Cybercrime: The Unintentional Effects of Oversharing Information on Facebook

Karen Paullet
paullet@rmu.edu

Jamie Pinchot
Pinchot@rmu.edu

Robert Morris University
Moon Township, PA 15108

Abstract

Sharing information on social network sites could potentially expose users to becoming victims of a cyber-related crime. This exploratory study of 146 undergraduate and graduate students examines the oversharing of information on Facebook and the possible consequences associated with this action. Research has found that students are concerned about sharing information and show concern about the effects of sharing information on Facebook. The results of the study reveal that students are worried about criminal activity such as identity theft, unauthorized access to online banking accounts, cyberstalking, cyberbullying, and child predators. Can information that is being shared on Facebook contribute to cybercrime? Should people think twice before posting personal information online?

Keywords: cybercrime, Facebook, oversharing information

1. INTRODUCTION

Social networking sites started out as a way for people to connect with family and friends. Today, they are used for everything from advertising to playing games. Aside from the positive attributes of social networking, there is a negative side that must be recognized. Social networking sites such as Facebook have become a way for cybercriminals to target victims. One of the most frightening parts of this is that cybercriminals gather information needed to target someone directly from the victim, who has often unwittingly provided the needed information in photos, status updates, and interests on their social network pages.

As more people begin to use social networking sites they are becoming more vulnerable to cyber-criminals. As people post personal data the distribution of this information might not be in their control. Cyber-criminals can easily search for a victim without ever leaving their house. Many users of social network sites are not aware of the possible pitfalls of failing to secure their personally identifiable information by using the privacy settings of the site. A failure to properly secure their profile information can lead to disaster. It is imperative that members of social networking sites understand the possible implications of the information that can be obtained from their profiles.

2. RELATED LITERATURE

Lampe, Ellison & Steinfield (2006) conducted a study of 1,440 first-year students at Michigan State University regarding attitudes about their Facebook profiles, and how they use Facebook

to browse or search for people. The authors defined "social searching" as using Facebook to find out more about people the respondents had met offline, such as old friends from high school, someone who lives in their dorm, classmates, and others they met socially. Social browsing was defined as looking for someone online to have an encounter with offline. This could include finding people to date, finding casual sex partners, or setting up face-to-face encounters with someone that they learned about through Facebook. Results of the study found that the majority of participants were using Facebook for social searching and were likely to use Facebook for social browsing.

Consumer Reports 2011 State of the Net study revealed that more than 5 million online households experienced some type of abuse on Facebook in the past year to include identity theft, cyberbullying, unauthorized online account access, and being harassed or threatened. This projection is up more than 30% from the previous year in 2010. Fifteen percent of participants have posted travel plans and their current location, 34% posted their full date of birth and 21% have posted photos of their children. Additionally, 23% of Facebook users admitted that they did not know some of the people that they accepted as friends (Consumer Reports, 2012).

According to Gross and Acquisti (2006), privacy implications associated with online social networking depend on the level of identifiable information that a person provides and the possible effects of its uses. Facial recognition software used to scan pictures posted on an individual's site can provide enough information to identify the profile owner's sites where the same or similar pictures have been posted (Lui & Maes, 2005). A direct link to other online accounts can then be formed.

Lampe, Ellison & Steinfield (2006) believe that online social networking sites may also foster a group surveillance function, allowing users to "track the actions, beliefs and interests of the larger groups to which they belong" (p.167) and "search for social cues that indicate group norms" (p.167). This surveillance function may serve as a subconscious mechanism for users to double-check their actions and self-projections to ensure that they are "fitting in" as a member of their social group.

Debatin, Lovejoy, Horn & Hughes (2009) conducted a survey of 119 college undergraduates to study Facebook information-sharing activities and privacy practices. Nearly 18% of the respondents reported that they had personally been a victim of cyberstalking or harassment, damaging gossip, or theft of data. Ninety-one percent claimed that they were familiar with Facebook privacy settings, but only 69% of participants had ever changed the default privacy settings on their account. Approximately 50% reported that they had set their privacy settings to "Friends Only." However, 10% of respondents claimed that they accept "anybody" as a friend, and 37% reported that they will accept someone "heard of through others" as a friend. This indicates that almost half of the respondents were willing to befriend strangers. The study found that even though participants claimed to understand Facebook privacy settings, their habits indicate that they have accepted large groups of friends, in some cases including people they have never met personally, and that they share high quantities of detailed personal information. The authors concluded that the gratifications of using Facebook outweighed the perceived threats to privacy for the respondents in their study.

A Carnegie Mellon University (CMU) study conducted by Gross and Acquisti (2006) surveyed over 4000 students in regard to privacy on Facebook. The researchers searched all CMU Facebook members using the website's advanced search feature to extract their profile IDs. Their findings revealed that 90% of profiles contained an image, 88% of users provided their date of birth, 40% listed their phone numbers to include cell phone numbers, and 50% listed their current residence. It must be mentioned that Facebook profiles can be fully identifiable by participants providing their first and last names in their profile. To evaluate whether or not students provided a real name and date of birth the researchers analyzed a subset of 100 profiles randomly accessed from the initial 4000 students for accuracy. Facebook users in 89% of the profiles analyzed used their real first and last name and 98% provide their actual date of birth to include the month, day and year even though they are not required to do so. Facebook only requires a first name and the month and year of birth.

Goettke & Christiana (2007) conducted a study of 300 random profiles of both males and females in Cincinnati, Ohio who use Facebook,

MySpace, Classmates.com and Friendster to determine if users are concerned with privacy. The study revealed that 75% of participants provided an image with their full name on their profile page, 58% allowed users to access their personal photos and 83% provided their full date of birth.

The Impact of Providing Personal Information

In July 2010, Ron Bowles, an Internet security consultant, collected and published personal data for approximately 100 million Facebook users in an effort to show concerns over the company's privacy settings. Bowles wrote a script to scan over 500 million Facebook profiles for information not hidden from privacy settings (Reals, 2010). After extrapolating the information from the user's profiles, Bowles posted the data online which included the URL of every Facebook users' profile, their name and unique ID.

Facebook is primarily used by people that want to socialize online. At the same time, there are people using social network sites that will take advantage of the publically available information that users post. A study conducted by the Daily Mail discovered that crimes facilitated with the use of Facebook have increased 700% from 2007 to 2010. Over 100,000 crime incidents were linked directly to Facebook users' profiles in 2010 (Bolan, 2010). To put things in perspective, there were only 1400 related incidents in 2005. The increase in the number of users could have contributed in the drastic increase in Facebook related crimes.

Before the Internet, for a child abduction to occur, a person would hang out in a local park or near a school playground searching for the right child. Now a predator can search and follow their prey from the comforts of their own home. Much of this can be accomplished with the use of social media, such as Facebook to assist with building a profile on the child. They can follow children in chat rooms and social networking sites waiting and hoping to become their friend. People in general list names, the school they are currently attending, the school that they graduated from, their hometown, their occupation, and pictures of family and friends on social network sites. All of the information that people readily make available online can give a cyber-criminal everything they need to stalk, abduct, track a child, or even steal a person's identity (Flinn, et.al. 2010). Cyber-criminals can use the personal information to harass, or even harm, a person and their family. A cyber-criminal "can choose someone they know or a complete stranger with the use of a personal computer and the Internet. The information that is available about people on the Internet makes it easy for a cybercriminal to target a victim" (Paullet, 2009).

Using profile information and pictures available on Facebook can provide the physical location of the user throughout the day. Facebook profiles include location, schedule, and the location of the last login. This information can provide a roadmap to a victim for a stalker (Gross & Acquisit, 2005). The 2011 Working to Halt Online Abuse (WHO@) (2012) cyberstalking statistics revealed that 34% of victims received threats and were stalked via email followed by 17% who were threatened on Facebook.

3. RESEARCH METHODOLOGY

This study examined online information-sharing habits, privacy concerns, and experiences with data privacy violations of college undergraduates with active Facebook accounts at a mid-Atlantic university. A survey was administered to 146 college undergraduates in March and April of 2012 using a convenience sample. Prior to administration of the survey, a pilot test was conducted with 62 college undergraduates to test the survey in February of 2012.

The questionnaire consisted of 23 questions. Survey participants were first asked to indicate age, gender, and Facebook account status. If a participant did not have an active Facebook account, the survey was ended. Those participants with active Facebook accounts indicated basic information regarding Facebook habits, including how often they read and share information on Facebook, types of information and photos shared, and number of friends. Participants also specified the information they added to their profile in Facebook, including employer, occupation, college/university, major, high school, graduation date, religion, political views, music, books, movies, television shows, games, current city, hometown, gender, sexual orientation, maiden name (for married females), and date of birth. Participants specified whether they were friends with any family members on Facebook and if they had identified those family members on their profile.

In order to better understand participants' practices and concerns related to privacy, they were asked to indicate the types of information that they share and whether or not they were concerned about the possible consequences of sharing information on Facebook such as identity theft, unauthorized access to bank accounts, cyberstalking, cyberbullying, and child predators. Lastly, participants were asked if they share personal photos on Facebook such as, pictures of themselves, friends, pets, and children.

4. FINDINGS

Possible Effects of Sharing Information

Sharing photos on Facebook can provide a plethora of information to criminals. As users post photos on Facebook they are probably not thinking about the potential dangers of oversharing personal information. As depicted in Figure 1, 91% of students share photos of themselves on Facebook, 68% share photos of their children, 74% share photos of their friends and 43% share photos of their pets. One might ask, why would this matter? As we will discuss in the next few sections the photos provided can lead to many problems especially if a cybercriminal can correlate the information depicted in photos with answers to personal security questions or by providing accurate locations of where one might live, work, and play.

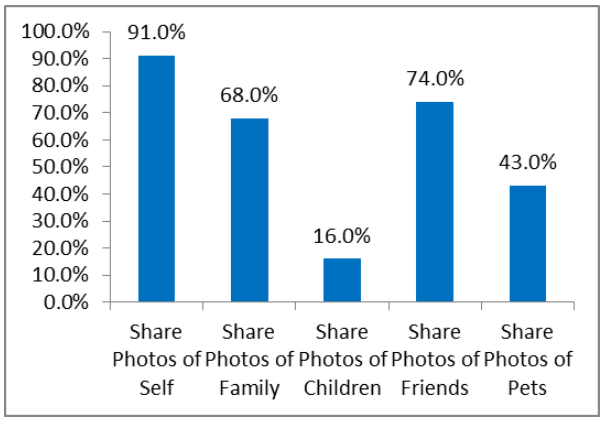

Figure 1. Percentage of students who share photos on Facebook.

The researchers do not believe that people are aware of the implications of oversharing information. For example, have you ever sat behind a car that has posted cartoon images of their family on the back window of their vehicle? A family might have an image of a father holding a briefcase, mom with a shopping bag, a little boy holding a football and a girl in a cheerleader outfit and think this is not a big deal. But a criminal looking at this information might think differently because they are now able to gather a ton of information about the family. What this scenario tells a criminal is that dad probably works in an office and that mom likes to shop. No big deal, right? WRONG. The family also provided a graphic roadmap to find their son and daughter. The images depicted on the back of the car in this scenario revealed the number and sports team of the son who plays football and the school where the daughter is a cheerleader. We now know what school their children attend and by providing the actual football number it will be extremely easy to find the son on the field and just as easy to locate the daughter at cheerleading practice. Pair this information with the license plate number and the name of the dealership that sometimes appears on the license plate frame of the car and we have more than enough information that can identify the family that is depicted in the graphics on the car. This scenario can be classified as an example of the effects of unintentional oversharing of information. Unintentional oversharing happens when people are able to extrapolate information about a person from information that they provided in things such as pictures. If we were able to pull information about people from decals on the back of a car imagine what a cybercriminal can gain from the information displayed on Facebook.

Photo tagging is a feature on many social network sites which allows people to link photos to each other's profile (Bessmer & Lipford,2010). As a result of the tagging feature people have reduced control over their images. Additionally, social network sites such as Facebook have caused users to lose control over their identity and information. Users of this feature have very little control to manage photo sharing and are forced to accept the problems due to their desire to participate (Besmer & Lipford, 2010).

Facebook is the largest photo sharing site on the Internet with over 1 billion photos uploaded monthly (Facebook, 2012). Increased access to an individual's photos has led to these images being used for purposes not intended (Besmer & Lipford, 2011). People post photos on Facebook daily. To many this might not seem like a big deal but in reality it can expose an individual to criminal activity. People post photos of their

pets, favorite sports team or an evening out with their closest friends. The information provided in these photos could cause a person to become a victim of identity theft or unauthorized access to their online banking accounts. Most accounts ask users to provide answers to security questions in case they forget their security pin. Asking security questions is a fallback authentication method set in place for the account owner to verify their identity.

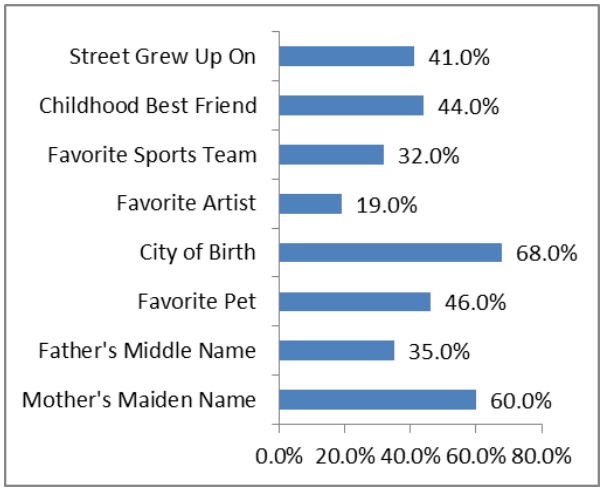

Figure 2. Percentage of people who used security questions when setting up and account online.

Students were asked a series of questions in regard to the security questions they used when setting up an online account. Figure 2 shows the list of security questions that were asked. Forty-one percent of students set up online accounts by providing the answer to the street that they grew up on, 44% provided their childhood place of birth, 32% provided their favorite sports team, 19% their favorite artist, 46% their favorite pet, 35% their fathers middle name, and 60% provided their mother's maiden name. If we take a look at some of the main security questions that are used when people set up a new account and compare them, review the photos and information provided in a person's profile in Facebook, one will be able to find the answers to many of the security questions by looking at the photos posted. Haga & Zviran (1991) conducted a study on personal security questions and then measured successful answer rates for the users and also the users' friends, family and significant others (Rabkin, 2009). Surprisingly, the user's friends were able to provide the correct answer to many of their friend's security questions. The photos that are depicted on Facebook can contain the user's favorite pet, the names of their closest friends and their favorite sports team to name a few. A criminal can note the name of the pet or friends and associate the information provided to possible security questions and then gain access to account information outside of Facebook.

Becoming a victim to any crime is not a laughing matter. Students were asked if they were concerned about the potential consequences of sharing information on Facebook. Sixty percent of students are concerned about becoming a victim of identity theft, 55% are concerned about someone gaining access to their online banking accounts, 37% are concerned about cyberstalking, 28% are concerned about cyberbullying and 28% are concerned about child predators. As depicted in Figure 3, people are concerned about being a victim of a computer related crime even though they continue to provide an enormous amount of personally identifiable information.

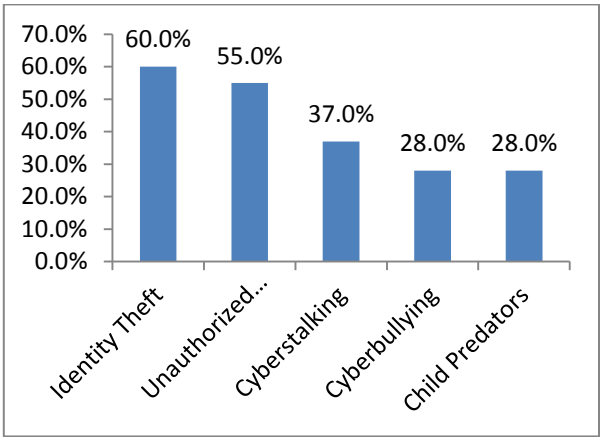

Figure 3. Percentage of people who are concerned about becoming a victim to a crime.

Sometimes posting innocent information online can pose risk of concern. Users of social network sites such as Facebook might be giving out more information than they are aware. Social network sites claim that they protect the user's information so that it can only be viewed by the people associated with the user's account. Although this is true, individual users' information can often be viewed by third party applications without their knowledge. Every time that a user clicks on a game or advertisement where they must accept the parties terms of service they have given the application the right to view their information. When using Facebook,

users should always check their settings to review the list of third party applications. One might be surprised to find out how many agencies, organizations or people have access to their accounts.

5. LIMITATIONS

The primary limitation of this study was the small sample size. Because of this, age and gender groups were not broken down into individual categories. The researchers encourage future studies to incorporate students from multiple universities or geographic regions to get a better cross-section of participants with active Facebook accounts.

6. CONCLUSION

Steps to Take to Stay Safe Online

There is no guarantee that the information that users provide on Facebook will remain safe and secure. Since social network sites are here to stay it is best that people follow a set of guidelines to help stay safe online. When a person leaves their home to go on vacation most likely they lock the doors, stop the mail, have at least one or two lights on in the house and possibly have a person stop over to check on the house. When using social network sites, people should follow similar rules to remain safe so that their valuable information is not stolen. Following the below safety measures for posting information does not guarantee safety but it can eliminate the risk of exposure just as locking the door to our homes limits the ability for a burglar to easily enter the house.

1. Pay attention to the information that can be identified in photos. Ensure that your photo background does not show your actual location.
2. Understand the privacy settings associated with the site.
3. Set appropriate privacy and security settings and choose a complex password that has nothing to do with the information that has been posted online.
4. Be careful when installing third party applications.
5. Only accept friend requests from people that you know. (It is strongly advised that you do not accept friends-of-friends.)
6. Read the privacy policy and terms of service.
7. Consider all information public.

7. REFERENCES

Besmer, A., & Lipford, H.R., (2010). Moving beyond untagging: Photo privacy in a tagged world. CHI:2010, Privacy, ACM.

Boland, R. (2010, December 20). More than 100,000 crimes linked to facebook in the last year. Internet News. Retrieved from: http://www.connectedinternet.co.uk/2010/12/20/100000-crimes-linked-facebook-year/

Consumer Reports Magazine. (June 2012). Facebook and your privacy. *Who sees the data you share on the biggest social network?* Consumer Reports Magazine retrieved from:
http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm

Debatin, B., Lovejoy, J., Horn, A., & Hughes, B. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior, 12(3),* 341-345.

Doyle, J. (2012, June 4). A Facebook crime every 40 minutes: from killings to grooming as 12,300 cases are linked to the site. Mail Online Newspaper, UK. Retrieved from: http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html

Goettke, R., & Christiana, J. (2007). Privacy and online social networking websites. *Special Topics in Computer Science Computation and Society: Privacy and Technology.*

Gross, R., & Acquisit, A. (2005). Information revelation and privacy in online social networks. *Proceedings of WPES '05*(pp. 71-80). Alexandria, VA: ACM.

Facebook. Statistics. (2012). Statistics. Retrieved from: http://www.facebook.com/press/ info.php?

Flinn, M., Teodorski, C., & Paullet, K. (2010). Raising awareness: an examination of embedded GPS data in images posted to the social networking site twitter. Issues in

Information Systems, Vol. XI, No. 1. Pp. 432-438, 2010.

Haga, W., & Zuiran, M. (1991). Queton-and-answer passwords: an empirical evaluation. *Information Systems,* 16(3):335-343.

Lampe, C., Ellison, N., & Steinfield, C. (2006). A Face(book) in the crowd: Social searching vs. social browsing. *Proceeding of ACM Special Interest Group on Computer-Supported Cooperative Work, ACM Press,* 167-170.

Liu, H & Maes, P. (2005). Interestmap: Harvesting social network profiles for recommendations. In Beyond Personalization – IUI 2005, San Diego, California.

Paullet, K. (2009). An exploratory study of cyberstalking; students and law enforcement in Allegheny County. UMI 3376412 retrieved March 22, 2010 from Dissertations and Thesis Database.

Rabkin, A. (2008) Personal knowledge questions for fallback authentication security questions in the era of facebook. *Symposium on Usable Privacy,* (SOUPS), Pittsburgh, PA.

Reals, T. (2010, July 29). Facebook personal information of 100 m users published. CBS News: Techtalk. Retrieved from http://www.cbsnews.com/8301-501465_162-20012031-501465.html

Working to Halt Online Abuse (2011). Online harassment/cyberstalking statistics. Retrieved from: http://www.haltabuse.org/ resources /stats/2011Statistics.pdf