HAAGA-HELIA
ammattikorkeakoulu

Käyttäjän tietoturvan parantaminen Facebookissa

Kristina Grabskaja

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

24.11.2014

Tekijä(t)
Kristina Grabskaja

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Käyttäjän tietoturvan parantaminen Facebookissa

Sivu- ja liitesivumäärä
42 + 3

Opinnäytetyön nimi englanniksi
Improving the user's information security on Facebook

Tämän opinnäytetyön tarkasteltavaksi tutkimuskohteeksi valittiin Facebook. Tarkoituksena oli selvittää Facebookin käyttäjien käsitystä Facebookin tietoturvariskeistä ja tutustua Facebookin perusominaisuuksiin. Työssä pyritään löytämään ratkaisut erilaisiin Facebookin kohdistuviin tietoturvauhkiin esimerkkitapausten avulla. Työn alussa esiteltiin, mitä ylipäätään sosiaalinen media tarkoittaa, jonka jälkeen lyhyesti kerrottiin kolmesta muusta valitusta sosiaalisen median palvelusta mm. Youtubesta, Twitterista ja Instagramista.

Opinnäytetyön teoreettisessa osuudessa syvennyttiin paremmin Facebookin tietoturvaan ja riskeihin. Työssä myös todettiin, että kaikki, mitä julkaisee Facebookissa, voi myöhemmässä vaiheessa elämää päätyä muiden nähtäväksi. Hyvänä sääntönä pidettiin sitä, että ei julkaise mitään tietoja, joiden tarkoitus olisi säilyä salassa. Lisäksi havaittiin, että Facebook kasvaa koko ajan ja sitä myötä erilaiset haittaohjelmat, identiteettivarkaudet ja huijaukset lisääntyvät, huolimatta siitä, kuinka tiukaksi käyttäjä olisi asentanut yksityisyysasetuksensa.

Työn tueksi tehtiin tutkimuskysely, johon osallistui 18 Facebookin käyttäjää. Tutkimuskysely toteutettiin Wordissa tehdyllä lomakkeella, joka lähetettiin käyttäjille. Kysely toteutettiin lokakuun lopussa ja vastaajilla oli viikko aikaa vastata kyselyyn. Kyselyn avulla pyrittiin saada käsitys siitä, kuinka hyvin Facebookin käyttäjät ovat tietoisia mahdollisista tietoturvariskeistä Facebookissa ja, osaavatko he suojautua esimerkiksi huijausviestejä vastaan.

Tutkimuksessa selvisi, että suurin osa vastaajista oli tietoisia Facebookiin kohdistuvista tietoturvariskeistä. Valtaosa vastaajista oli kuitenkin tyytyväisiä Facebookin tietoturvaa ja uskoi, että käyttäen maalaisjärkeä Facebooksissa pääsee hyvin pitkälle. Vastaajista vain yksi henkilö koki Facebookin uhkaavaksi palveluksi. Muuten vastaajat kokivat tutkimuskyselyn ikään kuin muistutuksena siitä, että yksityisyys- ja muut tietoturvaan liittyvät asetukset olisi hyvä olla ajan tasalla.

Asiasanat
Facebook, tietoturvariskit, sosiaalinen media, käyttäjä, tutkimuskysely

HAAGA-HELIA
ammattikorkeakoulu

Abstract

24.11.2014

Author(s)
Kristina Grabskaja

Degree programme
Degree programme in Information Technology

Report/thesis title
Improving the user's information security on Facebook

Number of pages and appendix pages
42 + 3

Facebook has been chosen to be the main subject of this thesis. The purpose of the study was to investigate what Facebook users knew about Facebook's information security risks and get them to know the basic points of Facebook. The study aims at giving solutions examples to different kinds of information security threats. Definition of what social media are is introduced in the beginning of the study. After that three different social media services: YouTube, Twitter and Instagram are briefly introduced.

The theoretic part of the study goes deeper into Facebooks security concept and the risks of it. The study also explains how everything that users will publish on Facebook can later end up being seen by everyone. The good theoretical idea is not to publish any information that should be kept personal or secret. The study also brought to the conclusion that by growth of Facebook, many viruses, identity theft and scams have also been growing of regardless of how strict the users' security settings are.

To support the study, a research survey was carried out with participation of 18 Facebook users. The survey was sent in a Word format to all the 18 users. The survey was carried out from at October 2014 and the users had one week to answer. Main goal of the inquiry was to find out how well the users were aware of possible security information risks and if they knew how protect themselves from scam or spam messages.

The results of survey were as follows: the majority of the users were aware of all the risks. Nevertheless they were satisfied with Facebook's information security, and they believed that by using common sense on Facebook, can get very far, with no further problems. Of all the respondents, only one person felt threatened by Facebook's service. Otherwise, the users who answered the questionnaire viewed the survey as a reminder of knowing what Facebooks security policies are. The respondents found it useful.

Keywords
Facebook, security risks, social media, user, research survey

Sisällys

1 Johdanto 1
2 Sosiaalinen media käsitteenä 2
2.1 Sosiaalisen median ominaisuuspiirteet 2
2.2 Suosituimmat sosiaalisen median palvelut 4
2.3 Sosiaalisen median tietoturvariskit 5
3 Facebookin tausta 8
3.1 Profiili ja etusivu 9
3.2 Kaveripyynnöt 10
3.3 Sovellukset 11
3.4 Tilapäivitykset ja viestit 12
4 Facebookin tietoturva 16
4.1 Facebookin tekijänoikeudet ja tiedon keruu 16
4.2 Yksityisyyden suoja 17
4.3 Facebookin kohdistuvat tietoturvauhat 19
4.4 Facebookin hyvät puolet 20
4.5 Ohjeet riskien välttämiseksi 21
5 Tutkimuksen toteutus 24
5.1 Tutkimuskyselyn tausta 24
5.2 Tutkimuskysymykset 24
6 Tutkimustulokset 25
6.1 Tulosten tarkastelu 25
6.2 Käsitys salasanan turvallisesta käytöstä 30
6.3 Käsitys Facebookin jaettuista tiedoista 32
6.4 Tutkimuskyselyn tulosten yhteenveto 36
7 Pohdinta 37
Lähteet 39
Liite 1. Tutkimuskysely 43

1 Johdanto

Tämän opinnäytetyön tavoitteena on selvittää Facebookin käyttäjien käsitystä Facebookin tietoturvasta ja sen tietoturvariskeistä. Tutkimuksen avulla pyritään selvittämään, mitä käyttäjän kannattaa ottaa huomioon, kun hän käyttää sosiaalisen median palveluita.

Opinnäytetyössä keskitytään yhteen sosiaalisen median palveluista eli Facebookiin. Tutkimuksen tueksi tehtiin kysely, johon osallistui 18 henkilöä eri ikäryhmää, pääosin vastaajat olivat 20-30-vuotiaita. Käyttäjille jaettiin kyselylomake vuoden 2014 lokakuun lopussa ja aikaa vastata kyselyyn oli viikko, jonka jälkeen täytetty kyselylomake kerättiin ja saatuja vastauksia analysoitiin kohta kohdalta.

Opinnäytetyön alussa esitellään lyhyesti, mitä sosiaalinen media käsite tarkoittaa, jonka jälkeen otetaan tutkittavaksi kohteeksi Facebook ja kerrotaan sen tausta. Tutkimuksen myötä syvennytään Facebookin tietoturvaan.

Aihe opinnäytetyöhön valittiin kurssin Tietotekninen selvitys ja kouluttaminen tehdyn tutkimuksen avulla liittyen Facebookin tietoturvaa, jossa oli valmiiksi pohjarunko tutkimukselle. Aiheen valintaa myös vaikutti se, että viimeaikoina lehdissä ja Internetissä on ollut paljon aiheeseen liittyviä artikkeleita ja Facebook on vuosien varrella saavuttanut nopeasti suuren suosion yhteiskunnassamme.

Tutkimuksen avulla tavoitellaan sosiaalisen median käyttäjäryhmille hyötyä, jotta tulevaisuudessa käyttäjillä olisi enemmän tietoa, miten Facebookia pystyy käyttämään turvallisesti ja, kuinka suojautua erilaisia tietoturvauhkia vastaan, koska monet käyttäjät eivät ole perehtyneet syvällisesti sosiaalisen median turvallisuuteen ja tietosuojaan.

Lopuksi yhteenvedossa pohditaan tutkimuksen tavoitteiden täyttymistä ja onnistumista.

2 Sosiaalinen media käsitteenä

Sanastokeskuksen TSK:n mukaan, sosiaalinen media on tietoverkkoja ja tietotekniikkaa hyödyntävä viestinnän muoto, jossa käsitellään vuorovaikutteisesti ja käyttäjälähtöisesti tuotettua sisältöä ja luodaan ja ylläpidetään ihmisten välisiä suhteita. Käytännössä tämä tarkoittaa sitä, että jokaisella käyttäjällä tai käyttäjäryhmällä on mahdollisuus olla aktiivinen viestijä ja sisällön tuottaja. (Valtiovarainministeriö 2010, 11.)

Yleisempiä sosiaalisen median verkkopalveluita ovat sisällönjakopalvelut, verkkoyhteisöpalvelut ja keskustelupalstat. Tyypillinen toiminta sosiaalisessa mediassa on esimerkiksi kollektiivinen sisällöntuotanto, avoin avainsanoitus, blogi kirjoitusten tuottaminen ja lukeminen, kuluttajien välinen sähköinen kaupankäynti esimerkiksi huutokauppapalvelut eBay ja Huuto.net sekä nettipelien pelaaminen. (Sanastokeskus TSK 40, 2010.)

Joskus sosiaalisessa mediassa puhutaan teknisistä ratkaisuista, millä tarkoitetaan alun perin Timothy O'Reillyn vuonna 2004 käyttöön ottamaa Web 2.0 termiä. Web 2.0 kokonaisuuteen sisältyvät muun muassa vuorovaikutteisuuden ja käyttäjälähtöisyyden mahdollistavat sovellukset. Sen lisäksi Web 2.0:n ajatusta pidetään myös Internetin sisältöjen tallennuspaikkana ja se toimii yhtä hyvin eri sovellusten alustana. (Sanastokeskus TSK 40, 2010.)

Sosiaalisen median toiminta kulttuuri perustuu pitkälti siihen, että ihmiset pyrkivät auttamaan toisiaan. Uusien palveluiden myötä ja vanhojen palveluiden uudistuksista huolimatta käyttäjät pystyvät perehtymään niihin kontaktiverkostojen avulla. Tämä mahdollistaa käyttäjiä osallistumaan erilaisiin yhteiskunnallisiin keskusteluihin ja vaikuttamaan yhteiskuntamme asioihin. (Edu 2011.)

Sosiaalisen median avulla on helppo myös löytää vanhoja ystäviä sekä uusia. Tämän kaiken mahdollistavat sosiaalisen median ominaispiirteet muun muassa nopeus, yksinkertaisuus ja helppokäyttöisyys. Monet käyttäjät sosiaalisessa mediassa yrittävät tuoda esille omaa persoonaa, mutta myös arvostella muita käyttäjiä. Vaikka näin voi käydä, silti kannattaa hyväksyä erilaisuus ymmärtäväisesti ja avoin mielin. (Edu 2011.)

2.1 Sosiaalisen median ominaisuuspiirteet

Tässä osiossa esitellään lyhyesti sosiaalisen media kuusi ominaisuuspiirrettä.

Käyttäjälähtöisyys tarkoittaa sitä, että käyttäjät pystyvät itse luomaan ja muokkaamaan sisältöä sekä jakaa informaatiota, johon voi liittyä ajatuksia, tietoa tai mielipiteitä. Käyttäjälähtöisiä palveluita ovat chatit, verkkohuutokaupat, erilaiset keskustelupalstat, nettipelit ja pikaviestintä palvelut. Näillä kaikilla palveluilla pyritään ylläpitämään käyttäjien välisiä suhteita. Käyttäjät pystyvät jakamaan sisältöä, joka voi koostua uudesta sisällöstä, kuten kuvista, tekstistä, musiikista ja videoista. Muokatuksi sisällöksi voidaan luokitella koosteet ja miksatut videot ja luokitelluksi sisällöksi voidaan sanoa soittolistoja, arvosteluja tai avainsanoja. (Alan.)

Vuorovaikutteisuuden ominaisuuspiirteellä tarkoitetaan sitä, että käyttäjillä on mahdollisuus vaikuttaa valinnoillaan median toimintaan. Hyvä esimerkki tällaisesta ominaisuuspiirteestä on palautteen antaminen julkaisijoille tai kommenttien jättäminen sisällöstä. Tämä ominaisuuspiirre luokitellaan sosiaalisen median yhdeksi selkeämmäksi piirteeksi. Vuorovaikutteisuus erottaa hyvin pitkälti sosiaalisen median perinteisestä mediasta. (Alan.)

Kaksisuuntaisuus syntyy vuorovaikutteisuuden myötä, joka tekee sosiaalisesta mediasta kaksisuuntaisen. Käyttäjälähtöisyyden perusteella sosiaalisessa mediassa viestitään monelta monelle ja näin ollen perinteiselle medialle ominainen viestintämalli yksisuuntaisuudesta ja viestijän sekä vastaanottajan välinen ero jää puuttumaan. (Alan; Itä-Suomen Yliopisto.)

Avoimuus merkitsee sosiaalisessa mediassa läpinäkyvyyttä ja luottamusta sekä rehellisyyttä, mitä kuluttajat ja kansalaiset odottavat yrityksiltä ja organisaatioilta vastineeksi. Tämä luonnollisesti vaatii yrityksiltä ja organisaatioilta rehellistä toimintaa käyttäen omaa nimeä julkisesti. (Alan.)

Demokraattisuudella tarkoitetaan yhtäläistä mahdollisuutta osallistua keskusteluihin ja materiaalin julkaisuun, jos käyttäjällä on pääsy Internetiin. Usein demokraattisuudella kuvataan myös sosiaalisen median keskustelevaa luonnetta. Kaksi sosiaalisen median keskeisintä ominaispiirrettä ovat omien mielipiteiden ja ideoiden tuominen esille verkossa. (Alan.)

Nopeus ja reaaliaikaisuus ovat toiset sosiaalisen median keskeisemmät piirteet. Tämän mahdollistaa nopea ja helppo tapa julkaista sisältöä, joka näkyy välittömästi julkaisun jälkeen verkossa. Sosiaalisen median tuotantoprosessit eivät ole samanlaisia kuin perinteisessä mediassa, jossa ensin käydään aineisto läpi. Käyttäjillä on mahdollisuus nähdä samaan aikaan muiden käyttäjien kommentit, äänestämiset ja linkit. Hyväksi esimerkiksi

tässä voi esitellä Aasian tsunamikatastrofin tai Iranin presidenttivaalien jälkeiset mellakat, jolloin sosiaalinen media julkaisi nopeampaa ja tarkempaa tietoa, kuin mikään muu media/lähde. Tämän kaiken mahdollisti julkaisu suoraan matkapuhelimesta varsinkin Iranin presidenttivaalien mellakoihin kohdistuvassa uutisessa, joka teki sosiaalisesta mediasta ylivertaisen uutislähteen. (Alan.)

2.2 Suosituimmat sosiaalisen median palvelut

Tässä kappaleessa esitellään suositumpia sosiaalisia medioita. Esiteltäväksi valittiin kolme palvelua, jotka ovat seuraavat Twitter, Youtube ja Instagram.

Twitter on verkkopalvelu, joka on muistuttaa paljon yhteisöpalvelua Facebookia. Siinä esiintyy yhteisö- ja mikroblogipalveluiden ominaispiirteitä. Twitterissä käyttäjät lähettävät lyhyitä viestejä eli twiittejä, joita muut käyttäjät voivat kommentoida ja jakaa. Twitterin etuna on se, että käyttäjä voi twiitata, millä tahansa mobiililaitteella, selaimella tai tabletilla paikasta riippumatta. Tämänlaisessa verkkopalvelussa viestien maksimipituus on 140 merkkiä, niinpä niiden tuottaminen on yhtä helppoa kuin tekstiviesti lähettäminen. Nämä lähettämät viestit voivat myös sisältää erilaisia linkkejä, jotka johtavat kuviin, artikkeleihin, teksteihin ja videoihin. (Pullinen 2011; Ranta 2011.)

Youtube perustettiin vuonna 2005, kehittämisprosessiin osallistuivat kolme PayPalin työntekijää Chad Hurley, Steve Chen ja Jawed Karim. Tällä hetkellä Youtube on Googlen omistamana ja suosituin suoratoistovideopalvelu. Tämän hetkinen Youtuben pääkonttori sijaitsee San Brunossa, Kaliforniassa. Youtuben videoita voi katsoa ilman, että kirjautuu sisään tai luon käyttäjätunnusta. Jos käyttäjä haluaa itse lisätä videon, hänen täytyy luoda käyttäjätunnus, joka mahdollistaa omien videoiden lataamisen palveluun muiden katsottavaksi. Halutessaan Youtube antaa mahdollisuuden lisätä videoita esimerkiksi blogikirjoituksiin ja sähköpostiin. Tilastotietojen mukaan Youtubea käyttää kuukausittain yli miljardi yksilöityä käyttäjää. Noin joka kuukausi käyttäjät katsovat yli kuusi miljardia tuntia videoita ja lataavat Youtubeen joka minuutti 100 tuntia videosisältöä. Palvelu on rekisteröity 61 maahan ja se on käännetty 61 eri kielelle. (Kalliala & Toikkanen 2009, 151; Web-opas; Youtube.)

Instagram on ilmainen kuvien ja videoiden jakamissovellus, jota voi käyttää Apple iOS, Android- ja Windows Phone- laitteissa. Palvelu avattiin lokakuussa 2010. Instagramia käyttää noin sata miljoonaa käyttäjää ympäri maailmaa. Sovellus antaa mahdollisuuden jakaa kuvia ja videoita sekä kommentoida ja tykätä niistä. Instagramissa käyttäjä voi seu-

rata muita kyseisen palvelun käyttäjiä, mikä tarkoittaa sitä, että seuraamasi henkilön lisäämät kuvat näkyvät etusivulla. Instagramille on myös ominaista hashtagien käyttö, millä tarkoitetaan kuvien merkitsemistä samalla tavalla kuin Twitterissa. Sovellus on pääosin tarkoitettu mobiililaitteella olevaan käyttöön, mutta Instagramia voi myös selata selaimella ja tarkastella seuraajien kuvia ja muiden profiileja. Kuvien lisääminen palveluun vaatii kuitenkin sovelluksen käyttöä. Instagramin sovellus mahdollistaa kuvien lataamisen ja niiden jakamisen myös muissa sosiaalisen median kanavissa esimerkiksi Twitterissa ja Facebookissa. Sovelluksesta löytyy myös kuvien muokkaus ominaisuus, näin käyttäjä voi muokata alkuperäisessä muodossa olevat kuvat haluamakseen. (Instagram 2014; Kanga 2013; Ulenius.)

Instagramiin voi luoda käyttäjätilin jo 13-vuotiaana. Ensin täytyy rekisteröityä sähköpostin avulla ja päättää käyttäjänimi. Instagramissa pystyy määrittelemään profiilinsa joko yksityiseksi tai julkiseksi. Yksityisen profiilin lisäämät kuvat tai videot voivat nähdä vain ne henkilöt, jotka on hyväksytty seuraamaan kyseistä profiilia. Käyttäjän ladattua kuvansa Instagramiin hän antaa samaa aikaa palvelulle oikeudet käyttää ladattuja kuvia haluamissaan kanavissa. Tämä pätee myös niihin käyttäjiin, joiden profiili on määritelty yksityiseksi. (Instagram; Kanga 2013.)

2.3 Sosiaalisen median tietoturvariskit

Viime vuosien aikana sosiaalisen median suosio on kasvanut huimasti, mutta myös tietoturvariskit ovat lisääntyneet. Hyvin yleisiä riskejä ovat identiteettivarkaudet, linkkien avulla leviävät virukset, tietojen kalastelu ja erilaiset roskapostit. Tämänlaiset uhat ilmenevät parhaiten yhteisöpalveluissa. Tässä kappaleessa esitellään keskeisemmät tietoturvariskit sosiaalisessa mediassa.

Sosiaalisen median keskeisemmät uhat perustuvat hyvin pitkälti käyttäjän omaan toimintaan sekä ammattimaiseen ja suunniteltuun toimintaan. Toimilla rikolliset, ääriryhmät ja valtiot pyrkivät saamaan käsiinsä luottokortti- ja henkilötietoja, yritysten salattuja tiedostoja, valtionsalaisuuksia tai jopa vaikuttamaan kuluttajien sekä yritysjohdon päätöksentekoon. Tyypillistä ammattirikollisille on taloudellisten etujen hyödyntäminen sosiaalisen median palveluissa ja sen kautta pystytään levittämään erilaisia haittaohjelmia. Yksi vaarallisimmista organisaatioihin kohdistuvista hyökkäyksistä voi olla hyvin suunniteltu haittaohjelma, jota organisaatioiden virustorjunta järjestelmä ei pysty tunnistamaan. (Valtiovarainministeriö 2010, 13.)

Keskeinen tehtävä tietoturvallisuuden toiminnassa on huolehtia tietoaineistojen luottamuksellisuudesta, eheydestä ja saatavuudesta. Pitää myös muistaa, että yksi merkittävimmistä sosiaalisen median tietoturvariskeistä on väärän tai virheellisen tiedon leviäminen verkossa, joka voi tapahtua hyvin nopeasti. Sosiaalisessa mediassa sähköisen tiedon leviämistä on hyvin hankalaa valvoa, myös tiedon eheyttä on vaikeaa taata, koska tieto voi muuttua matkan varrella palvelusta ja välittäjästä toiseen. (Valtiovarainministeriö 2010, 14.)

Käyttäjätunnustenvarkaudella tarkoitetaan käyttäjätunnusten joutumista vääriin käsiin, minkä jälkeen rikollinen tai hölmöilijä voi käyttää tunnuksia palvelun sisällön muuttamiseen, materiaalien julkaisuun organisaation nimissä, henkilötietojen varastamiseen sekä haittaohjelmien levittämiseen. Tästä seuraa luottamuksellisen tiedon päätyminen ulkopuolisten tahojen väärin käsiin, josta johtuen organisaatiolle yksityisiksi tarkoitetut tiedot näkyvät muille, mikä vaarantaa tiedon luottamuksellisuuden, eheyden ja saatavuuden varassa olevat velvoitteet. (Valtiovarainministeriö 2010,14.)

Identiteettiväärennöksillä tarkoitetaan yleensä toisen henkilön henkilöllisyyden varastamista. Tässä tapauksessa rikollinen luo varastetun käyttäjän henkilöllisyyden nimissä olevan profiilin esimerkiksi Facebookiin. Identiteettiväärennöksen avulla yleensä rikolliset tekevät maksuvälinepetoksia, jotka ovat hyvin suosittuja. Maksuvälinepetoksella tarkoitetaan sitä, että roisto ottaa pikavippejä, ostaa tavaraa tai lainaa rahaa pankista väärennetyillä tiedoilla. Tietoja voidaan hankkia esimerkiksi murtautumalla netissä oleviin tietokantoihin. Identiteettivarkaudet, jotka tapahtuvat sosiaalisessa mediassa liittyvät usein kiusaamiseen tai tekijäoikeuslakiin perustuvaan rikokseen. On ollut tapauksia jolloin varas tekee kaverin tai muun käyttäjän nimissä profiilin, johon lisää varastettuja kuvia ja käy haukkumassa toisia käyttäjiä. (Poliisi.)

Identiteettiväärennökset ovat myös yleisiä organisaatioiden keskuudessa. Ne monesti perustuvat siihen, että joku pystyttää verkkoon olemassa olevan organisaation liittyviä www-palveluita tai sen roolissa pyritään luomaan ryhmä, joka toimii sosiaalisen median palveluissa. Johtuen tämän tapaisista väärennöksistä organisaation toiminta ja julkisuuskanavat voivat saada hyvin paljon harmillista vahinkoa. (Valtiovarainministeriö 2010, 15.)

Tietojen kalastelulla eli phishing tarkoitetaan rikollisten toimintatapaa, jolla he pyrkivät saamaan ihmisten henkilökohtaisia ja salaisia tietoja, kuten pankin tilinumerot sekä niiden salasanat. Yleisin tapa, mitä rikolliset käyttävät kalastelussa on väärennettyjä sähköpostiosoitteita, jotka sisältävät linkkejä väärennetyille www-sivuistoille, joissa henkilöä pyydetään luovuttamaan henkilökohtaisia tietoja tai klikkaamaan sekä vahvistamaan joku asia.

Kalastelun seuraukset voivat olla seuraavat: rikollinen varastaa käyttäjän henkilötiedot, jolloin hän pystyy hakemaan luottokorttia käyttäjän nimissä, joka antaa rikolliselle mahdollisuuden tyhjentää uhriksi joutuneen henkilön pankkitilin tyhjäksi. Johtuen sosiaalisen median suosiosta ja helposta tavasta lähestyä käyttäjää turvallisuuden riskien huomioiminen jää vähäiseksi. On todettu, että käyttäjät ovat paljon varomattomampia sosiaalisen median palveluissa etenkin, jos linkki tai joku kutsu uuteen palveluun tulee tutulta henkilöltä, silloin he eivät välttämättä pysty olettamaan kyseistä linkkiä tai kutsua väärennetyksi. (Microsoft 2014; Valtiovarainministeriö 2010, 15.)

Roskapostilla eli ”spam” tarkoitetaan suuria määriä lähetettyjä sähköpostiviestejä ilman tarkkaan kohderyhmää. Roskaposti aiheuttaa sähköpostin tukkeutumista ja kaikkien roskapostien hävittäminen vie käyttäjän kallista aikaa niiden poistamiseen. Avatessa roskapostiviestin sen mukana voidaan levittää ikäviä yllätyksiä esimerkiksi jonkinlaisia haittaohjelmia. Myös sosiaalisen median palveluissa roskapostista on tullut huomattava ongelma. Ominaista sosiaalisen median palveluissa olevalle roskapostille on hakukoneiden roskapostien kohdentaminen tietyille käyttäjäryhmille ja ryhmien hyödyntäminen viestien lähettämiseen. Roskapostin lähettäjien viestit voivat sisältää linkkejä esimerkiksi tuotemyyntisivustoille tai pornografisiin sivustoihin. Roskapostin runsaus ja roskapostittajien usean lähdeosoitteen vaihto tekee roskapostin estämisestä hankalaa. Hyvä esimerkki huijauksesta on syksyllä 2010 Facebook- verkkopalvelussa levinnyt huijausviesti, jossa käyttäjää kehotettiin ”tykkäämään” (like), jolloin tykkäämällä huijausviestistä käyttäjä antaa rikollisille pääsyn profiilitietoihinsa ja samalla paljastaa matkapuhelinnumeronsa. Näin ollen huijauksen seurauksena käyttäjän matkapuhelinlaskuun lisättiin 19€ lisämaksu ylimääräisestä palvelusta. (Kuivanen 2004; Valtiovarainministeriö 2010, 18.)

Seuraavaksi esitellään tyypillisiä roskapostin tunnusmerkkejä:

- Postin lähettäjä on vastaanottajalle tuntematon tai vieras henkilö
- Usein viestin teksti on englanniksi tai todella huonosti suomennettu
- Viestin otsikko on epäselvä ja hyvin sekavia merkkejä täynnä
- Viestin otsikossa näkyy ”RE:” merkintä, joka tarkoittaa, että viestiin olisi vastattu
- Roskapostiviestissä saattaa olla liitetty liitetiedosto, joka voi olla aito tiedosto tai tieto siitä, että varsinainen viesti on HTML-muodossa (Web-opas.)

3 Facebookin tausta

Facebook on nykyisin suurin ja suosituin sosiaalisen median verkkoyhteisöpalvelu. Sen tarkoituksena on mahdollistaa yhteyden pitoa ystäviin, sukulaisiin tai jakaa kuvia, päivityksiä ja pelata erilaisia pelejä. Facebook on ilmainen, mutta vaatii rekisteröitymistä. Tuleva käyttäjä voi rekisteröityä Facebookiin myös yrityksenä tai yhteisönä. Kun käyttäjä haluaa rekisteröityä hänellä pitää olla toimiva sähköpostiosoite, johon rekisteröitymisen jälkeen lähetetään vahvistusviesti onnistuneesta liittymisestä Facebookiin. (Tiedonhaku internetistä.)

Facebook yhteisöpalvelun kehitti 19-vuotias Mark Zuckerberg 4. helmikuuta vuonna 2004 kolmen muun Harvardin yliopiston opiskelijan kanssa, jotka olivat Eduardo Saverinin, Dustin Moskovitzin ja Chris Hughesin. Facebook oli ensisijaisesti suunniteltu ainoastaan Harvardin yliopiston opiskelijoille, mutta myöhemmin siitä tuli suosittu muiden yliopistoiden keskuudessa. Vuodesta 2006 alkaen Facebookin jäseneksi pystyivät liittymään eri työyhteisöt ja melko pian kuka tahansa yli 13-vuotias henkilö, jolla oli toimiva sähköpostiosoite. Suomessa palvelusta tuli suosittu vasta vuonna 2007. Vuonna 2008 julkaistiin ensimmäinen Facebookin suomenkielinen versio. Tilastoiden mukaan keväällä vuonna 2009 Facebookia Suomessa käytti yli miljoona käyttäjää ja se vain jatkoi kasvua. Yksi Facebookin erityisominaisuus oli julkinen ohjelmointirajapinta (API), jonka avulla kuka vaan pystyi lisäämään lisätoimintoja Facebookiin. Parin vuoden aikana eri ohjelmia oli saatavilla kymmeniä tuhansia, joita Facebook jäsenet pystyivät lisäämään omiin profiileihinsa. (Carlson 2010; Kalliala & Toikkanen 2009, 135; Haasio 2009, 12-13.)

Facebookin käyttäjien keskimääräinen ikä on 22 vuotta. Social Bakersin mukaan Facebookissa on eniten yhdysvaltalaisia käyttäjiä, joita on yli 166 miljoonaa. Seuraavina tilastoiden mukaan listalla ovat Brasilia, Intia, Indonesia ja Meksiko. Suomalaiset käyttäjät ovat käyttäjätilastossa sijalla 60 ja heitä on noin 2,2 miljoonaa Facebookissa. (Töyrylä 2012.)

Nykyään Facebookia käyttää yli 1,23 miljardia käyttäjää, joista suurin osa on mobiililaitteiden käyttäjiä. Suurin osa mainonnan liikevaihdosta tuleekin mobiilimainonnasta. Tämän takia yhtiön voitto on noussut vuoden viimeisellä neljänneksellä 523 miljoonaa dollariin eli noin 383 miljoonaa euroon kahdeksankertaisesti vuoden takaisista lukemista. Näin ollen koko vuoden tulos kasvoi 1,5 miljardiin dollariin tammikuussa. Tämän vuoden 4. helmikuuta oli myös hyvin merkittävä päivä Facebookin perustajalle, sillä tänä vuonna juhlittiin yhtiön 10-vuotis syntymäpäivää. Huolimatta hyvästä menestyksestä Princetonin yliopiston tutkivat julkaisivat aiemmin tänä vuonna tutkimustulokset artikkelissaan, missä arvioidaan

Facebookin menettävänsä vuoteen 2017 mennessään noin 80 prosenttia nykyisistä käyttäjistään. (Iltalehti 2014.)

3.1 Profiili ja etusivu

Profiili sivulla tarkoitetaan käyttäjän omaa sivua, jota muut kaverit tai käyttäjät voivat tarkastella. Käyttäjän profiilin etusivun aikajanalla voidaan nähdä kaikki kyseisen henkilön tekemiset Facebookissa. Profiilia voi muokata tai täydentää haluamillasi tiedoilla esimerkiksi mitä koulua on käynyt, missä töissä on ollut, kotikaupungin, asuinpaikan ja iän. Profiilin oletuskuvan laittaminen on suositeltavaa, sillä se helpottaa toisen käyttäjän tunnistamista, koska Facebookissa voi olla tosi paljon samannimisiä käyttäjiä. Kun käyttäjä haluaa palata takaisin profiiliinsa, hänen ei tarvitse kuin klikata omaa nimeään näin hän pääsee siirtymään takaisin omaan profiiliin riippuen siitä, millä välilehdellä hän olisi. Yläreunassa on hakulaatikko, mikä helpottaa kavereiden, ryhmien ja sivujen etsimistä. Luotuaan profiilin käyttäjä voi silti, koska tahansa muuttaa profiilin tietoja ja sen yksityisyysasetuksia esimerkiksi kuka pystyy tarkastelemaan käyttäjän sivua. Ennen, kun lisää profiilinsa kaikkea, mitä sattuu pitää muistaa, että profiilin avulla voidaan päätellä paljon käyttäjästä. Pitää myös muistaa se, mitä käyttäjä päivittää itsestään päätyy kaikkien nähtäväksi, jos ei laita profiilia yksityiseksi. (Tiedonhaku internetistä; Haasio 2009, 22.)

Facebookin etusivulla käyttäjä voi nähdä viimeiset tapahtumat, kavereiden tilapäivitykset ja julkaisut, mitä erilaisissa ryhmissä tapahtuu. Etusivun kautta pystyy lisäämään kuvia, tilapäivityksiä, linkkejä videoihin ja luoda omille kuville albumeita sekä jakaa niitä kavereiden kanssa. Muiden kavereiden lisäksi Facebookin etusivulle voi julkaista omia kommentteja ja ajatuksia. Jos käyttäjä tykkää jostakin Facebookin sivustosta, ryhmästä, tai tilapäivityksestä se ilmestyy näkyviin etusivulle. (Haasio 2009, 23; Facebook- kurssi aloittelijoille.)

Kuva 1. Facebookin etusivun näkymä. Sivu on melko tyhjä, koska käyttäjä aloitti vähän aikaa sitten Facebookin käytön (Tiedonhaku internetistä.)

3.2 Kaveripyynnöt

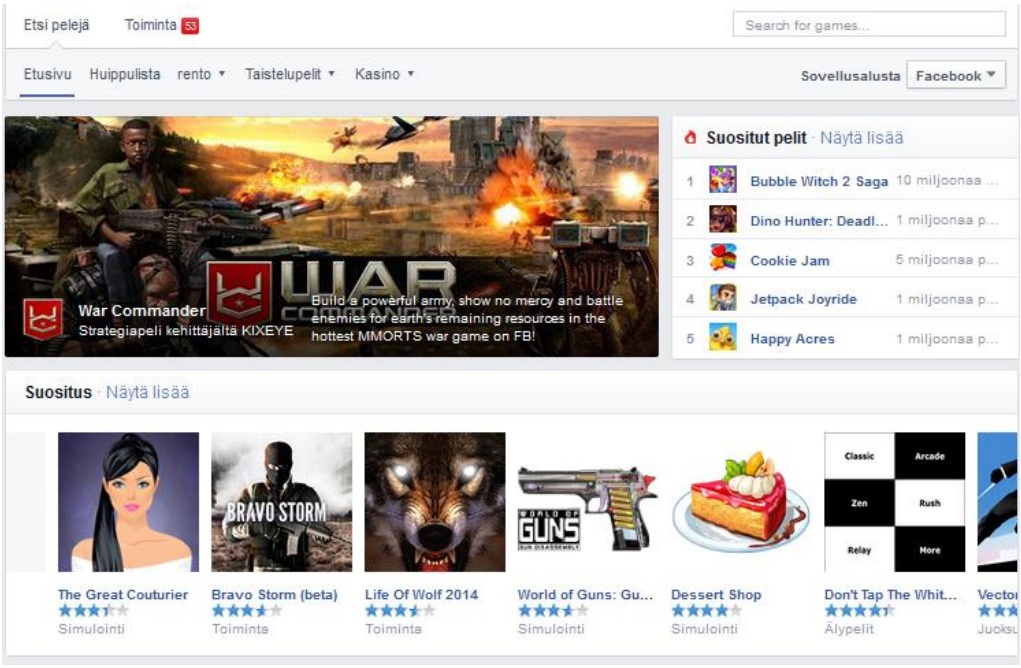
Kaverien etsiminen ja kaveripyyntöjen lähettäminen on Facebookin pääidea, joiden avulla käyttäjät voivat löytää vanhat kadonneet kontaktit ja saada uusia tuttavuuksia. Helpottaakseen kavereiden löytymistä Facebook itse ehdottaa käyttäjälle ensimmäisellä kirjautumiskerralla kavereiden etsimistä sähköpostiosoitteen yhteystietojen avulla. Kavereiden etsiminen onnistuu kirjoittamalla hakukenttään hakemasi henkilön nimen, kun etsimä henkilö osuu kohdalle hänelle voi lähettää kaveripyynnön. Kaveripyynnön kutsun lähettämisen jälkeen, jos toinen osapuoli hyväksyy pyynnön, niin käyttäjä pystyy näkemään kyseisen henkilön profiilin. Facebook ei kuitenkaan kerro kaveripyynnön lähettäjälle, jos kutsun saaja hylkään pyynnön. (Facebook.)

Käyttäjän ei tarvitse välttämättä itse etsiä kavereita, sillä Facebookilla on sellainen ominaisuus, jolloin se ehdottaa käyttäjälle kavereita keitä hän saattaa tuntea. Välillä ehdotukset osuvat oikeaan henkilöön, mutta Facebookin ehdotukset voivat olla myös sellaisia henkilöitä, joita käyttäjä ei tunne. Lista uusista kaveri ehdokkaista muodostuu sen perusteella, että moni ystävistä on kyseisen henkilön kaveri, samassa koulussa ollut henkilö tai ryhmien perusteella, mihin hän kuuluu. Kavereita on mahdollista ryhmitellä erilaisiin ryhmiin. Se tapahtuu seuraavalla tavalla käyttäjä klikkaa Kaverilistat- linkkiä tai Kaverit sivulla Luo uusi lista, jolloin voit luoda uuden ryhmän esimerkiksi perheelle ja sukulaisille sekä määritellä ryhmille erilaisia oikeuksia tarkastella profiilia. Samat henkilöt voivat olla use-

ammassa ryhmässä. Moni ajattelee, että Facebookissa pitää olla suurimäärä kavereita, mutta tärkeintä ei ole määrä vaan käyttäjän turvallisuus ja yksityisyyden säilyminen. Pitää muistaa, jos tuntematon henkilö lähettää kaverinpyynnön käyttäjälle ja hän hyväksyy sen niin samalla hän antaa kyseiselle henkilölle oikeudet nähdä profiilinsa ja siellä olevat tiedot ja tapahtumat, sillä tuntematon henkilö voi olla rikollinen, joka suunnittelee esimerkiksi varkautta. (Haasio 2009, 25 -72.)

3.3 Sovellukset

Facebookissa on käytettävissä useita erilaisia sovelluksia, kuten pelit, testit, kalenterit ja lahjat. Sovelluksien sivulla käyttäjällä on mahdollisuus nähdä kavereiden käyttämät sovellukset. Sovelluksia pystyy etsimään samalla tavalla, kuin kavereitakin eli kirjoittamalla sovelluksen nimen hakukenttään. (Facebook- kurssi aloittelijoille 2012.) Kun klikkaa Pelit-sivua aukeaa seuraavanlainen sivu, joka on esitetty esimerkki kuvassa.

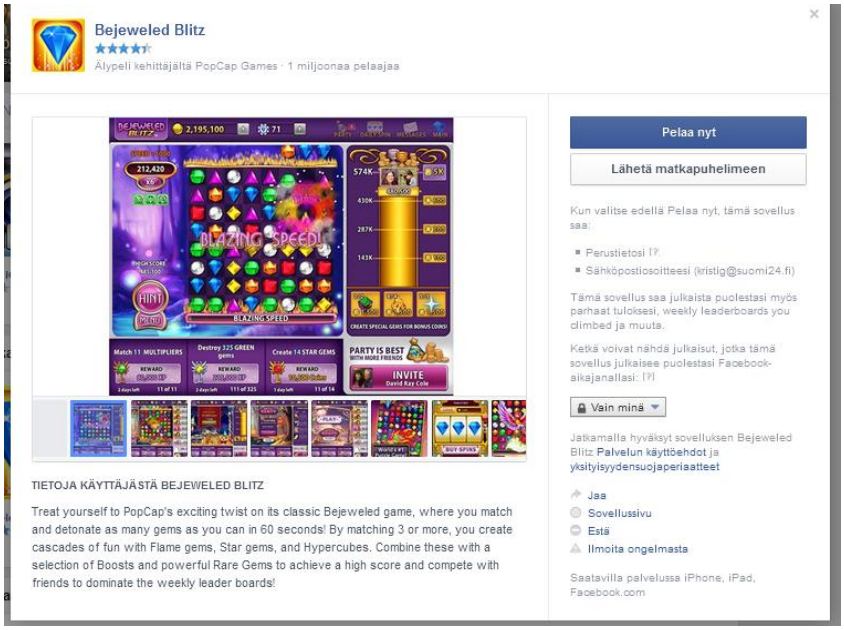


Kuva 2. Näkymä erilaisista peleistä Facebookissa

Suurin osa sovelluksista ei ole välttämättä Facebookin kehittämiä vaan palvelun käyttäjät ovat kehittäneet ne. Hyväksyessään sovelluksen pitää muistaa lukea tarkasti, mitkä tiedot sovellus saa käyttää jälkeenpäin käyttäjästä. On hyvä myös, tarkistaa kuka on sovelluksen kehittäjä ja, onko se Facebookin kehittämä. Facebookissa on olemassa sovelluksia, jotka lisäävät itsensä automaattisesti käyttäjän profiiliin ilman erillistä hyväksyntää esimerkiksi, jos käyttäjä on klikkailu kaverin päivitystä jostakin sovelluksesta. Turvallisuuden kannalta on hyvä tarkistaa jokaisen sovelluksen asetukset ja määritellä ne sitä mukaan,

mitä se saa tehdä käyttäjän profiililla. Asetuksia pääsee muokkaamaan Käyttäjätili- valikosta kohdasta Asetukset ja siitä valitsemalla Sovellukset. Samasta paikasta pystyy poistamaan sovelluksia, joille ei ole enää käyttöä. (Facebook- kurssi aloittelijoille 2012.)

Seuraavassa alla olevassa kuvassa nähdään, miltä näyttää Bejeweled Blitz sovelluksen sivu. Lisättäessä Facebookin sovellusta omalle sivulleen, käyttäjän pitää siirtyä sovelluksen sivulle ja painaa Pelaa nyt painiketta. Kuvasta näkee, että vain itse käyttäjä voi nähdä tulevat julkaisut, jotka sovellus julkaisee Facebookin aikajanalle. Ennen kun käyttäjä hyväksyy sovelluksen, on tärkeää, että hän lukee Palvelun käyttöehdot ja yksityisyydensuojaperiaatteet.



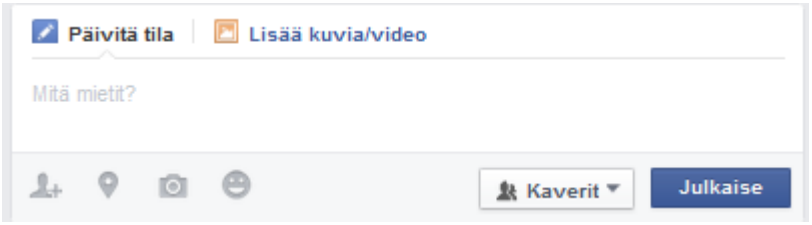
Kuva 3. Sovelluksen Bejeweled Blitz sivusto

Vaikka sovellukset vaikuttavatkin hauskalta ajanvietto mahdollisuudelta, niistä voi seurata harmia. On ollut tapauksia, kun Facebook pyytää käyttäjältä lupaa tallentaa koneelle tiedoston, asentaa ohjelman tai päivittää jotain koneella esimerkiksi Adobe Flash, tällöin on usein kyseessä jokin haittaohjelma. Tämän takia suositellaan, että käyttäjä ottaa selvää ennen kuin asentaa sellaisia sovelluksia tai jättää asentamatta ja asentaa vain tarpeellisia ja tuttuja sovelluksia. Facebook ei pysty tarkistamaan tai hyväksymään sovelluksia, jonka takia riskin todennäköisyys on suurempi törmätä haittaohjelmaan sovelluksen sijasta. On hyvä myös muistaa, ettei salli sovelluksille ylimääräisiä käyttöoikeuksia. (Luoma 2009.)

3.4 Tilapäivitykset ja viestit

Tilapäivityksillä tarkoitetaan käyttäjän tai kavereiden julkaisemia päivityksiä aikajanalle. Tämänlaiset päivitykset ilmestyvät käyttäjän profiilin seinälle ja kavereiden etusivulle.

Käyttäjä pystyy julkaisemaan profiilin sivulle sekä aikajanan etusivulle erilaisia päivityksiä. Tilapäivityksen julkaiseminen on hyvin yksinkertaista riittää vain, kun kirjoittaa Mitä mietit? – laatikkoon omat ajatuksensa ja painaa Julkaise –painiketta. Tilapäivityksiä pystyy myös kommentoimaan julkaisun jälkeen ilmaantuvassa kommentti-kentässä tai painaessa kommentti-linkkiä. Facebookissa tilapäivityksestä voi tykätä myös painamalla Tykkää-painiketta. Kaikki kommentit ja tykkäykset, jotka jätetään tilapäivityksen alle näkyvät kaikille niille käyttäjille, joille on sallittu nähdä käyttäjän julkaisut. Alla olevassa kuvassa esitellään, miltä näyttää tämä laatikko. (Facebook- kurssi aloittelijoille 2012.)



Kuva 4. Facebookin tilapäivitys laatikko

Tilapäivityksien julkaisu on yksi suosituimmista ominaisuuksista Facebookissa. Turvallisuuden kannalta käyttäjän on muistettava, ennen kuin julkaisee tilapäivityksiä aikajanalle, on hyvä tarkistaa asetuksista, kelle nämä tilapäivitykset näkyvät. Oman sijainnin julkaiseminen Facebookissa ei ole suositeltavaa, sillä jakaessa oman sijainnin siitä voi seurata vakavia seurauksia, jos tieto päätyy vääriin käsiin. Usein, miten tilapäivitykset näkee valikoitu joukko käyttäjän kavereista ja tähän on syynsä. Myrup Kristensenin mukaan Facebook on kehittänyt algoritminsa, joka mahdollistaa tilapäivitysten näkyvyyden säätelemisen. Näkyvyyttä säädellään sen perusteella, kenen kanssa käyttäjä on yhteydessä eniten. Lisäksi päivityksiin näkyvyyteen vaikuttaa se, että jotkut käyttäjät ovat muuttaneet asetukset niin, että he näkevät vain kavereiden merkittävämmät päivitykset. Toinen mahdollisuus, jos päivitykset eivät näy tietyille kavereille se johtuu siitä, että käyttäjä on estänyt kaikki päivitykset aikajanaltaan. Käyttäjille suositellaan Facebookin in-line toimintoa, jolloin ennen päivityksen julkaisua käyttäjä voi päättää, keille päivitys jaetaan. Toiminnolla pystytään kartoittamaan päivityksen sisällön avulla keille se tulee näkyville. Seurauksena voi olla se, että joku julkaisu näkyy vain esimerkiksi perheelle ilman käyttäjän päätösvaltaa. (Martikainen 2012; Ollinen 2012.)

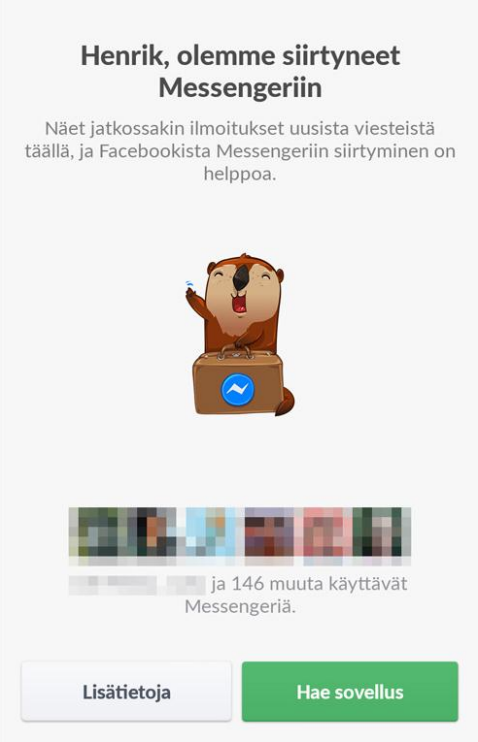
Facebookissa on ollut paljon erilasia tapauksia huijausviesteistä tilapäivityksissä. Näissä huijausviesteissä käyttäjälle luvataan, joko suuren summan lahjakortti tai pyydetään lähettämään eteenpäin viestiä, klikata linkkiä tai osallistua kilpailuun. Hyvänä esimerkkinä tämän kaltaisesta huijauksesta on K-Citymarketin järjestämä kilpailu, jossa osallistujalle luvataan 1000 euron lahjakortti K-Citymarketiin. Kilpailun mainosotsikossa käyttäjää keho-

tetaan hankkimaan lahjakortti mahdollisimman nopeasti, koska niitä on rajoitettu määrä. Todellisuudessa kyse ei ole mistään kilpailusta vaan se on huijausviesti, sillä annettu linkki vie cardsandgames32.com sivustolle ja kilpailusivuston domain on rekisteröity Pakistaniin. Tällaisessa tilanteessa ei missään nimessä ole suositeltavaa avata linkkiä eikä tietenkään jakaa omia yhteystietojaan vaan kehotuksena on poistaa mahdollisimman nopeasti huijausviesti omalta sivulta. (Rautiainen 2012.)

Toinen hyvä esimerkki Facebookissa leviävästä huijauksesta koskee dislike-nappia. Oletusasetuksina Facebookissa on vain like- toiminto eikä se sisällä ollenkaan dislike-toimintoa. Huijauksessa Facebook käyttäjiä kehotetaan asentaa sovellus, missä he voivat ilmaista mielipiteensä kaverin tilapäivityksestä myös dislike-napilla. Sovelluksen asennuksen jälkeen haittaohjelma pääsee käyttäjän tietoihin ja alkaa levittää muille kavereille kyseistä huijausviestiä, missä käyttäjä kehuu uuttaa dislike- toimintoa ja suosittelee muillekin sovelluksen käyttöä. Lisäksi itse toiminnon saaminen vaatii vastaamista verkkokyselyyn, joka mahdollistaa huijareiden tienata rahaa. Tietoturvayhtiö kehottaa käyttäjiä välittömästi poistamaan asennettu sovellus. Huijausnapin toiminnon poisto onnistuu Facebookin Käyttäjätili- valikon alla olevasta Sovellusasetukset kohdasta. (Taloussanomat 2010; Kolehmainen 2010.)

Facebookista myös löytyy viesti- toiminto, jolloin kukaan muu ei näe kyseisiä viestejä paitsi henkilö kelle ne on lähetetty. Viesteihin pääsee Facebookin etusivun vasemman laidassa olevasta Viestit –linkistä tai yläreunassa olevasta puhekupla näköisestä kuvakkeesta. Tämä on helppo tapa käydä keskusteluita ja viestitellä kavereiden kanssa chat- muotoisissa pikaviestikeskusteluissa. Aloittaakseen keskustelun riittää vain painaa henkilön kuvaa oikeassa laidassa. Lähetettyjä yksityisviestejä ei ole mahdollista poistaa tai peruuttaa vastaanottajan viestilaatikosta. Viestejä voidaan lähettää kelle tahansa, mutta jos vastaanottaja ei ole käyttäjän kavereissa viestit voivat päättyä Muut-kansioon. Tämän kansion tarkastelu onnistuu vain tietokoneelta. Nykyään Facebookissa on sellainen ominaisuus, kun vastaanottaja on lukenut viestin, se merkitään nähdyksi. Merkintä nähdystä yksityisviestistä näkyy Facebookissa tietokoneen ja puhelimen kautta. Wiretuts-sivusto kertoo, miten käyttäjä saa poistettua nähty-ilmoituksen Facebookista. Monet käyttäjät pitävät tämänlaista ilmoitusta tarpeettomana, koska kokevat, että viestiin on välttämättä pakko vastata luettuaan sen. Nähty-ilmoituksen on mahdollista poistaa asentamalla selaimelle lisäosan. Unseen- lisäosan käyttöönoton jälkeen yksityisviestin lähettäjä ei näe onko viestin vastaanottaja lukenut viestin sisältöä. Tämä pätee myös, jos vastaanottaja lähettää viestejä lähettäjälle niin hän ei näe, onko lähettäjä nähnyt viestejä. Lisäosan takia, käyttäjän saadut uudet viestit eivät muutu luetetuksi, vaikka hän avaa ne. (Facebook- kurssi aloittelijoille 2012; Facebook 2014; Jämsä 2013.)

Lähi aikoina on ollut paljon puhetta Facebookin Messenger sovelluksen käyttöoikeuksista, jotka ovat epäselkeät käyttäjille. Messenger on uusi mobiilisovellus, joka mahdollistaa pikaviestien lähettämisen Facebookissa. Uudistuksen myötä Facebook on pakottanut käyttäjiä siirtymään Messengerin mobiilisovellukseen. Tässä tapauksessa käyttäjä saa ilmoituksen saapuneesta viestistä, mutta viestiä hän ei pysty lukemaan, koska Facebook vaatii erillisen sovelluksen asennuksen. (Kärkkäinen 2014.) Alla olevassa kuvassa nähdään ikkuna, jossa pyydetään asentamaan Messenger-sovellus.



Kuva 5. Messenger- sovelluksen asennus näkymä (Kärkkäinen 2014)

Erityisesti Androidin käyttöjärjestelmässä Facebook Messenger-sovellus ottaa itselleen suuret käyttöoikeudet. Käyttöoikeudet, mitkä se ottaa käyttöön ovat muun muassa puhelimen, tekstiviestien, kameran ja mikrofoonin. Lisäksi se pyytää oikeutta tarkastelemaan laitteen puhelutietoja ja wlan- yhteyttä. Facebook perustelee Messegerin sovelluksen pakollista käyttöönottoa sillä, että se parantaisi viestittelyn ja Facebookin toimintaa mobiililaitteissa. Vaikka Facebook on perustellut tilanteen, silti perustelut eivät kata kaikkea käyttöoikeuksia, mitkä sovellus ottaa haltuunsa. Arvioiden tuloksien mukaan käyttäjät kokevat tulleen huijatuksi, myös sovelluksen yksityisyys arveluttaa heitä. (Kärkkäinen 2014.)

4 Facebookin tietoturva

Sosiaaliseen mediaan liittyy monia riskejä etenkin tietoturvaan ja tietosuojaan. Käyttäjän on hyvä havainnollistaa mahdolliset riskit ennen kuin hän aloittaa sosiaalisten mediapalveluiden käyttämisen. Tässä työssä tutkimiskohteeksi valittiin sosiaalisista medioista Facebook, koska se on suosituin yhteisöpalvelu ympärimaailmaa ja viime aikoina Facebookin tietoturva aukoista on ollut paljon puhetta muun muassa uutisissa. Facebookin yksityisyys on monesti nostettu keskustelun aiheeksi ja sen varmuudesta ollaan vieläkin eri mieltä. Näin ollen tämän työn avulla pyritään jatkossa ehkäisemään käyttäjän omaan toimintaan liittyviä tietoturvariskejä ja välttämään muita Facebookissa liikkuvia riskejä.

4.1 Facebookin tekijänoikeudet ja tiedon keruu

Mediassa on paljon keskusteltu Facebookissa julkaistun materiaalin tekijän oikeuksista. Vuonna 2009 Facebookissa syntyi käyttöehtokohu, kun palvelu ilmoitti, että saisi käyttää kaikkea materiaalia, vaikka käyttäjä olisi lopettanut Facebookin käytön. Tämä olisi tarkoittanut sitä, että Facebookilla olisi ollut oikeudet käyttää palveluun ladattuja kuvia, vaikka käyttäjä olisi sulkenut käyttäjätilinsä. Johtuen maailmanlaajuisesta mediakohusta, Facebook joutui palauttamaan vanhat käyttöehdot voimaan. Facebookin tekijäoikeuksien mukaan käyttäjällä on kaikki oikeudet tietoihin ja informaatioon, jota hän voi säädellä sen jakelua yksityisyys- ja sovellusasetusten avulla. Monet Facebookin käyttäjät eivät silti ole tietoisia, että Facebook jatkaa erilaisten tietojen keräämistä. Osa keräämistä tiedoista on verkkosivuston käyttötietoja esimerkiksi IP-osoite tai henkilökohtaisia tietoja, joita käyttäjä julkaisee Facebookissa. Palvelu saattaa kerätä myös käyttäjästä tietoja muista lähteistä esimerkiksi blogeista, pikaviestimistä, mainoksista ja muilta Facebookin käyttäjiltä palvelun toimintojen kautta. Lisäksi Facebookin käyttötilin sulkemisen jälkeen tietojen katoamiseen voi mennä pitkä aika. Käyttäjän on hyvä olla tietoinen, että Facebook voi välittää tietoa mainostajille niistä kiinnostavimmista mainoksista, joista käyttäjä on tykännyt eniten. (Haasio 2009, 65-67.)

Mainoksiin liittyvistä tapauksista Facebook aikoo julkaista uuden mainosalustan, joka tulee seuraamaan käyttäjien toimintaa vielä tarkemmin Facebookissa sekä sen ulkopuolella. Uuden Atlas-mainosalustan avulla Facebook voi seurata käyttäjien toimintaa verkossa myös, kun käyttäjät eivät ole käyttämässä Facebookia. The Wall Street Journal- sanomalehden mukaan uusi mainosalusta kerää tietoa käyttäjän verkkovierailuista erilaisilta sivuilta ja sovelluksista, joissa on olemassa Facebookin mainospaikkoja. Käyttäjien toiminnan seuraaminen on mahdollista myös puhelimen kautta, jolloin palvelu onnistuu yhdistämään puhelimella katsotuimmat verkkosivut käyttäjän Facebook- käyttäjätunnukseen. Tämä

seuranta tapahtuu jo sisäisesti Facebookissa, mutta Atlaksen ansiosta mainostaja pystyy saamaan tiedon, jos käyttäjä on selaillut mainoksia puhelimen kautta ja sen perusteella tehnyt ostoksen tietokoneella. Uusi toiminto näyttää mainostajille käyttäjätiedot anonyymi-nä, näin olleen yksittäisiä käyttäjiä ei ole mahdollista tunnistaa kerättyjen tietojen avulla. (Digitoday 2014.)

Näin suositussa palvelussa, kun Facebook erilaiset mainosohjelmat voivat paljastua hait-taohjelmiksi. Yleensä mainosohjelmat vetoavat puoleensa käyttäjiä tarjoamalla väärennet-tyjä lisäohjelmia Facebookin käyttöön, mutta oikeasti ne vain tukkivat aikajanan ja uutisvir-ran mainoksilla. Myös käyttäjän väärillä sisällön jakamisvalinnoilla voi olla vakavat seura-ukset. Paras keino estää mahdolliset tietoturva riskit näissä tapauksissa on välttää epäilyt-täviä lisäosaohjelmia ja estää kaikki Facebookin evästeet selaimelta ja käyttää eri se-laimia Facebookin selaamiseen. (Koskinen 2014.)

4.2 Yksityisyyden suoja

Facebookin yksityisyyden suojasta on keskusteltu erityisen paljon viime aikoina. Monet ihmiset eivät ole tyytyväisiä tarjolla olevaan yksityisyyden suojaan ja eivätkä luota siihen, tämän takia monet heistä eivät ole liittyneet Facebookin jäseniksi. Jos ei halua uhata yksi-tyisyyttä sekä henkilökohtaisia tietoja, kuten puhelinnumeroa, osoitetta, sähköpostiosoitet-ta tai salasanaa on hyvä laittaa Facebookin yksityisyysasetukset turvalliselle tasolle. (Haasio 2009, 71.) Yksityisyyttä voi muokata kohdasta Asetukset ja siitä Yksityisyys. Suo-situksena on hyvä asettaa yksityisyysasetukset seuraavanlaisiksi:

- Profiili: Vain kaverini
- Yhteystiedot: Vain kaverini
- Sovellusasetukset: Vain minä tai vain kaverini, turhat sovellukset kannattaa ehdot-tomasti poistaa
- Käyttäjätilinasetukset: Älä salli ylimääräisiä ilmoituksia sähköpostiisi, jos niille ei ole tarvetta.
- Käyttäjätiliasetukset: Missään nimessä ei saa lisätä luottokortinnumeroa tai antaa sitä, koska Facebook on ilmainen, muutoin tällaiset kyselyt ovat huijausta. (Luoma 2009.)

Seuraavassa kuvassa esitellään, miltä pitäisi näyttää yksityisyysasetuksien valikko. Kaikki oikeudet kannattaa määritellä vain kavereille, ettei kukaan ulkopuolinen pääse urkkimaan käyttäjän henkilökohtaisia tietoja.

Kuva 6. Yksityisyysasetukset on määritelty suojatuksi

Monet ihmiset ovat huolimatta vaaroista tottuneet jakamaan avoimesti tietoa itsestään Facebookissa, ajattelematta sen seurauksia. Harva heistä oikeasti lukee käyttöehdot ja muut sopimistekstit ennen kuin hyväksyy ja aloittaa käyttämisen yhteisöpalvelussa. Usein, miten käyttäjät haluavat uskoa, että kyseisen palvelun tarjoajat huolehtivat heidän yksityisyydestä, mutta todellisuudessa Facebookille on vain tärkeintä käyttäjien ajanvietto ja niiden tekemisien seuranta sekä rahastaminen sillä tiedolla. Toisaltaan käyttäjät itse sulkevat silmänsä ja teeskentelevät lukeneensa, ymmärtäneensä ja hyväksyneensä tarjotut toimintaperiaatteet. Todellisuudessa käyttäjät pitävät Facebookia paikkana, jossa he tulevat viihdytetyiksi muun muassa seuraamalla muiden tekemisiä, lukemalla päivän kuulumisia ja juoruja, pelaamalla pelejä. (Tranberg & Heuer 2013, 32.)

Hyvänä esimerkkinä yksityisyyden vaarantamisesta ja rikkomisesta voidaan pitää Australiassa Sydneyssa tapahtunutta tapausta, kun 17-vuotias tyttö oli auttanut isoäitiään laskemaan tämän rahoja. Laskennan jälkeen tyttö päätti julkaista Facebookiin kuvan kyseisistä rahoista. Arvaamatta, että julkaisun kuvaa seurasivat rikolliset, sillä muutaman tunnin kuluttua ryöstäjät ilmestyivät tytön äidin ovelle Bundanoosissa Sydneyn lähellä. Ryöstäjät alkoivat uhkailla tytön äitiä, lopulta heille selvisi, että tyttö ei enää asu samassa talossa. Ryöstäjät kävivät silti talon läpi ja veivät mukanaan pienen summan rahaa ja arvoesineitä. Tämän takia käyttäjiä varoitetaan jakamasta liian henkilökohtaisia tietoja, kuten syntymäaikaa ja osoitetta sekä loma suunnitelmia. Johtuen siitä, että tällaisilla tapauksilla voi olla hyvin vaaralliset ja ikävät seuraukset. (Linnake 2012.)

Facebook on tiukentanut lähi aikoina yksityisyyttä liittyen käyttäjien julkaisemiin päivityksiin. Nykyään oletusasetuksena on, että päivitykset näkyvät vain kavereille, kun ennen taas käyttäjän piti erikseen määritellä yksityisyysasetukset tiukemmiksi. Muutokseen päädyttiin runsaasta käyttäjien jättämästä palautteesta. Useammat käyttäjät eivät olleet tietoisia siitä, että kaikki, mitä he olivat julkaisseet palvelussa aikajanalleen, näkyi ulkopuolisille henkilöille. Facebook on myös luvannut jatkossa neuvoa käyttäjiä yksityisyysasetusten määrittelyssä. (MTV 2014.)

Kaikista suojautumistoimenpiteistä huolimatta Facebookiin tallentamat ja lataamat tiedot voivat joutua kolmansien osapuolien haltuun tai levitä muiden nähtäviksi Internetin ihmeelliseen maailmaan. Todellisuudessa mikään Facebookiin laittama tieto ei ole yksityistä. Hyvänä sääntönä voidaan pitää sitä, että ei julkaise mitään tietoja, joiden tarkoitus on säilyä salassa. (Tranberg & Heuer 2013, 232; Valtiovarainministeriö 2010, 32.)

4.3 Facebookin kohdistuvat tietoturvauhat

Suurin osa Facebookin kohdistuvista uhista ovat mainosohjelmat, haittaohjelmat, tietojenkalastelu, epäilyttävät sähköpostit ja ilmoitukset. Tietojenkalastelussa rikolliset luovat Facebookin aloitussivun näköisen sivun ja yrittävät sillä tavalla huijata käyttäjiä luovuttamaan käyttäjätunnuksia ja murtautua heidän tilille, joiden kautta rikolliset voivat levittää haittaohjelmia ja roskapostia. Seuraavaksi esitellään Facebookin vuosien varrelta kerättyjä tietoturvauhka tapauksia. (Saarinen 2011.)

Vuonna 2009 maaliskuussa Facebookissa havaittiin Koobface- niminen huijausviesti, joka tuli Facebookin käyttäjän kavereilta. Viestissä näkyi kaverin kuva, nimi ja linkki videoon. Linkistä kuitenkin avautui haittaohjelma, joka oli naamioituna Youtube videoon, jotta videon katselu onnistuisi, käyttäjän olisi pitänyt asentaa Adobe Flash player- päivitys. Todellisuudessa ohjelman päivitys ei asenna koneelle Adobe Flash playerin uutta versiota vaan Koobface –madon uuden version. Tämän viruksen avulla hakkerit pystyvät etsimään koneelta evästeitä ja niiden kautta kerätä käyttäjätunnuksia ja salasanoja ja sen seurauksena saastuttavat käyttäjän ystävien tietokoneita. Hakkereiden hyökkäyksiä vastaan on mahdollista suojautua, vain ajan tasalla olevilla virustorjuntaohjelmilla. Myös Facebookin ylläpitäjillä on suuri rooli uhkatilanteissa, sillä heidän pitäisi tarkistaa paljon tarkemmin sovelluksien tekijöiden henkilöllisyydet. Tämän pohjalta laatia jonkinlaiset varmistusmenetelmät ennen, kun sovelluksien kehittäjät voivat julkaista sovelluksensa. Näin on mahdollista välttyä erilaisilta Facebookiin kohdistuvilta hyökkäyksiltä. (Digitoday 2009.)

Samoihin aikoihin Koobface – madon kanssa Facebookissa liikkui toinen haittaohjelma, joka kalasteli käyttäjien identiteettien tietoja nimeltä Secrect Crush. Ohjelma levitti itseään muille käyttäjille ja sen jälkeen kalasteli käyttäjien henkilökohtaiset tiedot. Facebookissa liikkui toinen samantapainen hyötyohjelmaksi naamioitunut haittaohjelma nimeltä Error check system, joka kalasteli myös käyttäjien tietoja Facebookissa. (Luoma 2009.)

Tunnettu sähköposteissa oleva Nigerialaishuijaus 419, joka voi myös esiintyy Facebookissa. Huijaus leviää seuraavanlaisesti: käyttäjä voi saada viestin kaverilta, missä kerrotaan, että kaveri on ryöstetty esimerkiksi etelänmatkalla ja hän tarvitsee nopeasti rahaa tilille päästäkseen takaisin kotikaupunkiin. Tässä tapauksessa, jos käyttäjä uskoo tähän viestiin rikolliset saavat käsiinsä hänen henkilötiedot ja pystyvät murtautumaan käyttäjätilille. Mitään varsinaista ehkäisymenetelmää tähän ei ole, mutta on hyvä käyttää maalaisjärkeä ja tarkistaa kyseiseltä kaverilta onkohan asia näin ennen, kun alkaa toimenpiteisiin. (Luoma 2009.)

Yksi yleisimmistä huijauksista Facebookissa on Facebook- huhu viesti, jossa viestissä kerrotaan, että joku Facebook jäsen on hakkeri. Muita käyttäjiä kehotetaan jakamaan eteenpäin kyseinen varoitusviesti ja olla hyväksymättä hakkeriksi kuviteltu henkilö. Huijaus jatkuu niin pitkää kunnes uudet käyttäjät loppuvat ja kukaan ei jaa viestiä enää eteenpäin. Periaatteessa tällainen huijausviesti on vaaraton, mutta sitä voidaan pitää sosiaalisena viruksena, joka tukkii ja pelottaa käyttäjän mieltä. (Luoma 2009.)

Yksi mahdollisista huijauksista Facebookissa kohdistuu siihen, että käyttäjää pyydetään liittymään johonkin ryhmään, mutta todellisuudessa ryhmän perustaja ei ole edes ryhmän jäsen vaan häntä kiinnostaa ainoastaan lähettää roskapostia liittyneille ryhmänjäsenille. Tämän kaltainen huijaus ei ole kovin vaarallinen, mutta kuitenkin ikävä pila ryhmän käyttäjiä kohtaan. (Luoma 2009.)

4.4 Facebookin hyvät puolet

Yleensä, kun puhutaan Facebookista, niin esille tulee vaan huonot puolet eikä hyviä puolia käsitellä olleenkaan, mutta Facebookista löytyy hyviäkin puolia. Yksi Facebookin tärkeimmistä ominaisuuksista on sen monimuotoisuus. Facebookin avulla käyttäjät voivat hankkia uusia ystäviä, ylläpitää vanhoja kaverisuhteita ja sukulaissuhteita, jotka asuvat kaukana. He voivat liittyä erilaisiin ryhmiin esimerkiksi Haaga-Helian ammattikorkeakoulun perustamaan ryhmää, missä opiskelija voi olla ajan tasalla erilaisista tapahtumista, jotka järjestetään Haaga-Heliassa tai eri harrastusryhmiin liittyminen ja niiden sisällä toiminen. Käyttäjät voivat myös jakaa kuvia ja erilaisia matkaelämyksiä muiden käyttäjien kanssa.

Facebook on helppo ja nopea tiedonkulku kanava. Tieto kulkee hyvin nopeasti Facebookissa ja monen käyttäjän joka päiväseen rutiiniin kuuluu uusimpien uutisten linkittäminen seinälle, näin muut käyttäjät ovat myös ajan tasalla, mitä maailmalla tapahtuu.

Facebookin keskeisin hyvä puoli on helppokäyttöisyys ja se, että sen käyttö on ilmaista, sillä käyttäjät voivat lähettää viestejä ja soittaa puheluita kavereille ilmaiseksi. Tämän takia monelta käyttäjältä säästyy rahaa, koska ei tarvitse lähettää maksullisia tekstiviestejä niin kuin ennen vanhaa. Toisaltaan Facebookista on kehittynyt suosittu tavaroiden myyntikanava, tämä tarkoittaa sitä, että yhteisöpalveluun on luotu ryhmiä, jossa käyttäjät voivat myydä ja kierrättää muun muassa vaatteita, tavaroita, huonekaluja ja kirjoja. Tästä ilmiöstä on tullut hyvin suosittu käyttäjien keskuudessa, sillä tällainen tapa on paljon tehokkaampi päästä eroon turhista tavaroista ja tienata rahaa kuin se, että laittaa ne Huuto.net tai Tori.fi sivuille myyntiin.

Monelle käyttäjille Facebookista on tullut yksi tärkeimmistä kommunikoitivälineistä. Toisin sanoen Facebookissa ihmiset pyrkivät viihdyttämään itseään. Voidaan ajatella, että Facebook on jonkinlainen virtuaalinen huonetila, missä ihmiset voivat kommunikoida muiden kanssa, tapaa tuttuja, juoruilla ja pelata. Kyse on siitä, miten käyttäjä itse haluaa käyttää Facebookia joko pelkkänä viihdykkeenä tai monella muulla tavalla esimerkiksi mainostaa yritystä, tuoda yritykselle enemmän näkyvyyttä ja hankkia uusia asiakkaita. (Haasio 2009, 10-12.)

4.5 Ohjeet riskien välttämiseksi

Kun käyttää Facebookia pitää muistaa, että turhan hölmöilyn seurauksena käyttäjä saattaa pilata ihmissuhteensa, menettää työnpaikkansa ja tyhjentää pankkitilinsä. Tärkeintä on terveen järjen käyttö sosiaalisen median palveluissa ja muutenkin liikkuessa Internetissä. (Valtionvarainministeriö 2010, 36.)

On hyvä muistaa, kun kerran laittaa jotain tietoja itsestään Internettiin, niin ne jäävät sinne pitkäksi aikaa eikä niitä välttämättä saa koskaan pois sieltä. Käyttäjä ei voi olla koskaan varma, mihin tarkoitukseen joku sivusto käyttää luovutettuja tietoja henkilöstä. Varsinkin kuin lainsäädäntö eri maissa on erilainen ja käyttäjäsäännöt vaihtelevat sen mukaan nopeaan tahtiin hyvänä esimerkkinä voi pitää Facebookia. Jos sosiaalisessa mediassa aikoo mainita työnantajansa tai kommentoida jotain koskien organisaatiota on hyvä muistaa, että käyttäytyy asiallisesti, sillä negatiivisesta palautteesta voi seurata jopa työnpaikan menettäminen. Tällainen negatiivinen palaute näyttää mahdollisesti ulkopuolisen näkökulmasta tosi uskottavalta ja menetetyn maineen palauttamiseen voi mennä aikaa tai pa-

himmillaan sitä on mahdotonta palauttaa. Työnantajan ja organisaation mainetta saattaa uhata myös varastetut ja väärennetyt henkilöprofiilit. (Poliisi; Valtiovarainministeriö 2010, 22, 36.)

Yksi tärkeä ohje on, ettei käytä samoja salasanoja tai käyttäjätunnuksia eri palveluissa. Suositeltavaa on käyttää vahvoja ja pitkiä salasanoja vähintään 8 merkkiä. Selväkielisten sanojen tai itseensä liittyviä sanoja ja numeroita kannattaa välttää salasanoissa. Mitä enemmän salasanassa on numeroita, pieniä ja isoja kirjaimia ja erikoismerkkejä, sitä turvallisempi salasana on. Käyttäjän myös kannattaa vaihtaa aina välillä salasanansa uuteen. Välttyäkseen ongelmista, on muistettava, ettei käyttäjä kerro salasanaansa kenellekään tai talleta ja kirjoita sitä muistiin. Kannattaa välttää Facebookin käyttöä vierailta koneilta, sillä esimerkiksi julkisen paikkojen koneissa saattaa olla haittaohjelmia ja salasana voi mahdollisesti tallentua selaimeen, jolloin joku vieras henkilö onnistuu kirjautumaan käyttäjän tilille ilman minkäänlaista salasanaa. (Luoma 2009; Tehokas 2010.)

Omia henkilökohtaisia ja yksityiskohtaisia tietoja muun muassa kuvia ei kannata julkaista, koska palvelun tarjoajat voivat hyödyntää lisättyjä tietoja omiin tarkoituksiin. Erittäin tärkeää on tutustua ja lukea läpi sopimusehdot ennen kuin rekisteröityy palveluun. Rekisteröitymisen jälkeen ensimmäiseksi on laitettava yksityisyyden asetukset kuntoon, jotta kukaan ulkopuolinen henkilö ei pääsisi urkkimaan tietoja. (Valtiovarainministeriö 2010, 36.)

Ennen kuin rekisteröityy esimerkiksi Facebookiin, on hyvä ottaa käyttöön jonkinlainen salanimi, vaikka tällainen toiminta on vastoin Facebookin käyttöehtoja, tärkeintä on suojata omaa yksityisyyttä. Täyttäessä henkilötietoja on myös suositeltavaa, että käyttäjä ei mainitse oikeaa syntymäpäivämääräänsä, vaikka on kiva saada onnitteluita Facebookissa, mutta herää kysymys tulevatko ne suoraan sydämestä vai ainoastaan sen takia, koska Facebook muistuttaa siitä. Sillä oikealla syntymäpäivällä monet yritykset ja rikolliset voivat väärinkäyttää tietoa tai päätellä sen avulla todellisen käyttäjän henkilöllisyyden. (Tranberg & Heuer 2013, 228.)

Sosiaalisessa mediassa on myös otettava huomioon perheen ja ystävien yksityisyyssuoja. Vaikka käyttäjä itse käyttäisi aktiivisesti Facebookia, muut läheiset ihmiset eivät välttämättä ole yhtä aktiivisia käyttäjiä verkossa. Jos perheen jäsenet tai ystävät eivät halua, että heistä julkaistaan kuvia tai muita tietoja sosiaalisessa mediassa, on kunnioitettava heidän toiveita ja ennen julkaisemista kysyä lupaa. (Valtiovarainministeriö 2010, 36.)

Tuntemattomia kaveripyyntöjä ei tulisi missään nimessä hyväksyä listalle, ainoastaan sellaisia, joiden kanssa käyttäjä on ollut tekemisissä tai tavannut heidät. Tärkeintä ei ole ka-

vereiden määrä vaan, että on luotettavia ja oikeita kavereita. (Tranberg & Heuer 2013, 190.)

Jos käyttäjä ei halua, että hänen taloonsa murtaudutaan reissun aikana niin, parempi olisi olla mainitsematta verkossa lomasuunnitelmista ja loman ajankohdista. Ylipäätään, jos on pakko kertoa lomasuunnitelmista mieluimmin vasta sitten, kun on palannut lomilta. Näin ollen käyttäjä välttyy ikäviltä yllätyksiltä palattuaan lomalta. (Tranberg & Heuer 2013, 228.)

.

5 Tutkimuksen toteutus

Tämä tutkimus toteutetaan kyselylomakkeen avulla, jonka tarkoituksena on saada selville, minkälainen käsitys Facebookin käyttäjillä on palvelun tietoturvasta ja mahdollisista tietoturvariskeistä. Tutkimuksen tavoitteena on myös selvittää, kuinka hyvin käyttäjät suojaavat omaa yksityisyyttä ja, mitä he ylipäätään jakavat Facebookissa. Alun perin tutkimus oli tarkoitettu suorittaa jollakin kyselyohjelmalla, johon vain syötettäisiin kysymykset ja vastaajille lähetettäisiin linkki kyselyyn, mutta tiukan aikataulun ansiosta kysely jouduttiin toteuttamaan pelkällä kyselylomakkeella, joka lähetettiin käyttäjille sähköpostitse.

5.1 Tutkimuskyselyn tausta

Tutkimuskysymykset laadittiin työn tueksi ja pääosin kysymykset syntyivät perustuen työn teoriaan. Tutkimuskyselyssä oli 22 kysymystä, joista 6 olivat avoimia kysymyksiä ja loput 16 olivat monivalintakysymyksiä. Monivalintakysymyksissä käyttäjillä oli 3-6 vastausvaihtoehtoa. Tutkimuskysely toteutettiin lokakuun lopussa. Käyttäjille annettiin vastausaikaa viikon verran, jonka jälkeen vastaukset kerättiin analysoitavaksi. Kyselyyn vastanneita oli kaiken kaikkiaan 18 henkilöä. Kyselyyn vastanneista käyttäjistä seitsemän oli naispuolisia ja yksitoista miespuolisia henkilöitä. Kaikki vastaajista oli 20-30-vuotiaita. Tutkimuksen kaikki 22 kysymystä ovat luettavissa työn liite-osiossa (Liite 1).

5.2 Tutkimuskysymykset

Tutkimuskysymyksien avulla pyrittiin saamaan tarkempaa tietoa, kuinka hyvin käyttäjä on tietoinen mahdollisista riskeistä liitettyä Facebookiin ja, kokeeko käyttäjä oman yksityisyyden uhatuksi. Kaksi ensimmäistä kysymystä liittyivät siihen, onko vastaaja mies vai nainen ja, minkä ikäinen hän on. Kysymysten 3 ja 9 avulla saatiin tietoa, missä paikoissa ja milloin vastaaja käyttää palvelua esimerkiksi vapaa-ajalla ja, kuinka usein hän käyttää Facebookia vai käyttääkö olleenkaan. Kysymyksissä 4-8 keskityttiin pääosin käyttäjän yksityisyysasetuksiin liittyviin seikkoihin ja Facebookin tietoturvaan. Kuin taas 10–14 olevissa kysymyksissä käsitellään turvallisen salasanan käyttöä ja muita piirteitä. Kysymyksissä 15-21 vastattiin yleisesti Facebookin tietosuojasta ja palvelussa liikkuvista huijausviesteistä. Viimeisessä kysymyksessä haluttiin selvittää, muuttuiko vastaajan käsitys Facebookin tietoturvasta tehdyn kyselyn jälkeen.

Tutkimuskysely toteutettiin Word—ohjelmalla, johon kysymykset kirjattiin ylös.

6 Tutkimustulokset

Tutkimustuloksia analysoidaan samassa järjestyksessä kuin ne on esitettynä tutkimuskyselyssä, jotta tulokset hahmottuvat paremmin ne esitetään kaavioiden ja taulukoiden avulla. Monivalintakysymyksien vastaukset havainnollistetaan kaavioiden avulla ja avoimien kysymyksien tulokset esitetään kirjallisesti sijoitettuna taulukkoihin. Tulokset tullaan käsittelemään kohta kohdalta eli jokainen kysymys erikseen. Kaavioiden luontiin käytetään Excel- ohjelmaa, jonne syötetään monivalintakysymyksistä saadut tulokset.

6.1 Tulosten tarkastelu

Ensimmäisessä tutkimuskysymyksessä kysyttiin ”Käytätkö Facebookia ja kuinka usein?”, vastauksista selviää, että 94 % vastaajista käyttää päivittäin Facebookia ja jopa usealla heistä Facebook on auki lähes aina taustalla. Vain 6 % vastaajista oli käyttänyt ennen Facebookia, mutta tällä hetkellä ei käytä palvelua lainkaan, koska hän oli poistanut 8 kuukautta sitten käyttäjätilinsä.

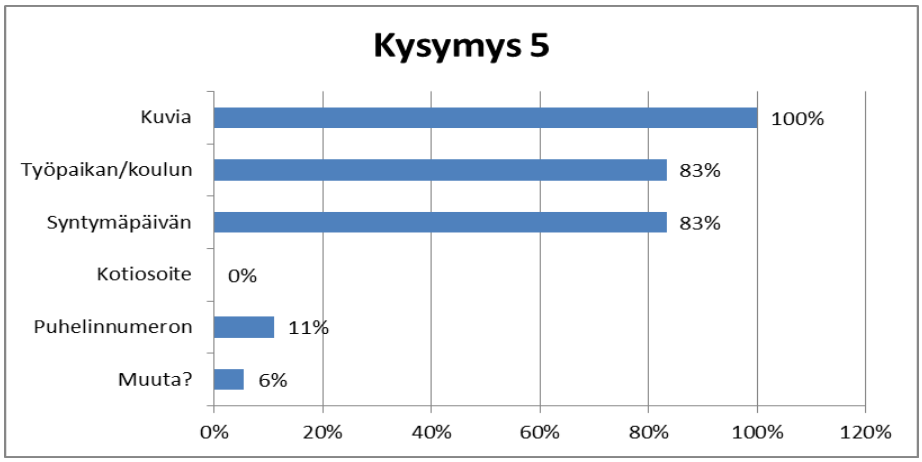
Kysymyksessä 4 kysyttiin ”Oletko perehtynyt Facebookin tietoturvallisuuteen esim. käyttöehdot? Ymmärrätkö mahdolliset Facebook käytön riskit?”. Tähän kysymykseen sai vastata vapaamuotoisesti. Suurin osa vastaajista oli perehtynyt ja ymmärtänyt Facebookin käyttöönoton mahdolliset riskit. Muutama vastaajista totesi, että eivät ole perehtyneet sen pahemmin esimerkiksi käyttöehtoihin, sillä heidän mielestä se on tylsää luettavaa. Pääosin he kuitenkin myöntävät ymmärtäneensä mahdolliset käytön riskit (Taulukko 1).

Taulukko 1. Kysymyksen 4 avoimet vastaukset

”Olen perehtynyt käyttöehtoin, sekä turvallisuuskysymyksiin. Ymmärrän myös riskit, sillä tämä perustuu myös sähköpostikäyttöön.
”Olen perehtynyt ja olen ottanut käyttöön mahdollisimman tiukat yksityisyysasetukset, koska en halua jakaa tietojani kaikille. Esimerkiksi, minun profiiliani ei löydä hakukoneiden avulla.”
”Ymmärrän riskit ja seuraan aihetta säännöllisesti.”
”Enpä oikeastaan, ei ole kiinnostanut, vaikka kylläkin tärkeä pointti!”
”Enpä oikeastaan.”
”Kyllä olen.”
”Rehellisesti sanottuna en ole tarkemmin perehtynyt Facebookin tietoturvaan tai käyttöehtoihin. (melko tylsää luettavaa rehellisesti sanottuna).”

”Olen perehtynyt käyttöehtoihin ym. yleisellä tasolla ja tiedostan palvelun käyttöön liittyvät riskit. Seuraan niitä koskevaa keskustelua myös mediassa ja oikeustieteessä.”
”En ole perehtynyt, joitain tiedän mutta en sen kummemmin.”
”Ymmärrän. Olen perehtynyt niihin, sillä tahdon tietää mitkä tietoturvaoikeudet minulla ovat.”
”Olen lukenut ehdot selaillen, mutta en kokonaan ajatuksella.”
”En ole tutustunut. Olen äitini Facebook ystävä, joten luulen, että se on isoin riski.”
”Ymmärrän, en julkaise tai säilytä henkilökohtaisia asioita Facebookissa.
”Liian huonosti perehtynyt, ymmärrän riskit. En jaa dataa esim. siitä milloin olen matkoilla, tai muuta mikä saattaa rikollisia kiinnostaa.”
”Olen lukenut, mutta en ota asia vakavasti.”
”Kyllä, haluan tietää, mihin tietoja käytetään ja kuinka niitä voidaan rajata.”
”Olen perehtynyt, mutta aika pintapuolisesti. Ymmärrän, että kaikki antamani tiedot uppoutuvat ohjelmaan ja jäävätkin sinne. Näin ollen näitä kuviani ja tietojani FB voi käyttää markkinointitarkoituksissaan, sillä kaikki käyttöehdot säilyvät Fb:llä.”
”En ole perehtynyt käyttöehtoihin, mutta ymmärrän siihen liittyvät riskit ja olen kuullut niistä puhuttavan. ”
”En ole perehtynyt. Ymmärrän riskit, en jaa liian henkilökohtaisia tietojani.”

Kysymyksessä 5 kysyttiin ”Mitä tietoja jaat Facebookissa?”. Tarkasteltaessa vastauksia voidaan huomata kuviosta, että 100 % vastaajista jakaa kuvia, 83 % työpaikan ja koulun, 83 % syntymäpäivänsä ja vain 11 % jakaa puhelinnumeronsa sekä 6 % jotain muuta esimerkiksi harrastuksen.



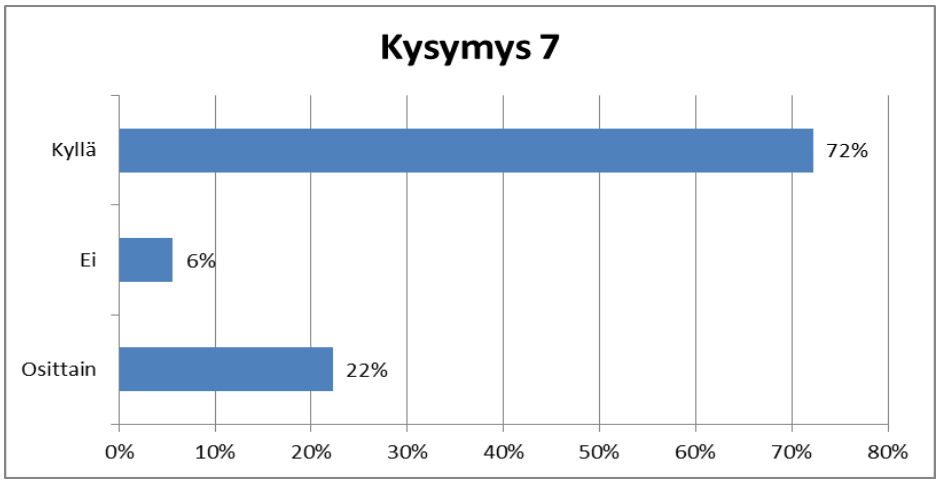
Kaavio 1. Tulokset, mitä vastaajat jakavat Facebookissa

Kysymyksessä 6 haluttiin saada selville, miten käyttäjä suojaa omaa yksityisyyttä ja, onko hänen profiilinsa julkinen vai yksityinen. Tähän kysymykseen vastaaja sai vastata vapaasti omin sanoin. Analysoimalla tutkimuksen vastauksia, voidaan huomata, että vain muutamilla henkilöillä oli julkinen profiili, muutoin loput vastanneista olivat rajanneet heidän profiilinsa ja suojanneet omaa yksityisyyttä asettamalla mahdollisimman tiukoiksi Facebookin yksityisyysasetukset (Taulukko 2).

Taulukko 2. Kysymyksen 6 avoimet vastaukset

”Profiilini ei ole julkinen, se näkyy vain kavereille. Olen rajannut profiilin omanlaisekseni.”
”Päivitykseni näkyvät vain kavereille lukuunottamatta rajoitettu-listaa. Tämä sen takia, että kaverilistallani on ihmisiä, joiden en välitä tietävän ihan kaikkia kuulumisiani.”
”Kuvat ja postaukset näkee vain kaverini (ainakin näin pitäisi olla).”
”Julkisesti näkyy vain tiettyjä juttuja.”
”Ei ole julkinen. Vain kaverit näkevät profiilin.”
”Tietääkseni profiilini ei ole julkinen, en koe mitään syytä jakaa asioitani julkisesti. Kavereiden kanssa tietenkin eri asia”
”Julkinen. Siellä todella vähän tietoja.”
”Profiilini on pääosin rajattu näkymään vain kavereilleni. En myöskään jaa tai julkaise mitään erityisen henkilökohtaista tietoa itsestäni.”
”Profiilini on julkinen, mutta ystäväni ovat piilotettuja tämä siksi että minut löytää.”
”Facebookista ja luultavasti jotkut ystäväni eivät halua löytää itseään omasta listastani.”
”Olen piilottanut Facebook profiilini, joten muut eivät sitä näe.”
”Profiilini näkyy vain hyväksytyille ystävilleni.”
”Ei ole julkinen, jostain valikosta sai näkyvyyttä rajoitettua.”
”Profiilistani näkyy muille kuin kavereille pelkkä kuva. En jaa muuta tuntemattomien kanssa. Omasta profiilistani ei pitäisi saada mitään irti julkisena”
”On julkinen. En lisää kaverilistaan ketään, jonka en tunne. Minulla on vähän kavereita, ja kaikki ovat koulukavereita. Facebook yhteisöni on tosi pieni ja suppea.”
”Profiilini on osaksi julkinen ja osaksi rajattu koska en halua kaikkien näkevän tietoni.”
”Profiilini on vain ystävien nähtävissä ja monet päivitykset ovat tarkoitettuja vain tietyille kavereille.”
”Kun käytin Facebookia, profiili oli julkinen. En lisännyt Facebook-tililleni sellaisia tietoja tai kuvia, joiden en halunnut näkyvän muille, tai mitkä vaarantaisivat yksityisyyden suojan.”

Kysymyksessä 7 kysyttiin ”Ovatko sinun Facebookin yksityisyysasetukset kunnossa?”. Kyselyn vastauksien perusteella voidaan päätellä, että reilusti yli puolet eli 72 prosenttia vastaajista ilmoitti laittaneensa yksityisyysasetukset kuntoon ja vain 6 prosentilla vastaajista ne eivät ollut kunnossa. Muut 22 prosenttia vastaajista ilmoitti, että heidän yksityisyydenasetukset ovat osittain kunnossa.



Kaavio 2. Tietoisuus yksityisyydenasetuksien kunnosta

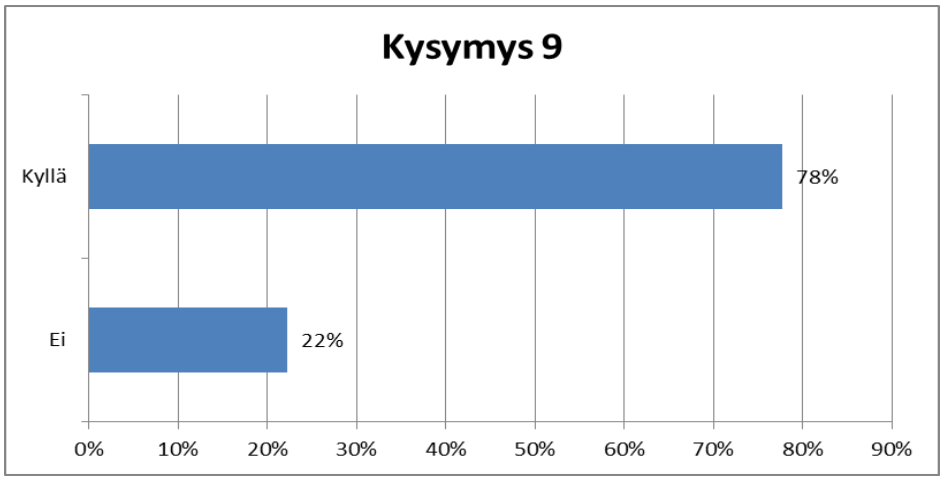
Kysymys 8 oli vapaamuotoinen kysymys, ja siinä haluttiin selvittää, kokevatko vastaajat Facebookin turvalliseksi ja luotettavaksi sosiaalisen median palveluksi ja onko heidän kohdalle tullut tilanteita, missä he eivät koe. Vastaajien vastauksista kävi ilmi, että suurin osa koki Facebookin turvalliseksi ja luotettavaksi ja he eivät olleet kohdanneet minkäänlaisia puutteita turvallisuudessa. Monet myös totesivat, että maalaisjärjen käyttö on yhtälailla sallittua Facebookissa kuin muussa Internetissä. Harva vastaajista koki Facebookin vaaralliseksi tai epäluotettavaksi palveluksi (Taulukko 3).

Taulukko 3. Kysymyksen 8 avoimet vastaukset

”En koe turvalliseksi, siksi en ole antanutkaan omia tietojani sinne ja en ole kohdannut tilanteita.”
”Koen kun tietää, miten sitä voi käyttää.”
”En koe, Facebookissa on tietoturvariskejä ja yksityisyyttä ei voi varmistaa 100%.”
”Turvallinen, ei ole tullut mitään.”
”Koen turvalliseksi, eikä ole tullut mitään tilanteita.”
”Koen facebookin melko turvalliseksi palveluksi. Toki uusia päivityksiä ja ominaisuuksia tulee koko ajan lisää, eikä niissä aina pysy perässä.”
”Koen riittävässä määrin. En ole kohdannut puutteita tässä.”

”Koen Facebookin turvalliseksi palveluksi.”
”Koen. Sillä en jaa siellä mitään joka olisi erityisen vaarallista minun henkilökohtaiselle elämälle. Eli en jaa henkilökohtaisuuksia.”
”Lähtökohtaisesti koen turvalliseksi. Luotettavaksi en niinkään, kun olen antanut Facebookille luvan käyttää tietojani.”
”Kyllä koen turvalliseksi. Julkaisen sinne sellaista matskua, mikä on tarkoitettu muille fb käyttäjille.”
”Koen Facebookin käytön turvalliseksi, maalaisjärkeä pitää käyttää aina Internetissä.”
”Itse koen kyllä, mutta tiedän, että useimpien ihmisten id oli hakkeroitu kaikista turvallisuusseikoista huolimatta. Facebook ei siis ole sen turvallisempi kuin mikä tahansa muu nettisivusto.”
”Ei juuri kokemuksia sen enempää kuin kerran kun halusivat minun henkilökortista/passista kopion, jotta tili avattaisiin taas.”
”Koen turvalliseksi, minun kohdalleni ei ole vielä osunut mitään tietoturvaa liittyvää ongelmaa.”
”Koen Facebookin turvalliseksi silloin, kun sinne laitettava materiaali on sellaista, mikä ei vaaranna yksityisyyttä. En laittaisi Facebookiin esim. tarkkaa tietoa, missä asun tai ilmoittaisi pitkistä lomamatkoistani. Maalaisjärjen käytöllä pärjää pitkälle.”
”Uskon että maalaisjärjen käytöllä pääsee tässäkin asiassa melko pitkälle.”
”En ole miettinyt sen enempää turvallisuutta. En jaa mitään yksityistä.”

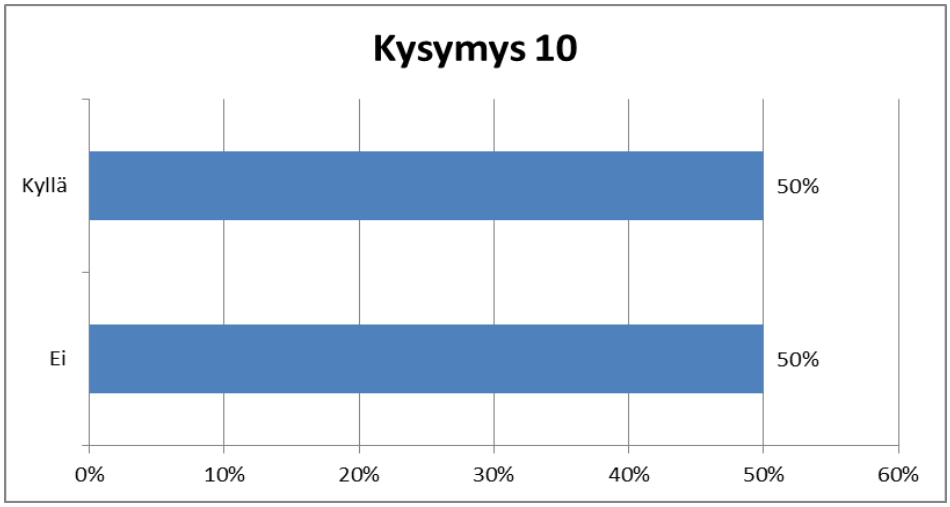
Kysymyksessä 9 kysyttiin ”Käytätkö Facebookia muulloinkin kun vapaa-ajalla?” Jos käyttäjä vastasi ”Kyllä” hän sai omin sanoin kertoa, missä muualla hän käyttää Facebookia. Vastauksista kävi ilmi, että 78 % vastaajista käyttää Facebookia muulloin, kun vapaa-ajalla mm. töissä, koulussa, ja harrastuksissa. Kun, taas 22 % vastaajista käytti Facebookia pelkästään vapaa-ajalla.



Kaavio 3. Tietoisuus Facebookin käytöstä muulloin, kun vapaa-ajalla

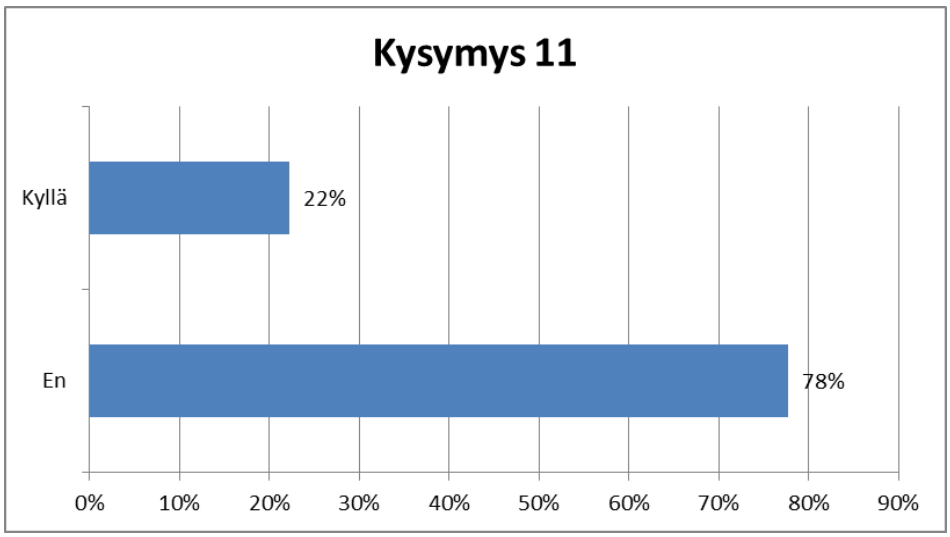
6.2 Käsitys salasanan turvallisesta käytöstä

Tutkimuskysymyksessä 10 kysyttiin ”Onko salasanasi valmiina tallennettuna, kun kirjaudut Facebookiin?”. Vastaajat vastasivat erittäin tasapuolisesti tähän kysymykseen, sillä tuloksista näkee, että 50 prosentilla vastaajista on salasana tallennettuna Facebookin etusivulla ja 50 prosenttia heistä eivät tallentaneet salasanaansa kirjautumissivulle.



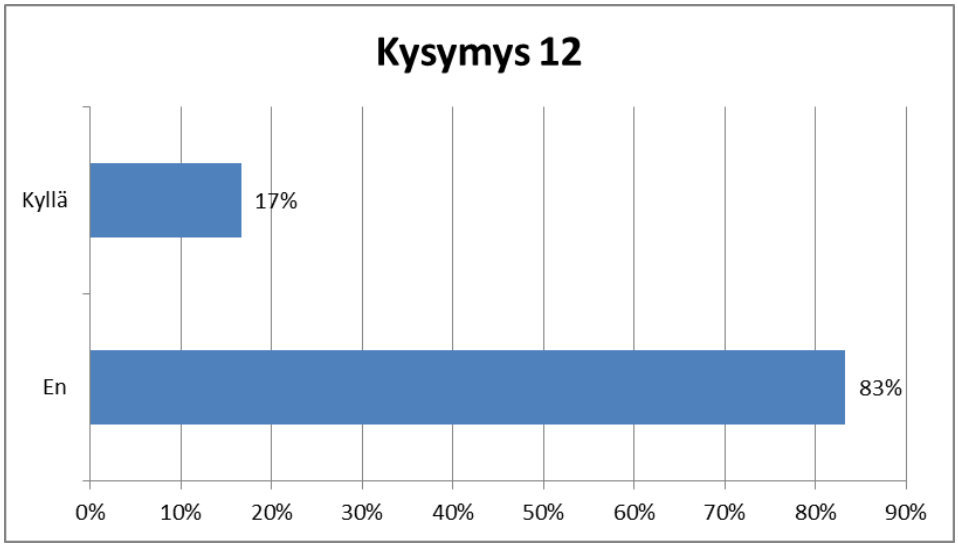
Kaavio 4. Käsitys tallenetusta salasanasta kirjautuessa Facebookiin

Kysymyksessä 11 käsitteltiin sitä, käyttävätkö he samaa salasanaa muissa palveluissa kuin Facebookissa. Valtaosa kysymykseen vastanneista jopa peräti 78% eivät käyttäneet muissa palveluissa samaa salasanaa kuin Facebookissa. Vain 22 % vastaajista vastasi, että he käyttävät samaa salasanaa eri palveluissa.



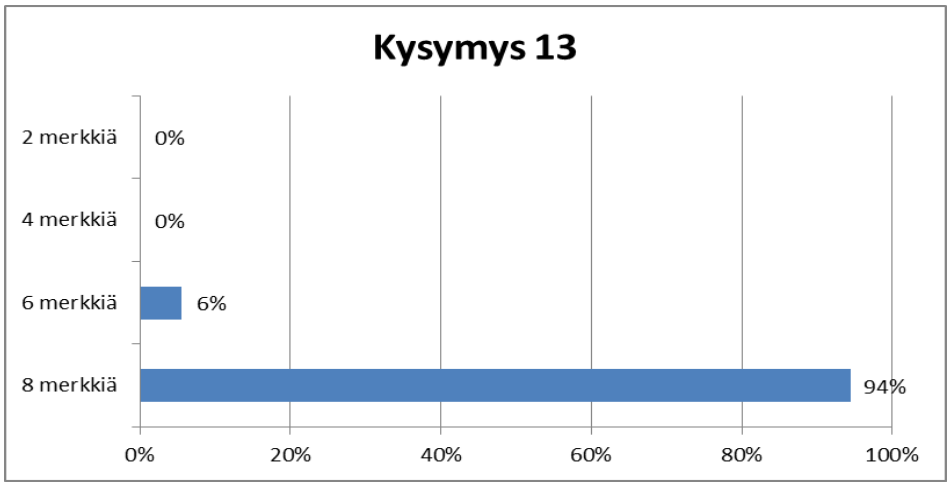
Kaavio 5. Saman salasanan käyttö muissa palveluissa

Tutkimuskysymyksessä 12 kysyttiin, ovatko vastaajat kertoneet salasanansa muille esimerkiksi sukulaisille tai kavereille. Vastauksista tuli selväksi, että 83 % vastaajista ei kertonut läheisille käyttämäänsä salasanaa, kun taas 17 % koki tarpeelliseksi kertoa muille salasanansa.



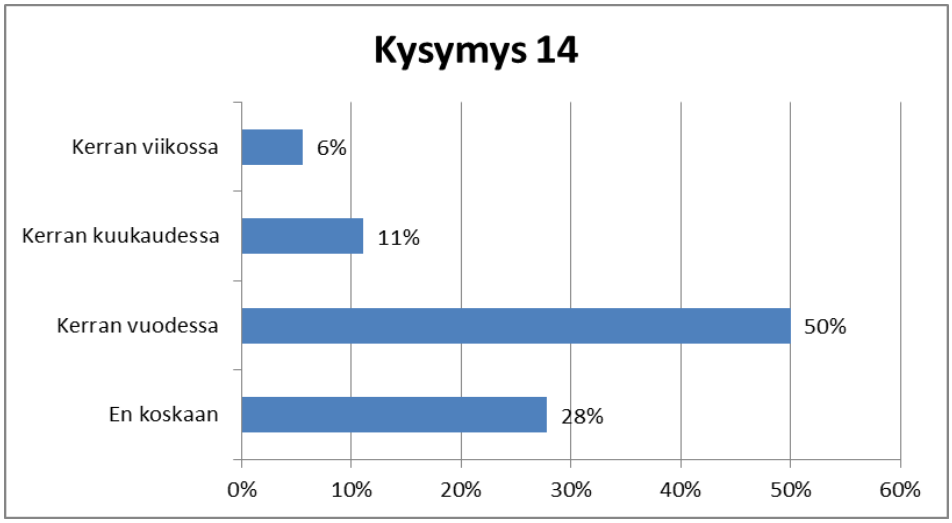
Kaavio 6. Tulokset siitä, kertovatko käyttäjät muille salasanansa

Kysymyksessä 13 kysyttiin, kuinka pitkä salasana on vastaajien mielestä riittävä. Melkein kaikki vastaajista vastasivat, että 8 merkkinen salasana on riittävä. Ainoastaan 6% vastaajista koki 6 merkkisen salasanan turvalliseksi. Kukaan vastaajista ei kokenut 2 merkkisen tai 4 merkkisen pitusen salasanan turvalliseksi. Tästä voi päätellä, että vastaajat ovat hyvin tietoisia turvallisen salasanan tunnusmerkeistä.



Kaavio 7. Turvallisen salasanan pituus

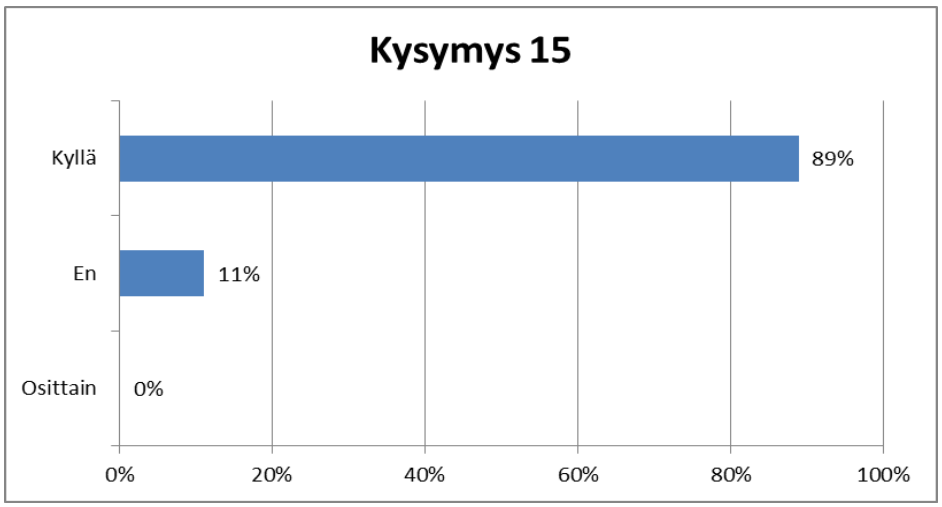
Kysymyksessä 14 kysyttiin, kuinka usein käyttäjä päivittää Facebookin salasanansa. Vastauksien perusteella kävi ilmi, että vain 6% vastaajista vaihtoi salasanaansa viikottain, 11% kerran kuukaudessa, 50% kerran vuodessa ja 28% vastaajista eivät ole koskaan vaihtaneet sitä.



Kaavio 8. Tietoisuus salasanan vaihdosta

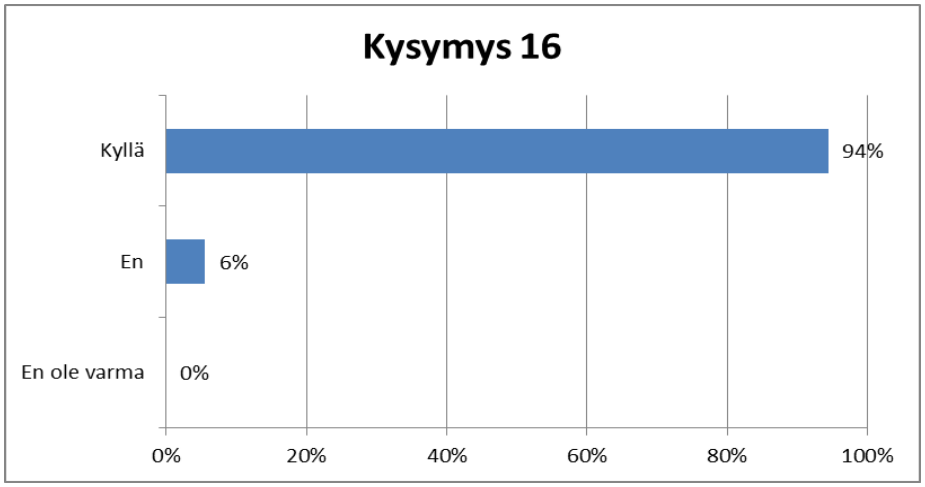
6.3 Käsitys Facebookin jaettuista tiedoista

Kysymyksessä 15 haluttiin selvittää, kuinka hyvin käyttäjät ovat tietoisia, mihin heidän syöttämät ja jakamat tiedot tallentuvat sekä, ovatko he miettineet, vaikka he poistaisivat kuvat Facebookista, silti ne voivat myöhemmin löytyä Internetistä. Vain harva vastaajista eli 11 % ei tiennyt, että heidän tietonsa voivat löytyä myöhemmin Internetistä, vaikka ne olisi poistettu Facebookista. Valtaosa vastaajista eli 89 % oli kuitenkin perehtynyt asiaan ja ei ollut huolissaan siitä.



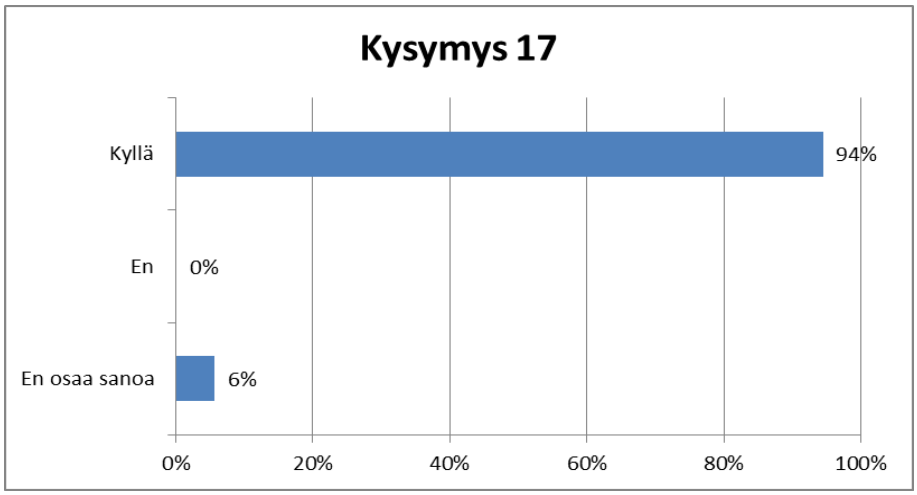
Kaavio 9. Huoli tiedon jäämisestä ja myöhemmässä vaiheessa sen löytämisestä

Tutkimuskysymyksessä 16 kysyttiin ” Tiesitkö, että kaikki sinun julkaisemat tiedot Facebookissa on käyttöehtojen mukaan heidän omistuksessa?”. Vastauksista voi huomata, että 94 % vastaajista oli tietoisia, että rekisteröidyttyä Facebookiin, he antavat samalla luvan heidän tietoihin. Ainoastaan 6 % vastaajista tämä tieto tuli yllätyksenä.



Kaavio 10. Tietoisuus käyttöehdoista

Kysymyksessä 17 kysyttiin, osaavatko käyttäjät tunnistaa mahdollisien huijauksien tunnusmerkit esimerkiksi roskapostin. Näin ollen vastauksista selvisi, että 94% vastaajista osaisi tunnistaa huijausviestin, jos näin pääsisi käymään. Vastaajista vain 6 % myönsi, ettei ole varma huijauksien tunnusmerkeistä.



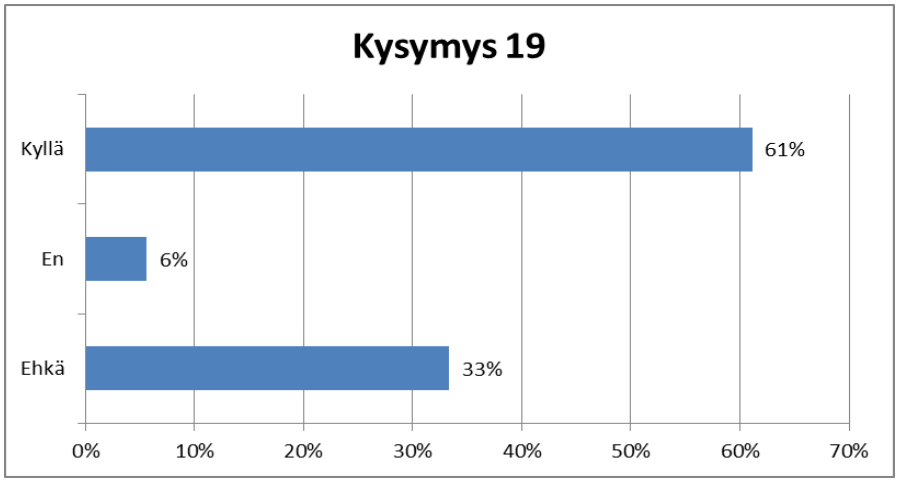
Kaavio 11. Käsitys huijauksien tunnusmerkeistä

Kysymys 18 oli avoin kysymys, ja siinä haluttiin tietää, ovatko käyttäjät törmänneet huijauksiin Facebookissa. Valtaosa vastaajista ei ollut törmännyt huijauksiin ja kävi ilmi, että vain harvan kohdalle oli osunut huijaukset. Alla olevassa taulukossa näkyy muutamia esimerkkejä avoimista vastauksista (Taulukko 4).

Taulukko 4. Kysymyksen 18 avoimet vastaukset

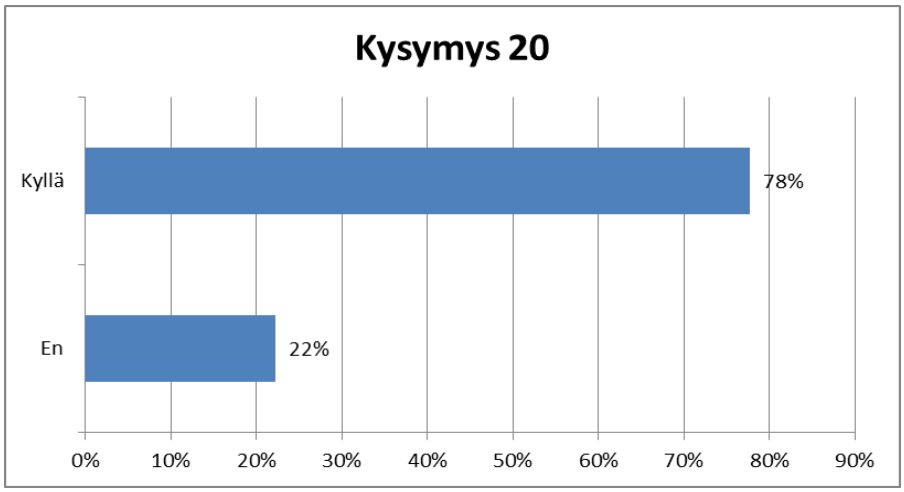
”En ole törmännyt, sillä olen rajannut tosi hyvin yksityisyys asetuksiani.”
”Olen törmännyt. Olen saanut parilta kaverilta fb-keskustelun kautta linkin, jota on pyydetty klikkaamaan. Nämä ovat olleet sellaisia kavereita, joiden kanssa en yleensä keskustele, joten olen osannut tunnistaa huijauksen.”
”Valeprofiilit, en ole hyväksynyt kavereiksi.”
”Kaiken maailman ”arvontoja” on. Tiedä sitten ovatko huijauksia mutta klikkailemaan en rahan toivossa lähtisi.”
”Roskaposteihin ainoastaan, jota painamalla siirryt automaattisesti jollekin sivulle.”
”Facebookissa levisi aika ajoin ihmisten nimissä jonkun toisen tekemiä haitallisia statuksia, joissa oli linkki johonkin sivustoon, jonka kautta yritetään esim. kalastella henkilötietoja tai levittää viruksia. Linkin edessä oli harhaanjohtava teksti, jolla pyrittiin saamaan mahdollisimman moni käyttäjä klikkaamaan linkkiä.”

Kysymyksessä 19 kysyttiin, osaako käyttäjä toimia oikein, jos hän epäilee tietoturvansa tai tietosuojansa olevan uhattuna. Vastaajista 61 % koki osanneensa toimia oikein, kun he ovat uhattuna, 6 % ei ollut minkäänlaista tietoa, miten toimia ja 33 % vastaajista vastasi, että on jonkinlainen käsitys asiasta.



Kaavio 12. Tietoisuus,miten toimia uhkatilanteissa

Kysymyksessä 20 kysyttiin ” Oletko tietoinen, että erilaiset mainosohjelmat keräävät jatkuvasti tietoja sinusta, vaikka olet kirjautunut ulos Facebookista?”. Yllättävän moni vastaajista oli tietoinen peräti 78 prosenttia, että mainosohjelmat keräävät jatkuvasti tietoa heistä, jopa kirjauduttua pois Facebookista. Kun, taas 22 prosentille vastaajista tämä tieto tuli ihan yllätyksenä.



Kaavio 13. Tietoisuus mainosohjelmien tiedon keruusta Facebookissa

Kysymys 21 oli avoin kysymys, jossa vastaajilta kysyttiin, ovatko he tietoisia, mitä muut jakavat heistä Facebookissa esimerkiksi kaverit. Vastauksista kävi ilmi, että muut jakavat vastaajista enimmäkseen kuvia ja päivityksiä. Muutama vastaajista kertoi, ettei heistä jaeta mitään tietoja. Yhdellä vastaajista ei ollut minkäänlaista käsitystä, mitä muut jakavat hänestä (Taulukko 5).

Taulukko 5. Kysymyksen 21 avoimet vastaukset

”Kaverit ovat jakaneet yhteisiä kuviamme. Niissä ei ole mitään pelottavaa..”
”Muutama on jakanut tiedon sukulais- tai perhesuhteesta. Valokuvia on jaettu myös.”
”Rehellisesti sanottuna en tiedä.”
”Olinpaikan, jos olemme kavereiden kanssa katsomassa esim. elokuvaa.”
”Minun jakamiani kuvia, jotka olen ottanut joltain sivustolta.”
”Kuvia, joskus tägättynä statuspäivitykseen.”
”Kuvia. Minun pitää ne ensin hyväksyä ennen kuin siirtyvät seinälleni.
”Tiedän, mitä muut minusta päivittää, en kyllä siitä pidä ja sanonkin ystävilleni, ettei julkaise kuvia, missä olen mukana, ellen hyväksy sitä itse.”
”Kuvia ja päivityksiä. Ollessa jossakin yhdessä jaamme toisistamme kuvia ja jotain muuta tietoa kuten sijaintia.”

”Ainoastaan yksi lisäämäni kuva on jaettu muiden toimesta.”
”Muut eivät jaa minusta mitään.

6.4 Tutkimuskyselyn tulosten yhteenveto

Kysymys 22 oli tutkimuskyselyn viimeinen kysymys, jonka avulla oli tarkoitus selvittää, muuttuiko vastaajien käsitys Facebookista kyselyn jälkeen. Kysymykseen sai vastata vapaamuotoisesti. Vastauksien avulla selvisi, että moni käyttäjä ei kokenut kyselyn myötä saavansa mitään uutta tietoa, joten monen käyttäjän käsitys Facebookista ei muuttunut lainkaan kyselyn jälkeen. Ainoastaan yhden vastaajan käsitys muuttui täysin kyselyn jälkeen ja hän päätti poistaa kokonaan Facebook käyttäjätilinsä. Muutoin suuria eroja kyselyssä ei ollut havaittavissa. Tutkimuskyselyn tarkoitus oli lähinnä muistuttaa vastaajia siitä, että yksityisyydenasetukset on hyvä aina välillä tarkistaa (Taulukko 6).

Taulukko 6. Kysymyksen 22 avoimet vastaukset

”Ei muuttunut. Facebook on hyvä verkoston hyödyke.”
”Kysely ei muuttanut käsitystäni Facebookista, lähinnä palautti mieleen ajatuksen oman profiilin asetusten tarkastamisesta.”
”Ei muuttunut, mutta ehtoihin pitäisi perehtyä paremmin.”
”Ei oikeastaan. Olen tietoinen Facebookin riskeistä.”
”Kyllä. Tunnen facebookia uhkaavaksi sivustoksi. Taidan poistaa tilini.”
”Käsitykseni ei muuttunut, sillä tiesin Facebookin haitat ja ymmärrän sen aiheuttamat riskit käyttäjän yksityisyydelle.Tiedot ja käyttökokemukseni ovat vähintään 8kk vanhoja ja vastasin kyselyyn sen perusteella, millaisena koin Facebookin silloin, kun minulla oli vielä tunnukset.”

7 Pohdinta

Opinnäytetyössä pääosin keskityttiin sosiaalisen median palveluun Facebookiin ja sen tietoturvaan sekä tutkittiin, millaisia ominaisuuksia Facebookissa on. Tutkimuksen avulla pyrittiin selvittää, millaisia ongelmia Facebookista löytyy ja, kuinka ne voitaisiin ratkaista jatkossa esimerkkitapausten avulla. Työssä myös tavoiteltiin sosiaalisen median etenkin Facebookin käyttäjäryhmille hyötyä käytön jatkon kannalta. Lisäksi työssä selviää, mitkä asetukset kannattaa ottaa käyttöön, jotta henkilökohtaiset tiedot pysyisivät mahdollisimman salaisina. Kokonaisuudessa opinnäytetyössä onnistuttiin saavuttamaan asetetut tavoitteet.

Työn teoria osion tekemisessä käytettiin pääosin erilaisia nettisivuja ja artikkeleja. Myös kahdesta kirjasta löytyi tosi paljon hyödyllistä tietoa tutkimusta varten. Opinnäytetyön tueksi tehtiin tutkimuskysely. Tutkimuskyselyn tavoitteena oli saada käsitys siitä, kuinka hyvin Facebookin käyttäjät ovat perehtyneet palvelun tietoturvaan ja tietoturvariskeihin sekä, kuinka he suojaavat omaa yksityisyyttä. Analysoidessa tutkimustuloksia huomattiin, että vastaukset olivat hyvin positiivisia, vaikka alun perin odotettavissa oli enemmän negatiivistä palautetta ja tyytymättömyyden ilmaisua sekä tietämättömyyttä liittyen Facebookkiin. Johtuen siitä, että monesti uutisten pääotsikoissa on ollut esillä Facebookin käyttäjien tyytymättömyys esimerkiksi yksityisyysasetuksiin. Kun taas tehdyssä tutkimuskyselyssä tulokset tuottivat vain positiivisia vastauksia ja valtaosa vastaajista oli tyytyväisiä Facebookin tietoturvaan eikä kokenut Facebookia uhkaavaksi palveluksi.

Tähän päivään mennessä Facebookin turvallisuudessa on huomattu monia puitteita ja todennäköisesti sen käyttö tuo tulevaisuudessa lisää turvallisuus ongelmia, mutta samalla myös uusien riskien ehkäisytapoja. Huolimatta puitteista käyttäjät ovat tottuneet viettää aikaa Facebookissa ja tämän takia monet käyttäjät eivät enää luopuisi Facebookin käytöstä, koska se on osa heidän elämää. Onhan Facebookin kuitenkin todettu hyödylliseksi yhteydenpitovälineeksi.

Johtopäätöksenä voi pitää sitä, että mitä enemmän käyttäjät jakavat tietoa itsestä maailman suuremmassa yhteisöpalvelussa, sitä enemmän he jatkossa tulevat olemaan huolissaan henkilökohtaisten tietojen mahdollisesta väärinkäytöstä. Vaikka jokainen meistä tietää, että kerran kun jotakin julkaisee Internetissä, sitä ei välttämättä enää koskaan saa sieltä pois. Tästä syystä johtuen, voimme vain elää toivossa, että jonakin päivänä saamme varmuutta siihen, ettei meidän yksityisyys ole vaarassa käyttäessä Facebookia tai muita sosiaalisen median palveluita. Tämän takia pitää myös muistaa käyttää maalaisjär-

keä ennen kuin jakaa tai julkaisee mitään henkilökohtaisia tietoja Facebookissa, sillä ei voi koskaan tietää, kuka on seuraamassa profiiliasi.

Tehdessä tutkimusta opin paljon uusia asioita liittyen Facebookiin ja monet ennestään tuntemattomat käsitteet tulivat tutuiksi. Työtä oli mielenkiintoista työstää, sillä aihe oli hyvin ajankohtainen ja siitä löytyi riittävästi tietoa. Toivon, että jatkossa tutkimusta pystyttäisiin hyödyntämään opetusmateriaalina esimerkiksi sosiaalisen median liittyvillä kursseilla.

Lähteet

Alan.fi. Mitä on sosiaalinen media? Luettavissa: http://alan.fi/mita-on-sosiaalinen-media/. Luettu 14.10.2014.

Carlson, N. 2010. How Facebook was founded. Business Insider. Luettavissa: http://www.businessinsider.com/how-facebook-was-founded-2010-3/we-can-talk-about-that-after-i-get-all-the-basic-functionality-up-tomorrow-night-1. Luettu 18.10.2014.

Digitoday. 2014. Facebookin uusi palvelu seuraa käyttäjää ja myy tiedon mainostajille. Luettavissa: http://www.digitoday.fi/mobiili/2014/09/23/facebookin-uusi-palvelu-seuraa-kayttajaa-ja-myy-tiedon-mainostajille/201413176/66?rss=6. Luettu 1.11.2014.

Edu.fi. Mikä ihmeen sosiaalinen media? Luettavissa: http://www.edu.fi/materiaaleja_ja_tyotapoja/tvt_opetuksessa/mika_ihmeen_sosiaalinen_media? Luettu 10.10.2014.

Facebook- kurssi aloittelijoille. 2012. Tampereen kaupunginkirjasto. Luettavissa: http://kirjasto.tampere.fi/files/8113/6328/1268/FB-materiaali_aloittelijoille.pdf. Luettu 22.10.2014.

Haasio, A. 2009. Facebook opas. BTJ Finland Oy. Helsinki.

Hintikka, K. Sosiaalinen media. Luettavissa: http://kans.jyu.fi/sanasto/sanat-kansio/sosiaalinen-media. Luettu:14.10.2014.

Iltalehti. 2014. Facebook tahkoaa jättivoittoja. Luettavissa: http://www.iltalehti.fi/digi/2014013017991505_du.shtml. Luettu 20.10.2014.

Iltalehti. 2014. Facebook tänään 10 vuotta. Luettavissa: http://www.iltalehti.fi/digi/2014020418005409_du.shtml. Luettu 20.10.2014.

Instagram. 2014. Mikä on instagram? Luettavissa: https://www.facebook.com/help/instagram/424737657584573?locale=fi_FI. Luettu 12.10.2014.

Itä-Suomen Yliopisto. Sosiaalisen median monet muodot ja mahdollisuudet. Luettavissa: http://www.uef.fi/fi/some/sosiaalisen-median-monet-muodot-ja-mahdollisuudet. Luettu: 18.10.2014

Jämsä, J. 2013. Nähty-ilmoituksen poistaminen Facebookin chatista. Wiretuts. Luettavissa: http://wiretuts.com/nahty-ilmoituksen-poistaminen-facebookin-chatista/. Luettu 24.10.2014.

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

Kanga, M. 2013. Mikä on Instagram? Grapevine. Luettavissa: http://grapevine.fi/2013/02/mika-on-instagram/. Luettu 12.10.2014.

Kolehmainen, A. 2010. Poista Facebookin dislike-nappi näin. Tivi. Luettavissa: http://www.tivi.fi/kaikki_uutiset/poista+facebookin+dislikenappi+nain/a488547?service=mobile. Luetta 30.10.2014.

Kuivanen, I. 2004. Roskaposti. Luettavissa: http://users.metropolia.fi/~kuivi/tietoturva/roskaposti.php. Luettu 15.10.2014.

Kärkkäinen, H. 2014. Tiedätkö, mitä asennat, kun Facebook pakottaa sinut Messengeriin? Digitoday. Luettavissa: http://www.digitoday.fi/data/2014/08/28/tiedatko-mita-asennat-kun-facebook-pakottaa-sinut-messengeriin/201411932/66. Luettu 30.10.2014.

Linnake, T. 2012. Tyttö näytti rahapinoa Facebookissa, äiti ryöstettiin. Digitoday. Luettavissa: http://www.digitoday.fi/tietoturva/2012/05/29/tytto-naytti-rahapinoa-facebookissa-aiti-ryostettiin/201230353/66. Luettu 6.11.2014.

Luoma, K. 2009. Ohjeita Facebookin turvalliseen käyttöön. Luettavissa: http://karriluoma.blogspot.fi/2009/09/facebook-tietoturva-ohjeet-turvallisuus.html. Luettu 22.10.2014.

Martikainen, T. 2012. Facebook paljasti: Näin päivityksesi näkyvät ystävillesi. Digitoday. Luettavissa: http://www.digitoday.fi/bisnes/2012/10/05/facebook-paljasti-nain-paivityksesi-nakyvat-ystavillesi/201239304/66. Luettu 24.10.2014

MTV. 2014. Facebook tiukensi yksityisyyttä - kaikki ei ole automaattisesti julkista. Luettavissa: http://www.mtv.fi/uutiset/it/artikkeli/facebook-tiukensi-yksityisyytta-kaikki-ei-ole-automaattisesti-julkista/3392946. Luettu 4.11.2014.

Ollinen, J. 2011. Facebook tilapäivitys-toiminnon uudistukset. Helpoimmat kaupat. Luettavissa: http://helpoimmatkaupat.blogspot.fi/2011/09/facebook-tilapaivitys-toiminnon.html. Luettu 24.10.2014.

Pitkänen, P. 2009. Tietoturvayhtiöt moittivat Facebookia: Virus taas! Luettavissa: http://www.digitoday.fi/tietoturva/2009/03/03/tietoturvayhtiot-moittivat-facebookia-virus-taas/20095752/66. Luettu 8.11.2014.

Poliisi. Identiteettivarkaudet. Helsingin poliisilaitos. Luettavissa: https://www.poliisi.fi/poliisi/helsinki/home.nsf/pages/4AA4B4D403026EC2C2257A7E0034F614?opendocument. Luettu 15.10.2014

Pullinen, J. 2011. Mikä on Twitter? Helsingin sanomat. Luettavissa: http://www.hs.fi/kotimaa/a1305550899552. Luettu 10.10.2014.

Ranta, P. 2011. Mikä on Twitter? Itä-Suomen Yliopisto. Luettavissa: https://wiki.uef.fi/pages/viewpage.action?pageId=15008104. Luettu 11.10.2014.

Rautiainen, J. 2012. Facebookissa leviää huijausviesti K-Citymarketin nimissä. Juhanin IT-blogi. Luettavissa: http://juhanit.wordpress.com/2012/11/17/facebookissa-leviaa-huijausviesti-k-citymarketin-nimissa/. Luettu 28.10.14

Saarinen, J. 2011. Facebookin käyttäjiin kohdistuvat tietoturvauhat. TWiki. Luettavissa: https://jop.cs.tut.fi/twiki/bin/view/Tietoturva/Tutkielmat/Facebookintietoturva. Luettu 2.11.2014.

Sanastokeskus TSK 40. 2010. Sosiaalinen media. Luettavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&qfind=sosiaalinen+media. Luettu 5.10.2014.

Taloussanomat. 2010. En tykkää - älä sorru tähän Facebookissa! Luettavissa: http://www.taloussanomat.fi/media/2010/08/17/en-tykkaa-ala-sorru-tahan-facebookissa/201011320/135. Luettu 28.10.2014

Tehokas, T. 2010. Millainen on hyvä salasana? Jyväskylän yliopisto. Luettavissa: https://www.jyu.fi/itp/ohjeet/tutoriaalit/vinkistae-vaari/hyva-salasana/. Luettu 8.11.2014.

Tiedonhaku internetistä. Facebook. Luettavissa: http://gallia.kajak.fi/opetusyhteistyo/kirjasto/Facebook.htm. Luettu 18.10.2014.

Transberg, P. & Heuer, S. 2013. Älä kerro kaikkea! Itsepuolustusopas verkkoon. Talentum. Helsinki.

Töyrylä, K. 2012. Facebookilla jo miljardi käyttäjää. Yle Uutiset. Luettavissa: http://yle.fi/uutiset/facebookilla_jo_miljardi_kayttajaa/6322267. Luettu 20.10.2014.

Ulenius, A. Meidän nuoret.fi. Instagramin käyttöön otto. Luettavissa: http://www.meidännuoret.fi/instagramin-kayttoon-otto/. Luettu 11.10.2014.

Valtiovarainministeriö 2010. VAHTI 4/2010. Sosiaalisen median tietoturvaohje. Luettavissa:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf. Luettu 5.11.2014.

Web-opas. Mikä on Youtube? Luettavissa: http://www.webopas.net/mika_youtube.html. Luettu 11.10.2014.

Web-opas. Roskaposti. Luettavissa: http://www.webopas.net/roskaposti.html. Luettu 15.10.2014.

Youtube. Tilastotiedot. Luettavissa: https://www.youtube.com/yt/press/fi/statistics.html. Luettu 30.10.2014.

Liitteet

Liite 1. Tutkimuskysely

Facebookin tietoturva käyttäjän näkökulmasta

1. Taustatiedot (Laita rasti vastauksen perään)
   a) Mies
   b) Nainen

2. Ikäsi (Laita rasti vastauksen perään)
   a) 20-25
   b) 25-30

3. Käytätkö Facebookia ja kuinka usein?

4. Oletko perehtynyt Facebookin tietoturvallisuuteen esim. käyttöehdot? Ymmärrätkö mahdolliset Facebook käytön riskit? Perustele vastauksesi.

5. Mitä tietoja jaat Facebookissa? (Laita rastit vastauksien perään)
   a) kuvia
   b) työpaikan/koulun
   c) syntymäpäivän
   d) kotiosoite
   e) puhelinnumero
   f) muuta? Perustele

6. Miten suojaat yksityisyyttäsi Facebookissa esim. onko profiilisi julkinen yms. Perustele vastauksesi.

7. Ovatko sinun Facebookin yksityisyysasetukset kunnossa?
   a) Kyllä
   b) Ei
   c) Osittain

8. Koetko Facebookin turvalliseksi/ luotettavaksi? Onko kohdallesi tullut tilanteita ettet koe? Perustele.

9. Käytätkö Facebookia muulloinkin kun vapaa-ajalla? (Laita rasti vastauksen perään)
   a) Kyllä
   b) En

Jos vastauksesi oli kyllä, missä käytät Facebookia? (Työ, harrastus seura yms.)

10. Onko salasanasi valmiina tallennettuna, kun kirjaudut Facebookiin? (Vastaa rastilla)
    a) Kyllä
    b) Ei

11. Käytätkö Facebookissa samaa salasanaa kuin muissa palveluissa?
    a) Kyllä
    b) En

12. Oletko kertonut salasanasi muille sukulaisille, kavereille yms.(Vastaa rastilla)
    a) Kyllä
    b) En

13. Kuinka pitkä salasana on mielestäsi riittävä? (Vastaa rastilla)
    a) 2 merkkiä
    b) 4 merkkiä
    c) 6 merkkiä
    d) 8 merkkiä

    _

14. Kuinka usein päivität Facebook salasanasi? (Vastaa rastilla)
    a) kerran viikossa
    b) kerran kuukaudessa
    c) kerran vuodessa
    d) en koskaan

15. Oletko tietoinen, mihin jakamat tiedot tallentuvat ja oletko miettinyt, että kaikki, mitä julkaiset Facebookissa esim. kuvat, videot, päivitykset voivat myöhemmin löytyä Internetistä, vaikka oletkin poistanut ne Facebookista?
    a) Kyllä
    b) En
    c) Osittain

16. Tiesitkö, että kaikki sinun julkaisemat tiedot Facebookissa on käyttöehtojen mukaan heidän omistuksessa? (Vastaa rastilla)
    a) Kyllä
    b) En
    c) En ole varma

17. Tunnistatko mahdollisien huijauksien tunnusmerkit esim. roskapostin, kalastelusähköpostin? (Vastaa rastilla)
    a) Kyllä
    b) Ei
    c) En osaa sanoa

18. Oletko törmännyt Facebook huijauksiin, jos olet niin mihin? Perustele.

19. Tiedätkö, miten toimia, jos epäilet tietoturvasi/ tietosuojasi olevan uhattuna?
    a) Kyllä
    b) En
    c) Ehkä

20. Oletko tietoinen, että erilaiset mainosohjelmat keräävät jatkuvasti tietoja sinusta, vaikka olet kirjautunut ulos Facebookista?
    a) Kyllä
    b) En

21. Mitä muut jakavat sinusta Facebookissa? Perustele vastauksesi.

22. Muuttuiko käsityksesi Facebookista kyselyn jälkeen?