkia. Tämä voi selittää sen, että ihmiset käyttävät palvelua, kiinnittämättä huomiota palvelun yksityisyyteen. Onneksi nykyisin internetissä Facebook uhkista tiedotetaan, yleisten tietoturvauhkien ohella. Tästä syystä on mielenkiintoista nähdä mihin suuntaan Facebookin yksityisyys ja siihen liittyvät uhat kehittyvät tulevaisuudessa.

Seuraavassa on HAAGA-HELIAN opiskelijoille suunnatun kyselyn tuloksia, pohdintoineen.

Kyselyyn vastasi kaikkiaan 103 henkilöä, joista (37 %) 38 kpl oli miehiä ja (63 %) 64 kpl naisia. Naispuolisten suuri vastausprosentti johtuu siitä, että suurin osa kyselyyn vastanneista liiketalouden opiskelijoista oli naisia.

1. Miten opiskelijat huolehtivat oman tietokoneensa tietoturvasta?

Tässä tutkimustavoitteessa löytyi yhdenmukaiset eroavaisuudet tietojenkäsittelyn ja liiketalouden opiskelijoiden välillä, jonka kyselyn tulokset selvästi osoittivat (luku 6.1).

Liiketalouden opiskelijat näyttäisivät huolehtivan tietokoneensa tietoturvasta suhteellisesti enemmän, käyttäen tietoturvaratkaisuja ja seuraten tietoturvavaroituksia sekä reagoiden niihin. Tämä huolimatta siitä, että **tietojenkäsittelyn** opiskelijat näyttäisivät käyttävän suhteellisesti hieman enemmän haittasuojausohjelmia sekä varmuuskopiointia, vertailtaessa aloittelevia opiskelijoita keskenään.

Tietojenkäsittelyn opiskelijat puolestaan näyttäisivät huolehtivan tietokoneensa tietoturvasta suhteellisesti enemmän, käyttäen tietoturvaratkaisuja ja seuraten tietoturvavaroituksia sekä reagoiden niihin, vertailtaessa lopettelevia opiskelijoita keskenään.

Tulosten perusteella näyttäisi siltä, että opiskelijat huolehtivat ja kiinnittävät huomiota tietokoneensa tietoturvaan.

2. Miten opiskelijat kiinnittävät huomiota omiin käyttäjätietoihin internetissä liikkuessaan?

Tässä tutkimustavoitteessa ei löytynyt sellaisia yhdenmukaisia eroavaisuuksia tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välille sekä lopettelevien opiskelijoiden välille, jotta voisi sanoa eroja olevan koulutusohjelmien välillä, koska erot jakaantuivat liikaa kysymyksien välillä, jonka kyselyn tulokset selkeästi osoittivat (luku 6.2).

Liiketalouden opiskelijat näyttäisivät olevan suhteellisesti enemmän tietoisia sosiaaliseen kanssakäymiseen liittyvistä uhkista ja vaihtavan salasanojaan suhteellisesti useammin. **Tietojenkäsittelyn** opiskelijat puolestaan näyttäisivät käyttävän suhteellisesti hieman pidempiä ja enemmän vaihtelevia salasanoja eri palvelujen kesken sekä jakavan suhteellisesti vähemmän henkilökohtaista tietoa internetissä. Salasanojen sisällön suhteen ei huomattavia eroja löytynyt, vertailtaessa aloittelevia opiskelijoita keskenään.

Liiketalouden opiskelijat näyttäisivät olevan suhteellisesti enemmän tietoisia sosiaaliseen kanssakäymiseen liittyvistä uhkista ja vaihtavan salasanojaan suhteellisesti hieman useammin. Tämän lisäksi liiketalouden opiskelijat näyttäisivät käyttävän suhteellisesti enemmän vaihtelevia salasanoja eri palvelujen kesken ja jakavan suhteellisesti vähemmän henkilökohtaista tietoa. internetissä. **Tietojenkäsittelyn** opiskelijat puolestaan näyttäisivät käyttävän suhteellisesti pidempiä ja sisällöltään turvallisempia (=merkistöltään) salasanoja, vertailtaessa lopettelevia opiskelijoita keskenään.

Tulosten perusteella näyttäisi siltä, että opiskelijat kiinnittävät pääsääntöisesti huomiota käyttäjätietoihin internetissä, mutta vaihtelevasti, riippuen asiasta.

3. Miten opiskelijat huolehtivat Facebookin yksityisyydestä?

Tässä tutkimustavoitteessa ei löytynyt sellaisia yhdenmukaisia eroavaisuuksia tietojenkäsittelyn ja liiketalouden aloittelevien opiskelijoiden välille sekä lopettelevien opiskelijoiden välille, jotta voisi sanoa eroja olevan koulutusohjelmien välillä, koska erot jakaantuivat liikaa kysymyksien välillä, jonka kyselyn tulokset selkeästi osoittivat (luku 6.3).

Liiketalouden opiskelijat näyttäisivät olevan suhteellisesti enemmän tietoisia Facebookin käyttäjäehtojen muutoksista. **Tietojenkäsittelyn** opiskelijat puolestaan näyttäisivät jakavan suhteellisesti vähemmän henkilökohtaista tietoa Facebookissa ja kiinnittävän suhteellisesti enemmän huomiota siihen, ketä ihmisiä hyväksyvät kavereiksi Facebookissa. Facebookin virtuaalisovellusten käyttöönotossa (kriteerit huomioiden) ja kiertoviesteihin reagoinnissa ei ollut huomattavia eroja, vertailtaessa aloittelevia opiskelijoita keskenään.

Liiketalouden opiskelijat näyttäisivät reagoivan suhteellisesti hieman enemmän Facebookin kiertoviesteihin ja jakavan suhteellisesti hieman vähemmän henkilökohtaista tietoa Facebookissa. **Tietojenkäsittelyn** opiskelijat puolestaan näyttäisivät olevan suhteellisesti enemmän tietoisia Facebookin käyttäjäehtojen muutoksista ja kiinnittävän suhteellisesti enemmän huomiota siihen, ketä ihmisiä hyväksyvät kavereiksi Facebookissa sekä millä kriteereillä ottavat virtuaalisovelluksia käyttöön, vertailtaessa lopettelevia opiskelijoita keskenään.

Tulosten perusteella näyttäisi siltä, että opiskelijat huolehtivat pääsääntöisesti Facebookin yksityisyydestä, mutta vaihtelevasti, riippuen asiasta.

Pohdintaa

Tuloksien pieniin eroihin voi mahdollisesti vaikuttaa kyselyn otoskoko, koska erot voisivat olla mahdollisesti suuremmat, jos otoskoko olisi ollut suurempi. Erojen erilaiseen vaihteluun voi mahdollisesti vaikuttaa se, että 2. tavoitteessa oli 6 kysymystä ja 3. tavoitteessa 5 kysymystä vrt. 1. tavoitteen 2 kysymykseen.

Aloittelevien opiskelijoiden suhteen voi mahdollisesti tuloksiin vaikuttaa, opiskelijoiden aiempi koulutustausta, joka ei ole tiedossani. Lisäksi opiskelijoiden tuloksiin voi mahdollisesti vaikuttaa liiketalouden naispuolisten suurempi vastausprosentti, joilla saattaa olla erilaiset käyttötarkoitukset tietokoneella ja ehkä enemmän varovaisuutta miespuolisiin verrattuna. Tämä voi mahdollisesti selittää sen, että liiketalouden aloittelevat opiskelijat näyttäisivät seuraavan suhteellisesti enemmän tietoturvavaroituksia sekä reagoivan niihin, käyttävän suhteellisesti enemmän tietoturvaratkaisuja, vaihtavan suhteellisesti useammin salasanoja ja olevan suhteellisesti enemmän selvillä sosiaaliseen kanssakäymiseen liittyvistä uhista sekä Facebookin käyttäjäehtojen muutoksista. Lisäksi voi mahdollisesti selittää sen, että liiketalouden lopettelevat opiskelijat näyttäisivät olevan suhteellisesti enemmän selvillä

sosiaaliseen kanssakäymiseen liittyvistä uhista, vaihtavan suhteellisesti useammin salasanoja, käyttäen vaihtelevia salasanoja palvelukohtaisesti ja tiedostaen millaista tietoa on turvallista jakaa internetissä sekä Facebookissa, ja reagoiden kiertoviesteihin Facebookissa.

Yleisesti tuloksiin voi mahdollisesti vaikuttaa se, etteivät läheskään kaikki opiskelijat välttämättä tiedosta, mikä on palomuurin ja virustorjunnan ero, mihin haittasuojaus- sekä muita suojausohjelmia tarvitaan. Varmuuskopioinnin käytön alhaisuuteen voi mahdollisesti vaikuttaa se, etteivät läheskään kaikki opiskelijat tiedosta, mikä kaikki on varmuuskopiointia ja mihin sitä tarvitaan. Käyttöjärjestelmän tietoturvapäivitysten suhteen voi mahdollisesti tuloksiin vaikuttaa se, että osa opiskelijoista on voinut automatisoida tietoturvapäivitykset, jolloin asiaan ei välttämättä reagoi vastatessa. Tietoturvavaroituksien seuraamisen ja reagoinnin suhteen voi mahdollisesti tuloksiin vaikuttaa se, etteivät läheskään kaikki opiskelijat välttämättä tiedosta tietoturvavaroituksien tärkeyttä tai eivät ole kiinnostuneita seuraamaan niitä.

Salasanojen suhteen voi mahdollisesti tuloksiin vaikuttaa se, etteivät läheskään kaikki opiskelijat välttämättä tiedosta, millainen salasanan tulisi olla pituudeltaan, sisällöltään ja kuinka usein salasanaa tulisi vaihtaa, jotta salasana on turvallinen. Salasanojen vaihtelevuuteen palvelukohtaisesti tuloksiin voi mahdollisesti vaikuttaa se, että osalla opiskelijoista saattaa olla useita eri internet-palveluja käytössään (Facebook, useampia sähköpostitilejä jne.), jolloin on helpompaa käyttää muutamaa salasanaa palvelujen kesken.

Tietojen jakamisen suhteen voi mahdollisesti tuloksiin vaikuttaa se, etteivät läheskään kaikki opiskelijat välttämättä tiedosta, mitä kaikkea tietoa on turvallista jakaa internetissä ja Facebookissa. On myös mahdollista, että osa opiskelijoista on vastannut lopuksi kohtaan ”en mitään henkilökohtaista”, jotta ei paljastaisi todellista, kenties tietoturvattomampaa näkemystään.

Virtuaalisovellusten käyttöönoton suhteen voi mahdollisesti tuloksiin vaikuttaa se, etteivät läheskään kaikki opiskelijat välttämättä jaksa perehtyä virtuaalisovelluksien käyttötarkoitukseen ja turvallisuuteen, vaan ottavat sovelluksen käyttöön mielenkiinnon perusteella.

8 Yhteenveto

Tutkimuksessa on käsitelty yleisiä tietoturvauhkia internetin sosiaalisessa kanssakäymisessä, Facebookin yksityisyyden uhkia sekä selvitetty kyselyllä HAAGA – HELIA tietojenkäsittelyn ja liiketalouden aloittelevien ja lopettelevien opiskelijoiden suhtautumista tietoturvaan, käyttäessään internetiä sosiaaliseen kanssakäymiseen. Lisäksi on käyty läpi suojaustoimenpiteitä, joiden avulla tietoturvauhkilta voidaan suojautua.

Millaiset olivat tulokset ennakko-odotuksiin nähden?

Yleisten tietoturvauhkien suhteen tulokset olivat odotetunlaiset. Facebookin yksityisyyden suhteen tulokset yllättivät, kun uhkia löytyi enemmän, kuin alun perin odotin.

Päätavoitteisiin pohjautuvan kyselyn tulokset olivat yllättävät, kun mietitään miten hyvin odotuksiini nähden liiketalouden opiskelijat kokonaisuudessaan huolehtivat tietokoneensa tietoturvasta, kiinnittävät huomiota omiin käyttäjätietoihin internetissä ja huolehtivat Facebookin yksityisyydestä verraten tietojenkäsittelyn opiskelijoihin. Tuloksissa yllätti myös se, että tietojenkäsittelyn ja liiketalouden lopettelevien opiskelijoiden välillä erot olivat lähes olemattomat. Tietokoneen tietoturvasta huolehtimisen suhteen tulokset lopettelevien opiskelijoiden välillä olivat, kuin alun perin odotin. Koulutusohjelmien väliset erot olivat kuitenkin kokonaisuudessaan pienempiä, mitä alun perin odotin.

Päästiinkö tavoitteisiin?

Tutkimuksen tavoitteisiin päästiin, koska sain selville lähdeaineistolla mitä yleisiä tietoturvauhkia internetin sosiaaliseen kanssakäymiseen liittyy ja mitä uhkia Facebookin yksityisyyteen liittyy. Sain selville, miten opiskelijat huolehtivat oman tietokoneensa tietoturvasta, kiinnittävät huomiota omiin käyttäjätietoihin internetissä ja huolehtivat Facebookin yksityisyydestä. Tavoitekohtaan (1) sain selville eroja koulutusohjelmien, aloittelevien välille sekä lopettelevien välille. Tavoitekohtiin (2) ja (3) en saanut selville sellaisia eroavaisuuksia, jotta voisin sanoa koulutusohjelmien, aloittelevien välillä sekä lopettelevien välillä olevan yhdenmukaisia eroja, koska erot jakaantuivat liikaa kysymyksien välillä. On mahdollista, että tilastollisilla analysointimenetelmillä olisin voinut saada yhdenmukaisempia eroja aikaiseksi tavoitekohtiin (2) ja (3), mutta ajan- sekä osaamispuutteen takia en käyttänyt tilastollisia analysointimenetelmiä.

Olen tyytyväinen saavutettuihin tuloksiin, runsaaseen ajankäyttöön suhteutettuna.

Hyviä jatkotutkimusaiheita voisi olla tutkia esimerkiksi sähköpostin tai muiden sosiaaliseen kanssakäymiseen tarkoitettujen palvelujen vaikutusta uhkiin, johon voisi sisällyttää myös Facebookin laajemmassa mittakaavassa. Tutkimuksen pohjana voisi toimia tämä tutkimus, mutta tutkittaisiin asioita laajemmassa mittakaavassa ja kohdistettaisiin joko opiskelijoille tai kotikäyttäjille tai voisi perustua myös pelkästään kirjallisuuteen sekä muuhun lähdeaineistoon.

Tutkittava aihe osoittautui tarpeelliseksi, koska aiemmin ei ollut tehty vastaavia opinnäytetöitä, joissa olisi selvitetty HAAGA-HELIA opiskelijoiden suhtautumista tietoturvaan käytettäessä internetiä sosiaaliseen kanssakäymiseen. Tietoturvan merkitys korostuu päivä päivältä, jos eri uutismedioita seuraa, joka vain korosti aiheen tarpeellisuutta.

Tutkimus antoi arvokasta tietoa siitä, millaista tietoturvaan suhtautuminen on kahden eri koulutusohjelman, tietojenkäsittelyn ja liiketalouden opiskelijoiden, aloittelevien välillä sekä lopettelevien välillä, käyttäessään internetiä sosiaaliseen kanssakäymiseen.

Tästä opinnäytetyöstä on varmasti hyötyä kaikille opiskelijoille, opettajille sekä muille asiasta kiinnostuneille, jo pelkästään aiheen ajankohtaisuuden ja tärkeyden perusteella.

Lähdeluettelo

Digitoday 2009. Tietoturva. Viitattu 1.3.2009.

http://www.digitoday.fi/tietoturva/2009/02/27/facebookissa-jo-toinen-vakoiluohjelma-viikon-sisaan/20095423/66

Digitoday 2009 -1. Tietoturva. Viitattu 4.3.2009.
http://www.digitoday.fi/tietoturva/2009/03/03/tietoturvayhtiot-moittivat-facebookia-virus-taas/20095752/66

Facebook 2009. Timeline. Viitattu 20.1.2009.

http://fi.www.facebook.com/press/info.php?timeline

Facebook 2009 -1. Factsheet. Viitattu 20.1.2009.

http://fi.www.facebook.com/press/info.php?factsheet

C. Abram, L. Pearlman 2008. Facebook for dummies. Hoboken (N.J.): Wiley

Elisa, 2009. Elisa laajakaista – tuotteet. Viitattu 16.1.2009

http://www.elisa.fi/yksityisille/laajakaista/laajakaista/tekniset_tiedot/

Iltasanomat, 2009. Digiuutiset – Virus uhkaa Facebookin käyttäjiä. Viitattu 06.02.2009

http://www.iltalehti.fi/digi/200812088734018_du.shtml

Järvinen P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo.

Korpela, J. – K. 2005. Turvallisesti netissä - kodin tietoturvaopas. Jyväskylä: Docendo.

Kuivanen, I. 2005. Tietoturvan perusteita – virukset. Helsinki: Stadia.
Viitattu 16.1.2009 http://cs.stadia.fi/~kuivanen/tietoturva/virukset.php

Mbnet 2005. Yksityisyyden suoja on kuluttujan oikeus. Viitattu 12.3.2009.

http://www.mbnet.fi/nettijatkot/2005/12/yksityisyydensuoja/

Microsoft 2006. Salasanan vahvuus ja salasanasuojaus. Viitattu 3.3.2009.

http://www.microsoft.com/finland/protect/yourself/password/create.mspx

Oulun yliopisto, 2009. Tietoturvatietoa – Roskaposti. Viitattu 17.1.2009 http://www.oulu.fi/tietohallinto/tietoturva/sisalto/tt-kampanja/www_materiaali_1_0/FI/roskaposti.htm

Saarijärvi, M. 2004. Tietoturva - ja verkkopalvelujen käyttö kodeissa – kyselytutkimus laajakaistayhteyden käyttäjille. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Pro Gradu – tutkielma. Viitattu 16.1.2009. www.cs.uta.fi/research/theses/masters/Saarijarvi_Marko.pdf

Opasmedia 2006. Suomen internetopas – tietoturva. Opasmedia Oy. Viitattu 17.1.2009 http://www.internetopas.com/yleistietoa/tietoturva/

Tietoturvaopas 2008. Yleistä internetistä. Viitattu 19.1.2009. http://www.tietoturvaopas.fi/perusohjeet/yleistainternetista.html

Tietoturvaopas 2008 1. Tietomurrot ja varkaudet. Viitattu 20.1.2009. http://www.tietoturvaopas.fi/uhatjaniidentorjunta/tietomurrotjavarkaudet.html

Tietoturvaopas 2008 2. Haittaohjelmat. Viitattu 22.1.2009. http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html

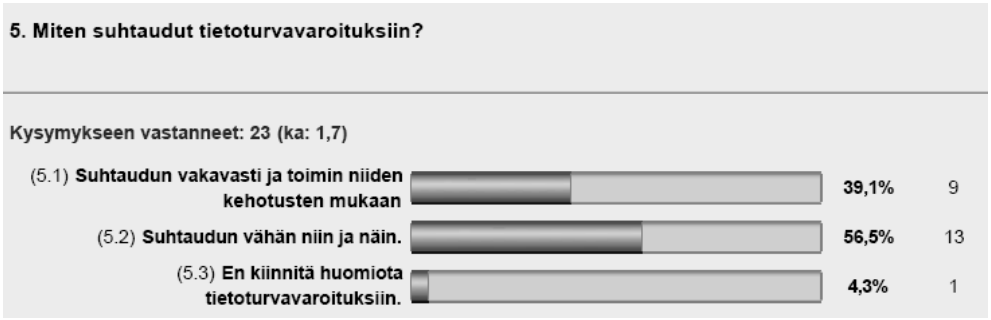
Tietoturvaopas 2008 3. Tietojen häviäminen. Viitattu 22.1.2009. http://www.tietoturvaopas.fi/uhatjaniidentorjunta/tietojenhaviaminen.html

T. Mikkola, O. Virkki 2006. ICT03D Tieto ja tiedon varastointi: Tietoturva tiedon varastoinnissa. Viitattu 19.1.2009. http://myy.haaga-helia.fi/~ict03d/johdanto/mats/ICT03d_Tietoturva.pdf

Liitteet

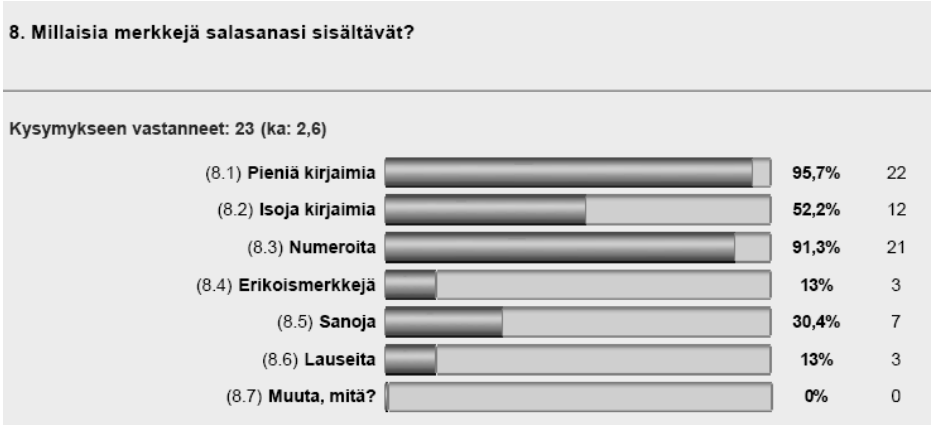
Liite 1. Tietojenkäsittelyn koulutusohjelman aloittelevien opiskelijoiden kyselytulokset

Kuva 17. Tietoturvaratkaisujen käyttö tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa



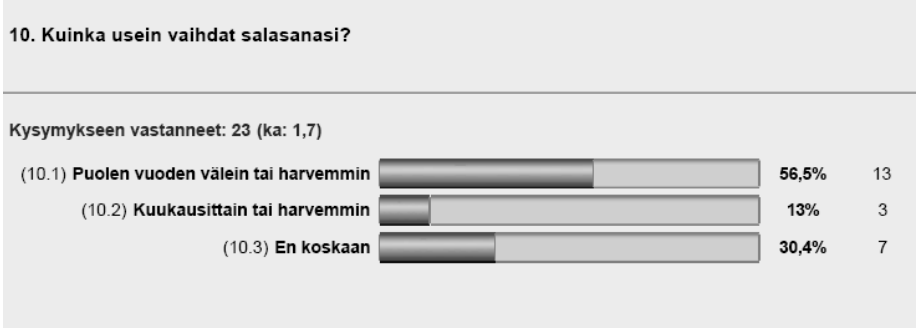
Kuva 18. Tietoturvavaroituksiin suhtautuminen tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa

Kuva 19. Internetin sosiaalisen kanssakäymisen uhkiin suhtautuminen tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa



Kuva 20. Salasanojen sisältö tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa

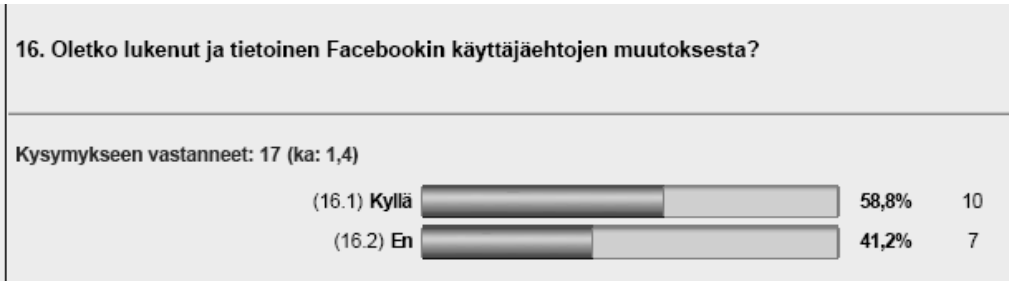
Kuva 21. Salasanojen pituus tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa



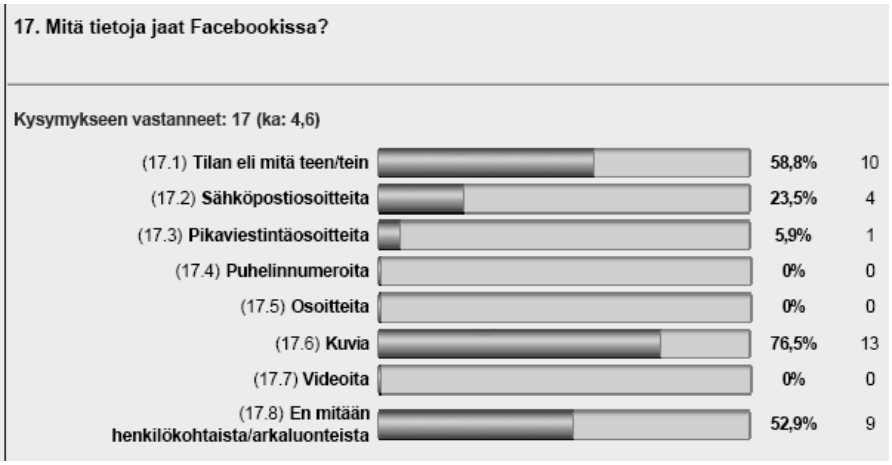
Kuva 22. Salasanojen vaihtoväli tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa

Kuva 23. Salasanojen vaihtelevuus eri palvelujen kesken tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa

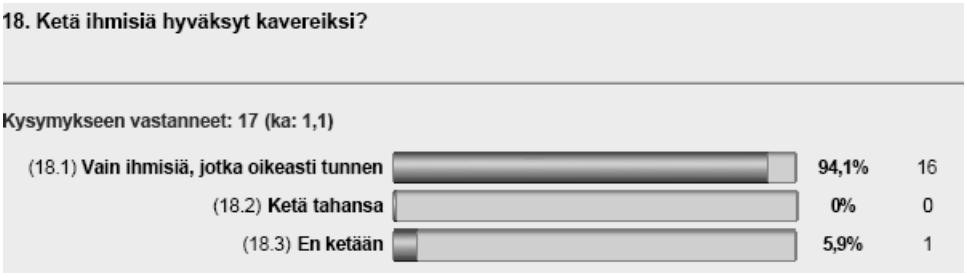
Kuva 24. Tietojen jakaminen internetissä tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa



Kuva 25. Tietoisuus Facebookin käyttäjäehtojen muutoksesta tietojenkäsittelyn aloittelevien opiskelijoiden keskuudess

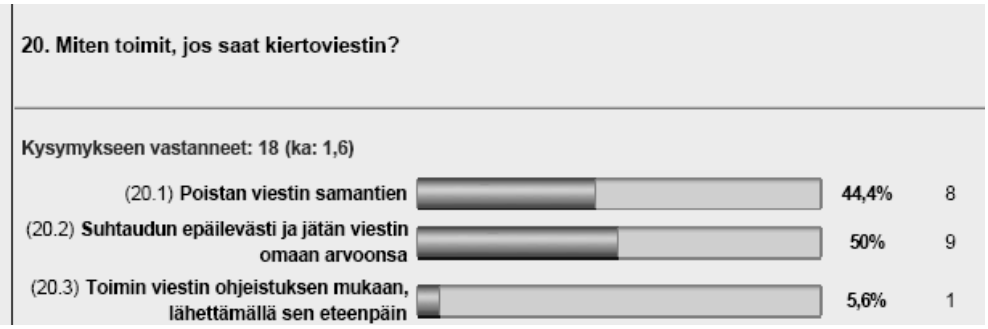


Kuva 26. Tietojen jakaminen Facebookissa tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa



Kuva 27. Facebookin kaveriksi hyväksymiskriteerit tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa

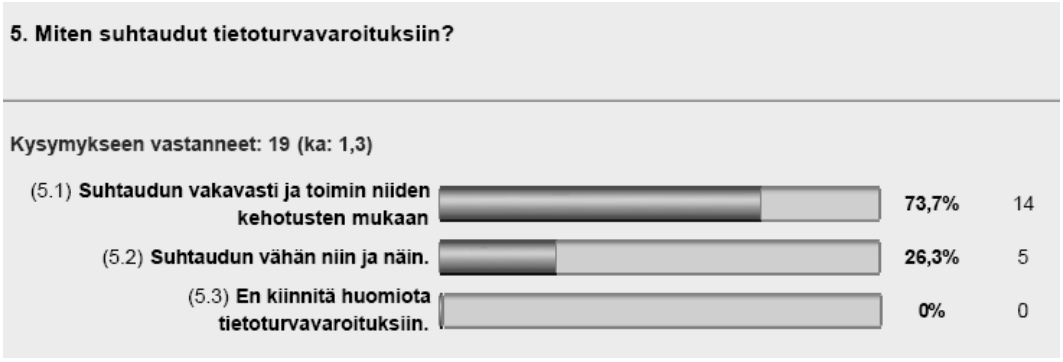
Kuva 28. Facebookin virtuaalisovellusten käyttöönotto kriteerit tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa



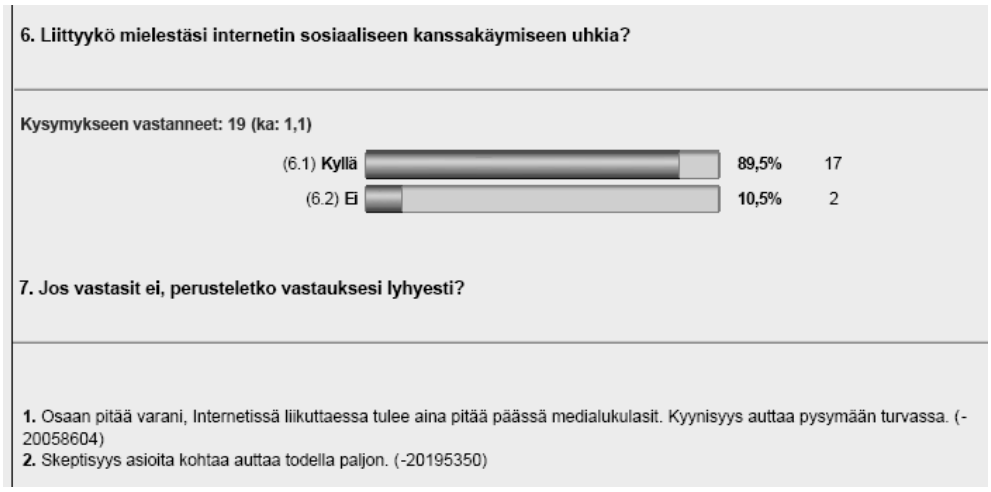
Kuva 29. Facebookin kiertoviestien toimintatavat tietojenkäsittelyn aloittelevien opiskelijoiden keskuudessa

Liite 2. Tietojenkäsittelyn koulutusohjelman lopettelevien opiskelijoiden kyselytulokset

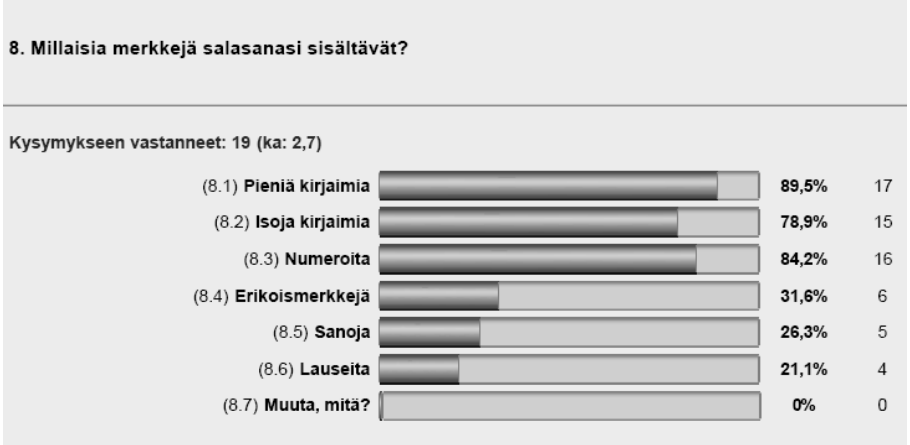
Kuva 30. Tietoturvaratkaisujen käyttö tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa



Kuva 31. Tietoturvavaroituksiin suhtautuminen tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

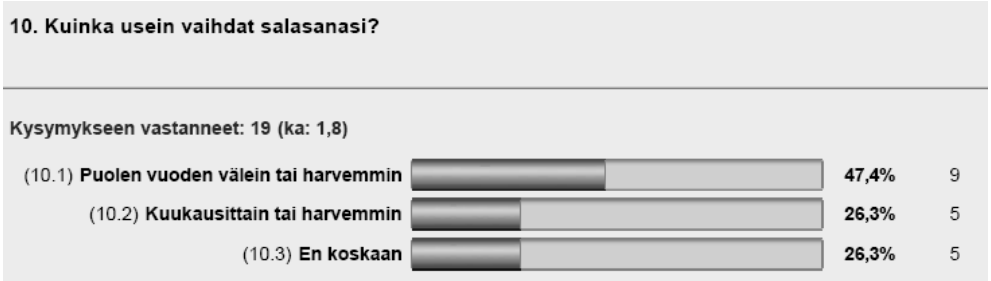


Kuva 32. Internetin sosiaalisen kanssakäymisen uhkiin suhtautuminen tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa



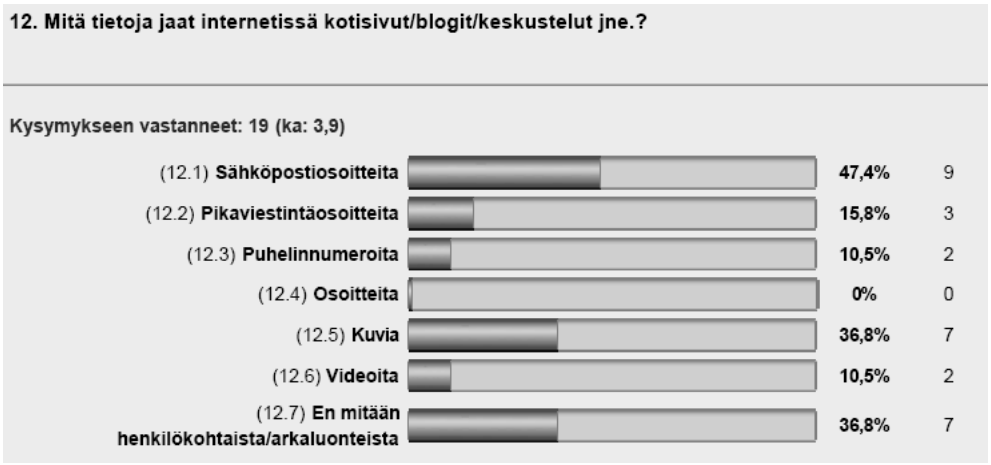
Kuva 33. Salasanojen sisältö tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

Kuva 34. Salasanojen pituus tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa



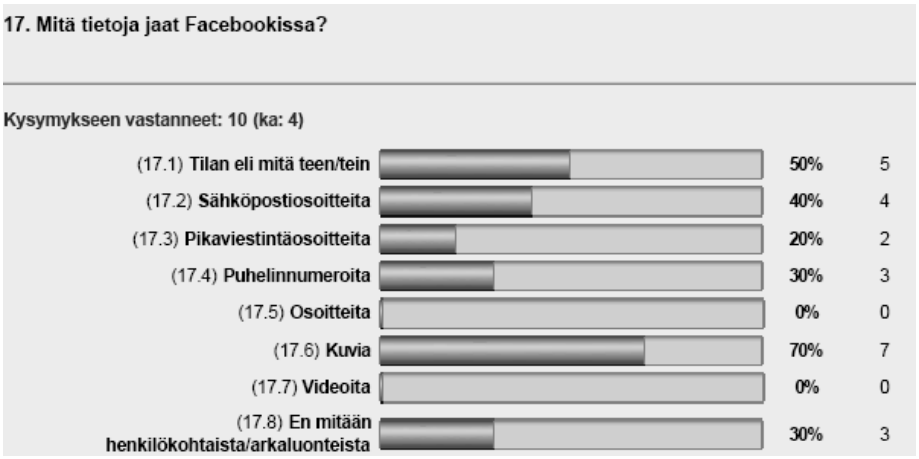
Kuva 35. Salasanojen vaihtoväli tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

Kuva 36. Salasanojen vaihtelevuus eri palvelujen kesken tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

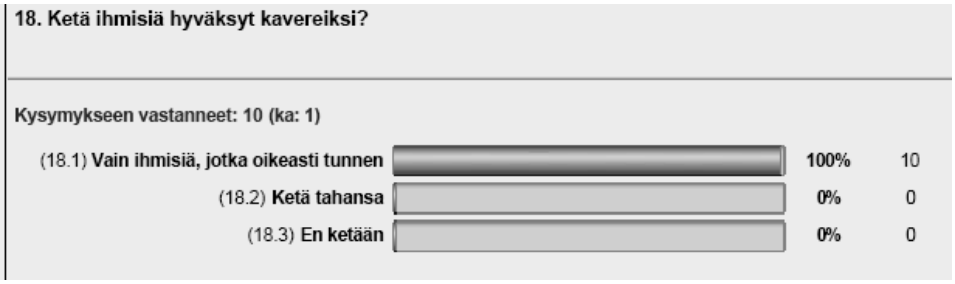


Kuva 37. Tietojen jakaminen internetissä tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

Kuva 38. Tietoisuus Facebookin käyttäjäehtojen muutoksesta tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

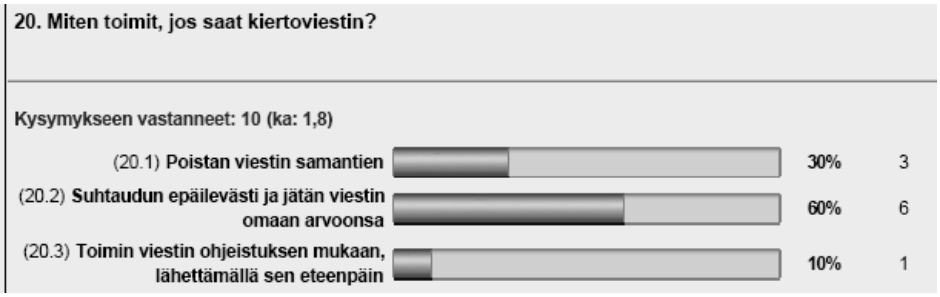


Kuva 39. Tietojen jakaminen Facebookissa tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa



Kuva 40. Facebookin kaveriksi hyväksymiskriteerit tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

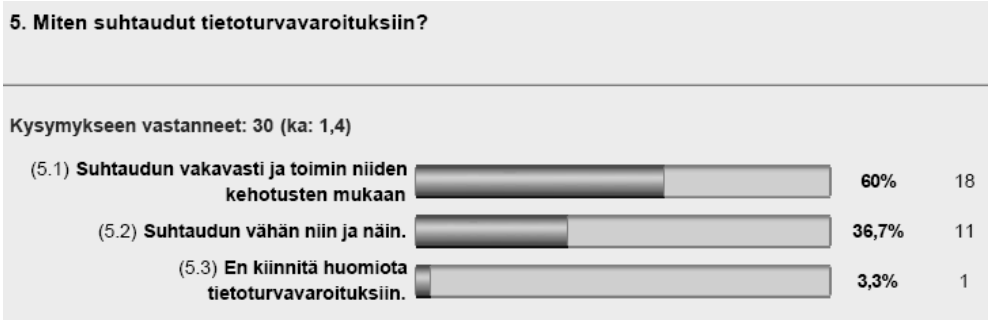
Kuva 41. Facebookin virtuaalisovellusten käyttöönotto kriteerit tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa



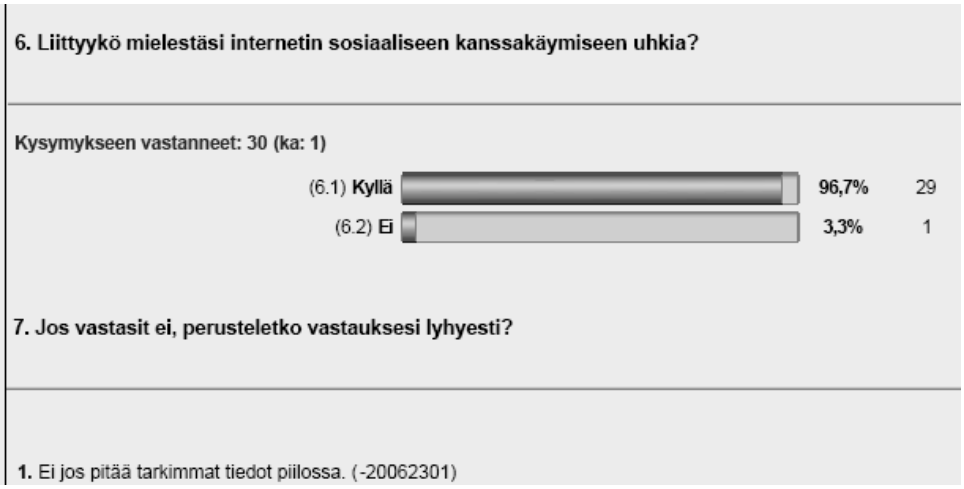
Kuva 42. Facebookin kiertoviestien toimintatavat tietojenkäsittelyn lopettelevien opiskelijoiden keskuudessa

Liite 3. Liiketalouden koulutusohjelman aloittelevien opiskelijoiden kyselytulokset

Kuva 43. Tietoturvaratkaisujen käyttö liiketalouden aloittelevien opiskelijoiden keskuudessa



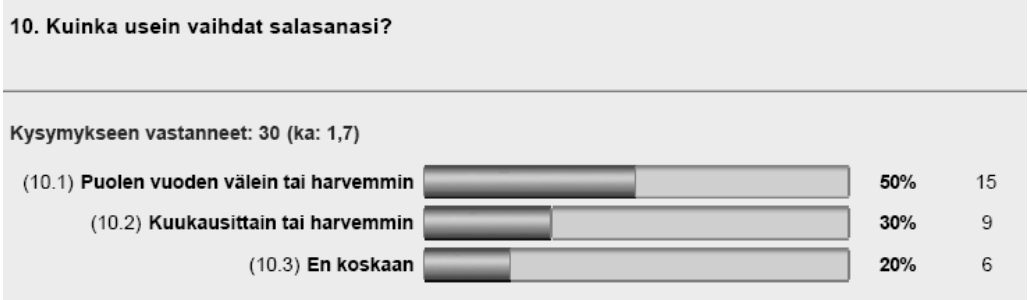
Kuva 44. Tietoturvavaroituksiin suhtautuminen liiketalouden aloittelevien opiskelijoiden keskuudessa



Kuva 45. Internetin sosiaalisen kanssakäymisen uhkiin suhtautuminen liiketalouden aloittelevien opiskelijoiden keskuudessa

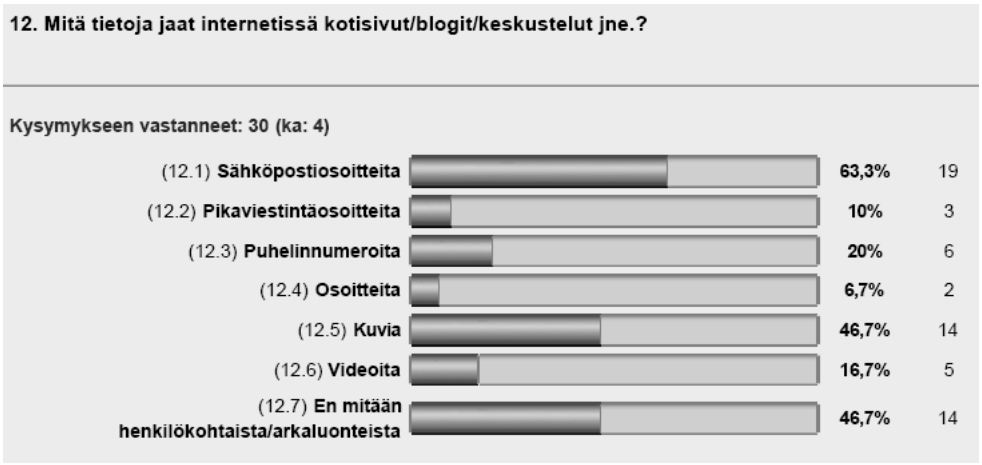
Kuva 46. Salasanojen sisältö liiketalouden aloittelevien opiskelijoiden keskuudessa

Kuva 47. Salasanojen pituus liiketalouden aloittelevien opiskelijoiden keskuudessa

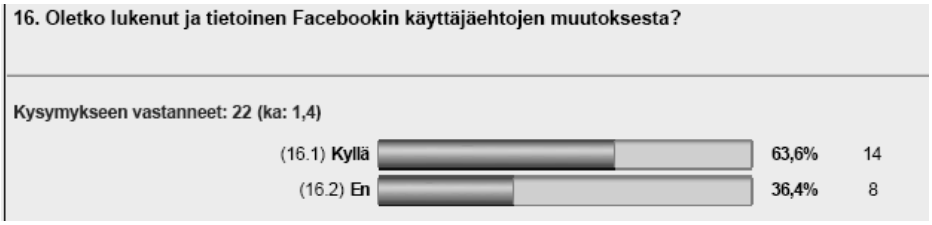


Kuva 48. Salasanojen vaihtoväli liiketalouden aloittelevien opiskelijoiden keskuudessa

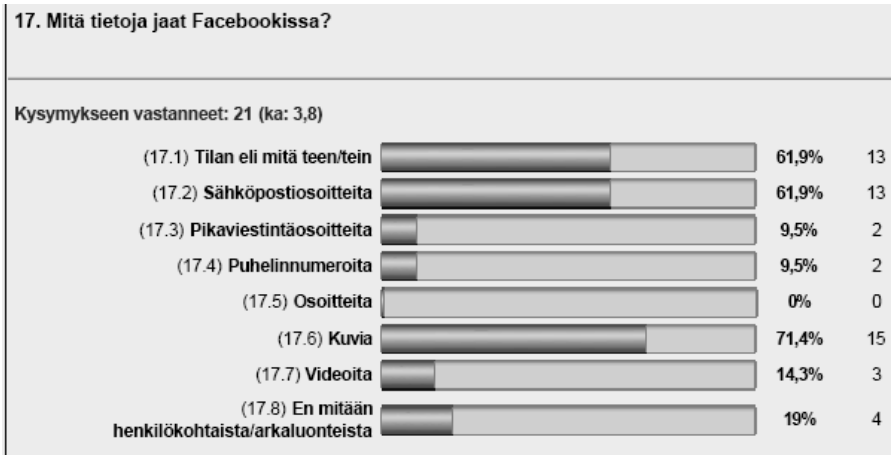
Kuva 49. Salasanojen vaihtelevuus eri palvelujen kesken liiketalouden aloittelevien opiskelijoiden keskuudessa



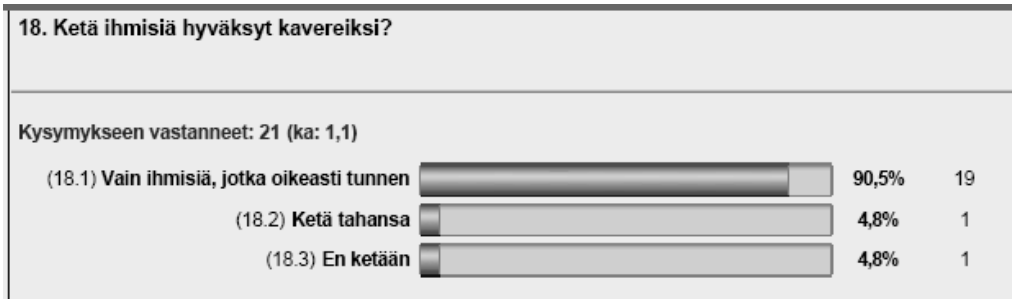
Kuva 50. Tietojen jakaminen internetissä liiketalouden aloittelevien opiskelijoiden keskuudessa



Kuva 51. Tietoisuus Facebookin käyttäjäehtojen muutoksesta liiketalouden aloittelevien opiskelijoiden keskuudessa

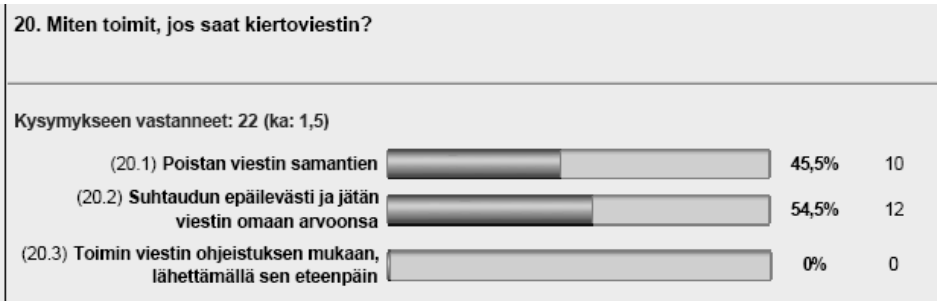


Kuva 52. Tietojen jakaminen Facebookissa liiketalouden aloittelevien opiskelijoiden keskuudessa



Kuva 53. Facebookin kaveriksi hyväksymiskriteerit liiketalouden aloittelevien opiskelijoiden keskuudessa

Kuva 54. Facebookin virtuaalisovellusten käyttöönotto kriteerit liiketalouden aloittelevien opiskelijoiden keskuudessa

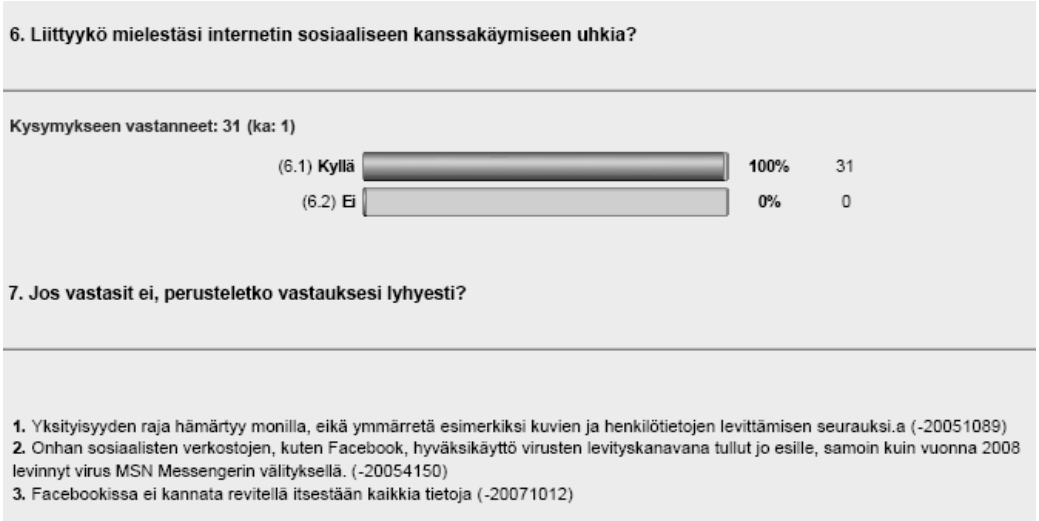


Kuva 55. Facebookin kiertoviestien toimintatavat liiketalouden aloittelevien opiskelijoiden keskuudessa

Liite 4. Liiketalouden koulutusohjelman lopettelevien opiskelijoiden kyselytulokset

Kuva 56. Tietoturvaratkaisujen käyttö liiketalouden lopettelevien opiskelijoiden kesken

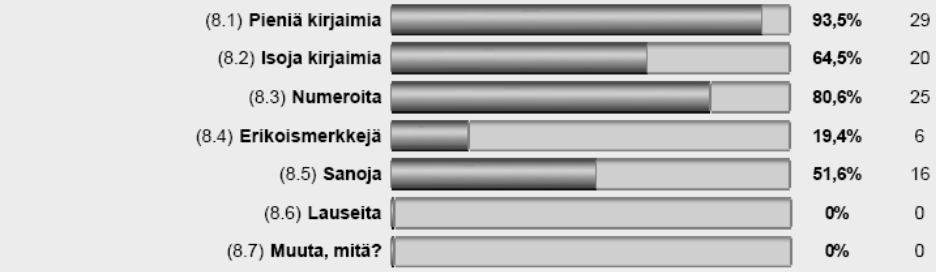
Kuva 57. Tietoturvavaroituksiin suhtautuminen liiketalouden lopettelevien opiskelijoiden kesken



Kuva 58. Internetin sosiaalisen kanssakäymisen uhkiin suhtautuminen liiketalouden lopettelevien opiskelijoiden keskuudessa

8. Millaisia merkkejä salasanasi sisältävät?

Kysymykseen vastanneet: 31 (ka: 2,6)



Kuva 59. Salasanojen sisältö liiketalouden lopettelevien opiskelijoiden keskuudessa

9. Kuinka pitkiä salasanasi ovat?

1. 11 merkkiä (-20050906)
2. 8 merkkiä (-20050924)
3. 8 (-20051030)
4. 6-10 (-20051089)
5. 8-9 (-20051174)
6. 7-9 merkkiä (-20051449)
7. 8 merkkiä (-20051843)
8. 6-8 merkkiä (-20052515)
9. 6-8 merkkiä (-20053443)
10. 6-10 merkkiä (-20054042)
11. 8-9 merkkiä (-20054150)
12. 5-10 merkkiä (-20054525)
13. 4-6 (-20055980)
14. 8-10 merkkiä (-20056356)
15. 6-8 kirjainta (-20057108)
16. noin 10 merkkiä (-20058456)
17. noin 8 merkkiä (-20062070)
18. 4-10 kirjainta (-20065995)
19. 5-10 kirjainta (-20067236)
20. 10 merkkiä tai yli (-20067232)
21. 8 (-20071012)
22. 5-8 (-20071174)
23. 6-10 merkkiä (-20071874)
24. 5-10 merkkiä (-20089335)
25. 10 (-20098748)
26. 5-8 merkkiä (-20100772)
27. 8 merkkiä (-20108525)
28. 7-9 merkkiä (-20109630)
29. 8-10 kirjainta (-20113272)
30. 8-12 sanaa riipuen salasanasta (-20122745)

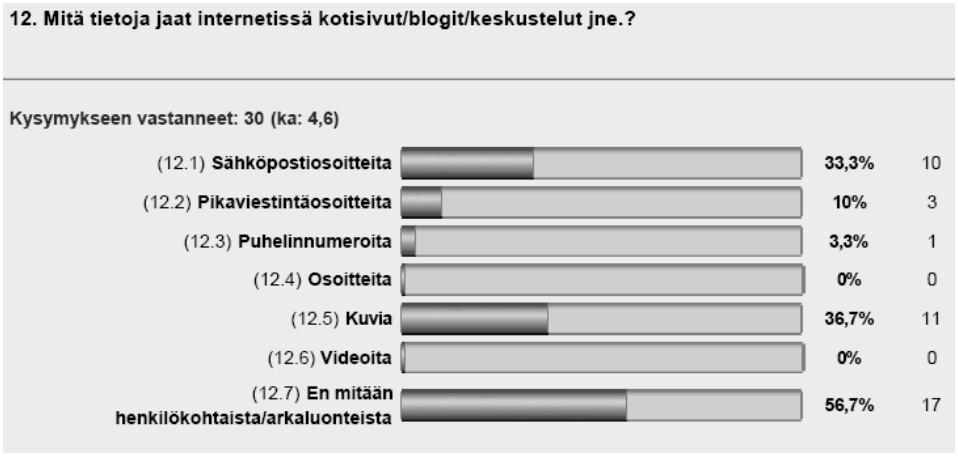
Kuva 60. Salasanojen pituus liiketalouden lopettelevien opiskelijoiden keskuudessa

10. Kuinka usein vaihdat salasanasi?

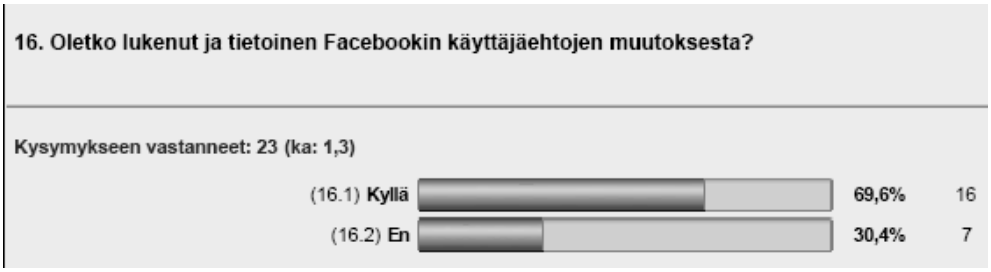
Kysymykseen vastanneet: 30 (ka: 1,9)

Kuva 61. Salasanojen vaihtoväli liiketalouden lopettelevien opiskelijoiden keskuudessa

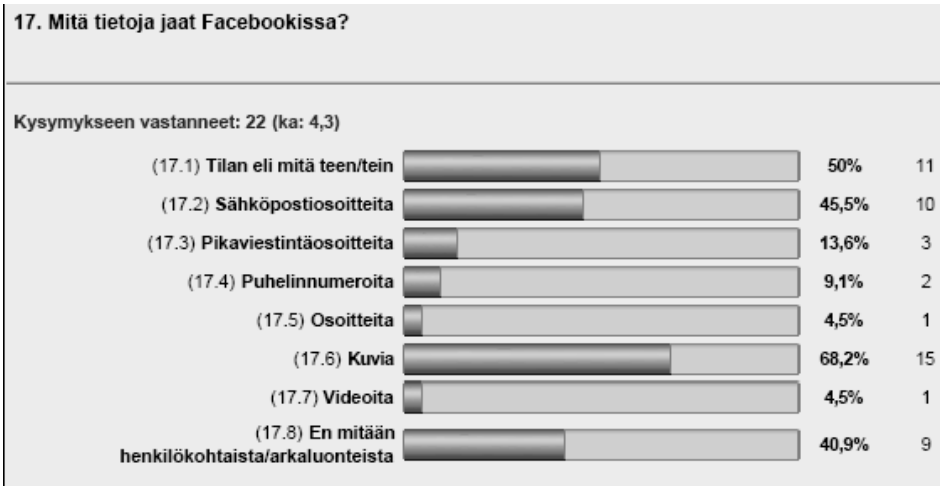
Kuva 62. Salasanojen vaihtelevuus eri palvelujen kesken liiketalouden lopettelevien opiskelijoiden keskuudessa



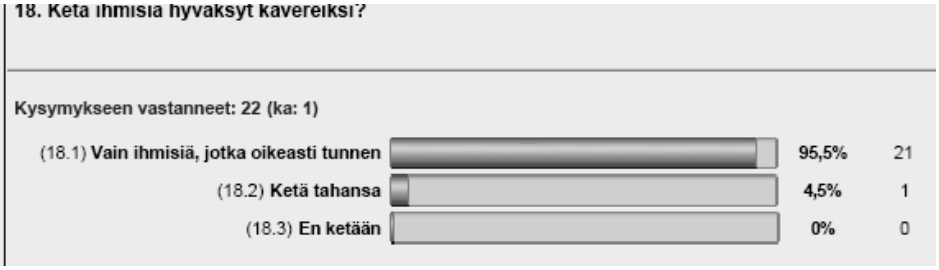
Kuva 63. Tietojen jakaminen internetissä liiketalouden lopettelevien opiskelijoiden keskuudessa



Kuva 64. Tietoisuus Facebookin käyttäjäehtojen muutoksesta liiketalouden lopettelevien opiskelijoiden keskuudessa

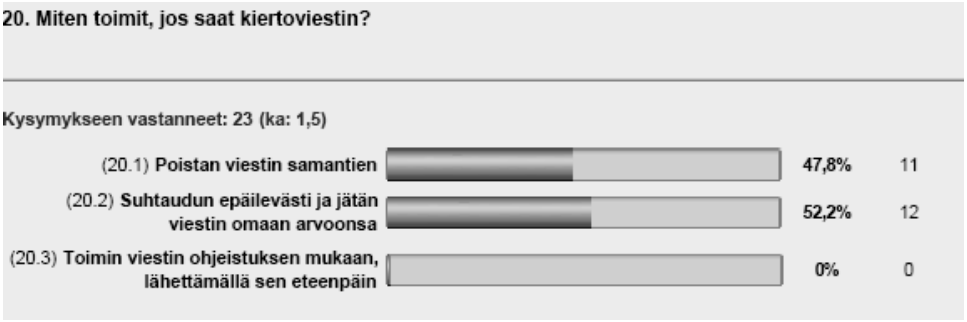


Kuva 65. Tietojen jakaminen Facebookissa liiketalouden lopettelevien opiskelijoiden keskuudessa



Kuva 66. Facebookin kaveriksi hyväksymiskriteerit liiketalouden lopettelevien opiskelijoiden keskuudessa

Kuva 67. Facebookin virtuaalisovellusten käyttöönotto kriteerit liiketalouden lopettelevien opiskelijoiden keskuudessa



Kuva 68. Facebookin kiertoviestien toimintatavat liiketalouden lopettelevien opiskelijoiden keskuudessa

Liite 5. Kyselylomake tietoturvaan suhtautumisesta sosiaalisessa kanssakäymisessä

TAUSTATIEDOT

1) Sukupuoli

o Mies

o Nainen

2) Mitä tietoturvaratkaisuja käytät säännöllisesti?

□ Käyttöjärjestelmän tietoturvapäivitykset

□ Palomuuria

□ Virustorjuntaa

□ Haittasuojausohjelmaa

□ Muuta suojausohjelmaa

□ Varmuuskopiointia

□ En mitään

3) Miten suhtaudut tietoturvavaroituksiin?

o Suhtaudun vakavasti ja toimin niiden kehotusten mukaan

o Suhtaudun vähän niin ja näin.

o En kiinnitä huomiota tietoturvavaroituksiin.

4) Liittyykö mielestäsi internetin sosiaaliseen kanssakäymiseen uhkia?

o Kyllä

o Ei

5) Jos vastasit ei, perusteletko vastauksesi lyhyesti?

6) Millaisia merkkejä salasanasi sisältävät?

□ Pieniä kirjaimia

□ Isoja kirjaimia

□ Numeroita

□ Erikoismerkkejä

□ Sanoja

□ Lauseita

□ Muuta, mitä?

7) Kuinka pitkiä salasanasi ovat?

8) Kuinka usein vaihdat salasanasi?

o Puolen välein tai harvemmin

o Kuukausittain tai harvemmin

o En koskaan

9) Vaihtelevatko salasanasi eri palvelujen kesken?

o Kyllä, jokaiseen palveluun on aina eri salasana

o Muutama salasana, jotka on käytössä eri palvelujen kesken

o Ei, yksi salasana on käytössä kaikissa palveluissa

10) Mitä tietoja jaat internetissä kotisivut/blogit/keskustelut jne.?

□ Sähköpostiosoitteita

□ Pikaviestintäosoitteita

□ Puhelinnumeroita

□ Osoitteita

□ Kuvia

□ Videoita

□ En mitään henkilökohtaista/arkaluonteista

11) Oletko lukenut ja tietoinen Facebookin käyttäjäehtojen muutoksesta?

o Kyllä

o En

12) Mitä tietoja jaat Facebookissa?

□ Tilan eli mitä teen/tein

□ Sähköpostiosoitteita

- ☐ Pikaviestintäosoitteita
- ☐ Puhelinnumeroita
- ☐ Osoitteita
- ☐ Kuvia
- ☐ Videoita
- ☐ En mitään henkilökohtaista/arkaluonteista

13) Ketä ihmisiä hyväksyt kavereiksi?

- o Vain ihmisiä, jotka oikeasti tunnen
- o Ketä tahansa
- o En ketään

14) Millä perusteella otat käyttöön virtuaalisovelluksia?

- o Selvitettyäni käyttötarkoituksen ja sovelluksen turvallisuuden
- o Todettuani sovelluksen olevan mielenkiintoinen
- o En ota käyttöön sovelluksia

15) Miten toimit, jos saat kiertoviestin?

- o Poistan viestin saman tien
- o Suhtaudun epäilevästi ja jätän viestin omaan arvoonsa
- o Toimin viestin ohjeistuksen mukaan, lähettämällä sen eteenpäin

HAAGA-HELIAN tietojenkäsittelyn ja liiketalouden koulutusohjelmien aloittelevien ja lopettelevien opiskelijoiden suhtautuminen tietoturvaan internetin sosiaalisessa kanssakäymisessä

Tutkimuksen loppuraportti

Toteuttaja: Juha Hirvonen

Pvm: 27.5.2009

1 Tausta

Projekti toteutettiin HAAGA – HELIAn tietojenkäsittelyn koulutusohjelmaan kuuluvassa opinnäytetyö opintokokonaisuudessa.

Projektin tavoitteena oli toteuttaa selvitys, jossa tutkitaan tietoturvaan suhtautumista internetin sosiaalisessa kanssakäymisessä, kun kohderyhmänä olivat HAAGA – HELIAn ammattikorkeakoulun Pasilan toimipisteen tietojenkäsittelyn ja liiketalouden koulutusohjelman aloittelevat ja lopettelevat opiskelijat.

Aiemmin vastaavia projekteja ei ollut tehty, jonka johdosta projekti oli tarpeellinen. Projektin tavoitteena oli aikaan saada kuvaus siitä, kuinka HAAGA-HELIA ammattikorkeakoulun kahden eri koulutusohjelman tietojenkäsittelyn ja liiketalouden (aloittelevat) ja (lopettelevat) opiskelijat suhtautuvat tietototurvaan, käyttäessään internetiä sosiaaliseen kanssakäymiseen. Työn edetessä sähköposti jäi pois alkuperäisestä suunnitelmasta poiketen, vedoten rajalliseen käytössä olevaan aikaan ja työn laajuuteen ilman sähköpostia.

Tuloksena syntynyt raportti antaa yhtenäisen dokumentaation tutkimuksen laatijalle ja ohjaajalle sekä muille osapuolille, jossa on selvitetyt asiat järjestyksessä.

2 Aikataulutilanne

Lopputulos saavutettiin lähes suunniteltujen aikataulujen puitteissa, vaikka vaiheittain pientä vaihtelua tapahtuikin projektin edetessä.

Taulukko 1. Projektin ajoitus

Vaihe	**Alkuperäinen suunniteltu aloituspvm**	**Uudelleen suunniteltu aloituspvm**	**Toteutunut aloituspvm**	**Alkuperäinen suunniteltu lopetuspvm**	**Uudelleen suunniteltu lopetuspvm**	**Toteutunut lopetuspvm**
Aloitusvaihe	Avoin	Avoin	Avoin	Avoin	Avoin	29.1.2009
Vaihe 1	29.1.2009	29.1.2009	29.1.2009	27.2.2009	5.3.2009	5.3.2009
Vaihe 2	28.2.2009	6.3.2009	6.3.2009	6.3.2009	3.4.2009	3.4.2009
Vaihe 3	7.3.2009	4.4.2009	4.4.2009	4.5.2009	7.5.2009	7.5.2009
Koko projekti	29.1.2009	29.1.2009	29.1.2009	4.5.2009	7.5.2009	7.5.2009

Taulukko 2. Projektin työmäärät

Vaihe	Alkuperäinen suunniteltu työmäärä	Toteutunut työmäärä	Ero työmäärä	Uudelleen suunniteltu työmäärä	Toteutunut työmäärä	Ero työmäärä
Aloitusvaihe	76	76	0	76	76	0
Vaihe 1	104	94	-10	104	94	-10
Vaihe 2	22	26	+4	22	26	+4
Vaihe 3	198	196	-2	198	196	-2
Koko projekti	400	392	-8	400	392	-8

Projektisuunnitelmassa suunniteltu työmäärä projektille oli 400 tuntia, josta toteutui 392 tuntia eli vain hieman jäätiin suunnitelluista tunneista projektissa.

3 Saavutetut tulokset ja kokemukset

Projektin tuloksena syntyi kuvaus, jossa kerrotaan kuinka HAAGA - HELIAn Pasilan toimipisteen tietojenkäsittelyn ja liiketalouden koulutusohjelmien aloittelevat ja lopettelevat opiskelijat suhtautuvat tietoturvaan käyttäessään internetiä sosiaalisessa kanssakäymisessä eli ”miten huolehtivat oman tietokoneensa tietoturvasta”, ”miten kiinnittävät huomiota käyttäjätietoihin internetissä” ja ”miten huolehtivat Facebookin yksityisyydestä”. Tämän lisäksi kuvauksessa kerrotaan ”mitä tietoturvauhkia yleisesti sosiaaliseen kanssakäymiseen liittyy”, ”mitkä uhkatekijät voivat mahdollisesti uhata Facebookin käyttäjän yksityisyyttä” ja ”suojaus- ja ennaltaehkäisymenetelmät”, joilla voidaan suojautua edellä mainituilta, yleisiltä ja Facebookin yksityisyyden uhilta.

Projektin tulokset on koottuna yhteen tulosraporttiin, joka sisältää kaikki yllämainitut selvityskuvaukset. Projektin tuottamat dokumentaatiot/tulokset eli aihe-ehdotus, projektisuunnitelma (sis. tutkimussuunnitelman), edistymisraportit, loppuraportti ja varsinainen tulosraportti/tutkimus on tallennettu projektinhallintakansioon. Projektin tulokset luovutetaan HAAGA - HELIALLE projektin ohjaajalle (sisältää projektinhallintakansion).

Olen tyytyväinen saavutettuun lopputulokseen saavuttuun kokonaistulokseen tavoitteet huomioiden ja luotan asetettujen laadullisten kriteerien täyttymiseen projektin tulosten osalta, vaikka todellisuudessa ne selviävät myöhemmin, kun projektin tulokset arvioidaan oppilaitoksen edustajien taholta.

4 Työn eteneminen

Projektin alussa työ eteni nopeasti, koska aihealue oli entuudestaan tuttu ja taustatietoa aiheeseen löytyi paljon. Hieman hankaluuksia tuotti aiheen rajaaminen riittävän tarkasti. Osittain työn etenemistä hankaloitti myös pienet toteutuneet riskit (lyhytaikaiset sairastumiseni), joiden vaikutuksen onnistuin minimoimaan suuremmilla ponnistuksilla aina sairastelun jälkeen ja näin projekti pysyi lähes suunniteltujen aikataulujen puitteissa. Kyselyn laatiminen tuotti hieman ongelmia, kun jouduin muokkailemaan kysymyksiä useampaan kertaan, jotta kysymyksistä tuli sellaisia, joilla sain selvyyden projektin päätavoitteisiin. Myös kyselyn vastauksien eli tulosten analysointi ja kirjoitus tuotti hieman ongelmia, koska oli hieman erilaiset näkemykset projektin ohjaajan kanssa siitä, että miten vastauksia tulisi käsitellä, tarkentaa ja kirjata työhön. Ongelmista selvisin projektin ohjaajan antamien neuvojen sekä parannusehdotusten avulla, jonka mukaan tein entistä suurempia ponnisteluja. Tiivistin projektin työskentelyä projektin edetessä loppua kohti, jolla varmistin työn etenemisen suurin piirtein suunnitellussa aikataulussa. Hyvä yhteishenki vallitsi koko projektin ajan ohjaajan ja tekijän välillä.

Projekti valmistui suurin piirtein suunnitellun aikataulun puitteissa ja oppimistavoitteet täyttyivät.

5 Resurssien käyttö

Projektin tehtävät jaoin käytössä olevan ajan mukaan kohtuullisen tasapuolisesti jaksottaen pääasiassa arkiviikoille. Pyrin siihen, että kaikki tehdyt ponnistelut projektin eteen olivat yhtä tärkeitä tavoitteen saavuttamisessa eli projektin lopputuloksen kannalta. Näin laajassa projektissa työresurssien vaihtelu on hyvin normaalia, koska yllättäviä esteitä usein tulee. Pysyin aikataulussa suurin piirtein läpi projektin ajan, jonka varmistin sillä, että tein välillä suurempia työmääriä kuin olin alun perin suunnitellut. Tehtäviin kului ajallisesti työresursseja lähestulkoon projektisuunnitelmassa suunniteltujen työtuntien mukaan, hieman vähemmän.

6 Ehdotukset jatkotoimenpiteiksi

Ehdotetaan, että projekti päätetään.