Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study

Neelima Bhatnagar
bhatnagr@pitt.edu

Michael Pry
mip84@pitt.edu

Information Sciences
University of Pittsburgh Greensburg
Greensburg, PA 15601

Abstract

This paper describes a study designed to collect student perceptions of personal social media risks and their knowledge of the use of privacy and security settings in social media applications. A paper-based survey was administered to 107 students at a regional campus of a major university in western Pennsylvania, representing 10 classes and 18 different academic majors. The findings suggest that students are aware of privacy and security risks in the use of social media platforms and do value and suggest additional training in this domain. This paper explores a new concept of a maturity model for the instruction of social media risks based on different levels of sophistication from simple account settings to advanced concepts of personal brand management. Future research is suggested in validating the social media, risk awareness and countermeasure maturity model (SMRA-CMM).

Keywords: social media, cybersecurity, privacy, awareness, risk, digital literacy

1. INTRODUCTION

The purpose of the research study was to determine students' attitudes, awareness, and perceptions of personal privacy and cybersecurity of social media sites. Within the context of this study, social media is defined as forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas or personal messages. Privacy is defined as "freedom from unauthorized intrusion" and the ability to control one's personal information so that only those the owner wishes to view their information are allowed. This includes both control over what information is viewable in social media as well as who can view it. According to Heiten (2016) digital literacy is defined as having three categories that include "1) finding and consuming digital content; 2) creating digital content; and 3) communicating or sharing it" (p.5-6). The authors believe that a fourth category that should be included in the definition of digital literacy is creating awareness of privacy/security risks and countermeasures. To that extent, a paper-based survey was administered to students enrolled in summer classes at a campus of a major university in western Pennsylvania. A paper-based survey was chosen in lieu of administering the survey online to increase the sample size. The three primary research objectives of the study are:

1. To assess student perception regarding social media privacy.
2. To assess whether security matters to college students.

3. To evaluate whether universities should be providing better education regarding cyber-security.

2. LITERATURE REVIEW

The use of social media is prevalent in both the general society and on college campuses. The increasing popularity of the use of social media sites has brought to the forefront a new set of problems and issues facing the 21st century. Today's college generation is facing an emerging risk to reputational harm or financial loss much more so than prior generations since social media is their main form of communication. According to Moallem (2018), "users' understanding of risks and how to protect themselves from cyber-attacks is therefore fundamental in modern life" (p. 80)." According to a study done by the Pew Research Center (2019), 69% of US adults use Facebook and 73% use YouTube. The percentage of users using Instagram, Pinterest, Snapchat, LinkedIn, Twitter, Reddit, and WhatsApp is considerably lower. Among the 18-24-year-old age group 80% use at least one social media site. More specifically 94% use YouTube, 80% use Facebook, 78% use Snapchat, 71% use Instagram, and finally 45% use Twitter. Richardson (2017) in her study reported 90% of the participants were using Facebook and Snapchat and 70% were using Instagram. Most users check their accounts multiple times a day (Pew Research Center, 2019).

Knight-McCord, Cleary, Grant, Herron, Jumbo, Lacey, Livingston, Robinson, Smith, and Emanuel (2016) had conducted a study to determine which social media sites were being used the most by students. They distributed a survey to 363 students both in-person and online. What they found was that like the other studies, Instagram was the most widely used site followed by Snapchat and Facebook. The ones that were not as much used were LinkedIn and Pinterest.

Rivera, Di Gangi, Worrell, Thompson, and Johnston (2015) stated that "…academics must consider how they prepare current and future college students to deal with the personal risks involved in using social media. News coverage has made everyone aware of some of the dangers of revealing personal information through social media, but most news stories sacrifice measured and helpful coverage in the interest of sensational headlines. As a result, it is fair to assume that most social media users have a distorted view of the personal risk associated with using social media" (p. 50). This creates a compelling reason for gaining a deeper understanding of students' attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media sites. Moallem (2018) established the importance of awareness to cybersecurity threats and cited prior studies that found the issue is not with awareness but action.

Sharma, Jain, and Tiwari (2015) found that 84% of students felt that sharing of personal information on social networking sites (SNS) was risky. Moallem (2018) investigated students' cyber security awareness at two California State Universities in Silicon Valley. An online survey was administered to students enrolled in three classes. The survey consisted of ten questions, but none of them focused on social media or privacy. One of the conclusions drawn was that students were "…not very aware of how to protect their data" (p. 86).

Goh, Di Gangi, Rivera, and Worrell (2016) discussed that social media risks can be classified in two areas: social risk and technology risk. They identified social risk to include topics such as cyberbullying, cyberstalking, and identity theft. Technology risk, on the other hand, includes malicious software or malware, hacks, unauthorized access to social media account, and service interruptions.

In summary the studies referenced in this section provided evidence that the use of social media is prevalent in both the general society and on college campuses. The literature further defined a list of commonly used social media platforms and their rate of adoption by different generations of users. The studies did not provide coverage of the topics of security and privacy within the use of social media indicating an opportunity for this research study.

3. METHODOLOGY

The design of the survey was based on the need to identify students' perceptions of cyber-security risk and privacy concerns with the use of social media. Motivating this research was the desire to use the outcomes of the research as input to the development of new curriculum that would be taught at the undergraduate level and would help enhance students' digital literacy and improve the safety of their online behavior.

Upon receiving IRB approval, the authors obtained a list of summer course offerings, from

the campus website, that included information about the summer sessions, instructors, times and locations. Courses that were being taught online were not included. Courses offered in the first and second six weeks sessions along with 12-week sessions were considered. Instructors were contacted via email and asked for permission to come to their classes to administer the paper-based survey. The survey was administered during class time. A paper-based survey was chosen in lieu of an online survey since it would provide the greatest access to students and a larger sample size. During a six-week period, ten classes were visited. The courses represented a variety of disciplines. Only those courses where the instructors agreed were surveyed. The authors visited each class and provided each student with a copy of the recruitment script. If they agreed to participate in the research study, they were provided with a copy of the survey. Students who had already completed the survey in another class, self-reported and opted out of re-taking the survey. Responses were entered into an Excel spreadsheet for analysis. A total of 107 students completed the survey.

Surveys were numbered and closed-ended questions were coded. For the open-ended questions, that required a text response, a consolidation process was used to synthesize the many responses into similar categories. The process began with the authors reviewing all of the responses provided by the students within a specific question. From the responses, common themes emerged and these became the designated "categories" for classification purposes. Each response was re-read and a decision was made as to which category the response belonged in. This allowed for the consolidation of the responses into categories for analysis purposes. The two primary categories of classification were social risk and technical risk.

4. ANALYSIS OF DATA AND FINDINGS

Our findings show that of the 107 respondents, 100 (or 93%) currently use social media while the remaining 7% (7/107) do not. As can be seen in Figure 1, Snapchat and Instagram are the two most widely popular social media platforms in use. Most students used multiple forms of social media. A further breakdown of the responses showed that 23.36% had a single account, 74.76% had multiple accounts, and 1.86% had no accounts. Participants' average age was 21.6 years old, with the youngest being 18 and the oldest 45.

Of the 107 surveys completed, 18 majors were represented. The highest concentration occurred in the following five majors: accounting, biochemistry, biology, business management, education, and psychology. More females (57%) than males (41%) responded to the survey.

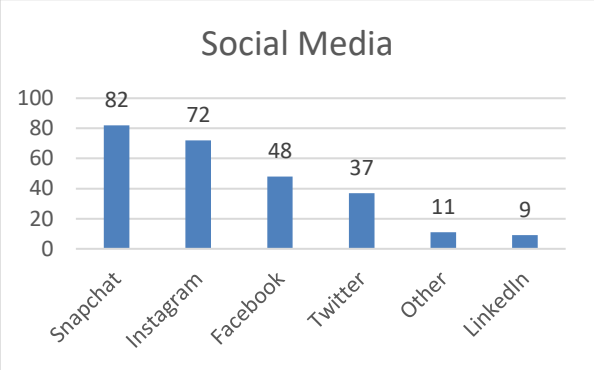

Figure 1. Social Media Use by Platform

Figure 2 below shows the distribution of the student ranks.

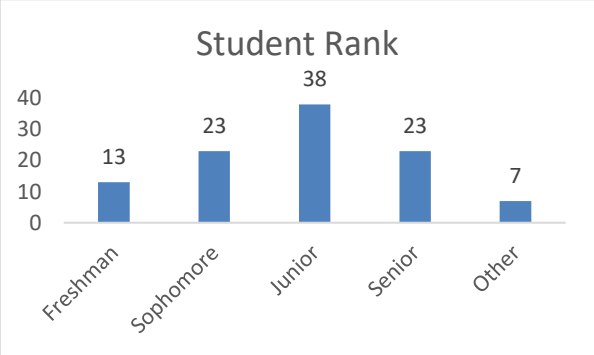

Figure 2. Representation by class rank.

Risk

Social media is a growing platform for student interaction and communication. This research focused on understanding student awareness of risk in the context of cyber security and privacy as it relates to social media. As noted earlier, 93% of the students indicated that they use at least one form of social media. Surprisingly today's digital native has a high level of security awareness with 72.6% understanding the risk of their profile being public and 78.5% knowing how to use the security features available by their social media provider. Participants were asked if they had been a victim of a cybersecurity attack, breach or had experienced a loss of privacy. The majority (71.03%) had

not been a victim. Our survey also showed that students had experienced incidents of both social and technical risk. Of the 30 respondents that had experienced social or technical risk, the majority (90%) had experienced a technical risk. Only 6.67% had experienced a social risk. Naturally, having been victimized the students saw a benefit of setting security features. Interestingly, there were three primary motivations for setting security features to include: risk reduction (31.78%), privacy (30.84%), and control (24.29%). The risk reduction motivation is the act of staying safe from a perceived harm. The privacy motivation is the mechanism to keep their information private. According to common themes found in comments provided for survey question ten, the control motivation implies empowerment over their personal information and acts as a gatekeeper to keep their information safe. Although many would argue that the advantages outweigh disadvantages, the students made three compelling arguments as to why there is a disadvantage to setting security features. These arguments include that security settings limit the full-functionality of the social media application (22.42%), are inconvenient (25.23%), and they are not full-proof (8.41%). However, most students did not see a disadvantage to setting security features (27.10%). See Appendix A for a detailed listing of the descriptive statistics.

Consistent with the high levels of security awareness and sophisticated use of security settings, 50% (or 53/107) of the students cared about knowing the social media privacy policy and did not feel comfortable with their habits being tracked. However, a noteworthy division was noticed in that 52.43% of the students were okay with sacrificing their privacy in exchange for the use of free applications or services and of those comfortable with their habits being tracked, 48.78% saw a direct benefit to being tracked because of targeted advertising. While 24.39% simply saw it as an accepted norm in participating in online activity.

Awareness

Another aspect of our research was to gauge the students' awareness of the importance of using security features. According to question 11 of the survey what we found is that the majority (78.09%) are using security features which corresponds to question four of the survey for which 69% of the respondents stated that their social media accounts are private. This confirms the fact that 84% of the students know how to navigate the social media system settings and set the security options that are available. A combined 80% rated privacy as being very important (48% or 51/107) and important (31% or 33/107) on a 5-point Likert scale.

Education

Our research found that 80% of the students did feel that training should be offered on the concepts of risk to the use of social media and how to use the security settings to mitigate that risk. Our next concern was related to the timing of when that training should be offered. The research found that almost 85% felt training should be offered during the freshman year.

Most students did use the privacy settings in social media to mark their account private. Others wanted to keep their account public because they used their social media accounts for promoting their own small business and felt that security was a negative if it reduced their marketing reach.

Some students create fake accounts/pen names to provide anonymity of their activity on social media to manage their social media presence.

Based on the survey results, students do understand the risk of engaging in unsafe behaviors that compromises their privacy on social media platforms and do know what to do about it. As far as the question related to the need for formalized instruction and its implications on digital literacy in a university setting, the authors were biased in thinking that formalized instruction would be needed and focus on the need to increase awareness of privacy risks in the use of social media and in the use and configuration of security settings.

5. SUMMARY AND CONCLUSIONS

From conducting the study all three research objectives were achieved satisfactorily and the following conclusions emerged:

- Students are aware of the risk of using social media and could provide good examples of issues that have occurred in the past to include account compromise and identity theft.
- A migration is occurring in the use of social media platforms by generation z students. The migration is moving away from Twitter and Facebook to the use of Snapchat and Instagram.
- When security settings were not used the most common reason was that they are hard to understand and use. They

also indicated that it limited their online reach.
- Students do value the need for training on cybersecurity and privacy in the use of social media and feel this should occur in the students' freshman year.

From our research, the authors have formulated a maturity model (see Figure 3) based on a student's sophistication with the use of social media privacy and security behaviors. This model can serve as a guide for future research on the development of training topics and their optimum teaching modality. At the base of the pyramid, setting strong passwords is commonplace amongst the most commonly used social media providers. At the next level, privacy settings include setting an account to be either private or public. At the third level, a secure configuration could include the use of two-factor authentication and geolocation. Fourth is self-regulation, which from the human behavior perspective, determines how one chooses to control their online postings. At the top of the pyramid, the intentional design of the personal brand, otherwise known as their social media presence, is crucial to managing public personal perception such as in the case of hiring or firing decisions and to that extent students must also understand that there is a positive relationship between the use of LinkedIn and obtaining relevant work in their field of study. Richardson (2017) had suggested "social media provides the opportunity for students to create their own persona and branding, whether this is positive or negative. Students can have a true identity, a pseudo identity through social media, and possibly even an anonymous identity as they post and comment. Research that studies the affect that social media has towards forming traditional relationships and identity development would also provide useful information" (p. 94).

The SMRA-CMM is founded on the principles outlined in the NIST Cybersecurity Framework. Specifically is PR.AC-1 which outlines the importance of identities and credentials being properly managed for authorized users (Strong Passwords), PR.DS-5 protection against data leaks are implemented (Privacy Settings), PR.IP-1 a baseline configuration of information systems is created and maintained (Secure Configuration), and PR.AT-1 and PR.AT-2 all users are informed and trained and understand their roles and responsibilities (Self-Regulation of Posting). The concept of self-responsibility defined in PR.AT-1 and PR.AT-2 are further developed in the SMRA-CMM's focus on the end user intentionally crafting their personal brand (what they want others to know and think about themselves online) as this measure of expanded self-responsibility to managing ones privacy and personal security online is consistent with the intent of the NIST Cybersecurity Frameworks section on awareness and training. The elements defined in the NIST Cybersecurity Framework elements are further supported by the SANS Top 20 Critical Security Controls. Specifically, SANS control #3 Secure Configuration, #13 Data Protection, and #17 Security Skills Assessment & Appropriate Training to Fill Gaps. The consistency in guidance for cybersecurity provided by NIST and SANS supports the development of the SMRA-CMM as a model to provide for the basic education of undergraduate students on the necessary elements to protect their privacy and security online while also supports the need for an element of personal responsibility in the self-regulation of their own online behavior once they have implemented the security mechanisms of strong passwords and secure configurations of their social media accounts.

Through this research study a gap was discovered in the knowledge students had related to the importance of self-responsibility in managing their online social media activity. As self-reported by the students through the survey results, 78% had indicated that they were using the security features of their social media platform thus addressing the technological risk however 52% of students indicated they were okay with sacrificing their privacy for the opportunity to use the social media application indicating a need for additional awareness of training that expands from the technical risk but embraces the social risks as well. To this extent a definition of social risk that includes the influence of social media on future employers and job selection will require additional research. For the purposes of the SMRA-CMM the authors suggest that undergraduate education related to the students' risk to the loss of privacy and security online will require curriculum that first establishes the basis of cyber security basics to include the use of strong passwords and the use of a secure profile configuration to mitigate the technical risk and then further develops an understanding of the social risk that requires the regulation of online social media activity.

Our research has made a unique contribution to Information System education by addressing a gap that currently exists in that there is no formal structure to assess and develop privacy/cybersecurity awareness training for

college students. This study proposes a maturity model that will develop students beyond the use of simple security settings to active management of their online identity and personal brand.

Future research should be conducted on changing attitudes of digital natives with regards to their perception of accepted norms and benefits to loss of some privacy. An opportunity within academia lies in helping students understand the importance of reading and understanding the privacy policies of the sites they visit or applications they use. Additionally, a longitudinal study to understand students' perceptions on cyber-security would also prove to be beneficial.

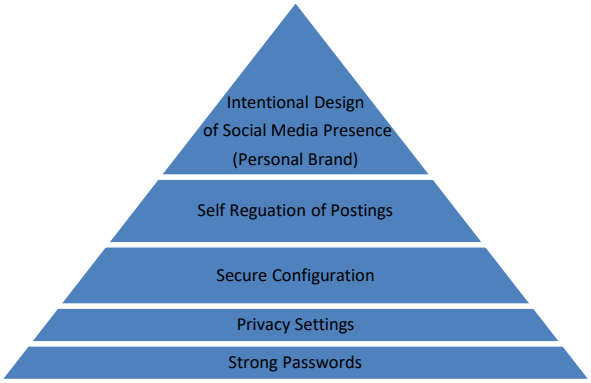

Figure 3. Social Media, Risk Awareness and Countermeasure Maturity Model (SMRA-CMM)

6. ACKNOWLEDGEMENTS

We would like to thank the faculty for allowing us to survey their classes for this important research endeavor.

7. REFERENCES

Cybersecurity Framework, National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframework

Goh, S. H., Di Gangi, P. M., Rivera, J. C., & Worrell, J. L. (2016). Graduate student perceptions of personal social media risk: A comparison study. *Issues in Information Systems*, *17*(4), 109-119.

Heiten, L. (2016). Digital literacy: An evolving definition. Retrieved from https://www.edweek.org/ew/articles/2016/11/09/what-is-digital-literacy.html

Hurt, N. E., Moss, G. S., Bradley, C. L., Larson, L. R., Lovelace, M., Prevost, L. B., ... & Camus, M. S. (2012). The 'Facebook' effect: College students' perceptions of online discussions in the age of social networking. *International Journal for the Scholarship of Teaching and Learning, 6*(2), Article 10, 1-24.

Knight-McCord, J., Cleary, D., Grant, N., Herron, A., Jumbo, S., Lacey, T., Livingston, T., Robinson, S., Smith, R., & Emanuel, R. (2016). What social media sites do college students use most. *Journal of Undergraduate Ethnic Minority Psychology, 2*(21), 21-26.

Moallem, A. (2018). Cyber security awareness among college students. T.Z. Ahram & D. Nicholson (Eds.), *International Conference on Applied Human Factors and Ergonomics* (pp. 79-87). Springer International Publishing AG. doi.org/10.1007/978-3-319-94782-2_8

Richardson, C. (2017). *Student perceptions of the impact of social media on college student engagement* (Doctoral dissertation). Retrieved from https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=5444&context=etd.

Rivera, J. C., Di Gangi, P. M., Johnston, A. C., & Worrell, J. L. (2015). Undergraduate student perceptions of personal social media risk. *Information Security Education Journal, 2*(2), 49-56.

Sharma, B. K., Jain, M., & Tiwari, D. (2015). Students perception towards social media with special reference to management students of Bhopal Madhya Pradesh. International *Journal of Engineering and Applied Sciences, 2*(1), 30-34.

Top 20 Security Controls, SANS Institute. Retrieved from https://www.sans.org/critical-security-controls

Pew Research Center. (2019). Social Networking Fact Sheet. Retrieved from https://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Appendix A

Descriptive Statistics (N=107)

Item	Frequency	Percentage (%)
Do you use social media?		
Yes	100	93%
No	7	7%
Not applicable	0	0%
Are you aware of security features offered by social media providers?		
Yes	84	79%
No	23	21%
Not applicable	0	0%
What is your current social media account profile status?		
Public	24	22%
Private	70	65%
Don't know	1	1%
Not applicable	6	6%
Both public and private	6	6%
Do you see risk with your social media profile being public?		
Yes	77	72%
No	16	15%
Don't care	6	6%
Not applicable	7	7%
No and not applicable	1	1%
Do you know how to navigate the social media system setting and set the security options that are available?		
Yes	90	84%
No	14	13%
Not applicable	3	3%
Have you been a victim of a cyber-security attack, breach, or loss of privacy?		
Yes	31	29%
No	76	71%
Not applicable	0	0%
On a scale of 1-5 (1- very important, 5 – unimportant), how important is privacy to you?		
Very important	51	48%
Important	33	31%
Moderately important	19	18%
Of little importance	4	4%
Unimportant	0	0%
Are you aware of the privacy policy of how your data is used by social media providers?		
Yes	53	50%
No	49	46%
Not applicable	4	4%
No answer	1	1%
Do you care about how your data is being used by social media providers?		
Yes	59	55%
No	10	9%
Not applicable	3	3%
Haven't given it much thought	34	32%
No answer	1	1%
Is the advantage of having a free social media application greater than the risk of your information being used by the provider or 3rd party as part of "big data analytics"?		
Yes	54	50%
No	36	34%

Not applicable	13	12%
No answer	4	4%
Are you comfortable with having your habits tracked by the social media provider for the purpose of having targeted advertising based on your likes and dislikes or preferences?		
Yes	33	31%
No	71	66%
Not applicable	3	3%
Do you think training should be offered on personal privacy and cyber security awareness?		
Yes	86	80%
No	10	9%
Don't care	11	10%
If you answered yes to the previous question, when should training be offered?		
Freshman	73	68%
Sophomore	7	7%
Junior	3	3%
Senior	0	0%
No answer provided	18	17%
Options 1-4	5	5%
Options 2-3	1	1%

Appendix B

Student attitudes, awareness, and perceptions of personal privacy and cyber security
Student Survey

The survey seeks to gather data for a research study on students' personal privacy and cyber security awareness and its implications on digital literacy.

Cyber-security

1. **Do you use social media?**
   a. Yes
   b. No
   c. Not applicable

2. **What 'brand of social media do you use most frequently? Check all that apply.**
   a. Facebook
   b. Snapchat
   c. Twitter
   d. Instagram
   e. LinkedIn
   f. Other: please specify _____

3. **Are you aware of security features offered by social media providers?**
   a. Yes
   b. No
   c. Not applicable

4. **What is your current social media account profile status?**
   a. Public
   b. Private
   c. Don't know
   d. Not applicable

5. **Do you see a risk with your social media profile being public?**
   a. Yes
   b. No
   c. Don't care
   d. Not applicable

6. **Do you know how to navigate the social media system setting and set the security options that are available?**
   a. Yes
   b. No
   c. Not applicable

7. **Have you been a victim of a cyber security attack, breach, or loss of privacy?**
   a. Yes
   b. No
   c. Not applicable

8. **If you answered yes to #7, please provide any details of the incident that you would be willing to share.**

9. **What do you see as the benefit of setting security features?**

10. What do you see as a disadvantage of setting security features?

11. Are you using the security features? Please explain.

Privacy

12. On a scale of 1-5 (1 – very important, 5 - unimportant), how important is privacy to you?
1. Very important
2. Important
3. Moderately important
4. Of little importance
5. Unimportant

13. Are you aware of the privacy policy of how your data is used by social media providers?
a. Yes
b. No
c. Not applicable

14. Do you care about how your data is being used by social media providers?
a. Yes
b. No
c. Not applicable
d. Haven't given it much thought

15. Is the advantage of having a free social media application greater than the risk of your information being used by the provider or a 3rd party as part of "big data analytics"?
a. Yes
b. No
c. Not applicable

16. Are you comfortable with having your habits tracked by the social media provider for the purpose of having targeted advertising based on your likes and dislikes or preferences?
a. Yes
b. No
c. Not applicable

17. If you answered Yes to #16, why are you willing to give up your privacy?

18. Do you think training should be offered on personal privacy and cyber security awareness?
a. Yes
b. No
c. Don't care

19. If you answered yes to #18, when should training be offered?
a. Freshman
b. Sophomore
c. Junior
d. Senior

Demographics

20. What is your age? _____

21. What is your major? _____

22. What is your level?

a. Freshman
b. Sophomore
c. Junior
d. Senior
e. Other: _____

23. To which gender identity do you most identify?

a. Male
b. Female
c. Transgender female
d. Transgender male
e. Gender variant/non-conforming
f. Not listed _____
g. Prefer not to answer