The Journal of Social Sciences Research
ISSN(e): 2411-9458, ISSN(p): 2413-6670
Special Issue. 6, pp: 839-846, 2018
URL: https://arpgweb.com/journal/journal/7/special_issue
DOI: https://doi.org/10.32861/jssr.spi6.839.846

Academic Research Publishing Group

Original Research Open Access

Security Behaviors on Social Network Sites Used For Academic Purposes: A Comparison of Security Preparedness and Awareness Among IT and Non-IT Postgraduate Students

Somia Moh. T. L. Ashafee[*]
School of Computing, Universiti Utara, Malaysia

Nur Haryani Zakaria
School of Computing, Universiti Utara, Malaysia

Hatim Mohamad Tahir
School of Computing, Universiti Utara, Malaysia

Norliza Katuk
School of Computing, Universiti Utara, Malaysia

Mohd Nizam Omar
School of Computing, Universiti Utara, Malaysia

Abstract

Security and privacy issues are a major concern to users of social network sites (SNS). These issues range from unauthorized access to personal information to cyber bullying. Previous researchers have been exerting different perspectives including technical, psychological and law to study privacy and security issues. However, the issues of security and privacy seems to be ongoing. In view of the security threats and privacy issues of student using SNS, this study sets out to examine the security awareness, preparedness towards cyber-attacks and security behaviors among IT and Non-IT postgraduate students. As such, 400 postgraduate students were surveyed using a self-administered questionnaire. The findings reported in this study revealed that IT students have significantly high security awareness and behavior as compared to Non-IT students. However, there is no significant difference between the preparedness towards cyber-attacks of both IT and Non-IT students. Finally, this study demonstrates that there is a significant relationship between preparedness towards cyber-attacks and security behaviors. The theoretical and practical implications of this study highlight the importance of security awareness and understanding of technical-know how in preempting security attacks among SNS users.

Keywords: Security awareness; Security behaviors; Social network sites.

1. Introduction

The popularity of Social Network Sites (SNS) continues to increase among university students leading to a serious concern in security and privacy issues. University students, especially postgraduates use SNS for myriad of academic purposes which include collaborative learning, accessing learning materials and interacting with instructors and peers (Sattikar and Kulkarni, 2011). As postgraduate students go about these sincere activities, they may be vulnerable to so many security and privacy threats on SNS (Kim, 2013).

It is undoubtable that social network sites such as Facebook, Twitter and LinkedIn are popular among IT and Non-IT students alike (Koloseni, 2015). These sites are beneficial to students in a number of ways including communicating, networking and accessing educational materials. However, information security threats, privacy issues such as cyber-attacks remain a challenge to many users (Orito *et al.*, 2014). In fact, scholar like (Whitman, 2003) have categorized SNS information security threats into human errors, compromises to intellectual property, privacy espionage or trespass, information extortion, sabotage or vandalism, theft, software attacks, forces of nature, quality of service aberration from service providers, hardware and software failures and technological desuetude. However, security threats such as human error, compromises to intellectual property, information extortion, sabotage are vandalism are often caused by users' negligence and errors. Therefore, users are one of the most important focuses in discussing security threats and cyber-attacks. Thus, users are expected to take the personal responsibility of protecting their own privacy and ensure their own security while using SNS (Sherif *et al.*, 2003). However, not many users have the awareness of protecting themselves against information security threats or have the preparedness to take themselves out of cyber-attacks (Kim, 2013).

SNS value the openness, connecting and sharing with others. However, these features of openness fertilize cyber-attacks and encourages cyber criminals. Due to lack of awareness, users often post personal information on social networks which subsequently make them vulnerable to cyber and physical attacks. Previous researchers on

[*]Corresponding Author

social media and SNS information and privacy issues (Beye *et al.*, 2010); (Krasnova *et al.*, 2009) have concluded that majority users are not aware of the risks associated with uploading their personal and sensitive information such as personal data including user names, e-mail addresses, phone numbers, dates of birth and affiliations that are often required for social media and SNS users' registration. Even though, many of the social media and SNS such as Facebook, Twitter, and Instagram have certain security and privacy setting, studies have shown that many of the users are unaware of how to use the privacy settings (Orito *et al.*, 2014).

Studies have shown that the naivetés caused by the lack of preparedness and awareness to security threats are not the same with users who have high level of technological-related education such as IT students(Kim, 2013); (Harris *et al.*, 2014). This is because their trainings must have prepared them to know the amount of information that can be deposited in a public repository like SNS. Furthermore, IT students are also expected to be savvy of privacy and security approaches such as authentication characteristics and installing anti-virus. This expertise might not be the same with non-IT students which further extend their vulnerability to cyber-attacks and security threats. In order to improve privacy and information security, practices promoting good end security behavior is imperative (Koloseni and Omary, 2011). One key step to achieve this, is through security awareness and preparedness assessment (Koloseni, 2015). Therefore, this study examines the preparedness and security awareness of students in relation to their attitude towards security behaviors when using social networks platforms. By working definition IT-students are students taking IT degree and non-IT students are students other than IT-students from the College of Arts and Sciences, UUM. In specifics, this study sets out to achieve the following research questions;

1. To compare between the security awareness of both IT and Non-IT students on SNS.
2. To compare between security behaviors among both IT and Non-IT students on SNS.
3. To compare between the security preparedness towards cyber-attacks among both IT and Non-IT students on SNS.
4. To determine the relationship between security awareness, security preparedness and security behaviors.

2. Literature Review

2.1. Cyber-Attacks and Security Threats on SNS

Koloseni conducted survey among students on their level of awareness towards security threats and risks on SNS (Koloseni, 2015). The study categorized awareness into the following four stages which include; awareness of outcomes of improper operation of social networks, reporting of security incidences, measuring in handling personal sensitive information and taking precautions during accessing social networks. However, the study conducted by Beye *et al.* (2010) relied on the social psychology theory to categorize information security awareness into three stages namely; user knowledge which stands for cognition, attitude which mirrors effect and behavior is represented by the type of actions users take to prevent security threats.

However, an empirical measure for the information awareness and adopted the Kruger and Kearney model to categorize awareness level into levels namely knowledge and behavior (Candiwan and Nurshabrina, 2016). Subsequently, this study approaches the security behavior of users by categorizing it into awareness which represents both knowledge and attitude and preparedness which reflects what users do to prevent security threat.

Information security awareness model explains the level of users' knowledge about the importance of information security best practices while adopting information technologies. Generally, users of SNS have varying levels of security awareness. They are also increasingly engaging in dangerous online activities such as social networking, blogging and instant messaging with a considerable number of users unaware of their exposure to security risks while doing so R. J. Mejias and Balthazard (2014). Users' security behaviors are the primary factor that leads to costly attacks and privacy breaches. Subsequently, the information security awareness model according explains the level of users' knowledge, behaviors and attitude in reacting and preparing to cyber-attacks on SNS (Kearney and Kruger, 2006).

The model of information security awareness is further explained and defined as the degree to which users of SNS understand the importance of security policies, perceive options for appropriate levels of secure behavior and exercise options regarding their responsibility in maintaining the security of their information systems (R. J. Mejias and Balthazard, 2014); (Shepherd *et al.*, 2014); (Hong and Thong, 2013). Bulgurcu defined information security awareness is defined as the users' overall knowledge and understanding of the potential issues and ramifications of information security (Bulgurcu *et al.*, 2010).

Adopting this argument, many security-based studies have highlighted the importance of motivating users of SNS to increase their awareness in preventing of cyber-attacks and security risks via mandatory information security awareness programs (Chen *et al.*, 2012); (Slusky and Partow-Navid, 2012). The underlying argument for suggesting information security program is that, having knowledge and awareness of the possibilities, methodologies and techniques of attacks is an important component in decreasing the vulnerability of users' falling a victim to cyber-attacks and threats (Bulgurcu *et al.*, 2010).

Any user of information system must first of all acquire a significant level awareness of the nature of security threats and the risks that are related to cyber-attacks. Hence, when users perceive a forthcoming security threat, with their adequate knowledge and awareness they will be able to incorporate avoidance behavior to reduce the occurrence or impact of an attack. Therefore, technological education, orientation and training becomes critical for users who are adopting information systems such as SNS to have safe computing experiences (Shepherd *et al.*, 2014).

2.2. Past Studies on Security Awareness, Preparedness and Security Behaviors

A considerable number of studies have examined users' awareness, attitude and preparedness towards privacy issues and security threats on SNS. These studies have focused on different types of security threats and different types of users. However, only few empirical studies have considered the security behaviors of students in spite of the fact that students constitute a noticeable population of SNS users. For instance, Kim (2013) surveyed 800 undergraduate students in a business college. The study employed the information awareness scale suggested by the National Institute of Standard and Technology. The survey focuses on users' attitude and awareness towards information security training, use of anti-virus programs, updating virus definitions and constantly scanning system for new viruses. The findings of Kim (2013) was corroborated by (Bilge *et al.* (2009)) who bemoaned that youngsters on SNS do not care about their privacy settings in SNS.

Similarly, a study by Harris examined and compared the information security awareness of both IT students and IT professionals towards their security concerns in using mile devices (Harris *et al.*, 2014). The study reported certain security concerns that users are failing to address such as failing to secure their personal mobile devices. The results presented in the study further confirmed the argument that users determines the effectiveness of security policies and technologies by their attitude and awareness of implementation (R. J. Mejias and Balthazard, 2014).

A paper by Chewae *et al.* (2015) focused on how personal information is being affected by SNS media and how the privacy become a risk and how to assign security awareness to prevent security breach. They highlighted the current situation on using SNS and threats that can affect the users. The result indicates that security awareness is a significant deterrent to security threats on SNSs. Similarly, it is revealed that teenagers do not focus on the security setting made in SNS (Gangopadhyay and Dhar, 2014). A study on the attitudes of Japanese social media users on the level of their personal data security and personal data handling. The study employed both surveys and interviews to collect data from social media users. The study concluded that, social media users prioritize online socialization to privacy protection and often feel vaguely insecure about their privacy when using social media (Orito *et al.*, 2014).

3. Methodology

A survey research design is employed in this study using a self-administered questionnaire distributed to 400 IT (200) Non-IT (200) respondents at the Universiti Utara Malaysia (UUM). The questionnaires were self-administered in classrooms and library of the university. The survey-instrument in this study was face validated in order to specifically avoid issues of double barreled question and ambiguity in the research instrument. As for construct validity, the result of the pilot study revealed that the Cronbach's Alpha obtained for the items under each variable are reliable. The Cronbach's Alpha for security awareness (0.828), security behaviors (0.899), and users preparedness (0.771) are above the threshold of 0.60 and 0.70. A systematic random sampling technique is employed for selecting an adequate sample size from the total population of both IT and non-IT students at UUM. According to the information obtained from the Student Affairs Department of UUM, there are total number of 5,601 active postgraduate students which are registered across the three academic colleges namely; College of Arts and Sciences (CAS), College of Business (COB) and College of Law, Government and International Studies (COLGIS). The Krejcie and Morgan (1970) sample table was used to determine the sample size for this study. Therefore, the appropriate sample size in this study is 361. Subsequently, 361 is rounded-off to 400 and divided between IT students (200) and Non-IT students (200). Therefore, 400 questionnaires were distributed among 200 IT students and 200 Non-IT students.

Out of the 378 returned questionnaires, 199(99.5%) were IT postgraduate students and 179(89.5%) are Non-IT postgraduate students. However, 13 questionnaires were exempted from this study mainly because the respondents have left more than 50% questions in the questionnaires unanswered. Finally, the analysis of this study is based on 365 respondents which leave the study with 91% response rate. The collected data in this study is analyzed by using the statistical package for social sciences (SPSS) version 22 to answer the research questions of this study. Prior to the main data analysis, data preparation and screening such as coding, data editing, omission and transformation are conducted to ensure that the collected data are qualified to be used for the main data analysis. The specific statistical techniques used are Pearson product-moment correlation which is used to determine the linear relationship between two variables (the independent and dependent variable). This study employs correlation analysis to determine the bivariate relationship between the Security Awareness, User's Attitude towards Security Behavior and User's Preparedness towards Cyber-Attacks. According to Pallant (2011), the strength and the direction of the relationship between the variables is revealed by using Pearson product-moment correlation. Also, the Independent Sample T-Test is used to assess the differences between IT students and non-IT students.

3.1. Measurements of Variables

The following sections present the measurement scales employed for measuring the factors understudied in this study. The variables include security awareness, attitude and preparedness towards cyber-attack and security threats on SNS.

3.2. Security Awareness

As discussed under the literature review section, this study operationalizes security awareness as the level of knowledge of users towards security threats and risks on SNS (Kearney and Kruger, 2006). To measure the security awareness of both IT and non-IT students, Table 1 presents 7 questions adopted from Tuunainen *et al.* (2009) to determine the security awareness of student users of SNS. The questions will be anchored with 5 scales ranging from 1 “Strongly Disagree” to 5 “Strongly Agree”.

Table-1. Measurements for Security Awareness

S/N	Items
1	I am aware of the kinds of people who see my profile on social networking sites
2	I am aware that, I can change my privacy settings on social networking sites
3	I know how to implement security settings on social networking sites
4	I know how to use privacy and security settings on social networking sites
5	I am aware of that if I download an application through my profile on social networking sites, I have given the access to my profile to third party
	I am aware that, social network sites can share my personal information with third parties for marketing purposes
7	I understand the privacy policies of social networking sites

3.2.1. Users Attitude toward Security Behaviors

Users attitude referred to the reactions and approach of students towards security and privacy behaviors on SNS. This operationalization is in line with the information security awareness model (Kearney and Kruger, 2006). Subsequently, 10 questions were adopted from Orito *et al.* (2014) to measure users’ attitude towards security behaviors on SNS. Table 2 presents the items. The questions will be anchored with 5 scales ranging from 1 “Strongly Disagree” to 5 “Strongly Agree”.

Table-2. Measurements for Users’ Attitude towards Security Behaviors

S/N	Items
1	I don’t mind disclosing my personal data such as; name, current locations and address on social networking sites
2	I use my true name and I honestly disclose my personal data as much as possible on social networking sites
3	I only disclose my personal data to my close friends on social networking sites
4	I don’t mind disclosing my real information on social networking sites
5	I have different methods of disclosing my personal information on social networking sites
6	I always modify privacy settings on social networking sites to control the extent of the disclosure of my personal data
7	Only users approved by me can access my personal data on social networking sites
8	I don’t mind clicking on unknown links on social networking sites
9	I don’t mind downloading files or programs from strangers on social networking sites
10	I don’t use browser enabled pop-blocker for social networking sites

3.2.2. Users’ Preparedness towards Cyber-attacks

Users’ preparedness is operationalized as the actions and behaviors that are taken by users of social networking sites to prevent cyber-attacks and security risks. To measure, the types of security behaviors that are practiced by users of SNS, Table 3 presents 9 questions adopted from Hiatt and Choi (2016) to measure users’ preparedness towards cyber-attacks. The responses to the questions are anchored by 5 scale scores ranging from 1 “Extremely Unimportant” to 5 “Extremely Important”.

Table-3. Measurements for Users’ Preparedness towards Cyber-attacks

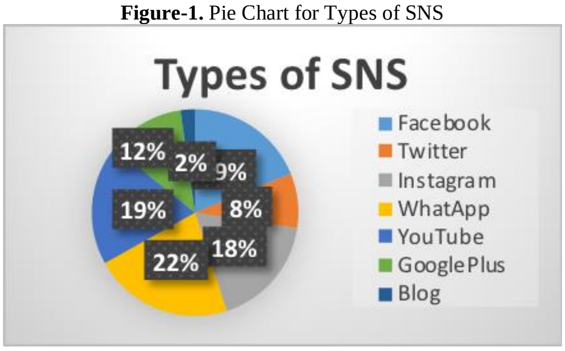
S/N	Items
1	Need for security training before using social networking sites
2	Need of an Internet-security software on your computer before using social networking sites
3	Frequent update of anti-virus software
4	Regular scanning of computer(s) and storage device(s)
5	Installing and enabling a personal firewall
6	Installing software patches whenever available
7	Encrypting important files
8	Frequent changing of password on social networking sites
9	Using different password for different profiles on social networking sites

4. Findings

4.1. Demographic Characteristics of the Respondents

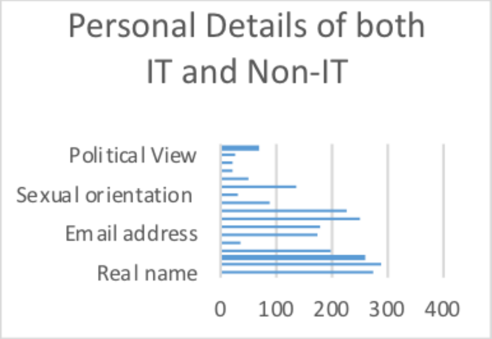
This section presents the demographic profile of the population of respondents surveyed in this study. Majority of the respondents in this study are Female (55.3%) and 44.7% are Male. These findings reflect the real ration of male to female students at UUM, hence there are more female students than male students in UUM. Additionally, the demographic profiling of the respondents in this study reveal that, 342 (90.5%) respondents are less than 25 years old. This is followed by 28(7.4%) respondents who are between 25 and 30 years old. The reaming 8(1.11%) are more than 31 years and less than 60 years old. This distribution reflect that, this study is based on young adult who are expectedly active users of social media networks. Hence, this an indication that the respondents in this study exhibit the representativeness of the targeted population. As expected, the respondents in this study confirm that, they are all post graduate students, 247 (65.3%) are Master students and 129(34.1%) are PhD candidates. Again, this shows the respondents in this study are the expected population in this research. Finally, the demographic profiles also show that, 183 (48.4%) respondents are students from College of Arts and Sciences. This is followed by 157(41.5%) respondents from College of Business and finally, 38(10.1%) are from College of Law, Government and International Studies. Additionally, the researcher examines the level of adoption of SNS among the respondents. To that effect that Figure 2 revealed that, WhatsApp is the most used SNS among the respondents as 22% of both IT and Non-IT students use WhatsApp. This is followed by both Facebook and YouTube by having 19% adoption rate among other SNS. 18% of the respondents adopts Instagram and 12% use Google+. However, Twitter (8%) and Blog (2%) are the both least used SNS among the respondents in this study.

Figure-1. Pie Chart for Types of SNS



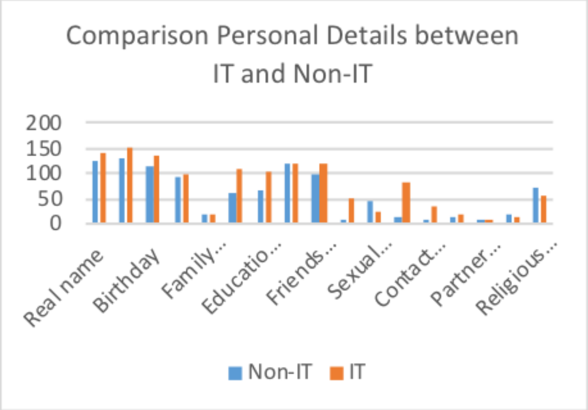
In an attempt to depict the level at which respondents in this study reveal their personal details in SNS. The result presented in Figure 2 show that, more than 250 respondents reveal their; real name, birthday, self-pictures, friend pictures and profile pictures on SNS. Also, more than 50 respondents reveal their favorite entertainment are music, movies and religious views. Meanwhile, the least revealed information among the respondents are political views, family details and relationships status.

Figure-2. Bar Chart for Personal Details of both IT and Non-IT



Surprisingly, Figure 3 demonstrates that, IT students, reveal more personal details as compared with non-IT students. Specifically, the result shows that, IT students reveal more of their real name, profile pictures, email address, self-pictures, friend pictures, favorite entertainment, contact number.

Figure-3. Comparison of Personal Details between IT and Non-IT on SNS



However, it is only religious view that non-IT students revealed more than the IT students. However, it is hard to say that, IT students are more vulnerable to cyber-attacks than the Non-IT students for revealing mush information on their personal SNS platforms. Meanwhile it can be said that, non-IT students have devolved moderate or less personal details on their SNS platforms which indicate that, non–IT students have cautious security behaviors.

4.1.1. The Comparison Security Awareness, Users Attitude and Users Preparedness between among IT and Non-IT Students

To compare the difference between IT students and Non-IT students in terms of their Security Awareness, User's Attitude towards Security Behaviors and User's Preparedness towards Cyber-Attacks. The results revealed that as expected there is a significant higher security awareness (IT Mean = 3.94, Non-IT Mean = 3.63, P<0.01) for IT students as compared to Non-IT students. This provide the basis for accepting H1. This result shows that IT students have higher security awareness when using SNS.

Furthermore, the results demonstrate that there is a significantly higher user awareness towards security behavior as compared to Non-IT students (IT Mean = 3.15, Non-IT Mean = 3.04, P < 0.05). On this basis, H2 is supported. This result indicates that IT students are more cautious of their security behaviors when using SNS. Finally, the results evinced that there is no significant difference between the preparedness towards cyber-attacks of IT students and Non-IT students on SNS. This result reveal that both IT and Non-IT students have a moderate level of preparedness towards cyber-attacks on SNS.

4.1.2. The Relationship between Security Awareness, Security Behavior and Users' Preparedness

The Pearson product-moment correlation analysis was employed in this study to determine the strength and the direction of the bivariate relationship between each of the independent variables (Security Awareness and User Preparedness towards Cyber-Attacks) and the dependent variable (User's Attitude towards Security Behavior) (Pallant, 2011). The result of the correlation analysis is presented in Table 4 below.

Table-4. Pearson Product-Moment Correlation Analysis

Variables		Security Behavior
Security Awareness	Pearson Correlation	.027
	Sig. (2-tailed)	.603
	N	365
User's Preparedness	Pearson Correlation	.144**
	Sig. (2-tailed)	.006
	N	365

Note: **. Correlation is significant at the 0.01 level (2-tailed).

The result presented in Table 4 above, the Pearson product-moment correlation revealed that the relationship between security awareness and security behavior is an insignificant relationship with the coefficient of correlation value (r) = 0.027 (P>0.05). On this basis, H4a is not supported. Meanwhile, relationship user preparedness and security behavior is strong positive and significant relationship with a coefficient of correlation value (r) = 0.144(P<0.01). On this basis, H4b is supported. This result indicates that the variance in security behavior is explained by 14.4% variance in users' preparedness. Therefore, the more preparedness users have towards cyber-attacks, the more favorable attitude they exhibit in their security behaviors.

5. Discussions

The result presented in this study revealed that IT students exhibit high level of security awareness as compared to Non-IT students. This specific result indicates that the research objective one is achieved. The implication of this finding is that IT students have the awareness, the knowledge and the understanding of security and privacy settings on SNS. The result of this study however highlighted the importance of technical knowledge such as IT-related knowledge in protecting users against security attacks on SNS. Furthermore, this result is indicative of the fact that, IT students are cautious of revealing their personal details and they are aware of harmless method and approaches of disclosing their personal information in a manner that is harmless to them. Also, the result shows that because of the technical knowledge of IT students, they do not click on unknown links or download files from unknown source on SNS. These are attitudes which are an implication of IT-related knowledge which moderate the behavior of IT students better than that of Non-IT students to preempt security attacks on SNS. The result reported in this study demonstrates that there is no significant difference between preparedness towards cyber-attacks between IT students and Non-IT students. The implication of this study is that both IT students and Non-IT students have the same level of preparedness in terms of security training, installation of anti-virus software, encryption and so forth. These findings revealed that Non-IT students do not need IT-related expertise before they acquired and implement security tactics while using SNS.

6. Conclusions

The theoretical implications of this study are dynamically numerous. One of the most significant of the implications is that this study provides an empirical evidence to the IT-related expertise of the important role in protecting SNS users against cyber-attacks. Even though the demographic analysis presents in this study evinced that Non-IT students reveal more of their personal information as compared to IT students and IT students have more favorable security behaviors and security awareness. Consequently, this study proffers a bold theoretical implication to explain that devolving more personal information on SNS does not increase the vulnerability of users to security attacks. What actually increase security vulnerability is the approach of revealing these details. Another theoretical implication of the findings reported in this study is that this study provides an empirical evidence to the information security awareness model. Even though, this research could not establish a significant difference between the preparedness towards cyber-attacks among IT and Non-IT students, however this study validates the importance of security awareness as an antecedent to reasonable security behaviors. The revelations reported in this study are in line with the theoretical perspective of information security awareness model which emphasizes on users awareness in terms of understanding of security policies as predicting factor to security behaviors (Hong and Thong, 2013); (Bulgurcu *et al.*, 2010).

Practically, this research has certain contributions and implications that are insightful to stakeholders both in the corporate world and in the academia. As underlined in this study, postgraduate students are the next generation workers. Thus, the security behavior of these students today reflects the security level of tomorrow. Therefore, this study has documented certain auspicious revelation and the reason to remain hopeful about the security level of tomorrow's workers. Furthermore, this study has not aimed to forecast the nature of security attacks on SNS and couldn't suggest that cyber-attacks will subside in the nearest future. However, it is clear that, without IT-related knowledge and expertise, majority of student users of SNS have reasonable level of security awareness, preparedness and reasonable level of security behavior on SNS. Additionally, the result of this study provides an insight for the academia to continuously increase the preparedness of both IT and Non-IT students to prevent them against the current and future security threats on SNS.

This research has been conducted in a cross-sectional survey method which means that data has been collected in one short period. Additionally, it can be noticed that the factors that are examined in this study are not exhaustive especially in terms of the security behaviors of postgraduate students and the factors that predict those behaviors. Finally, the data in this study has been collected from a single source which gives the potential for a common method variance bias. Therefore, based on the use of a longitudinal data of time horizon at which data from this similar study will be collected over a long period of time in order to be able to tell the impact of these factors over time. More so, future studies should also attempt to include more factors such as other attitude variables as part of the factors that can influence responsible security behaviors among postgraduate students on SNS. Finally, researchers may also collect data by using a secondary data to avoid bias as a result of common method bias.

Acknowledgment

The authors would like to express our gratitude to the Ministry of Higher Education (MOHE), Malaysia under FRGS 2014-2 grant S/O 13143, UUM Research & Innovation Management Center (RIMC) and the School of Computing, Universiti Utara Malaysia for funding this research.

References

Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R. and Tang (2010). Literature overview-privacy in online social networks. Available: http://doc.utwente.nl/74094/1/literaturereview.pdf

Bilge, L., Strufe, T., Balzarotti, D., Kirda, E. and Antipolis, S. (2009). All your contacts are belong to us : Automated identity theft attacks on social networks, www 2009. 551–60.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Manag. Inf. Syst. Q.*, 34: 523–48.

Candiwan, P. K. S. and Nurshabrina, N. (2016). Assessment of information security management on Indonesian higher education institutions. 362:

Chen, Y., Ramamurthy, K. and Wen, K. W. (2012). organizations' information security policy compliance: Stick or carrot approach? *J. Manag. Inf. Syst.*, 29(3): 157–88.

Chewae, M., Hayikader, S., Hasan, M. H. and Ibrahim, J. (2015). How much privacy we still have on social network ? *Academia.Edu*, 5(1): 1–5.

Gangopadhyay, S. and Dhar, D. (2014). Social networking sites and privacy issues concerning youths. *Glob. Media J. - Indian Ed.*, 5(1): 1–7.

Harris, M. A., Furnell, S. and Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *J. Inf. Priv. Secur.*, 10(4): 186–202.

Hiatt, D. and Choi, Y. B. (2016). role of security in social networking. *(IJACSA) Int. J. Adv. Comput. Sci. Appl.*, 7(2): 12–15.

Hong, W. and Thong, J. Y. L. (2013). internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Q*, 37(1): 275–98.

Kearney, H. A. and Kruger, W. (2006). A prototype for assessing information security awareness. *Elsevier*, 25(4): 289–96.

Kim, E. B. (2013). information security awareness status of business college: Undergraduate students. *Inf. Secur. J. A Glob. Perspect*, 22(4): 171–79.

Koloseni, D. (2015). Security, privacy awareness VS. Utilization of social networks and mobile apps for learning: Students' preparedness. *Adv. Comput. Sci. an Int. J.*, 4(3): 111–17.

Koloseni, D. and Omary, Z. (2011). Towards using social networks and internet-enabled mobile devices for learning: Students' preparedness. *Communications in Computer and Information Science*, 251 CCIS(PART 1): 13–21.

Krasnova, H., Günther, O., Spiekermann, S. and Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity Inf. Soc.*, 2(1): 39–63.

Orito, Y., Fukuta, Y. and Murata, K. (2014). I will continue to use this nonetheless: Social media survive users' privacy concerns. *Int. J. Virtual Worlds Hum. Comput. Interact*:

R. J. Mejias and Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *J. Inf. Priv. Secur.*, 10(4): 160–85.

Sattikar, A. and Kulkarni, R. (2011). A review of security and privacy issues in social networking. *Int. J. Comput. Sci. Inf. Technol*, 2(6): 2784-87.

Shepherd, M. M. G., Mejias, R. J. and Klein (2014). A longitudinal study to determine the effects of non-technical deterrence on reducing employee internet abuse frequency. *Proc. 47th Hawaii Int. Conf. Syst. Sci.*: 3159–68.

Sherif, J. S., Ayers, R. and Dearmond, T. G. (2003). Intrusion detection: the art and the practice. Part I. *Inf. Manag. Comput. Secur.*, 11(4): 175–86.

Slusky, L. and Partow-Navid, P. (2012). students information security practices and awareness. *J. Inf. Priv. Secur.*, 8(4): 3–26.

Tuunainen, M. H., Virpi, K. and Olli, P., 2009. "Users' awareness of privacy on online social networking sites-case Facebook." In *22nd Bled eConference E-Enablement Facilitating an Open.* p. 42.

Whitman, M. E. (2003). Enemy at the gates: Threats to information security. *Commun. ACM*, 46(8): 91–95.