Abstract

The study of online privacy management is a relatively new field, which suffers from a lack of empirical studies and needs to be examined in greater depth. This study identified security behaviors and attitudes for social network users from different demographic groups, and assess how these behaviors map against privacy vulnerabilities inherent in social networking applications.

1. Introduction

Social network sites allow an individual to create a public or “semi-public” profile, engage in activities with other users with whom they share interests [5]. In these virtual worlds individuals interact with each other both socially and professionally [16]. The 2009 Facebook Demographics and Statistics Report have shown dramatic increases in Facebook users, for age groups 18 – 24, 20.6% growth; 25 – 34, 101.5% growth; 35 – 54, 276.4% growth; 55 and over, 194.3% growth [8]. The dramatic increase in web users’ participation in online social networks has sprung some concerns. The posting of sensitive personal and private information in these domains opens the user to public scrutiny possible creating permanent records which can in the future affect them negatively [25]. Information posted on these sites can lead to security risks such as, identity theft, online stalking, and cyber harassment [22][23]. IUIPC has three controlling factors: collection of personal information, control of personal information, and awareness of privacy practices [6] [4].

Corporations have embraces the use of social computing services as a way of doing business, creating new avenues to exchange information, recruit, market goods and services, and collaborate [26]. The use of social computing services requires the creation of personal profile, and the upload of corporate data. Information posted on these sites can lead to organizations’ security risks such as, the exposure of corporate data to the public; individuals’ private information can also be exposed in the workplace [30]. To mitigate these risks, managers have proposed security measures, such as, IS security policies, but effective IS security requires that employees comply with IS security policies and guidelines [18]. Compliance with IS security policy is an important issue. CSI survey 2007 [7], respondents sees compliance as an issue in IS security. Employees seldom comply with proposed security measures, jeopardizing organization assets and business [18] [28] [19] [10]. Mahmood, Pahnila, and Siponen[18] have found that employee intention to compliance with IS security policy is impacted by, attitude, normative beliefs and habits.

The IUIPC construct [18] [4] was tested in an online social networking environment through a survey. Users of online social networks were asked about their behavior and attitudes towards securing their privacy on online social networks. Early study by Brown and Zukowski [6], found that certain user demographic factors influence the Internet users information privacy concerns (IUIPC) such as age, education and income level. The Internet Users’ Information Privacy Concern (IUIPC) [18] [4] model was used to show the valuation of personal information on social network sites, and the value users place on their information during the registration process, which helps to shape their attitude and behavior towards information privacy. The information posted to their profile could subject the user to security risks.

This study investigates the influence of demographic factors on social network users’ attitude and behavior towards privacy risks, and threats associated with these activities. This paper presents preliminary results from an online survey of online social network users’ attitudes and stated behaviors within the context of online social networking. We build theoretical model (Figure 1) explaining how the social network users’ attitude and behavior as to privacy risks can impact organizational security policy.
1.1 Hypothesis Development

1.2 IUIPC model

IUIPC has three controlling factors: collection, control, and awareness [18] [4]. It is the model used to explain the value users place on the personal information during e-commerce transactions. Users expect e-commerce sites to adequately protect their personal information they give to the site during account creation and checkout process. Users of social network sites can use the IUIPC model the same as e-shopping. Figure 2 shows our new model in an online social networking environment. However, unlike e-shopping, social networking have two different parts; the registration process and the profile setup. The registration process requires the users to give information to the social network to setup an account. The profile setup is controlled by the user and not by the site. Social network users should use IUIPC the same way for both processes.

Brown and Zukowski [6] found that older internet users are more concerned about information privacy than younger Internet users. This finding gives support to the following hypothesis:

**Hypothesis #1:** Younger online social network users are less concern about information privacy, therefore, they post more sensitive information on their profile which can lead to security risk

1.2.1 IS Security Risk Cost

There is a potential cost to electronic crimes; The Computer Security Institute (CIS) conducts an annual survey on computer crime and security. The 2007 survey had 494 respondents from diverse industries. Of the respondents, 149 claim a total loss of $66,930,950, an increase from $52,494,290 for 313 respondents in 2006. Organizations allocate 5 – 26 % of their IT budget to information security. Security is viewed as far broader than technology alone, data breaches are also driven by human error and careless prompting contribution IS security budget from audit and legal departments. Ironically 48 % spends less than 1% of security dollars on awareness and training program even though the study found that 64% of respondents attribute losses to insiders [7].

1.2.2 Normative beliefs

It is suggested that individual’s interactions influence their behavior, therefore normative belief reflects the normative expectation of an individual’s associations, such as, colleagues, or peers, and family. [18] [4], “Membership of a social environment or the influence of important people may have a persuasive influence on whether or not to perform a specific behavior”, Mahmood, Pahnila, and Siponen [18] [4]. This finding gives support to the following hypothesis:

**Hypothesis 2:** Normative belief impacts online social network users risk perception.
1.2.3 Habits

“A habit is unconscious or automatic behavior, as opposed to intentions or conscious behavior”, Mahmood, Pahnila, and Siponen [18] [17], they found that habits affect an employee intention to comply with IS security policy. It is suggested that the influence of habits on actual behavior increases over time, while the influence of behavioral intentions decreases [18] [17]. Therefore, we suggest that two hypotheses:

Hypothesis 3: Online social networks users’ long term risky behavior creates habits

Hypothesis 4: Habits impacts long term online social network users intention to comply with IS security policy

1.2.4 Attitude

“Attitude indicates a person’s positive or negative feelings toward some stimuli”, Mahmood, Pahnila, and Siponen[18] [3]. In regards to compliance with IS security policy, the Theory of Reasoned Action [12] indicates that a person’s behavioral intention is depended on the person's attitude about the behavior and subjective norms. This gives support to the following hypothesis

Hypothesis 5: Users’ attitude toward security risk in online social networks impacts their behavior.

1.2.5 Identity Theft

Identity theft is defined by US CERT [21], the government agency in charge of Internet risks, as “people obtaining personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it.” The information type users post an user’s profile can give unauthorized users access to personal information. Identity theft is one of the largest risks associated with social networks.

1.2.6 Cyber Harassment and Cyber Stalking

Cyber harassment and cyber stalking are another common threat to social networking sites. Cyber stalking and cyber harassment are very similar. Most people use them interchangeably, but there is a subtle distinction, typically relating to the perpetrator’s intent and the original motivation for their behavior. While the two situations usually involve many of the same online tactics, cyber stalking is almost always characterized by the stalker relentlessly pursuing his/her victim online and is much more likely to include some form of offline attack. This offline aspect makes it a more serious situation as it can easily lead to dangerous physical contact, if the victim’s location is known [11]. Therefore, we suggest the following hypothesis:

Hypothesis 6: We hypothesize that the amount of information that users post can lead to identity theft and cyber stalking.

2. Methodology and Model

2.1 Methodology

For the purpose of the study, the demographics of our survey focused on age, gender and education. Early study by Brown and Zukowski [6], found that certain user demographic factors influence the Internet users information privacy concerns (IUIPC). The age of our respondents varied from 15 years of age to 64 years of age. Education levels ranged from high school to Ph.D. About 66.10% of our respondents were male and 33.90% were female between the ages of 15 to 64.

Our team developed a survey, which asked users what type of information they make available on social network sites such as Facebook, our primary focus in our study. The survey for our study was distributed via mass email from the Pace University school email system by the system administrators, contacts from client’s address books, users of social network sites from friends, family, coworkers, students and classmates. We asked users’ questions that help us determine their attitudes and behaviors in terms of privacy on such social networking sites. The survey results were about the same in terms of age and gender.

Our respondents replied with the types of information they post in their profile that would present possible risks, threats or vulnerabilities. The survey consisted of questions that include users’ activities on social network sites like Facebook, Myspace, Twitter, LinkedIn and Flixster. In terms of privacy, we’ve
also asked users about consumer privacy and security settings. The users responded to each scenario using the seven point Likert scale from strongly agree to strongly disagree. In Section 4, we will use the results from our survey that is relevant to our current study in terms of users’ attitudes and behaviors on social networking sites.

3. Online social networks

Social network sites are defined as a web-based service that allows an individual to create a public or “semi-public” profile, gather a list of other users with whom they share interests and/or activities or who are interested in exploring the interests and activities of others within the social network. The nature and arrangement of these connections may vary from site to site. Social networking websites are being used by millions of people and now seems that social networking websites will be a part of our everyday life. [5]

There are many different types of social networking sites. Some social networks have additional features, such as the ability to create groups that share common interests, upload or stream live videos, and hold discussions in forums. Social networks are constructed in a way linking users by six degrees of separation. According to Milgram’s paper written in 1967; everyone is separated by six hops [31].

4. Results from the Survey

4.1 Demographics of survey respondents

4.1.1 Age

<table>
<thead>
<tr>
<th>Age</th>
<th>15-24</th>
<th>25-34</th>
<th>35-44</th>
<th>45-54</th>
<th>55-64</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>63.50%</td>
<td>68.70%</td>
<td>69.80%</td>
<td>61.80%</td>
<td>67.90%</td>
<td>66.10%</td>
</tr>
<tr>
<td>Female</td>
<td>36.50%</td>
<td>31.30%</td>
<td>30.20%</td>
<td>38.20%</td>
<td>32.10%</td>
<td>33.90%</td>
</tr>
<tr>
<td>Response</td>
<td>52</td>
<td>96</td>
<td>96</td>
<td>76</td>
<td>28</td>
<td>348</td>
</tr>
</tbody>
</table>

Table 1 – Age by percentage.

Our survey demographics included age, gender and education levels of respondents, ranging from age 15 year olds to 64 year olds.

The 15 to 24 year old age groups were 63.50% males while 36.50% of the respondents were females. The total response from this age group was 52 responses out of 348. The 25 to 34 year old age groups were 66.70% male and 33.30% female. Total response from this age group was 96 out of 348. The 35 to 44 year old age groups were 69.80% males and 30.20% females. Total response from this age group is 96 responses out of 348. The 44 to 54 year old age groups were 61.80% males and 38.20% females. Total response was 76 out of 348. Finally, the 55 to 64 year old age groups were 67.90% males and 32.10% females. Total response was 28 out of 348.

As we can see in Table 1, the 25 to 34 year old age groups and 34 to 44 year old age groups tie in terms of response rate to this survey. This is relevant to the recent study by iStrategy labs in which the 35 to 55 year old age groups are the growing trend on social networking sites [8]. Overall, male response totals were 66.10% in our survey while female responses were 33.90% with a total of 348 responses from all age groups.

4.1.2 Education

<table>
<thead>
<tr>
<th>Education</th>
<th>Age</th>
<th>15-24</th>
<th>25-34</th>
<th>35-44</th>
<th>45-54</th>
<th>55-64</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some School, did not graduate High School</td>
<td>11.00%</td>
<td>11.00%</td>
<td>11.00%</td>
<td>11.00%</td>
<td>11.00%</td>
<td>11.00%</td>
<td>11.00%</td>
</tr>
<tr>
<td>High School Graduate</td>
<td>19.20%</td>
<td>21.00%</td>
<td>27.00%</td>
<td>18.70%</td>
<td>17.30%</td>
<td>19.30%</td>
<td>19.30%</td>
</tr>
<tr>
<td>Some College, did not graduate College</td>
<td>26.00%</td>
<td>29.20%</td>
<td>21.90%</td>
<td>23.70%</td>
<td>14.30%</td>
<td>24.40%</td>
<td>24.40%</td>
</tr>
<tr>
<td>Associates Degree</td>
<td>1.00%</td>
<td>1.00%</td>
<td>1.00%</td>
<td>1.00%</td>
<td>1.00%</td>
<td>1.00%</td>
<td>1.00%</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>23.00%</td>
<td>21.00%</td>
<td>20.00%</td>
<td>22.00%</td>
<td>22.00%</td>
<td>22.00%</td>
<td>22.00%</td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>11.00%</td>
<td>19.80%</td>
<td>20.80%</td>
<td>13.80%</td>
<td>15.70%</td>
<td>18.70%</td>
<td>18.70%</td>
</tr>
<tr>
<td>Professional Degree</td>
<td>1.00%</td>
<td>8.30%</td>
<td>4.20%</td>
<td>2.00%</td>
<td>1.40%</td>
<td>8.00%</td>
<td>8.00%</td>
</tr>
<tr>
<td>Doctorate Degree</td>
<td>3.00%</td>
<td>1.00%</td>
<td>1.00%</td>
<td>5.30%</td>
<td>3.60%</td>
<td>2.60%</td>
<td>2.60%</td>
</tr>
<tr>
<td>Response</td>
<td>52</td>
<td>96</td>
<td>96</td>
<td>76</td>
<td>28</td>
<td>348</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 – Demographics by age and education.

The survey asked respondents to indicate their education level. Only a small portion of our respondents were under 18 years old. The respondents from the survey were at least a high school graduate between the ages of 18 to 64 years old. Most of our respondents ranged from attending some college but did not graduate yet to having a bachelor’s degree. The most responses we received were from individuals who attended college but did not graduate with an overall percentage of 24.40% between 18 and 64 years old and respondents either are enrolled in a program with a bachelor’s degree or already have a bachelor’s degree with a response rate of 22.70% between the ages of 18 to 64. Table 2
shows the percentages of the education levels of our respondents.

4.3. Personal Information

<table>
<thead>
<tr>
<th>13. Have you read the terms of use for your social networking site(s)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Response Count</td>
</tr>
</tbody>
</table>

Table 3 – Users who read terms of service.

All sites, e-commerce and social networks, have terms of agreement for users to read during the account creation process. This document outlines how your information will be protected by the social network. Also, it explains how the social network will handle your information in regards to third party vendors. Table 3 shows the amount of times users actually read the terms of agreement. These two parts of the terms of agreement are only a small piece of the entire document. It gives a small snapshot regarding the IUIPC model on social networks.

Social network users can maintain their privacy and security by using the IUIPC model. By using this model to create their profiles they can have a safe environment to network with others on the Internet. They need to value their personal information the same way they do for e-shopping or the registration process.

4.4 Attitudes and behaviors toward risks engaged in social networking

4.4.1 Updating security settings

<table>
<thead>
<tr>
<th>14. Have you customized your security settings for your social networking site(s)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Response Count</td>
</tr>
</tbody>
</table>

Table 4 – Users who updated security settings

In terms of security, Table 4 is our results from the survey in which we asked users of social networking sites that whether or not they’ve updated their security settings such as those found in Facebook or Myspace. Majority of the respondents responded that they indeed updated their security settings based on the results found in Figure 8 from all age groups.

In Table 4, from the age group of 15 to 24 year olds, 90% responded that they did update their security settings while 10% responded that they have not. The 25 to 34 age group responded with 74.40% that their security settings were updated while 25.60% responded that they did not. The 35 to 44 age group responded with 67.80% that their security settings have been updated while 32.20% responded with they have not updated their settings. The 45 to 54 age group responded with 53.70% that their security settings have been updated while 46.30% have not updated their settings. Finally, the 55 to 64 age group responded with 52% that they updated their security settings while 48% have not updated their settings.

Interesting fact about these results is that all the age groups have updated their settings. The overall response rate was 68.90% that all users updated their privacy settings. The total number of users who did not update their settings was at 31.10% from our survey from all age groups.

Based on the results of the study, Hypothesis #1 does not prove to be valid. The results suggest that younger online social network users are concern about information privacy.

Risk Beliefs

We test risk beliefs by giving the respondents by scenario. The scenario asked the following questions: A person who claims to have attended school with or worked with you previously asks to connect with or friend you on your social network, but you can't remember who they are. There results showed that 31% of 15-25 age, 65% of 25-34 age, 69% of 35-44 age, 57% of 45-54 age, and 38.2% of 55-64 age finds there is no uncertainty associated with giving this information to a requester on a social networking site. This suggest that there are some validity to Hypothesis 5 that users’ attitude toward security risk in online social networks impacts their behavior.

4.3.2 What do they post to their profile?
The amount of information a user posts on their profile may present risks in terms of safety and threats such as identity theft, cyber harassment / cyber stalking and cyber bullying. We've asked users to indicate what type of information is made available on social networking sites. Table 5 is the results from user input as to what information is made available on their profiles on Facebook.

Based on our results of the study, Hypothesis # 6 proves to be valid. Since the amount and type of information posted on a profile on a social network may lead to risks, threats and vulnerabilities presented on these sites. Users age 15-24 consistently post more information at a higher percentage than all other age group, except for their name. Users should therefore limit the amount of information posted on their profiles to prevent potential stalking, harassment and identity theft or spamming. By posting information such as your birthday, location, activities, hobbies and interests, potential thieves would be able to take advantage of the user based on this information [21].

5. Prevention of Risks, Threats and Vulnerabilities

In order to prevent the risks mentioned in Section 4.3.2, users of social networking sites must limit the amount of information they provide. Social networking sites such as MySpace, Facebook, and Linkedin may differ but they all allow you to give your personal information in profiles, forums, chat rooms, email, instant messaging etc, where you go to connect with other people. Some sites let you search or browse for people and other sites require you to be ‘introduce’ to new people. Essentially the sites are a way to meet people with similar interests, hobbies and so on. [21].

The following are tips to stay safe on social networking sites: [21]

- Limit the amount of personal information you post - Do not post information that would make you vulnerable (e.g., your address, information about your schedule or routine). If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing.
- Remember that the Internet is a public resource - Only post information you are comfortable with anyone seeing. This includes information in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.
- Be wary of strangers - The Internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites.
- Be skeptical - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, a product of exaggeration, or a joke.
- Check privacy policies - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam.

5.3 Risk Analysis

Risk assessment is the least thought out process analyzing social networks [14]. Social network developers and founders do not complete a basic risk analysis of network to understand the implications on the user. Social networks could possibly develop risk assessment programs to educate users to the potential
dangers of posting certain information or replying to unsolicited messages. Users could use these programs to become better aware of the dangers around them on the network. A well developed and thought out risk assessment plan could possibly go a long way.

It could enhance the overall user experience of the social network user. Risk assessment touches all three factors of the IUIPC model; collection, control, and awareness. The network would better collect and store user profile information; making certain information only visible to the actual user. The user would be able to control the information they post to their profile developing a basic assessment chart or graph. The user would become more aware by viewing a risk matrix. The risk assessment process is a valuable tool to the social network site and user if the proper tools are used.

6. Conclusion

This study is preliminary; all results require some further analysis. Based on our study results, social network sites have become a popular trend. As the number of users increase on social networking sites, so do the risks, threats or vulnerabilities. Users age 15-24 consistently post more information at a higher percentage than all other age group, except for their name. The amount of information users post in their profiles may present risks to their privacy and their safety. Such risks, threats or vulnerabilities include social engineering such as identity theft and phishing scams, cyber harassment/cyber stalking, and cyber bullying. Therefore, it is important to limit the amount of information posted on profiles for social networking sites such as Facebook. Hypothesis 2, Hypothesis 3, and Hypothesis 4 could not be validated or disproved for the results of our survey, which require further studies.

IS security managers should be concern about age group 15-24 because they soon will be entering the workforce. Compliance is an issue in IS security. If the employee’s normative belief, as to privacy risk, can be viewed as risky, and an employees’ behavioral intention depended on the person’s attitude about the behavior and subjective norms, then long term risky behavior can lead to habits, which could impact IS security policy.

7. References


