2012

An Exploratory Study of a User's Facebook Security and Privacy Settings

Brandon Charles Hoffmann
Minnesota State University - Mankato

An Exploratory Study of a User's Facebook Security and Privacy Settings

By

Brandon Charles Hoffmann

A Thesis Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

In

Information Technology

Minnesota State University, Mankato

Mankato, Minnesota

December, 2012

An Exploratory Study of a User's Facebook Security and Privacy Settings

Brandon Charles Hoffmann

This thesis has been examined and approved by the following members of the thesis committee.

Dr. Michael G. Wells, Advisor

Dr. Christophe V. Veltsos

Dr. Jennifer R. Veltsos

Abstract

There are many potential security risks with social networking sites and the individuals who use them. These sites have been adopted by people of all ages worldwide, empowering new opportunities for the presentation of the self-learning, construction of a wide circle of relationships, and the management of privacy and intimacy. This study analyses the effect of social networking security practices, more specifically Facebook and its security and privacy settings. We identify four hypotheses: The more important Facebook users believe security is an important factor in choosing a social network, the more often they will change their security settings, the more important protection against ID theft is for Facebook users, the more frequently they will change their privacy settings, Facebook users who have left their security on a default setting have more frequently fallen victim to a virus or malware attack, and users of Facebook who have their privacy set to a custom setting are less likely to receive an attack on their profile. Brandon Hoffmann is a graduate student earning his Master of Science in Information Technology at Minnesota State University, Mankato. Mankato, Minnesota.

Table of Contents

Introduction

Students are relying on the Internet to make connections with their counterparts on a daily basis. As the Internet has developed and grown, so have the capabilities for interaction. Social networking online involves using the web to share information with others and connect with them by creating a profile that may include a personal web page and a blog. Social networking sites like Facebook are a group of web sites that provide people with the opportunity to create an online profile and to share that profile with others (Barnes, 2006). Generally, users are able to post personal information, including photographs, videos, and blog entries (WiseGeek, 2012). Social networking sites, like Facebook, are a part of every college student's everyday lives (Bugeja, 2006).

There are sites to meet almost any topic of interest. The most commonly used are Facebook, with over 800 million unique users, Twitter with 250 million users, and LinkedIn, with over 110 million unique users (eBizMBA, 2012). Social networking sites have a variety of options and applications that make them attractive to a broad audience. Facebook has made it possible for individuals to meet online and has grown tremendously in popularity in recent years. Facebook offers an effortless way to rapidly correspond with friends. However, when studied in detail, there are problems social networking can introduce, such as addiction, privacy and security issues. (Krug, 2009).

In delivering these services, social networking sites collect vast amounts of sensitive information and distribute it more quickly and extensively than traditional consumer data-gathering firms. Data gathering is a unique tool when used to help a user find old friends or see ads to new consumer products, but questions arise when users wonder how much information is being collected about themselves (Consumer Reports,

2012). How is this data being used? Could this information fall into the wrong hands? Do users understand how secure their information really is on social networks?

To help answer these questions, this study analyzes four hypothesizes. The first hypothesis states that users who consider security an important factor in a social networking site more are likely to change their settings on at least a monthly basis. The second states users who have acknowledged identity theft is as an important privacy concern are more likely to adjust their settings on at least a yearly basis. The third hypothesis states that users of Facebook who have left their security on a default setting have fallen victim to a virus or malware attack. Finally, the forth hypothesis states users of Facebook who have their privacy set to a "Custom" setting haven't received an attack on their profile.

Understanding Social Networking Sites

Social networking sites are set up to provide individuals with a means for communicating and interacting with one another. To join a site, individuals sign up as a member; this process may include providing personal information such as an e-mail address, permanent address, and/or zip code. Then users create a sign-in name and password for their personal profile. This requirement may create a false sense of security and the impression their information is private, similar to entering a gated community (Hodge, 2006). It is easy to understand why users may be concerned about what is considered private.

A profile contains the information that an individual chooses to share within a social networking site. Most profiles provide users with an option to share home town,

physical address, e-mail addresses, and phone numbers. There are also opportunities for users to post information regarding where they attend or attended school, where they are employed, personal interests, and more trivial information, such as favorite movies and music. (Timm, 2008).

Progression of Social Networking

Prior research found involvement in social networking to be positively related to the entertainment provided on the internet. This suggests young adults using social networking sites might score high on openness to controversial political issues since social networking sites are a new fascination with today's society (Pelling, 2009). Ten years ago, the concept of online social networking was little more than creating a profile for message boards. With Facebook, Twitter, LinkedIn, and other social networking sites growing rapidly, it's not surprising to see the number of social networking users has doubled since 2007 (Ostrow, 2009). Specifically, one third of the population in the United States now visit social networks at least monthly, according to a new report from Forrester Research. That's up from just fifteen percent of adults in 2007 (Ostrow, 2009).

In 2002, Friendster became the first social network to capture the attention of a global audience. One of the first to use online profiles, Friendster allowed users to meet new people and connect to friends at an accelerated pace when compared to everyday life and face-to-face interactions. The site went live attracting millions of users quickly as media outlets heavily publicized its success. Friendster declined in popularity as competitors arose within the industry, namely MySpace in 2005, and later gave way to Facebook as the most popular social networking site on the Internet (Donald, 2009).

These historical events pave the way for social networking to have a strong impact in the future with the efficiency of maintaining and acquiring relationships. To consider a social network like Facebook an upgrade to human interaction is unnecessary, but social networking connected to physical interaction justifies its status as a phenomenon (Wilson, 2010). Social networking sites provide games and applications for their users to influence signing up, logging on, and staying on. Social networks began creating extensive music databases, giving countless bands notoriety, and attracting millions of fans. Profiles became customizable, and pictures and videos could be uploaded. These reasons alone are not enough to encourage users to register for an account on a social network, but the success of these websites can be based on social instincts (Raacke, 2008).

Social interaction is a human need and an unavoidable occurrence. Humans strive for contact, relationships, friendships, and love (Pelling, 2009). Before social networking, these connections needed to be made through face-to-face interaction, which was not always an easy task. Making acquaintances online is no more difficult than clicking a button. Communicating with current friends and reconnecting with old ones can all be accomplished through one medium. Social networking has taken these inevitable occurrences and made them effortless (Donald, 2009).

Measuring how deeply social networks have permeated society is easy, but as research progresses further into this study, reasons for their success are impossible to quantify. As with any phenomenon, social networks touched upon a need within society and provided an innovative way to satisfy psychological needs. Social networking allows people to communicate in an easy and efficient environment and, with the resources at its

disposal, has the potential to become integrated even further into the framework of individuals lives (Donald, 2009).

The future of social networking is endless; Facebook may be the most popular social networking site currently, but eventually some new social networking site will come along with far greater features. The industry itself is leaning more towards corporations; in the future, more shopping capabilities or educational systems using social networks for scholarly research purposes might be seen (Wilson, 2010). Michael Rogers, columnist for MSNBC, wrote, "The Net planet is relentlessly enthusiastic in its embrace of the newest and biggest, and this year's new taste has been social networking. Involving MySpace, Facebook, LinkedIn, Twitter, and Bebo, social networking would seem poised to get more than the World Wide Web." (Hughes, 2011). Users logging on and checking social network notifications every day might seem second nature to many, but social networking will become more like human nature as time progresses (Donald, 2009).

There seems to be cultural pressure when using social networks. Students and faculty are communicating faster with their counterparts than ever before. Smartphones allow users to carry networks with them, allowing faster communication with each other. This places a necessity for younger students to have a social network account to stay in touch with social aspects of life (FTC, 2009). Nearly 63% of males and 59% of females stated that they like to read other users status updates to find out what they are doing. A majority of students, nearly 54%, stated they would feel socially incompetent if they did not have a social networking profile (FTC, 2009).

There are mainstream social networking sites that are established for a particular function and purpose. Some of these functions include: expanding your network of acquaintances and contacts, sharing files, and some for professional and business networking. Mainstream networking sites like Facebook, Twitter, and MySpace are mainly used to form and expand a group of friends from all over the world. These sites are popular and mainly used by students who are infatuated over the purpose of collecting and gathering as many contacts and friends as they can (ProCon, 2012).

Social networking is one way users stay in touch with individuals today, where as a decade ago, emphasis was on person to person interaction. Students now communicate with others using social networking sites to explain their personal affairs publicly. It is a user's responsibility to understand the uses of this technology and the issues surrounding privacy and how it relates to a student's rights (Estinson, 2011).

This can be done by researching the rights and responsibilities of involvement pertaining to social networking sites and setting a standard for the behavior when in use. This type of technology is not just a fad that will wear off in time. Issues with students' involvement in social networking sites raise issues of vulnerability; it is up to a user to be aware of the implications involved. Social networking can be an excellent resource for school, work, and communication if used properly (Estinson, 2011).

Social Networking Influence

Users are at a point where they are beginning to benefit from longstanding development in online communications (Horne, 2010). Less than a decade ago, connecting to people meant communicating via snail-mail, fax, phone calls, and beepers.

Since then, communication evolved into email and instant messaging through mobile phones. Today, these methods are considered simple communication tools that do not give additional personal experience and information (Exforsys, 2010).

The social networking industry is influencing the way people want to share more, and at the same time learn more about individuals with whom they communicate every day. Simple email exchanges provide necessary data about each party, but today, just two individuals sharing data is considered inefficient (Exforsys, 2010). Originally, social networking was based on activities where people gathered at one website and shared their thoughts through comments on articles and instant messaging with other members (Exforsys, 2010). Thus, new social networking mechanisms were created, and through an online platform, people share thoughts, post pictures and videos, and invite people to events. Social networking's major players have created virtual communities where communication is not just based on the needed information, but goes beyond a personal level (Raacke, 2008).

The true phenomenon is how big social networking has grown. According to an article by CNN reporter Lisa Respers France, "in an period when even the president of the United States has a Facebook page and spectators texted and tweeted about Inauguration Day, the electrical power of online and digital social networking is clear." (Hughes, 2011). The four largest social networks, Facebook, Twitter, LinkedIn, and Google+, have over a billion accounts combined (Facebook, 2012). Approximately 10 percent of the world's population is currently talking to each other online (Horne, 2010). It is the next step for social networking sites to increase the ability to communicate with each other.

Securing Identity in Social Networking

In an era where our online identity overshadows our actual identity, potential security risks associated with these social networks can be intimidating. Over the years, researchers and hackers alike have identified a handful of security risks ranging from people, process, and application (Wang, 2009).

The information a user posts in an online environment can be used by those with malicious intent to conduct social engineering scams, attempt to steal a user's identity, or access important data (Pelgrin, 2010). Social networks are increasingly becoming sources of worms, viruses and other malicious code. It is important to realize that the information a user posts can be viewed by a broad audience and the use of this information such as inappropriate photos, status updates, and incorrect employment positions could have negative effects in areas as the workplace and schools (Pelgrin, 2010).

The nature of social networking sites persuades users to post personal information. As new vulnerabilities are discovered on applications vendors scramble to create patches, or updates to the systems. Every day new malicious encryption is discovered through viruses and worms. Users generally aren't aware of the need to patch and update consistently (Bradley, 2012). Because of a false sense of security on the Internet, users may provide more information about themselves and their life online than they would to a stranger in person (Pelgrin, 2010).

In European nations, security committees have been formed such as the European Network and Information Security Agency (ENISA). According to ENISA's website, this organization is working for the European Union (EU) Institutions and Member States.

ENISA is the EU's response to these cyber security issues of the European Union. The organization strives to make ENISA the European exchange of information, showcasing best practice and awareness in the field of information technology security (ENISA, 2011).

There are a few common tips to keep protected from information intrusions on social networking sites. First, use long passwords containing letters and numbers with unique characters. Second, only allow people you truly know and trust to access your profile. Third, be cautious with games and applications. Finally, check the social networking sites security settings weekly. Some networking sites, such as Facebook, adjust preferences on their websites without the user's consent as most have already agreed to their terms of service (FTC, 2009).

Facebook Scams

With over one billion users (Black, 2012) Facebook continues to be the most popular social networking website in the world. For this reason alone it is important to study the privacy and security concerns this website faces. On February 9, 2012, five anti-scam websites (Hoax-Slayer, That's Nonsense, The Bulldog Estate, Facecrooks, and facebookprivacyandsecurity) alerted users about a Facebook hoax exploiting pictures of sick babies (Protalinski, 2012). After gaining national attention virally, the media asked for in an open letter to news organizations. Facebook reacted by taking down the offending images and explained why it was necessary for their removal:

> "In addition to Facebook's regular ongoing improvements to our automatic spam detection systems, we are looking specifically at these types of violations and how

> they can be more quickly and efficiently taken down. We are very aware of the baby charity scam issue and are looking at some technical solutions that will make their removal quicker and more comprehensive" (Protalinski, 2012).

Facebook is now working to remove scams and hoaxes. The social networking giant is creating a program to prevent the upsetting images from going viral. Their strategy may work as Facebook attempts to improve its systems. In the meantime, users should keep using Facebook's photo reporting feature to inform their friends that a company or organization will never donate money based on the amount of times something is Liked, shared, and/or commented on (Protalinski, 2012).

Facebook Security Issues

A study from the United Kingdom found that Facebook's security settings confuse its users. Almost half of Facebook users aren't keeping track of recurrent changes to their privacy and security settings (Tahseen, 2011). Facebook has changed its privacy policies eight times, including changes that automatically tells the user where they are and a change that let third parties access users' telephone numbers and addresses (Tahseen, 2011).

According to *The Montreal Gazette*, a University of British Columbia study exposed Facebook's security system when it failed to stop a large-scale intrusion in which personal information on Facebook users accounts were collected. Researchers said they collected 250 gigabytes of information from Facebook users by using bots, or computer-generated fake Facebook profiles controlled by programming (Shaw, 2011).It took eight weeks for the bots to gather this information, first by sending friend requests

from the fake account to about 5,000 random Facebook users. When people accepted those requests, the bot sent friend requests by using Facebook features such as Friend-Finder. If fake or phished Facebook users join a network, it could mean users are vulnerable to data theft and misinformation campaigns (Shaw, 2011).

Facebook's persistent tweaks to privacy and security settings leave many people questioning how secure their Facebook account is. In December 2011, Facebook founder Mark Zuckerberg was hacked when 14 private photos of Zuckerberg leaked to photo-sharing sites with the caption: "It's time to fix those security flaws." Facebook later confirmed the hack was the result of a recent code push and was live for a small time period, affecting not just the founder's account but also thousands of user accounts (Burnham, 2011).

Facebook and other social networks are changing the way the modern world operates and "rewriting the rules" of social engagement, Chief Operating Officer Sheryl Sandberg says (Consumer Reports, 2012). Facebook has partnered with the Department of Labor and others to assist job seekers and employers, developing systems to make job postings viral. For example, the network keeps active-duty soldiers in touch with families, and allows posting of severe weather to be easily accessible. Millions turn to Facebook to express views on government and industries, stretching their collective influence in ways never thought possible before (Consumer Reports, 2012).

Facebook Privacy Concerns

In a study at Ohio University, researchers discussed the privacy concerns outlined by several reports and studies on Facebook. The study referenced a report on twenty-

three Internet service companies, charged Facebook with severe privacy flaws, placing it in the second lowest category for a large, all-inclusive privacy threat (Debatin, Lovejoy, Horn, and Hughes, 2009). Facebook tied with six other companies. This rating was based on concerns with data mining, transfers to other companies, and in particular Facebook's questioning policy on how the company may collect information about their websites users other sources, such as newspapers, blogs, instant messaging services, or any external Facebook service (Debatin, Lovejoy, Horn, and Hughes, 2009).

Many of Facebook's users say Facebook doesn't address the core issues when it comes to a user's privacy. Consumer Reports stated "In the U.S., […] there are strong federal privacy laws covering your financial and health data. But Americans have few federal rights to see and control much of the information they share through social networks." It's important to question what data Facebook keeps about its users (Consumer Reports, 2012).

Dr. Eben Moglen, a Columbia University law professor who favors dispersed data sharing which is the practice of making research readily available to investigators. Dr. Moglen disagrees with Facebook's focus on privacy controls is "like a magician who waves a brightly colored handkerchief in the right hand so that the left hand becomes invisible. From a consumer's viewpoint, Facebook's fatal design error isn't that Johnny can see Billy's data. It's that Facebook has uncontrolled access to everybody's data, regardless of the so-called privacy settings." Users are usually surprised where their information end up (Consumer Reports, 2012).

One way data can leak is through Facebook games and apps. "Whenever you run one, it gets your public information, such as your name, gender, and profile photo, as well as your list of friends even if you haven't made that list public," says Consumer Reports Magazine. If you give the app certain permissions, it can peer deeper into your data and see information your friends share with you, unless they specifically forbid involvement with apps in their privacy settings (Consumer Reports, 2012).

Previous Research on Facebook Privacy

A considerable amount of research has been performed in the area of Facebook security such as *Imagined Communities Awareness, Information Sharing, and Privacy on the Facebook* by Alessandro Acquisti and Ralph Gross of Carnegie Mellon University. These authors surveyed fellow university students using Facebook in 2006, a time when social networking was only starting to become a global phenomenon. The researchers looked for an underlying demographic or behavioral difference between the communities of the network's members and nonmembers and analyzed the impact of privacy concerns (Acquisti and Gross, 2006).

The study found that an individual's privacy concerns are only a weak predictor of his/her membership to the network. In fact, individuals who are concerned about privacy join the network and reveal great amounts of personal information. Some managed their privacy concerns by trusting their ability to control the information they provide and the external access to it. However, researchers found significant misconceptions among some members about the online community's reach and the visibility of their profiles (Acquisti and Gross, 2006).

There are many studies similar to Acquisti and Gross such as Harvey Jones and Jose Hiram Soltren's *Facebook: Threats to Privacy* where discussion of privacy and security threats caused by malware, viruses, and other fishing attempts outside of the profile itself, but one aspect of social networking that hasn't been scrutinized is the default security settings on a user's profile.

A currently unpublished study conducted at Wayne State College investigated the propensity of social networking with college students. The questionnaire was administered to a broad spectrum of participants in the school of Business and Technology. This survey included open-ended questions, where respondents could express their opinions pertaining social networking. The study analyzed the phenomenon of social networking and identified the range of positive and negative reinforcements social networking had on a subset of the students and faculty at the School of Business and Technology at Wayne State College. The research found that student users, in some instances, use social networks as a way to pass the time during long classroom lectures rather than using the site for academic (Hoffmann, 2011).

The data showed there are a variety of ways a social networking site can be used and the majority of Business and Computing students use them. There are various ways to communicate on a social networking site and it appears students are using every option. The findings show students and faculty are posting on others' profiles, keeping in touch via instant messaging features, and sharing stories by uploading pictures and videos to their profiles (Hoffmann, 2011).

In the study, questions examined the propensity of social networking. Propensity is an inclination or natural tendency to behave in a particular way. Initially this study

focused on the educational aspects of social networking by how students interact with their instructors on campus, but only sixteen percent of student said they interact with their professors on social networking sites, many of them claiming it depended on who the professor is and how they relate on a personal level as opposed to a professional level. This could mean students are using social networks in an informal setting and not to display themselves professionally in society (Hoffmann, 2011).

One problem identified was fifty-two percent of students preferred arguments over the internet rather than face to face confrontation, which is why cyber bullying having a major impact on our society by the way we converse with others. One participant stated "Social networking is a great way for [us] to connect with friends, but there is quite a bit of drama [in social networking sites]." The distinction between genuine friends and acquaintances are unclear. Some students are spending time maintaining relationships with people they don't really care about. A majority of students were neutral concerning face to face confrontation as indicated by opting out of that question. Fifty four percent of students, especially females, would prefer to settle conflict online. This is an interesting phenomenon that can lead to security questions such as cyber-bulling (Hoffmann, 2011).

A study from the Massachusetts Institute of Technology examined how Facebook affects privacy, and exploring flaws in the system. Information is shared constantly by users of Facebook, but research of the privacy and security within the site is scarce. The study stated "privacy on Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook" (Jones and

Soltren, 2005). The research based its end-user findings on a survey of MIT students and statistical analysis of Facebook data from MIT, Harvard, NYU, and the University of Oklahoma (Jones and Soltren, 2005).

The study looked into the Facebook framework in terms of its information practices in accordance with the Federal Trade Commission. MIT's study used a threat model to analyze specific privacy risks stating: "Specifically, university administrators are using Facebook for disciplinary purposes, firms are using it for marketing purposes, and intruders are exploiting security holes" (Jones and Soltren, 2005). For each threat, this research analyzed the effectiveness from current protection, and when solutions were inadequate, researchers made recommendations on how to address these issues (Jones and Soltren, 2005).

The research concluded "anyone who analyzes the threats to privacy a system poses will inevitably adopt a negative tone about the target of its examination" (Jones and Soltren, 2005). And while data mining is difficult, it's not necessarily impossible. Facebook's requirement of having a school or business email account to sign up and signify previous or present enrollment it can prevent fake accounts in what could be problem of Facebook identity theft (Jones and Soltren, 2005).

Research Methodology

The data collection consisted of surveys, Facebook screen shots, as well as journal logs from the researchers report. The survey was instrumented to measure the user's attitudes and beliefs regarding roles and responsibilities of Facebook privacy and security. The questionnaire was administered in the Academic Computing Center of

Wissink Hall at Minnesota State University, Mankato to a broad spectrum of participants from different majors including Exercise Health, Business, Engineering, Education, and Technology. The goal was to interview approximately 150 participants who embodied a range of identity positions and who came from different communities.

A survey was distributed and collected for information in order to understand the problem and carry out the research. The questionnaire was set up via the polling software *SurveyMonkey* and a response was sought from students at Minnesota State University, Mankato's IT 101: Personal Productivity with Information Systems and IT 202: Computers in Society courses. A usability test was also conducted asking the participants to take screen shots of their Facebook privacy and security settings, and then send those images to the researchers email. The survey included open-ended questions, where responding participants could express their opinions pertaining to Facebook privacy and security.

The study allowed the investigator to determine how social networking is used in student's lives by identifying four hypotheses: Facebook users who consider security as an important factor in a social networking site are more likely to change their settings on at least a monthly basis. Users who have acknowledged identity theft is as an important privacy concern are more likely to adjust their settings on at least a yearly basis. Users of Facebook who have left their security on a default setting have fallen victim to a virus or malware attack, and users of Facebook who have their privacy set to a custom setting haven't received an attack on their profile. This study was approved by the Institutional Review Board at Minnesota State University, Mankato. IRB number 317597-1. The

consent form and survey questions as they appeared to the participants are available in the appendix.

Questionnaire

What is the importance of these factors in choosing to use a social network?
Very Important Important Neutral Somewhat Unimportant Unimportant

Privacy
Security
My Friends Use It
Ease of Use
Look and Style

What problems or attacks have you faced on social networks?

Received spam messages
Received phishing
Received virus or malware
Account hijacked or password stolen
Account used to send spam
Like-jacking attacks

Do you feel social networks need to do a better job against these attacks?

Very Important Important Neutral Somewhat Unimportant Unimportant

Received spam messages
Received phishing
Received virus or malware
Account hijacked or password stolen
Account used to send spam
Like-jacking attacks

Do you think that friends share too much online?
Yes
No
Not Sure
Other (Please Specify)

Why is privacy on social networks important to you?
(Rate on a Scale of 1 to 5, with 5 being the most important)

Protect your personal reputation	1	2	3	4	5
Protect against identity theft	1	2	3	4	5
Protect against physical harm	1	2	3	4	5
Protect your family and friends	1	2	3	4	5

Other (Please Specify)

_____

Do you adjust your security settings on Facebook?
Yes
No
Other (Please Specify)

_____

What Privacy setting is your Facebook currently set to?
Public
Friends
Custom (Explain)

_____

Do you edit your privacy and security settings on a:
Daily Basis
Weekly Basis
Monthly Basis
Yearly Basis
Not Sure
Other (Please Specify)

_____

Do you leave your security settings on default?
Yes
No
Not Sure
Other (Please Specify)

_____

Questionnaire Analysis

This section presents the findings and statistical analysis of the data from the subjects who are users of Facebook. Out of 110 participants, 100 responses were collected. Ten were found unusable because they were incomplete or corrupt. Respondents were taken from the IT 101: Personal Productivity with Information Systems and IT 202: Computers in Society courses of the Computer Information Science department at Minnesota State University, Mankato. Table 1 shows participant responses concerning important factors in choosing social networks using a five point likert scale of very important, important, neutral, somewhat unimportant, and unimportant.

Table 1 – Important Factors of Choosing a Social Network

	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant	Response Count
Privacy	50.0% (50)	35.0% (35)	12.0% (12)	12.0% (12)	0.0% (0)	100
Security	64.0% (64)	28.0% (28)	7.0% (7)	1.0% (1)	0.0% (0)	100
Friends Use It	52.0% (52)	33.0% (33)	9.0% (9)	6.0% (6)	0.0% (0)	100
Ease of Use	45.5% (45)	45.5% (45)	7.1% (7)	2.0% (2)	0.0% (0)	99
Look and Style	18.0% (18)	51.0% (51)	22.0% (22)	6.0% (6)	3.0% (3)	100

This statistic shows privacy and security are in the top three choices when deciding what social networks a student uses. Participants were allowed an additional option on the survey to express their views on the subject or adding additional facets.

Two of the responses stated: "To stay in touch with people," and "advertisements, the less the better."

Table 2 shows problems or attacks that users faced on social networks. Users were allowed to select more than one item. Additional open ended responses were; "new employers requesting access to My Face Book User name and password," "minor stalking," and "I think they used my account to send spam, but I had a post about a weight loss program that worked and I never made the status." Significant results include seventy six who claimed they received spam attacks, 21 had their account hijacked or password stolen, 34 accounts were used to send spam, and 20 had not received an attack on a social networking website.

Table 2 – Attacks on Social Networks

Problems Faced	**Percent**	**Frequency**
Received spam messages	76%	76
Received phishing	10%	10
Received virus or malware	12%	12
Account hijacked or password stolen	21%	21
Account used to send spam	34%	34
Like-jacking attacks	3%	3
Haven't received an attack	20%	20

Participants (see table 3) felt protection from attacks on Facebook was important. The table shows a user's profile getting hijacked or password stolen posed the greatest threat to their personal security on Facebook. It is also significant to point out that virus and malware, along with spam, came in a close second. Participants were then asked if they thought their friends shared too much online. Eighty eight percent said yes, 8% said no, and 4% were not sure. Two open ended responses were added saying "Some friends share [too] much, some are okay" and "I would say around 15% of my friends share too

much on Facebook." The fifth question asked if users adjusted their security settings on Facebook. Seventy nine percent said yes, 14% said no, 4% said they were not sure, and 3% chose "Other" with specified responses. Two of those responses were: "I have but I don't know what I have for settings right now so it's been a long time" and "I did originally look at the settings but have not kept up with them as often as I should."

Table 3 – Importance of Attack Protection to the User

	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant	Response Count
Received Spam Messages	58.0% (58)	34.0% (34)	6.0% (6)	1.0% (1)	1.0% (1)	100
Phishing	49.5% (49)	30.3% (30)	20.2% (20)	0.0% (0)	0.0% (0)	99
Virus or Malware	65.0% (65)	21.0% (21)	12.0% (12)	1.0% (1)	1.0% (1)	100
Hijacked Accounts and Stolen Passwords	66.7% (66)	24.2% (24)	7.1% (7)	0.0% (0)	2.0% (2)	99
Account Used to Send Spam	64.0% (64)	29.0% (29)	5.0% (5)	1.0% (1)	1.0% (1)	100
Like-jacking	57.6% (57)	26.3% (26)	14.1% (14)	0.0% (0)	2.0% (2)	99

Participants (see table 4) place identity theft privacy on a higher rating above any other Facebook setting at 53%. Reputation came in a close second with 53% of the response count. The table shows a likert scale of 1 being the lowest importance and 5 being the highest protection importance. This is in contrast with Facebook consistently pressing its users to make more personal information public (Elden, 2010), which the

company says will allow it to offer better products to users. It is significant to point out users found physical harm at 34% to be a lesser importance when it came to privacy protection. Participants also valued family and friends protection of privacy at a 42% high (5 scale) rating.

Table 4 – Importance of Privacy to Protect Against:

	1	**2**	**3**	**4**	**5**	**Rating Average**	**Response Count**
Reputation	7.0% (7)	2.0% (2)	12.0% (12)	26.0% (26)	53.0% (53)	4.16	100
Identity Theft	5.0% (5)	4.0% (4)	6.0% (6)	26.0% (26)	59.0% (59)	4.30	100
Physical Harm	14.0% (14)	15.0% (15)	24.0% (24)	13.0% (13)	34.0% (34)	3.38	100
Family/ Friends	7.0% (7)	8.0% (8)	14.0% (14)	29.0% (29)	42.0% (42)	3.91	100

Participants revealed their current privacy settings on Facebook: 19% said public, 64% said friends, 17% had the custom option. The pubic option, the most inclusive level, allows the user to publicly display all aspects of their profile to the world. These individuals usually want their profile found. The friend or friend of friends option is the second level of inclusiveness, it allows only individuals who have added the user as a friend to view their content. The custom option combines aspects of public and friends by allowing the user to individually select what content is visible on their profile. Some additional responses included: "I block most of my family from seeing most of my profile, Publicly I share profile pictures and some photo albums and my religion and

political views and birthday and month., I once changed my privacy settings to make sure only my friends can see my profile, Only Friends can view, and friends of my friends can only ask to be friends. Participants seem to favor limiting full access of their profile to close friends and family.

It seems that participants do not often edit their privacy and security settings. Only 1% said a daily basis, 2% weekly, 22% monthly, 50% yearly, and 25% had a custom or not sure response. Of those with custom settings, users said: "Always has been set to friends, Every new software or app update, They have remained the same since I got my account, Whenever I think about it, and Never, I have them on friends and they are staying that way."

Some users (15%) even admitted that they left their security settings on default, 17% were not sure, and 2% had a custom response saying: "I know I've changed some in the past but it's been a very long time' and 'For the most part unless it is a setting I don't agree with." Few users read the terms of service agreements when they are adjusted on Facebook: 19% said yes, 72% said no, and 9% were not sure or had a custom response.

Usability Task Analysis

The usability of this research focused on participants' Facebook privacy and security settings. Each individual was instructed to sit at a computer, take a screen shot of both their privacy and security settings and paste them into a Microsoft Word document later to be emailed to the researcher. The privacy settings on Facebook are divided into three selections of visibility: public, friends, and custom. Out of 113 participants who participated in the usability test portion of the analysis, 18 had public as their privacy

option, 69 chose friends, and 16 had custom settings. It is important to note that out of the 113, only 103 screen displays were included in this study due to sample size restrictions caused by the screen shots emailed to the researcher. Tables A shows the results of each screen shot analyzed.

Table A: Privacy Settings Usability Task Results

Setting	**Response Count**	**Responses Analyzed**
Public	18	103
Friends	69	103
Custom	16	103

The security settings on Facebook are divided into "enabled" and "disabled." The user is able to adjust settings if he or she wishes. The default setting on all of the security is disabled. Twenty-eight individuals had enabled secure browser settings while 73 had disabled the settings. Seven individuals had enabled login notifications while 94 left the settings disabled. Only one individual had login approval enabled while the rest had their setting disabled. No participant had a mobile application password set up, and 11 individuals had recognized devices enabled while 90 had this function disabled. Out of the 113 screen shots, only 101 screen displays were included in this study due to sample size restrictions caused by the screen shots emailed to the researcher. Table B shows the results of each screen shot analyzed.

Table B: Security Settings Usability Task Results

Setting	Enabled	Disabled	Responses Analyzed
Secure Browsing	28	73	101
Login Notifications	7	94	101
Login Approval	1	100	101
App Passwords	0	101	101
Recognized Devices	11	90	101

Hypothesis Analysis

This study investigated the four hypotheses:

- Hypothesis 1 states the more important Facebook users believe security is an important factor in choosing a social network, the more often they will change their security settings.
- Hypothesis 2 states the more important protection against ID theft is for Facebook users, the more frequently they will change their privacy settings.
- Hypothesis 3 states that users of Facebook who have left their security on a default setting are more likely to have fallen victim to a virus or malware attack.
- Hypothesis 4 states users of Facebook, who have their privacy set to a "Custom" setting, are less likely to receive an attack on their profile.

In this section I present the results of the tests of these hypotheses.

H1: The more important Facebook users believe security is an important factor in choosing a social network, the more often they will change their security settings.

Participants generally felt security was an important factor, but aren't necessarily checking up on Facebook's security settings. Ninety two percent of users felt security is at least an important factor, with 64% of those users saying it was a very important issue. But only 50% of those users updated their settings on a yearly basis, 22% favored a monthly change, and only 2% updating their settings weekly. Privacy and security settings change frequently and users are often not aware of the changes unless they monitor what is going on with privacy and security through official Facebook pages.

Facebook's privacy settings are extremely detailed. The site gives you the ability to fine-tune all privacy aspects for an account. For most users, this level of micromanagement makes Facebook's privacy settings a convoluted mess. Additionally, these settings frequently change. A user may think they know everything concerning these settings, only to be welcomed with a completely different layout and new privacy and security options the next time a user visits the settings page (Schroeder, 2011).

H2: The more important protection against ID theft is for Facebook users, the more frequently they will change their privacy settings.

Hypothesis 2 examined users who acknowledged identity theft as an important privacy concern. This hypothesizes how users are more likely to adjust their settings on at least a yearly basis. Fifty nine percent of users that rated identity theft protection as a top concern and 50% reported that they updated their settings on a yearly basis.

We notice that users aren't paying particular attention each year they update their settings. It is also significant to note that Facebook users cannot adjust settings to their recommended placement unless the user already has assigned their settings to a custom format.

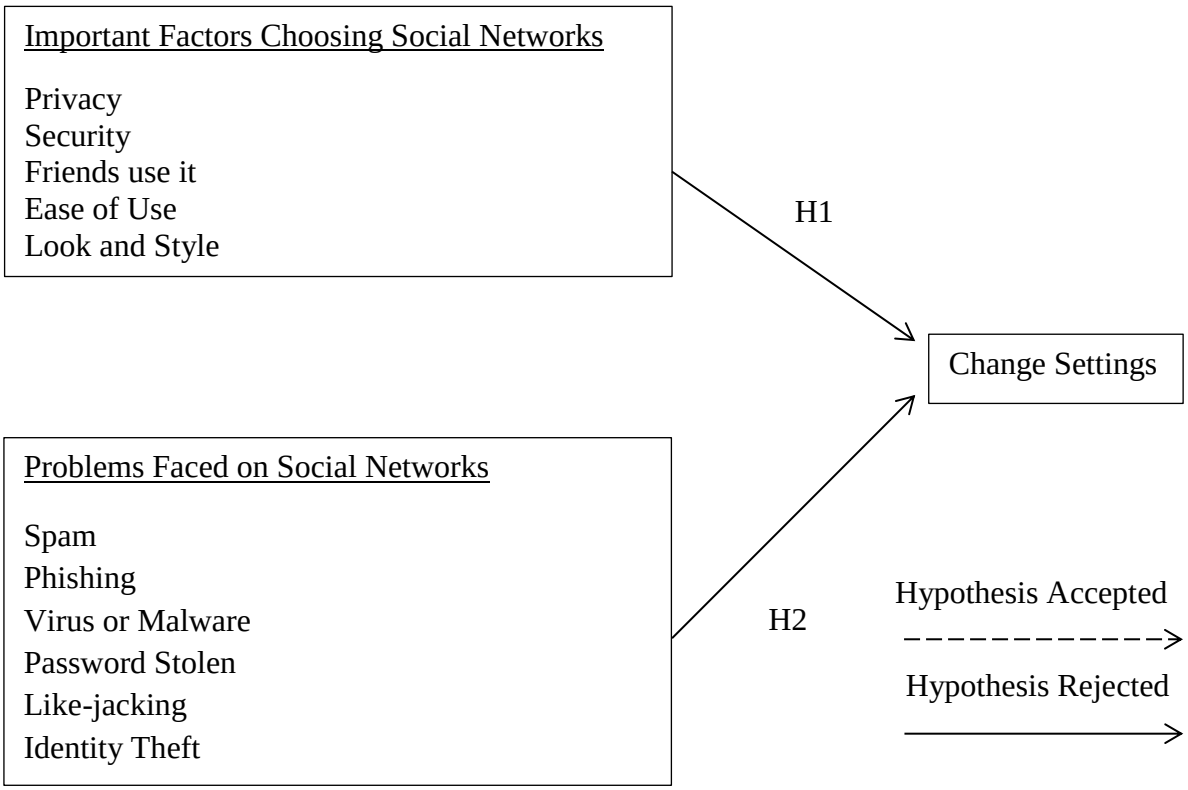
The Pearson correlation coefficient was chosen for the statistical analysis of the variables identified in hypothesis one and two. When using a correlation analysis, a measure of the relationship or association between two continuous numeric variables is used to indicate both the direction and degree to which they co-vary with one another from case to case, without implying that one is causing the other (Yount, 2006). The variable names used in this analysis are defined in Table 5.

Table 5 - Variables

Variable Name	Variable Definition
Security - Settings	The more important Facebook users believe security is an important factor in choosing a social network, the more often they will change their security settings.
Theft - Settings	The more important protection against ID theft is for Facebook users, the more frequently they will change their privacy settings.

The summary of hypothesis one and two used in this analysis are defined in Table 6. For two of the questions correlated together we look to find the relationships between choosing a social network, and the problems faced from them. The figure also shows the second portion of the research model and whether the hypotheses were rejected or accepted.

Table 6 – Summary of Hypotheses One and Two



The correlation analysis showed the factors related to the frequency a user might change their Facebook security or privacy settings.

Table 7 – Summary of Correlation Analysis

Hypotheses	**Variable**	**Correlation Coefficient**	**Level of Significance**	**Result**
H1	Security - Settings	0.15	.0000	Reject
H2	Theft - Settings	0.03	.0000	Reject

The significance of the Pearson correlation coefficients was determined by using t-tests. T-value is the observed value of the t-statistic used to test the hypothesis that two attributes are correlated (IBM, 2009). The t-value can range between -infinity and +infinity. A t-value near 0 is evidence for the null hypothesis that there is no correlation

between the attributes. A t-value far from 0, either one negative or positive, is evidence for the alternative hypothesis when there is correlation between the two attributes (IBM, 2009).

With the first hypothesis, security importance was not found to be negatively correlated with changing security settings by its correlation coefficient of .15 and t-test value of .0000. Thus, hypothesis H1 was rejected. Reasons for this could be that users don't look at their settings enough to fully comprehend the constant changes going on. They also may not be as concerned with security settings, but rather focus on the amount of privacy other users can see from there profiles. In the second hypothesis, identity theft was also significantly negatively correlated with changing security settings by its correlation coefficient of 0.03 and t-test value of .0000. Thus, hypothesis H2 was rejected. The reason for this may be that users may not have received these types of attacks on their profiles, or they could have witnessed these issues from other users and found ways to prevent these attacks.

H3: Users of Facebook who have left their security on a default setting are more likely to have fallen victim to a virus or malware attack.

To examine hypothesis 3, users of Facebook who have left their security on a default setting were looked at to see if they have fallen victim to a virus or malware attack. From the questionnaire, 66% of users stated they do not leave their settings on default, 15% saying they do, and 2% were unsure. Additionally, the usability test found that only 28 users had enabled the secure browsing feature, significant to cyber-security attacks. Only one user had login approvals enabled, and none of the users had mobile

application security enabled, or a password set. The default settings on all of these features were not enabled.

The recommended settings Facebook provides may not always be the best choice (Burnham, 2010). While the goal of Facebook's privacy settings is to be simple and easy to understand, it does keep the option to individually tweak each setting. "If you use Facebook both professionally and personally and if you use it frequently and post often this is when you really want to take the time to create friend lists and tweak your settings based on groups of acquaintances and their respective levels of sharing" (Burnham, 2010).

Many Facebook apps gather data from users' friends. This means even if a user doesn't use a particular app it could have access to your data just by way of one of your friends who is using it. The United States online privacy laws are generally weaker than those in other places (DesMarais, 2012).

H4: Users of Facebook, who have their privacy set to a "Custom" setting, are less likely to receive an attack on their profile.

For the final hypothesis, users of Facebook who have their privacy set to a custom setting were examined to determine if they have received an attack on their profile. In the survey only 17% claimed they adjusted their profile to a custom setting; while 64% opted for the pre-configured "friends" tab; and 19% chose the "public" setting.

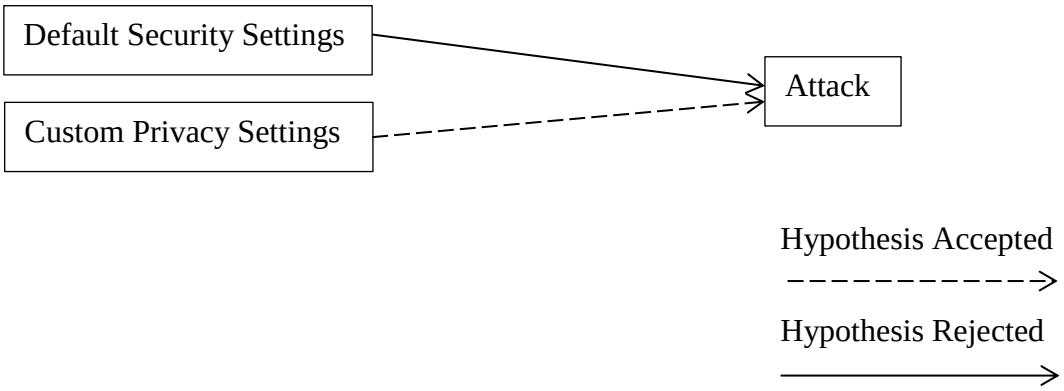
It comes down to whether users are configuring their privacy controls correctly. Nearly 13 million users have never set or don't know about the social networking privacy

tools. More than a quarter of users have shared their wall posts with an audience broader than their friends (DesMarais, 2012).

It turns out that the first thing a user sees when they browse the settings page on Facebook are their current settings. It is the easiest way a user can control who sees certain material. If a user selects "Everyone," then everyone gets to see all these items, and if a user selects "Friends only," then only friends can see them. But if a user selects "Friends of Friends," only some items such as your status, relationships, and photos a user has been tagged in are visible to friends of friends (McCracken, 2010).

The Pearson correlation coefficient was chosen for the statistical analysis of the variables in hypothesis three and four. Chi-square is a statistical test commonly used to compare observed data with expected data to obtain in accordance with a specific hypothesis. The chi-square test is continually analyzing the null hypothesis, stating that there is no significant difference between the expected and observed result (McLaughlin, 1996).

Table 8 – Summary of Hypothesis Three and Four



The chi-squared analysis was used to test hypothesis three and four, along with their subcategories designed to identify the related effected to Facebook security and

privacy adjustments. A variable definition allowed the researcher to hypothesize a raw statistic of the data in support of hypothesis three and four. The variable names used in this analysis are defined in Table 9.

Variable Name	Variable Definition
Adjust - Attacks	Hypothesis 3A: Facebook users that adjust their security settings receive attacks 5% of the time
Not Adjust - Attacks	Hypothesis 3B: Facebook users that do not change their default security settings receive privacy attacks 40% of the time
Custom - Attacks	Hypothesis 4A: Facebook users that utilize custom privacy settings receive privacy attacks 5% of the time
Not Custom-Attacks	Hypothesis 4B: Facebook users that do not change their default privacy settings receive privacy attacks 40% of the time

The procedure used to test the significance of contingency tables is similar to all other hypothesis tests. That is, a statistic is computed and then compared to a model of what the world would look like if the experiment was repeated an infinite number of times when there were no effects (Stockburger, 1998). This procedure is shown in Tables 9 and 10 for the hypothesis three and four. For Table 9 in the first column "Security Adjusted", a 1 signifies that yes, the user has left their security settings on default. A 2 signifies no, the user has changed their settings. Additionally in the second column "User Attacked," a 1 signifies the user has been a victim of an attack and 2 signifies no, the user has not received an attack. The percentages come from the chi-test formula used on excel.

Table 9 – H3 Significance of Contingency

Security Adjusted	User Attacked	Observed Frequency	Expected Distribution	Percentages
1	1	70	71.25	0.05
1	2	5	3.75	0.05
2	1	5	12.5	0.5
2	2	20	12.5	0.5

1: Yes 2: No

For Table 10 in the first column "Privacy Adjusted", a 1 signifies that yes, the user has left their privacy settings on default. A 2 signifies no, the user has changed their privacy setting. In the second column "User Not Attacked," a 1 signifies the user has not fallen victim of an attack and 2 signifies yes, the user has had their privacy violated on the site.

Table 10 – H4 Significance of Contingency

Privacy Adjusted	User Not Attacked	Observed Frequency	Expected Distribution	Percentages
1	1	13	18.05	0.05
1	2	6	0.95	0.05
2	1	7	40.5	0.5
2	2	74	40.5	0.5

1: Yes 2: No

The chi-squared analysis showed the factors related to the frequency a user might receive a malicious attack based on the adjustments they make to their security or privacy settings. We examine the subsets of each hypothesis whether adjustments to a user's security settings leads to an attack versus not adjusting ones setting. We then examine the

effects of the customization option Facebook gives its users and whether taking the time to customize ones settings leads to an attack or in fact prevents an attack.

Table 11 – Summary of Chi-Squared Analysis

Hypotheses	**Variable**	**Chi-Test**	**Alpha**	**Result**
H3 - A	Adjust - Attacks	0.5	.05	Reject
H3 – B	Not Adjust - Attacks	0.002	.05	Reject
H4 - A	Custom – Attacks	1.06	.05	Accept
H4 - B	Not Custom-Attacks	9.73	.05	Accept

Hypothesis H3-A, "Facebook users that adjust their security settings receive attacks 5% or less of the time," was rejected due to the direction of the hypothesized relationship. From exploratory research, users who adjust their setting more often tend to be more aware of what is going on in their social networks and are far less likely to fall victim of an attack. It was rejected because the Chi-test was not significant. Even those users who adjust their Facebook settings are receiving attacks more frequently than 5% of the time.

Hypothesis H3-B, "Facebook users that do not change their default security settings receive privacy attacks at least 40% of the time," was also rejected because the Chi-test was not significant. Those users that do not adjust their security settings, self-reported security attacks less than the hypothesized 40% frequency rate.

Hypothesis H4-A, "Facebook users that utilize custom privacy settings receive privacy attacks 5% or less of the time," was accepted. Privacy and Security intrusions happen in different ways, privacy is far easier to compromise whether a picture is stolen or an email address is used for advertising. When a user utilizes the custom option Facebook offers, does it maximize their privacy and are they are less likely to fall victim to an attack?

Hypothesis H4-B, "Facebook users that do not change their default privacy settings receive privacy attacks at least 40% of the time," was accepted. This overwhelming statistic leads to more questions, alongside exploratory research presented in the hypothesis analysis, that Facebook users may not be configuring their privacy controls correctly. There are numerous ID fraud pursuers targeting Facebook and other social networking sites to harvest information about them. Facebook provides exceptional ways for its users to protect themselves online. It depends on the user to adjust their settings accordingly.

Concluding Thoughts

This study conducted an empirical evaluation of security and privacy settings in Facebook looking in-depth at how users are assigning their settings, asking if users are keeping their profile secure. The survey gathered data on questions such as: Do Facebook users consider security an important factor? Do users adjust their privacy and security settings? Are users of Facebook falling victim to a virus or malware attack? Are users who custom set there settings more secure?

The findings of these questions lead me to believe users are genuinely concerned about their privacy and security on Facebook, however users are having trouble following the constant changes Facebook is making to their layout and settings. With all these changes it is hard for a user to keep track of all the adjustments happening to a user's profile, keeping track of a profiles changes can benefit in the long run by having less exposure to virus, spam, and malware being linked on Facebook's news feeds. Eighty percent of our 100 responses claimed they have received an attack on Facebook while fifty percent of those users only adjust their security settings on a yearly basis. Additionally, 72% of users claimed they did not read the terms of service when they are adjusted. This study recommends that privacy and security settings be checked on at least a monthly basis if not on a two week rotation. This allows the user to be up to date on the latest adjustments keeping them less prone to an attack. Facebook constantly tweaks its settings and due to the massive amount of users, Facebook can reset a user's adjusted preferences to the default settings (Bosker, 2011).

However, other studies have christened Facebook's privacy and security settings fundamentally flawed. With over 900 million users and 30 billion items such as web links and blogs, when Facebook adds new features and tweaks settings it's expected there will be confusion. Effective privacy and security tools should be formed from how individuals use social networking sites and enable users to adjust what they share based on the information a post contains, rather than according to the type of data it represents (Bosker, 2011).

Facebook also shares personal information by default while marketing algorithms are discovering what their users look like, using this information without the user's

approval. Most Facebook users avoid setting their privacy options safely, finding the whole system confusing. It's even difficult to keep control when Facebook changes the user's settings without consent (Cluley, 2011). Using the "Custom" setting whenever possible is a smart option. This allows the user to set whatever preferences they choose, rather than a preconfigured setting.

Facebook users should always look into their security and privacy settings thoroughly and not assume that Facebook has its best interests for the user. Even though three of these studies hypotheses were rejected, users should not assume that leaving your settings unchanged will result in better protection. The average user doesn't understand the important of cyber security. Only when they have fallen victim to an attack will they pay close attention to their settings. It is important to note Facebook is now public. Everyday businesses are looking into Facebook as a haven to advertise their products and study the users' interaction on the site. It is vital to read through and research what these privacy and security setting do, and what information is accessible to the public.

Limitations and Recommendations for Future Research

For future researchers using this study as a tool, a larger and more diverse selection of participants would be beneficial. There were numerous occasions during the usability test where individuals would raise their hand and ask the researcher inquiries such as "where are the privacy and security settings located?" This is significant to note, however, as it is leading to the question: Do users truly understand these settings and the threats they face from not configuring them correctly?

Although the correlation and chi-squared analysis conducted in this research is a good starting point, more in-depth analysis could provide additional insights into the relationship between how users adjust their privacy and security settings and the related perceived effects this has on phishing scams and virus attacks. The hypotheses themselves were worded in a way to prove users were not adjusting their settings accurately. Reasoning behind why they were rejected could be that Facebook users are savvier at not clicking suspicious links directing the users to malware and other virus infected webpages. Future research should seek to correlate the effects of privacy and security settings, on the frequency and severity of attacks.

Appendix

Appendix A: IRB Application

Application for the Conduct of Research Involving Human Subjects

University policy requires that all research involving human subjects be reviewed by the Institutional Review Board (IRB). In completing the application, be aware that the persons reviewing it may be unfamiliar with the field of study involved. Present the request in typewritten form and in non-technical terms. Incomplete proposals will be returned without review. **Data collection may not begin until written approval is received from the IRB**.

After you complete this form, please upload and submit it on IRBNet.

I. General Information

a. Principal Investigator (PI) Any research under the auspices of Minnesota State University, Mankato must have an MSU faculty member or MSU professional employee designated as the responsible person.

PI Name: Michael Wells

Department: Computer Information Science

Campus mail address: WH273

Phone number: 507-389-6659

E-mail address: Michael.wells@mnsu.edu

b. Co- Principal Investigator (PI)

PI Name:

Department:

Campus mail address:

Phone number:

E-mail address:

c. Sub-Principal Investigator(s) Person(s) who will be collaborating with the primary investigator conducting the research (for example, collaborating faculty, MSU employees, or graduate students completing capstone projects/research). If

there is more than one is SI, provide the information listed below for each SI. You can do this by copying and pasting the requested information

SI Name: Brandon Hoffmann

Department: Information Technology

Mailing address: 1400 Warren Street Apt #H26

Phone number: 402-750-9353

E-mail address: Brandon.hoffmann@mnsu.edu

c. Project Title:

Online Security of Facebook

d. Proposed dates during which data will be collected (indicate the anticipated timeframe during which data will be collected from human participants)

From (3-27-2012): to (4-27-2012)

e. Location of data collection*

ACC 125A

f. Source of funding

[x] no outside funding has been obtained to support this research

g. Previous human subjects approval:

Has this proposal been submitted to another human subjects committee?
[ ] yes [x] no

Has this proposal been approved by another human subjects committee?
[ ] yes [x] no

If the answer to either of the previous questions is yes, list the name of the agency/university:

II. General Purpose of the Research Project

We are performing this research for my thesis in the Master of Science in Information Technology program to test the privacy and security practices of users, to perform my defense and provide feedback of my research to improve the overall effectiveness of save social networking practices. We are going to observe test subjects using the website and conduct a brief survey after. This information will be used to prepare a thesis. We will be observing how each user uses there security settings on the website and how they react to the website layout. The timeline is to complete the testing approximately a month. We will use observation, note taking, questioning, and a brief questionnaire. A copy of the questionnaire has been included. There will be no observation forms, just note taking detailing the participants' movements throughout the website.

The intent of the study will be verbally explained. They can assume the risks after learning the intent. At this point they will be asked to sign the consent form. Since the risks are less than minimal, we anticipate that no participants will have a problem with this. The consent forms will be locked in a file cabinet in the PI's office at Minnesota State University, Mankato for 3 years. All names will be removed from gathered information.

III. Description of Participants, Sampling, and Recruitment Procedures

a. **Anticipated ages of participants** (check all groups that are likely to participate)

[ ] 0-17 year olds (minors) **[x]** 18-64 year olds **[ ]** 65+ year olds

b. **Anticipated number of participants** (check one)

[ ] 1-10 **[ ]** 11-25 **[ ]** 26-50 **[ ]** 51-100 **[X]** 101-200 **[ ]** 200+

c. **Describe briefly the demographic characteristics of the participants**
The study will not purposefully recruit members of a vulnerable population. The intent of the study will be verbally explained. They can assume the risks after learning the intent. At this point they will be asked to sign the consent form. Since the risks are less than minimal, we anticipate that no participants will have a problem with this.

d. Describe how people will be recruited to participate in the study
Participants will be chosen from the IT101 course. The following will be read to the participants to the IT101 course by the survey facilitator: "If you would like to

receive a small amount of extra credit for this class (IT101), you can voluntarily go to the ACC at one of the specified times and participate in a usability study. This activity is NOT required and there are no other benefits to you and no sensitive information will be collected."

IV. Project Description

a. **In a paragraph, broadly describe the methodological design used to gather data**
The methodology design will be used through a questionnaire/survey.

b. More specifically, explain the study procedures in a detailed, chronological sequence by documenting the steps that occur after you have recruited people to participate. Including:
Study Procedure:

1. Sit subject down at the computer
2. Give brief instruction
3. Give them a task list
4. Observe them
6. Give them a short questionnaire
7. Dismiss

Discuss the potential risks participants may encounter by participating, and address how you will insure these risks are managed and minimized.

The risks will be less than minimal. We will ensure that the participant is comfortable doing every task; they may choose to stop the survey at any point. All names will be removed from gathered information.

Describe potential benefits for participating in the research

The benefits include learning more about human computer interaction and the design processes web developers take when designing a website.

Describe any compensation to the participants.

No compensation will be given.

V. Protection of Participants' Rights

a. Have you attached the necessary consent form(s) required for use to conduct the proposed study?
[x] yes **[ ]** no

When working with minors, or adults who are not able to read and complete a consent form of their own volition, it is required that you also prepare and use an assent form. Is an assent form necessary in this proposed study?
[x] yes **[ ]** no

b. We are going to observe test subjects using there Facebook accounts and conduct a brief survey after. We will use this information to prepare the final capstone thesis requirement for graduate students. We will be observing how each user navigates the website and how they react to the website layout. The timeline is to complete the testing approximately a month.

c. The intent of the study will be verbally explained. They can assume the risks after learning the intent. At this point they will be asked to sign the consent form. Since the risks are less than minimal, we anticipate that no participants will have a problem with this.

d. The consent forms will be locked in a file cabinet in the PI's office at Minnesota State University, Mankato for 3 years.

e. All names will be removed from gathered information.

VI. Signatures

By electronically signing the IRBNet proposal, I agree to the following:

"In making this application, I certify that I have read and understand the Policies and Procedures for Projects that Involve Human Subjects, and that I intend to comply with the letter and spirit of the University Policy. Changes in the protocol will be submitted to the IRB for approval prior to these changes being put into practice. Informed consent/assent records of the participants will be kept by the Principal Investigator in a secure location at Minnesota State University, Mankato for at least three years after the completion of the research."

A member of the Minnesota State Colleges & Universities System. MSU is an Affirmative Action/Equal Opportunity University. This document is available in alternative format to individuals with disabilities by calling the College of Graduate Studies and Research at 507-389-2321 (V), 800- 627-3529 or 711 (MRS/TTY).

Attachments

Attach copies of the following, if applicable:

1. Permission from other participating institutions
2. Cover letters, recruitment scripts, flyers or other information that will be given to participant prior to participation in the study
3. Consent forms and permission forms for parents or guardians
4. Assent forms to be used by children or when subjects are unable to give legal consent
5. Questionnaires, surveys, interview scripts
6. Any other relevant or supporting documentation

Appendix B: Usability Test Consent Form

Usability Test Consent Form

Please read and sign this form.

In this usability research:

- You will be asked to perform certain tasks on a website.
- You will be asked to fill in a questionnaire.

Participation in this usability research is voluntary. All information will remain strictly confidential. The descriptions and findings may be used to help improve the web site. However, at no time will your name or any other identification be used. You can withdraw your consent to the experiment and stop participation at any time. The risk is less than minimal for the tasks we will be asking you to perform. You may choose not to partake in this survey at any time. The survey will last approximately ten (10) to fifteen (15) minutes. Your decision whether or not to participate will not prejudice your future relations with Minnesota State University, Mankato. A copy of the consent is available for the participant.

For questions about the treatment of human subjects, please contact Dr. Barry Ries at 507-389-2321. If you have any questions after today, please contact Michael Wells at 507-389-6659.

I am at least 18 years old. I have read and understood the information on this form and had all of my questions answered.

Brandon Hoffmann

_____ _____

Subject's Signature Date

_____ _____

Usability Consultant Date

Appendix C: Usability Testing Script

FACILITATOR: Hello, my name is Brandon Hoffmann and I will be walking you through this usability testing session. Just to clarify, you have come in today to participate in testing the privacy and security features of the website Facebook to see what settings you have adjusted. I want you to understand that the purpose is to test the website, not you. If you are unable to complete one of these tasks, do not feel as though you are not contributing. These results will help me with the study and the information I need to support my thesis defense. I will be observing how you navigate the site to take screen shots of the privacy and security settings. If you have questions, feel free to ask. Your information and responses will be kept confidential.

I will now ask you to perform a series of tasks. For any tasks that require information I will provide you with the data. You will not be required to use your own information for any of these tasks unless you choose to. If you are unable to reach your goal or complete a task it is acceptable to give up on the task.

1. Log into your Facebook account
2. Go to your security settings and take a screenshot
3. Go to your privacy settings and take a screenshot

Now that we have gone through these tasks we will ask you to perform one more task. Please fill out this short online questionnaire that reflects your experience with privacy and security of Facebook. Survey will be in another browser via SurveyMonkey.com.

Thank you for coming in today and helping me with my project. I appreciate your contributions.

Appendix D: Survey Monkey Questionnaire

*** 1. What is the importance of these factors in choosing to use a social network?**

	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant
Privacy	○	○	○	○	○
Security	○	○	○	○	○
My Friends Use It	○	○	○	○	○
Ease of Use	○	○	○	○	○
Look and Style	○	○	○	○	○

Other (please specify)

*** 2. What problems or attacks have you faced on social networks?**

- ☐ Received spam messages
- ☐ Received phishing
- ☐ Received virus or malware
- ☐ Account hijacked or password stolen
- ☐ Account used to send spam
- ☐ Like-jacking attacks
- ☐ Haven't received an attack

Other (please specify)

*** 3. Do you feel social networks need to do a better job against these attacks?**

	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant
Received spam messages	○	○	○	○	○
Received phishing	○	○	○	○	○
Received virus or malware	○	○	○	○	○
Account hijacked or password stolen	○	○	○	○	○
Account used to send spam	○	○	○	○	○
Like-jacking attacks	○	○	○	○	○

Other (please specify)

*** 4. Do you think that friends share too much online?**

- ○ Yes
- ○ No
- ○ Not Sure

Other (please specify)

*** 5. Do you adjust your security settings on Facebook?**

- ○ Yes
- ○ No
- ○ Not Sure
- ○ Other (please specify)

*** 6. Why is privacy on social networks important to you? (On a scale of 1-5 with 5 being the most important)**

	1	2	3	4	5
Protect your personal reputation	○	○	○	○	○
Protect against identity theft	○	○	○	○	○
Protect against physical harm	○	○	○	○	○
Protect your family and friends	○	○	○	○	○

Other (please specify)

Q7 Edit Question ▼ Add Question Logic Move Delete

*** 7. What Privacy setting is your Facebook currently set to?**

- ○ Public
- ○ Friends
- ○ Custom (please specify)

*** 8. Do you edit your privacy and security settings on a:**

- ○ Daily Basis
- ○ Weekly Basis
- ○ Monthly Basis
- ○ Yearly Basis
- ○ Not Sure

Other (please specify)

*** 9. Do you leave your security settings on default?**

- ○ Yes
- ○ No
- ○ Not Sure
- ○ Other (please specify)

*** 10. Do you read the Terms of Service (TOS) agreements when they are adjusted on Facebook?**

- ○ Yes
- ○ No
- ○ Not sure

Other (please specify)

References

Acquisti, Alessandro, and Gross, Ralph. (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook***.** June 28-30. Retrieved from http://petworkshop.org/2006/preproc/preproc_03.pdf

Barnes, S. (Aug. 15, 2006). *A Privacy Paradox: Social Networking in the United States*. First Monday: Peer-Reviewed Journal on the Net, Retrieved from http://firstmonday.org/issues/issue11_9/barnes/index.html.

Black, Edward. (October 5, 2012) *Celebrating Facebook's 1 Billion Users and Our Commitment to Internet Freedom* Retrieved from http://www.huffingtonpost.com/edward-j-black/celebrating-facebooks-1 b_b_1942629.html

Bosker, Bianca. (June 6, 2011) *Facebook- Focused Study Finds Existing Privacy Settings 'Fundamentally Flawed.'* Retrieved from http://www.huffingtonpost.com /2011/04/13/online-privacy-settings-study_n_848771.html

Bradley, Tony. (2012). *False Sense of Security: Home Users Need Basic Security Knowledge.* Retrieved from http://netsecurity.about.com/od/ newsandeditorial1/a/falsesense_3.htm

Bugeja, M. J. (January 24, 2006). *Facing the Facebook*. Chronicle of Higher Education. Retrieved from http://chronicle.com/article/Facing-the-Facebook/46904

Burnham, Kristen. (February 23, 2011). *Facebook Privacy: 10 Must-Know Security Settings*. PCWorld. Retrieved from http://www.pcworld.com/article/220444/ facebook_privacy_10_mustknow_security_settings.html

Burnham, Kristen. (December 8, 2011). *Facebook Security Tips to Stay Safe in 2012.* CIO. Retrieved from http://www.cio.com/article/696212/4_Facebook_Security_ Tips_to_Stay_Safe_in_2012_

Burnham, Kristen. (June, 3, 2010). *Facebook Privacy Settings: Recommended vs Custom.* CIO. Retrieved from http://www.cio.com/article/595854/Facebook_Privacy_ Settings_Recommended_vs._Custom?page=2&taxonomyId=3169

Debatin, Bernhard., Jennette P. Lovejoy., Horn, Ann-Kathrin., and Hughes, Brittany N. (November 17, 2009). *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2009.01494.x/full

DesMarais, Christina. (May 6, 2012). *Facebook Users Share and 'Like' Too Much, Report Says.* Retrieved from http://www.pcworld.com/article/255100/facebook_users_share_and_like_too_much_report_says.html

Consumer Reports Magazine. (June, 2012). *Facebook and your privacy.* Retrieved from http://www.consumerreports.org/cro/magazine/2012/06/facebook-your privacy/index.htm

Donald, Ben. (November 18, 2009). *A Social Networking Phenomenon.* Retrieved from http://www.academicperspective.com/2009/11/18/a-social-networking phenomenon/

eBizMBA Inc. (January, 2012). *Top 15 Most Popular Social Networking Sites*. Retrieved from http://www.ebizmba.com/articles/social-networking-websites

Elden, Eric. (May 11, 2010). *Analysis: Some Facebook Privacy Issues Are Real, Some Are Not.* Retrieved from http://www.insidefacebook.com/2010/05/11/analysis some-facebook privacy-issues-are-real-some-are-not/

Estinson, Daniell. (March 2011). *Final Project Research [On Social Media]*. Retrieved from http://daniteachtech.wordpress.com/category/eci831/

ENISA - European Network and Information Security Agency. (November, 2011). *About Us*. Retrieved from http://www.enisa.europa.eu/about-enisa

Exforsys Inc. (February 14, 2010). *Social Networking Overview.* Retrieved from http://www.exforsys.com/career-center/social-networking/social-networking-overview.html

Facebook. (June 8, 2012). *Statement of Rights and Responsibilities*. Retrieved from https://www.facebook.com/legal/terms

Facebook Stats. (October 6, 2011) Retrieved from http://gold.insidenetwork.com/facebook/facebook-stats/.

Federal Trade Commission. (April 24, 2009). *Social Networking Sites: Safety Tips for Tweens and Teens.* Retrieved from http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

Hoffmann, Brandon. (May 8, 2011). *An Exploratory Study of Social Networking Propensity and its Related Perceived Effects*. Wayne State College, Wayne, Nebraska.

Horne, David. (November 23, 2010). *The Overnight 25 Year Social Networking Phenomenon*. Retrieved from http://andynathan.net/2010/10/the-overnight-25 year-social-networking-phenomenon/

Hughes, Cheryl. (February 8, 2011). *Social Networking: A Brief Overview.* Retrieved from http://socialnetworkingindustry.com/social-networking/social-networking-a brief-overview.html

Hunter, Jessica. (May, 2011). *Facebook Identity Theft -- Can We Relax Yet?* Retrieved from http://www.identitytheftfixes.com/facebook_and_identity_theft_-- _can_we_relax_yet.html

IBM. (April 30, 2009). *Data Warehouse Center Administration Guide.* Retrieved from http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp?topic=/ com.ibm.db2.udb.doc/admin/c0006909.htm

Krug, Megan. (November 25, 2009). *Negatives of Social Networking.* Retrieved from http://www.effinity.us/index.php/blog/2009-11-25-10-00-28.html

Ostrow, Adam. (July, 28, 2009). *Number of Social Networking Users Has Doubled Since 2007.* Retrieved from http://mashable.com/2009/07/28/social networking-users-us/

Pelgrin, William. (March, 2010). *Security and Privacy on Social Networking Sites.* Retrieved from: http://msisac.cisecurity.org/newsletters/2010-03.cfm

Pelling, Emma L., Sc., B.Behav., White, Katherine. Ph.D. (Number 6, 2009). *The Theory of Planned Behavior Applied to Young People's Use of Social Networking Web Sites* Retrieved from DOI: 10.1089=cpb.2009.0109

McLaughlin, Jacqueline, Ph.D. (1996). *Chi-Squared Test.* Retrieved from http://www2.lv.psu.edu/jxm57/irp/bio-110.html

ProCon. (January 5, 2012). *Are Social Networking Sites Good For Our Society?* Retrieved from http://socialnetworking.procon.org/

Protalinski, Emil. (February, 9, 2012). *Facebook admits it needs to fight scams more efficiently.* Retrieved from http://www.zdnet.com/blog/facebook/facebook-admits it-needs-to-fight-scams-more-efficiently/8980

Purewal, Sarah. (May, 21, 2012). *10 Ways Facebook Will Rule Our Lives.* Retrieved from http://www.pcworld.com/article/255876/10_ways_facebook_will_rule_our_lives html

Raacke, John, Ph.D., and Bonds-Raacke, Jennifer, Ph.D. (November 2, 2008). *MySpace and Facebook: Applying the Uses and Gratifications Theory to Exploring Friend-Networking Sites.* Retrieved from DOI: 10.1089/cpb.2007.0056

Schroeder, Stan. (February 7, 2011). *Facebook Privacy: 10 Settings Every User Needs to Know*. Mashable Social Media. Retrieved from http://mashable.com/2011/02/07/facebook-privacy-guide/

Shaw, Gilligan. (November 7, 2011). *Facebook fails to stop bots accessing personal information: B.C. study*. The Gazette. Retrieved from http://www.canada.com/technology/Facebook+fails+stop+bots+accessing+personal+information+study/5668487/story.html

Sjogreen, Carl. (January 18, 2012). *The Facebook Blog*. Retrieved from https://blog.facebook.com/

Stockburger, David. (February 19, 1998). *Chi-Square and Test of Contingency Tables.* Retrieved from http://www.psychstat.missouristate.edu/introbook/sbk28m.htm

Tahseen, Ismat. (November 4, 2011). *Facebook's setting changes confuse users: Study.* The Times of India. Retrieved from http://articles.timesofindia.indiatimes.com/2011-11 04/social media/30358941_1_facebook-users-people-more-control

Timm, Dianne T., and Duven, Carolyn J., (January, 2008). *Privacy and Social Networking Sites.* Retrieved from http://ryanpstone.com/yahoo_site_admin /assets/docs/socialnetwork1.250104344.df

Wang, Edward. (April 9, 2009). *Social Network Security: A Brief Overview of Risks and Solutions.* Retrieved from: http://www.cs.wustl.edu/~jain/cse571-09/ftp/social.pdf

Wilson, Kathryn., Fornasier, Stephanie., and White, Katherine, Ph.D. (Number 2, 2010) *Predictors of Young Adults' Use of Social Networking Sites*. Retrieved from DOI: 10.1089=cyber.2009.0094

WiseGeek. (June, 2012). *What is a Social Networking Site?* Retrieved from http://www.wisegeek.com/what-is-a-social-networking-site.htm

Yount, Rick. (2006). *Correlation Coefficients.* Retrieved from http://www.napce.org/documents/research-design-yount/22_correlation_4th.pdf