HAAGA-HELIA
ammattikorkeakoulu

Kahdeksasluokkalaisten tietoisuus tietoturvauhkista sosiaalisessa mediassa ja sen vaikutus heidän käytökseensä

Maria Laaka

Tutkimussuunnitelma
Tietotekninen selvitys ja koulutta-
minen, ICT2TN011-5
27.10.2011

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

27.10.2011

Tietojenkäsittely

Tekijä tai tekijät Maria Laaka	**Ryhmätunnus tai aloitusvuosi** 2009
Raportin nimi Kahdeksasluokkalaisten tietoisuus tietoturvauhkista sosiaalisessa mediassa ja sen vaikutus heidän käytökseensä	**Sivu- ja liitesivumäärä** 16+0
Opettajat tai ohjaajat Pilvi Heinonen, Tero Karvinen	

Tutkimussuunnitelma pohjustaa tutkimusta suomalaista yläastetta käyvien kahdeksasluokkalaisten tietoisuudesta sosiaaliseen mediaan liittyvistä ja sen kautta leviävistä haittaohjelmista ja huijauksista. Lisäksi tutkimus pyrkii selvittämään sitä, miten tämä tietoisuus vaikuttaa heidän käytökseensä sosiaalisessa mediassa.

Aiheesta ei ole aiemmin tehty tutkimusta, joka keskittyisi haittaohjelmiin ja huijauksiin. Sosiaalisessa mediassa tapahtuvaa kiusaamista ja seksuaalista ahdistelua on sen sijaan tutkittu viime vuosina runsaasti. Myös sosiaalisen median käyttämistä haittaohjelmien levittämiseen on tutkittu, mutta nuorten asemaa päätöksiä tekevänä subjektina leviämisprosessissa ei ole aiemmin pyritty selvittämään.

Tutkimus toteutetaan lomakekyselynä. Lomakkeet tullaan jakamaan valitun yläasteen kahdeksasluokkalaisille oppilaille ja heitä pyydetään vastaamaan nimettöminä kyselyyn.

Tutkimuksella pyritään tuottamaan tietoa nuorten käytöksestä sosiaalisessa mediassa suhteessa siihen, miten paljon he tietävät siellä olevista tietoturvariskeistä ja miten vaarallisiksi he ne kokevat. Tutkimustuloksia voitaneen käyttää hyväksi arvioitaeessa tarvetta tietoturvaopetukselle peruskoulussa ja lisätessä tietoisuutta sosiaalisen median tietoturvariskeistä.

Asiasanat
Tietoturva, sosiaalinen media, nuoret, haittaohjelmat

Sisällys

1 Johdanto 1
2 Teoriatausta 2
2.1 Lasten ja nuorten internetin käyttö 2
2.2 Lasten ja nuorten näkemykset tietoturvasta 3
2.3 Sosiaalisen median vaaroja 4
3 Tavoitteet 8
4 Tutkimusmenetelmät 8
5 Aikataulu 10
6 Hyväksikäyttömahdollisuudet 13
Lähteet 14

1 Johdanto

Käytännössä melkein kaikki suomalaiset lapset ja nuoret viettävät aikaansa internetissä. Jo vuosina 2005 ja 2006 94 prosenttia suomalaisvanhemmista raportoi lapsensa käyttävän internetiä (The Gallup Organisation 2008, 11). MySpace'n ja Facebookin kasvatettua suosiotaan etenkin sosiaalinen media on tullut osaksi nuorten elämää: 58 prosenttia 14-vuotiaista ilmoitti jo vuonna 2008 käyttävänsä erilaisia internetin verkostopalveluita, kuten MySpace'ä (Noppari, Uusitalo, Kupiainen & Luostarinen 2008, 90).

Aihepiiriltään tietoturvan piiriin kuuluva tutkimukseni selvittää suomalaisyläastelaisten tietämystä haittaohjelmien leviämisestä sosiaalisen median kautta. Lisäksi tutkimuksella pyritään kartoittamaan myös sitä, miten nuorten tietämyksen taso vaikuttaa heidän jokapäiväiseen sosiaalisen median käyttöönsä sekä mielikuvien että käytännön tasolla.

Tutkimus tulee antamaan tietoa siitä, miten paljon nuoret panostavat tietoturvaansa sosiaalisessa mediassa ja ylipäätään kuinka huolissaan he siitä ovat. Aihetta ei ole tutkittu aiemmin paljonkaan johtuen osittain luultavasti siitä, ettei sosiaalinen media ole ollut suosionsa huipulla vielä kuin muutaman vuoden. Tutkimuksia nuorten internetissä kohtaamasta uhkaavasta sisällöstä on, mutta se keskittyy yleensä joko sosiaaliseen uhkaan tai nuorten vahingossa löytämiin väkivaltaista tai pornografista aineistoa sisältäviin sivustoihin. Sosiaaliseksi uhkaksi voidaan laskea nuoren joko myös todellisessa maailmassa tai vain virtuaalisesti tuntemien henkilöiden taholta tapahtuva kiusaaminen, uhkailu, ahdistelu tai häirintä.

2 Teoriatausta

Siitä, miten suomalaiset kahdeksasluokkalaiset antavat ymmärtämyksensä ja tietämyksensä tietoturvaan liittyvistä vaaroista ja uhkista vaikuttaa heidän sosiaalisen median käyttöönsä, ei ole aiemmin tehty paljonkaan tutkimusta. Koulukiusaaminen niin sosiaalisessa mediassa kuin internetin välityksellä ylipäätään on nostettu esille useissa tutkimuksissa viimeisen vuosikymmenen aikana (muun muassa Palolampi 2007; European Commission 2008; Köntti 2010), mutta nuorten kokemukset sosiaalisen median kautta leviävistä haittaohjelmista ovat saaneet vähemmän huomiota osakseen. Itse haittaohjelmien leviämistä on tutkittu etenkin Facebookissa ja Twitterissä (muun muassa Grier, Thomas, Paxson & Zhang 2010; Gao, Hu, Wilson, Chen, Li & Zhao 2010), mutta tutkimuksissa on keskitytty enemmän leviämismekaniikkaan jättäen itse käyttäjät tilastollisen keskiarvon mukaan toimiviksi leviämisen mahdollistajiksi.

2.1 Lasten ja nuorten internetin käyttö

Tietokonetta tarvitaan nykyään melkein kaikkeen ja useimmissa suomalaisissa kodeissa onkin tietokone (Kosonen 2009, 19; Toivonen 2009, 3). Suurin osa viides- ja kuudesluokkalaisista raportoi käyttävänsä tietokonetta sekä koulussa että vapaa-ajalla: koulussa käytetty aika vaihtelee opetussuunnitelman mukaan, mutta vapaa-ajallaan oppilaat käyttivät tietokonetta keskimäärin noin 6,6 tuntia viikossa eli tilastollisesti alle tunnin päivässä (Kosonen 2009, 31). Nykyään suomalaislapset ja -nuoret käyttävät internetiä lisäksi myös kännyköiden ja muiden mobiilisovellusten kautta runsaasti: jopa 30 prosenttia kertoo itse käyttävänsä internetiä kännykällä säännöllisesti (Pelastakaa Lapset ry 2010, 3). Viides- ja kuudesluokkalaiset oppilaat myös arvioivat oman osaamisensa tietokoneiden käytössä olevan korkealla tasolla (Kosonen 2009, 34). Samaisten oppilaiden opettajia haastateltaessa selvisi kuitenkin, että heidän näkemyksensä mukaan oppilaat jakavat yhteystietojaan, käyttäjätunnuksiaan ja salasanojaan liian helposti (Kosonen 2009, 35). Tästä voidaan päätellä, että joko oppilaiden ja opettajien käsitykset turvallisesta tietokoneen ja internetin käytöstä poikkeavat toisistaan merkittävästi tai heidän arvionsa ei ole totuudenmukainen. Inhimilliseltä kannalta katsottuna on luultavaa, että oppilaat arvioivat osaamisensa hivenen paremmaksi kuin mitä se on, mutta toisaalta

tutkimuksesta ei käy ilmi, kuinka hyvin opettajat olivat perehtyneet oppilaiden tietoturvakäytäntöihin.

Lapset käyttävät internetiä pääasiassa pelaamiseen ja viestintään (Pelastakaa Lapset ry 2006, 6–8; Pelastakaa Lapset ry 2010, 3; Kosonen 2009, 32–33). Viestintä on tapahtunut aiemmin pääasiassa Messengerin ja sähköpostin välityksellä (Kosonen 2009, 32–33), mutta nyttemmin myös Facebook on nostanut suosiotaan nuorten joukossa (Pelastakaa Lapset ry 2010, 3). Vaikka Facebookiin rekisteröitymisen alaraja on 13 vuotta (Facebook 2011) johtuen yhdysvaltalaisesta Children's Online Privacy Protection Act of 1998 -laista, kuitenkin 56 % 10–12-vuotiaista suomalaislapsista ilmoitti käyttävänsä Facebookia Pelastakaa lapset ry:n (2010, 3) suorittamassa kyselyssä. Tämän johdosta voitaneen pitää todennäköisenä, että yli puolet suomalaisista kahdeksasluokkalaisista (iältään 13–15-vuotiaita syntymäajasta riippuen) käyttävät Facebookia. Tutkimuksen aihe koskenee siis luultavasti valtaosaa tutkitusta ikäryhmästä etenkin, jos muut vähemmän käytetyt sosiaalisen median palvelut, kuten MySpace, Twitter ja Google+, otetaan siihen mukaan.

2.2 Lasten ja nuorten näkemykset tietoturvasta

Lasten ja nuorten tietoturvakäytöksestä löytyy jonkin verran tutkimusta (muun muassa Chai, Bagchi-Sen, Morrell, Rao & Upadhyaya 2006; Staksrud & Livingstone 2009; Marjamäki 2006; Savijoki 2009; Youn 2008). Osassa tutkimuksista on kuitenkin keskitytty vanhempien mielikuviin lasten tietokoneella ollessaan kohtaamista vaaroista sekä siihen, miten vanhempien asenteet tietoturvaan vaikuttavat lasten käytökseen ja tietoturvaosaamiseen (esimerkiksi Youn 2008; Savijoki 2009). Yleisellä tasolla ammattikorkeakoululaisten tietoturvaan kohdistuvasta kiinnostuksesta ja perustietämyksestä on Suomessa ehditty tehdä opinnäytetyö (Marjamäki 2006). Opinnäytetyössään Marjamäki ei kuitenkaan käsittele erityisesti sosiaalisen median kautta leviäviä haittaohjelmia vaan keskittyy enemmän sähköpostitse leviäviin viruksiin sekä ”khalasteluun” (engl. phishing).

Kaikki suomalaiset ammattikorkeakouluopiskelijat eivät kuitenkaan näe tietoturvan koskevan heitä itseään (1,7 %) tai koe sitä kiinnostavaksi (13,8 %). Kysymys oli tosin

kohdistettu vain niille opiskelijoille, jotka eivät seuraa tietoturvatiedotuksia, joten todellisuudessa prosentuaalinen luku kaikista ammattikorkeakouluopiskelijoista lienee huomattavasti pienempi. Opiskelijoista mm. vain 1,7 prosentilla ei ole lainkaan virustorjuntaohjelmaa eikä 2,6 prosentilla palomuuria omalla tietokoneellaan. Salasanojen suhteen tilanne on huonompi, sillä noin 55 prosenttia ilmoitti, ettei koskaan vaihda salasanojaan. (Marjamäki 2006, 54–75.)

2.3 Sosiaalisen median vaaroja

Tehtyjen tutkimusten painotuksia tulkitsemalla voi tehdä sen päätelmän, että edelleen suurimpina sosiaalisen median tuomina uhkina nähdään internetin kautta tapahtuva koulukiusaaminen (engl. cyberbullying) ja seksuaalinen ahdistelu. Suurin osa seksuaalisen ahdistelun uhreista on tyttöjä (Ybarra & Mitchell 2007, e354; Pelastakaa Lapset ry 2008, 8), ja tavallisimmin uhrit ovat noin 13–15-vuotiaita (Lampainen 2011, 103). Todellisuudessa seksuaalinen ahdistelu sosiaalisessa mediassa on harvinaista tai ainakaan lapset eivät mielellään raportoi sitä, sillä 1588 10–15-vuotiaasta yhdysvaltalaislapsesta vain 4 prosenttia ilmoitti kokeneensa seksuaalista ahdistelua tai seksuaalissävytteistä häirintää sosiaalisessa mediassa (Ybarra & Mitchell 2007, e354). Kuitenkin suomalaisviranomaisten mukaan sekä tavallisin alusta, jolla seksuaalisen häirinnän uhriin on otettu ensikontakti, että alusta, jossa kommunikaatiota on jatkettu, on ollut jokinlainen internetyhteisö, joksi Facebook ja suurin osa sosiaalisesta mediasta lasketaan (Pelastakaa Lapset ry 2011, 6–7). Tämä on suorassa ristiriidassa professorien Ybarran ja Mitchellin Yhdysvalloissa 2007 tekemään tutkimukseen, jossa uhreiksi joutuneet lapset ilmoittivat kokeneensa seksuaalista häirintää ja ahdistelua eniten pikaviestikeskusteluissa; suomalaistutkimuksessa pikaviestikeskustelut olivat vasta kolmannella sijalla. Tämä saattaa selittyä sekä kulttuurisilla eroilla että sosiaalisen median käytön kasvamisella nuorten keskuudessa tutkimusten välillä kuluneella ajanjaksolla.

Ei-seksuaalinen kiusaaminen on noin kaksi kertaa yleisempää sosiaalisessa mediassa kuin seksuaalinen häirintä siitä päätellen, että noin 9 prosenttia 1588 nuoresta ilmoitti kokeneensa sitä (Ybarra & Mitchell 2007, e354). Täytyy kuitenkin ottaa huomioon, että tässä kiusaaminen oli rajattu kattamaan vain ilkeät tai töykeät kommentit sekä juorujen levittämisen.

Lapset ja nuoret eivät kuitenkaan näytä aktiivisesti pyrkivän suojautumaan tuntemattomien yhteydenotoilta sosiaalisessa mediassa. Suomalaislapset uskovat kykyynsä hallita internetiin laittamaansa tietoa, mutta eivät kuitenkaan rajoita sosiaalisessa mediassa olevien profiiliensa käyttöoikeuksia (Noppari, Uusitalo, Kupiainen & Luostarinen 2008, 103). Toisaalta yhdysvaltalaisnuoret ovat oletettavasti huolestuneempia tietoturvastaan, sillä 66 prosenttia nuorista, joilla on profiili sosiaalisessa mediassa, rajoittaa siihen pääsyä jotenkin ja 46 % niistä, jotka eivät rajoita profiilinsa näkyvyyttä, myöntää julkaisseensa siinä paikkansapitämätöntä tietoa (Lenhart & Madden 2007, 24–26).

Kiusaamisen ja seksuaalisen häirinnän lisäksi sosiaalisen median kautta leviää myös haittaohjelmia sekä ei-toivottuja mainoksia. Kahdeksan prosenttia mikroblogipalvelu Twitterissä julkaistuista URL-osoitteista vie sivuille, jotka ovat jollain tunnetuista estolistoista (engl. blacklist) (Grier, Thomas, Paxson & Zhang 2010, 29). Sekä Facebookissa että Twitterissä eniten haitallisille sivuille vieviä osoitteita levittävät käyttäjätilit, jotka on niiden omistajan tahtoa vastaan kaapattu, samalla kun vain pieni osa käyttäjätileistä, jotka levittävät haittaohjelmia sisältäville sivuille johtavia osoitteita, on pelkästään sitä varten perustettuja (Gao, Hu, Wilson, Chen, Li & Zhao 2010, 43; Grier, Thomas, Paxson & Zhang 2010, 31–33). Koska yksi yleisimmistä tavoista levittää haittaohjelmia sosiaalisen median kautta on houkutella käyttäjä avaamaan linkki, joka vie sivustolle, jolla käyttäjää pyydetään antamaan luottamuksellisia tietoja, kaapatun käyttäjätilin käyttäminen lisää potentiaalisen uhrin luottamusta siihen, että linkki on vaaraton ja siksi turvallinen avata. Toiseksi tavallisin huijaus on saada käyttäjä menemään sivulle, jolta latautuu haittaohjelma hänen koneeseensa joko automaattisesti tai vasta käyttäjän hyvässä uskossa painaessa painiketta, jolla luulee esimerkiksi siirtyvänsä seuraavaan ruutuun tai hyväksyvänsä käyttöoikeussopimuksen (Gao, Hu, Wilson, Chen, Li & Zhao 2010, 42). Huolimatta siitä, miten tavallista linkkien lähettäminen käyttäjille näille tutun henkilön kaapatun käyttäjätilin nimissä on, Twitterissä klikataan edes kerran vain 2,3 prosenttia lähetetyistä linkeistä, jotka vievät haittaohjelmia sisältäville sivuille (Grier, Thomas, Paxson & Zhang 2010, 30–31).

Haittaohjelmia sisältäviä linkkejä ei levitetä sosiaalisessa mediassa pelkästään satunnaisesti vaan muun muassa Facebookissa ja Twitterissä on huomattu niin kutsuttuja

spämmikampanjoita. Nämä tunnistetaan yleensä siitä, että ajallisesti lähellä toisiaan alkaa levitä identtisiä tai melkein identtisiä viestejä, jotka sisältävät linkin kalastelusivulle tai haittaohjelmia sisältävälle sivulle. Useat käyttäjät levittävät usein tahtomattaan näitä viestejä, minkä lisäksi viestejä saattaa olla levittämässä lukuisia sitä varten luotuja käyttäjätilejä. Vaikka viestejä saatetaan julkaista pitkänkin aikaa, kampanjan intensiivisin vaihe kestää yleensä vain hyvin lyhyen aikaa. (Gao, Hu, Wilson, Chen, Li & Zhao 2010, 40-43; Grier, Thomas, Paxson & Zhang 2010, 33–35.)

Sitä, kuinka usein nuoret törmäävät tällaisiin viesteihin ja aukaisevat niillä olevan linkin, ei voida varmuudella sanoa, koska nuoret eivät aina yhdistäne koneelleen tullutta haittaohjelmaa aikaisemmin avattuun linkkiin, joka vaikuttaa tulleen heidän ystävältään. Suomalaisista ammattikorkeakouluopiskelijoista 28,4 prosenttia kuitenkin raportoi törmäävänsä viruksiin koneellaan kerran kuussa (Marjamäki 2006, 58), joten täysin he eivät osaa haittaohjelmia välttää. Marjamäen tutkimuksessa (2006, 65) virusten – johon luettiin kaikki haittaohjelmat – lähdettä ei selvitetty kovin tarkasti, mutta 68,1 prosenttia vastanneista oli sanonut niiden tulleen tietokoneelle internetistä.

Siitä on kuitenkin saatu näyttöä, että lapset, jotka kokevat hallitsevansa tietoturvan perusteet ja saavat tietoturvaan liittyvää tietoa ympäristönsä kautta, kiinnittävät enemmän huomiota tietokoneen käyttönsä turvallisuuteen ja myös käytännössä aktiivisesti ylläpitävät sen turvallisuutta (Chai, Bagchi-Sen, Morrell, Rao ja Upadhyaya 2006, 132–133; Youn 2008). Suomalaiset viides- ja kuudesluokkalaiset raportoivat käyttävänsä tietokonetta koulussa vain noin 1,2 tuntia viikossa, mutta luku vaihtelee hyvin paljon koulun ja opettajan käytännöistä riippuen (Kosonen 2009, 24 ja 35). Tästä voinee tehdä sen päätelmän, että oppilaat tuskin saavat kovinkaan paljon opastusta internetin ja sosiaalisen median käytön tietoturvasta. Lapset eivät myöskään mielellään käänny opettajien puoleen internetiin liittyvissä ongelmissa, ellei se selkeästi liity jotenkin kouluun tai ole tekninen ongelma (Toivonen 2009, 7–8).

Useat tutkimukset ovat osoittaneet, että vanhempien tavallisimpia huolenaiheita lasten internetin käyttöön liittyen ovat näiden joutuminen seksuaalisesti ahdistelluiksi, pedofiilin uhreiksi tai koulukiusatuiksi tai ajautuminen väkivaltaisille tai pornografisille sivustoille (The Gallup Organisation 2010, 28–29; Toivonen 2009, 44). Lisäksi monien tut-

kimusten kysymysten asettelusta tai aiheen rajauksesta pystyy lukemaan, että näitä pidetään tavallisimpina uhkina internetiä käyttäville lapsille ja nuorille (muun muassa Savijoki 2009; Köntti 2010). Tämä antaa ymmärtää, että vaikka lapsia pyritään varjelemaan näiltä, heille annetaan harvemmin keinoja suojautua sosiaalisessa mediassa liikkuvilta huijauksilta. Saattaa olla, että vanhemmat eivät yksinkertaisesti ole tietoisia esimerkiksi haittaohjelmia sisältäviin ohjelmiin tai sivustoille vieviä linkkejä sisältävien huijausviestien sekä sosiaalisessa mediassa leviävien haittaohjelmia sisältävien selainpelien tai lisäosien yleisyydestä. Tutkimustietoa siitä, kuinka usein lapsia ja nuoria on opetettu, kuinka päätellä, onko sosiaalisessa mediassa ystävältä tai ventovieraalta saatu viesti huijausta, ei löytynyt. 84 prosenttia 4.–6.-luokkalaisten lasten vanhemmista on toisaalta joka tapauksessa ohjeistanut näitä olemaan jakamatta henkilökohtaisia tietojaan internetissä (Toivonen 2009, 43). Koska kysymystä ei ollut määritelty tarkemmin, on kuitenkin mahdotonta sanoa, kuinka moni vanhemmista oli sisällyttänyt esimerkiksi yhteystietoja tai salasanoja kysyvät sosiaalisen median lisäosat tai linkin takana olevat sivustot tähän ja kuinka moni oli puhunut vain kodin osoitteen ja oman puhelinnumeron antamisesta ventovieraille pikaviestipalvelussa.

3 Tavoitteet

Tutkimukseni aihe nostaa keskeisimmäksi kysymysongelmaksi sen, kuinka syvällä tasolla nuoret ovat tietoisia sosiaaliseen mediaan liittyvistä haittaohjelmista. Tämän alaongelmana on se, miten tietoisuus tietoturvaan liittyvistä uhkista vaikuttaa nuorten käytökseen sosiaalisessa mediassa.

4 Tutkimusmenetelmät

Tutkimusaineistona käytetään suomalaisessa yläasteessa tai peruskoulussa kahdeksannella luokalla opiskelevien koululuisten kyselytutkimuksessa ilmaisemia mielipiteitä ja antamaa tietoa sosiaaliseen mediaan (etenkin Facebookiin ja Twitteriin) liittyvistä tietoturvauhista ja niiden vaikutuksesta heidän käytökseensä.

Otannaksi valittiin kahden tai kolmen suomalaisen yläasteen tai peruskoulun kahdeksasluokkalaiset, koska opiskelijoina nämä on helppo tavoittaa ja kyselytutkimuksen tekemisestä voi kollektiivisesti sopia koulujen rehtorin ja aineopettajien kanssa. Kustakin koulusta on tarkoitus ottaa kyselyyn kahdesta neljään luokkaa niin, että suurin piirtein sama määrä oppilaita vastaisi kyselyyn joka koulusta. Tavoiteltu vastaajamäärä on noin 200 oppilasta.

Koulut ja luokat on valittava niin, että ne edustaisivat mahdollisimman hyvin suomalaista keskivertokahdeksasluokkaa. Tämä rajaa muun muassa esimerkiksi matemaattisia aineita, kuvataiteita tai liikuntaa painottavat luokat tutkimuksen ulkopuolelle. Ihanteellisessa tilanteessa koulut valitaan eri puolilta Suomea, mutta koska kaksi tai kolme koulua ei riitä kattamaan kaikkia Suomen läänejä, täysin tarkkaa kuvaa tutkitun aiheen maakuntakohtaisista eroista ei tutkimuksella pystyttäne kuitenkaan tarjoamaan.

Suurin syy itse ikäryhmän valinnalle on se, että useimmat sosiaalisen median palvelut pohjaavat toimintansa Yhdysvaltain lakiin (esimerkiksi Facebook ja MySpace). Yhdysvalloissa 21.4.2000 voimaan tullut Children's Online Privacy Protection Act of 1998 (COPPA) säätelee sitä, mitä tietoja internetsivut voivat säilyttää alle 13-vuotiaista. Tähän kuluisi ylimääräisiä resursseja, joten useimmat sosiaalisen median palvelut, joita ei

ole suoranaisesti kohdistettu alle teini-ikäisille, ovat kokonaan kieltäneet alle 13-vuotiaiden rekisteröitymisen käyttäjiksi, vaikka eivät valvo kieltoa mitenkään.

Kyselytutkimus valittiin tiedonkeruumetodiksi, koska se on kattava tapa kerätä kvantitatiivista tietoa valitusta aiheesta. Kysely toteutetaan paperilla kaikille kouluista valittujen luokkien oppilaille jaettavana lomakekyselynä. Jotta vastaukset olisivat mahdollisimman todenmukaisia, kysely on anonyymi. Lisäksi nimen ei voi katsoa antavan mitään erityistä lisäarvoa tutkimukselle, koska lomakekyselyn lisäksi kyselyyn vastaajiin ei olla muuten yhteydessä. Syy toteuttaa kysely paperisena eikä sähköisessä muodossa on se, että kaikilla oppilailla on todennäköisemmin käsillä lyijykynä kuin internetiin kytketty tietokone. Lisäksi kyselyn täyttäminen oppitunnin alussa opettajan ollessa luokassa lisännee vastaajien lukumäärää siihen verrattuna, että oppilaille annettaisiin vain linkki internetissä olevaan kyselyyn koulun jälkeen täytettäväksi. Tämä tietenkin aiheuttaa enemmän logistisia haasteita kuin sähköinen kysely, joka on kaikkien saatavilla heidän fyysisestä olinpaikastaan riippumatta. Koulun sijaitessa kaukana tutkimuksen tekijästä kyselyn voi silti lähettää opettajille heidän mieltymyksensä mukaan joko sähköisessä muodossa, jolloin he voivat tulostaa siitä tarvittavan määrän kappaleita, tai jo valmiiksi tulostettuna Suomen postilaitoksen kautta. Takaisin täytetyt kyselylomakkeet jouduttaneen lähettämään kirjattuna kirjeenä tai pakettina niiden turvallisen matkan takaamiseksi, mutta niiden skannaaminen tietokoneelle on tietysti yksi vaihtoehto, mikäli kouluilla on siihen tarvittavat välineet ja kiinnostusta tehdä se.

Vaikka saatua tietoa pyritään analysoimaan mahdollisimman objektiivisesti, siinä otetaan kuitenkin mukaan ihmisten omista toimistaan raportoidessa syntyvä virheen mahdollisuus. Vaikka huonomuistisuus on aina yksi mahdollinen syy, kuitenkin on myös mahdollista, että kyselyn täyttäjä kaunistelee tilannettaan tai suorastaan tietoisesti valehtelee, sillä osa nuorista ei ehkä halua myöntää aiheuttaneensa omilla toimillaan koneensa saastumista haittaohjelmista.

5 Aikataulu

Aihe-ehdotuksen ja tutkimussuunnitelman teko on jätetty aikataulusta pois, koska ne on tutkimussuunnitelmaa palautettaessa jo tehty eikä siten niiden aikatauluttamisen voida katsoa tuovan mitään ylimääräistä lisäarvoa tutkimuksen toteuttamisen realistisuudesta kiinnostuneelle lukijalle.

Kaikki kestoajat on annettu työtunteina.

Aiheesta tai siihen keskeisesti liittyviltä lähialueilta aiemmin tehtyihin tutkimuksiin perehtymisen jatkaminen
Tämän oletetaan alkaneen jo aihe-ehdotuksen tekemisen yhteydessä ja jatkuneen tutkimussuunnitelman aikana. Vaihe tulee käytännössä jatkumaan vaihtelevalla intensiviteetillä läpi koko tutkimuksen tekemisen. Arvioitu kesto: 64 tuntia

Tutkimuksen taustan kirjoittaminen
Vaihe sisältää tutkimuksen niiden osien kirjoittamisen, jotka eivät ole riippuvaisia kyselyn tuloksista, kuten selvityksen siitä, miten aihetta on aiemmin tutkittu ja millä metodeilla sitä aiotaan tutkia. Tutkimussuunnitelma voi osittain toimia tämän pohjana. Vaihe jatkuu läpi koko tutkimuksen teon valmiin tutkimuksen oikolukemiseen asti. Arvioitu kesto: 100 tuntia

Lomakekyselykohteen selvittäminen
Tutkimukseen sopivan yläasteen löytäminen ja kyselytutkimuksen tekemisestä sopiminen koulun rehtorin ja niiden opettajien kanssa, joiden tunnilla kysely tehdään. Tämä vaihe voidaan tehdä osin rinnakkain itse kyselylomakkeiden tekemisen kanssa, sillä niitä ei tarvitse räätälöidä koulukohtaisiksi. Arvioitu kesto: 8 tuntia

Kyselylomakkeiden sisällön suunnittelu
Kyselylomakkeiden painopisteet ja kysymysten ryhmittely suunnitellaan. Tämä vaihe sisältää myös itse kysymysten hiomisen viimeiseen muotoonsa. Vaihetta voi tehdä jo ennen kuin kohdekoulu on saatu selville. Arvioitu kesto: 24 tuntia

Kyselylomakkeiden tekeminen

Kysymykset kirjoitetaan koneella ja asetellaan paperille. Lopuksi kyselylomakkeita tulostetaan haluttu määrä, minkä lisäksi niitä tulostetaan myös ylimääräisiä kappaleita varalle. Arvioitu kesto: 10 tuntia

Kyselyyn vastausajankohta

Aika, jolloin oppilaat täyttävät kyselyn. Tapahtuu todennäköisesti jonkin oppitunnin alussa. Tämä vaihe ei vaadi itse tutkimuksentekijältä mitään toimenpiteitä, mutta on silti hyvä olla kalenterissa ylhäällä. Aika on voimakkaasti riippuvainen kustakin koulusta, jossa kysely suoritetaan.

Kyselylomakkeiden takaisin kerääminen

Mahdollisimman pian oppilaiden täytettyä kyselyn opettajan kanssa sovitaan aika, jolloin täytetyt kyselylomakkeet ovat haettavissa koululta tai postitetaan tutkimuksen tekijälle. Aika riippuu koulusta ja opettajan omasta aikataulusta. Arvioitu kesto: 3 tuntia

Kyselylomakkeiden tulosten läpikäynti ja analysointi

Tämä vaihe ei voi alkaa ennen kuin oppilaiden täyttämät kyselylomakkeet on saatu takaisin. Vastaukset kerätään alustavasti taulukoiksi, listoiksi tai prosenttiluvuiksi kysymystyypistä riippuen mahdollisimman objektiivisesti, minkä jälkeen niistä tehdään johtopäätöksiä. Arvioitu kesto: 32 tuntia

Kyselyn tuloksia analysoivan osan kirjoittaminen

Vaihe sisältää kyselyn tuloksiin pohjautuvan osan jäsentelyn viimeistelyn ja kirjoittamisen. Arvioitu kesto: 104 tuntia

Tutkimuksen loppuun kirjoittaminen

Tämä vaihe sisältää muun muassa tutkimustekstin yhtenäistämisen sekä loppupäätelmien ja tiivistelmän kirjoittamisen. Vaihetta ei voi aloittaa ennen kuin itse tutkimusteksti on kirjoitettu lähestulkoon valmiiksi. Arvioitu kesto: 30 tuntia

Tutkimuksen viimeistely

Tässä vaiheessa tutkimuksen muun muassa varmistetaan noudattavan tilaajan tai oppilaitoksen raportointistandardeja sekä täyttävän kaikki muut vaadittavat kriteerit. Arvioitu kesto: 8 tuntia

Tutkimuksen oikoluku

Koko tutkimus oikoluetaan ja tarkistetaan tyylivirheiden varalta. Löydetyt virheet korjataan. Tämän vaiheen voi tehdä vasta tutkimuksen valmistuttua lopulliseen muotoonsa. Arvioitu kesto: 8 tuntia

Tutkimuksen palauttaminen

Esityksen suunnittelu

Suullisen esityksen rakenteen ja sisällön luonnostelu ja päättäminen. Lopputuloksena pitäisi olla selkeä käsitys siitä, kauanko esitys tulee kestämään, mitä siinä käsitellään, kuinka laajasti ja missä järjestyksessä. Arvioitu kesto: 8 tuntia

Esitykseen valmistautuminen

Esityksen oheismateriaalin (esimerkiksi powerpointesityksen tai tulosteiden) tuottaminen. Myös esitystä varten tehtävien diagrammien, taulukoiden ja histogrammien teko kuuluu tähän kohtaan. Lopputuloksena pitäisi olla esityskelpoinen kokonaisuus. Arvioitu kesto: 40 tuntia

Esityksen harjoittelu

Esityksen harjoitteleminen ja viimeinen hiominen. Myös puhenopeuden, -tyylin ja esitykseen rytmitettävien eleiden harjoittelu kuuluu tähän vaiheeseen. Lopputuloksena pitäisi olla itsevarma ja asiantunteva esiintyminen tätä edeltävässä vaiheessa tehdyn esityksen tukemana. Arvioitu kesto: 4 tuntia

Esitys

Itse tilaisuus, jossa tutkimus esitellään muille.

6 Hyväksikäyttömahdollisuudet

Koska tutkimus kartoittaa nuorten tietämystä sosiaalisen median tietoturvauhkista sekä sitä, miten he reagoivat niihin käytöksessään, tutkimustuloksia voidaan käyttää antamaan suuntaviivoja sille, pitäisikö sosiaalisen median tietoturvan opetusta olla kouluissa joko yläasteella tai jo ala-asteella. Tällä hetkellähän tietoturva jää kohtalaisen vähälle huomiolle peruskoulun tietotekniikan opetuksessa: muun muassa MAOL ry:n ohjeistus peruskoulun tietotekniikan tavoitteista ja opetussisällöistä ei mainitse lainkaan tietoturvaa.

Paitsi selvittämään, onko sosiaalisen median arkikäytön tietoturvan opetukselle Suomessa tarvetta, kyselyä voidaan käyttää nostamaan tietoisuutta haittaohjelmien, käyttäjätilien kaappaamisen ja huijausten olemassaolosta sosiaalisessa mediassa. Aikuisten on tärkeä tiedostaa lapsia ja nuoria ohjatessaan, että nämä todennäköisesti törmännevät edellä mainittuihin riskeihin alkaessaan käyttää sosiaalista mediaa.

Lähteet

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R. ja Upadhyaya, S. 2006. Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior. Teoksesta Issues in Informing Science and Information Technology 3/2006, s. 127–135. Luettavissa: http://wings.buffalo.edu/academic/department/som/isinterface/papers/IISITCha191.pdf Luettu: 22.10.2011

Children's Online Privacy Protection Act of 1998

Facebook, 2011. Statement of Rights and Responsibilities. Luettavissa: http://fi-fi.facebook.com/terms.php?ref=pf Luettu: 19.10.2011

Gao, H., Hu, J., Wilson, C., Chen, Z., Li, Y. & Zhao, B. 2010. Detecting and Characterizing Social Spam Campaigns. Teoksesta IMC'10, November 1–3, 2010, s. 35–47. Melbourne (Australia) Luettavissa: http://dl.acm.org/citation.cfm?id=1879141.1879147&coll=DL&dl=GUIDE Luettu: 24.10.2011

Grier, C., Thomas, K., Paxson, V. & Zhang, M. 2010. @spam: The Underground on 140 Characters or Less. Teoksesta CCS'10, October 4–8, 2010, s. 27–37. Chicago, IL (USA) Luettavissa: http://dl.acm.org/citation.cfm?id=1866307.1866311&coll=DL&dl=GUIDE Luettu: 24.10.2011

Kosonen, K. 2009. Viides- ja kuudesluokkalaisten oppilaiden tietotekniikkaosaaminen ja käyttö. Amk-opinnäytetyö. Lahden ammattikorkeakoulu. Lahti. Luettavissa: https://publications.theseus.fi/bitstream/handle/10024/2121/Kosonen_Kari.pdf Luettu: 21.10.2011

Köntti, M. 2010. Sosiaalisen median ja internet-tiedonhaun opas lasten kasvattajille. Amk-opinnäytetyö. Seinäjoen ammattikorkeakoulu. Seinäjoki. Luettavissa:

https://publications.theseus.fi/bitstream/handle/10024/15995/Kontti_Maija.pdf Luettu: 21.10.2011

Lampainen, K. 2011. Grooming internetissä ja lapsen seksuaalinen hyväksikäyttö. Pro gradu -tutkielma. Jyväskylän yliopisto. Jyväskylä. Luettavissa: https://jyx.jyu.fi/dspace/bitstream/handle/123456789/26619/URN%3ANBN%3Afi%3Ajyu-201103011839.pdf Luettu: 23.10.2011

Lenhard, A. & Madden, M. 2007. Teens, Privacy and Online Social Networks. Projektiraportti. Luettavissa: http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf Luettu: 24.10.2011

MAOL ry. (vuosi tuntematon). Mitä peruskoulun päättävän tulisi tietää tietotekniikasta? Matemaattisten Aineiden Opettajien Liiton ohjeistus. Luettavissa: http://www.mit.jyu.fi/OPE/kurssit/TIES461/Materiaali/maol_ohjeistus.pdf Luettu: 25.10.2011

Marjamäki, K. 2006. Opiskelijat ja tietoturva. Case: Huittisissa opiskelevat opiskelijat. Satakunnan ammattikorkeakoulu. Huittinen. Luettavissa: https://publications.theseus.fi/bitstream/handle/10024/804/Marjamaki_Katariina.pdf Luettu: 24.10.2011

MySpace. 2009. MySpace.com-sivuston käyttöehtosopimus. Luettavissa: http://www.myspace.com/Help/Terms Luettu: 22.10.2011

Noppari, E., Uusitalo, N., Kupiainen, R. & Luostarinen H. 2008. ”Mä oon nyt online!” Lasten mediaympäristö muutoksessa. Julkaisuja A 104/2008. Tampereen yliopisto.Tampere.

Palolampi, J. 2006. Lapset ja Internet – opas vanhemmille. Amk-opinnäytetyö. Tampereen ammattikorkeakoulu. Tampere. Luettavissa: http://www.lapsetjainternet.net/opinnaytetyo.pdf Luettu: 22.10.2011

Pelastakaa Lapset ry. 2011. Grooming internetissä ja lapsen seksuaalinen hyväksikäyttö. Luettavissa: http://www.pelastakaalapset.fi/@Bin/368105/Grooming-+raportti_final.pdf Luettu: 23.10.2011

Pelastakaa Lapset ry. 2010. Raportti lasten netin käytöstä. Lapsen ääni -kysely. Luettavissa: http://www.pelastakaalapset.fi/@Bin/194776/Lapsen+%C3%A4%C3%A4ni+kysely+2010.pdf Luettu: 22.10.2011

Pelastakaa Lapset ry. 2008. Raportti lasten netin käytöstä. Lapsen ääni -kysely. Luettavissa: http://www.pelastakaalapset.fi/@Bin/91427/lapsena%CC%88a%CC%88nikysely_2008_VALMIS_22.8_2008.pdf Luettu: 22.10.2011

Pelastakaa Lapset ry. 2006. Netti liittää lapset toisiinsa. Lapsen ääni -kysely. Luettavissa: http://www.pelastakaalapset.fi/@Bin/91435/Lapsen_%C3%A4%C3%A4ni2006.pdf Luettu: 22.10.2011

Pelastakaa Lapset ry. 2005. Lapsen ystävät ovat netissä. Lapsen ääni -kysely. Luettavissa: http://www.pelastakaalapset.fi/@Bin/91447/Lapsen-ystavat-ovat-netissa.pdf Luettu: 22.10.2011

Savijoki, R. 2009. Nuoren IT-suoja. Amk-opinnäytetyö. Mikkelin ammattikorkeakoulu. Mikkeli. Luettavissa: https://publications.theseus.fi/bitstream/handle/10024/5566/Microsoft%20Word%20-%20Savijoki_Riitta.pdf Luettu: 21.10.2011

Staksrud, E. & Livingstone, S. 2009. Children and online risk: powerless victims or resourceful participants? Teoksesta Information, communication and society, 12 (3). s. 364–387. Luettavissa: http://eprints.lse.ac.uk/30122/1/Children_and_online_risk_%28LSERO_version%29.pdf Luettu: 22.10.2011

The Gallup Organisation. 2008. Towards a safer use of the Internet for children in the EU – a parents' perspective. Analytical report. Luettavissa: http://ec.europa.eu/public_opinion/flash/fl_248_en.pdf Luettu: 25.10.2011

Toivonen, S. 2009. Lapset, vanhemmat ja internet. Amk-opinnäytetyö. Keski-Pohjanmaan ammattikorkeakoulu. Kokkola. Luettavissa: https://publications.theseus.fi/bitstream/handle/10024/4206/samppa_toivonen.pdf Luettu: 19.10.2011

Ybarra, M. & Mitchell, K. 2008. How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs. Teoksesta PEDIATRICS Volume 121, Number 2/2008, s. e350–357. Luettavissa: http://pediatrics.aappublications.org/content/121/2/e350 Luettu: 20.10.2011

Youn, S. 2008. Parental Influence and Teens' Attitude Toward Online Privacy Protection. Teoksesta The Journal of Consumer Affairs, Volume 42, Issue 3/2008, s. 362–388. Luettavissa: http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2008.00113.x/full Luettu: 24.10.2011