INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS

Received: 17.12.2020

Accepted: 26.04.2021

Published: 30.04.2021

Citation: Mariani MJP, Wacas RU (2021) A Study on the Social Networking Sites Security Awareness Among Users in Tabuk City. Indian Journal of Science and Technology 14(15): 1212-1218. https://doi.org/10.17485/IJST/v14i15.2019

* **Corresponding author**.

Tel: +639171138690
mpmariani@ksu.edu.ph

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

A Study on the Social Networking Sites Security Awareness Among Users in Tabuk City

Mathew Jun P Mariani[1]*, Ronald U Wacas[1]

1 Kalinga State University, Philippines. Tel.: +639171138690

Abstract

Objectives: To analyze security awareness among social media users in Tabuk City and the relationship when grouped according to gender, educational attainment, age, and years in social media. **Methods/Statistical analysis:** The descriptive correlational research method was utilized to accomplish the study's objectives. A total of 385 respondents were selected using a random sampling of Social Media Users of Tabuk City, Kalinga, Philippines. Statistical Packages for Social Sciences (SPSS) software was used in assessing the frequency and computing the collected data's multivariate test, which determines the relationship of the respondent's response. **Findings**: The study showed a significant relationship between social networking security among users when grouped into gender and educational attainment, while as to age and years in social media, there is no significant relationship. The results revealed that most respondents are vulnerable to threats due to low social networking security awareness. **Novelty**: Social networking can be a form of data exchange that can be exploited. Therefore, this study highlighted the issues and challenges in the vulnerability of social networking site users.

Keywords: Social Network; Security; Awareness

1 Introduction

Social networks have become a popular way of communication for all people around the globe. People use it in various ways, such as meeting old friends, making new friends, sharing and viewing information, and fulfilling their social needs to interact with people. Furthermore, recreating connections with old friends and making new friends allow disclosure of personal information such as name, gender, photos, and age, sharing of contact number, and sexual preferences[(1)]. According to Dr. Ben-Joseph, most teens use social networking platforms and have profiles on a social networking site. They post photos of themselves online or use their real names on their profiles, reveal their birth dates and interests, post their school name and the town where they live. These can make them easy targets for online predators and others who might mean harm to them[(2)].

Social networking sites have been a potential option for perpetrators due to private information availability and broad user base. Security and confidentiality issues in online social networks are now increasing and becoming riskier[3]. The disclosure of this information could set someone at risk as individuals may use it for fraudulent activities, such as identity fraud, credit card applications, or even physical/emotional damage to consumers. However, empirical research has revealed that while users are sometimes aware of the privacy and security issues associated with social networking sites, they do not always have a good grasp of the risks of disclosing information to their online social networks[4].

Several research articles investigated the security flaws and privacy concerns of social networking sites and made recommendations on mitigating security risks[5]. Social media sites responded in improving their security vulnerabilities and made a way that end-users will be reminded of the security status every time they need to log in to the system. However, most users tend to ignore such security reminders. Thereby, the study on security awareness is significant to know the level of awareness of Filipino social networking users.

The number of incidents involving cybercrime is continuously increasing[6–8]. Despite this problem, Eastern Asia and Southeast Asia accounted for the highest and second-highest share of social networking site users worldwide in 2020, respectively[9]. The Philippines is among the most significant numbers of social network users across Southeast Asia, with a social media prevalence rate of roughly 67 percent as of January 2020. Filipinos spend almost four hours a day on social media, on average. One of the reasons that contributed to the increase in social network users was its accessibility. Social networking sites gather millions of data points from users, allowing hackers of all types to gain entry and resulting in cybercrime. As of 2019, over 460 thousand hacking cases had been registered in the Philippines. Given this, the prevalence of social networking sites shows no signs of abating, with most Filipinos stating that they are unlikely to use less social media in the future[10].

The increasing number of cybercrimes caused by irresponsible use of social networking sites needs to be addressed. It is imperative to study users' awareness to educate them on the importance of securing personal information.

With this, a group of respondents with different demographic profiles (educational background, age, and gender) responded to the survey questionnaire about their social networking sites' experiences. The results were analyzed based on the groups of issues relating to the necessary need for awareness, technological awareness, advocacy, and responsiveness to social networking sites' proper use. The research was able to accumulate and evaluate the awareness measurement of social networking sites[11].

2 Materials and Methods

The descriptive correlative method of research was utilized in accomplishing the objectives of the study. Descriptive research is involved in gathering data that describe events and then organizes, tabulates, depicts, and describes the data collected. This research aimed to shed light on SNS users' information disclosure behavior, privacy protection settings, privacy policies, and users' SNS privacy knowledge and awareness. The research was performed using factor analysis to classify the relationship between gender, educational achievement, and age on the scale of personal information disclosure and user-applied protective privacy settings. As a cross-section of social networking platforms, the four most popular SNS sites were chosen, each serving a particular function for the users and audiences of the sites, from predominantly text-based to original video and graphics-based sites such as Facebook, Twitter, Instagram, and Snapchat.

The respondents were selected using random sampling. It will be sampled randomly from the Social Media Users of Tabuk City, Kalinga. It was found that the total number of samples was 385 using the formula n = ((z)^2 p(1-p))/d^2.

Where n= sample size, z = Level of confidence according to the standard normal distribution, p estimated proportion of the population presents the characteristics (when unknown, we use p=0.5, d = tolerated margin of error.

The primary sources of data were a survey questionnaire and interviews with the different end-users. The interview covers the current issues related to securing information, and the survey questionnaire determines the awareness of social networking security among users in the area.

2.1 Statistical analysis

Statistical Packages for Social Sciences (SPSS) software is used to assess the frequency and compute the collected data's multivariate test. The hypothesis of the research problem, if accepted or rejected, was based on Table 1 . Frequency is used to determine the profile of respondents in terms of gender and educational attainment. It was also used to determine the users' responses in Tabuk City on Social Networking Security Sites' awareness.

Table 1. Hypothesis of the research problem

Condition	Decision
P-value > 0.05	Accept the null hypothesis
P-value ≤ 0.05	Reject the null hypothesis

The researchers used this tool to determine the relationship of the respondent's response to social networking sites in terms of gender, educational attainment, age, and years of using social networking.

Hypothesis 1: Is there a significant relationship between gender and social networking security awareness?

Hypothesis 2: Is there a significant relationship between age and social networking security awareness?

Hypothesis 3: Is there a significant relationship between educational attainment and social networking security awareness?

Hypothesis 4: Is there a significant relationship between years of using social media and social networking security awareness?

3 Results and Discussion

Results are classified based on various groups- basic information on social networking awareness, professional awareness on safe social networking, social networking awareness advocacy, and response to events and doubtful accounts on those sites. The results are evaluated based on gender, educational achievement, age, and years of social media [11] [12] [13]. The following present the respondents' profile:

Table 2 shows the number of respondents in terms of gender. It revealed that there were 179 male respondents at 46.5 % and 206 female respondents at 53.5 %. It has a total of 385 valid respondents.

Table 2. Frequency Table on the Profile of Respondents in terms of Gender

Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Male	179	46.5	46.5	46.5
Female	206	53.5	53.5	100.0
Total	385	100.0	100.0	

Table 3 shows the number of respondents in terms of age. It revealed that 169 respondents at 43.9 % range from 15 – 20 years old, 107 respondents at 27.8 % are 15 – 20 years old, 54 respondents at 14 % are 26 – 30 years old, and 55 respondents 14% are more than 31 years old.

Table 3. Frequency Table on the Profile of Respondents in terms of Age

Age	Frequency	Percent	Valid Percent	Cumulative Percent
15 - 20 years old	169	43.9	43.9	43.9
21 - 25 years old	107	27.8	27.8	71.7
26 - 30 years old	54	14.0	14.0	85.7
31 and above	55	14.3	14.3	100.0
Total	385	100.0	100.0	

Table 4 shows the number of respondents in terms of educational attainment. It shows that 174 respondents at 45.2% are in high school, 177 respondents at 46% are college undergraduates, 31 respondents at 8.1% are college graduates, and three respondents at .8% are postgraduates.

Table 4. Frequency Table on the Profile of Respondents in terms of Educational Attainment

Educational Attainment	Frequency	Percent	Valid Percent	Cumulative Percent
High School	174	45.2	45.2	45.2
College Undergraduate	177	46.0	46.0	91.2
College Graduate	31	8.1	8.1	99.2
Post Graduate	3	.8	.8	100.0
Total	385	100.0	100.0	

Table 5 shows the number of respondents in terms of years of using social media. It revealed that 162 respondents at 42.1% range from 3 years and below, 105 respondents at 27.3% are 4 – 6 years, 57 respondents at 14.8 % are 7 – 9 years, and 61 respondents at 15.8% are more than 10 years and above.

Table 5. Frequency Table on the Profile of Respondents in terms of Years of Using Social Media

Years of Using Social Media	Frequency	Percent	Valid Percent	Cumulative Percent
3 years and below	162	42.1	42.1	42.1
4 -6 years	105	27.3	27.3	69.4
7-9 years	57	14.8	14.8	84.2
10 and above	61	15.8	15.8	100.0
Total	385	100.0	100.0	

2. Frequency on the Respondent’s Security Awareness on Social Networking Sites per Classification

Table 6 shows the Frequency Table on the Respondent’s Security Awareness on Social Networking Sites per classification. It revealed that 227 respondents are unaware of the necessary security feature on essential awareness, while 106 are aware. For technical awareness, 274 respondents are unaware of the advanced security feature, while 110 are aware. It was also evident that the majority, whether absolutely or slightly, disagreed with both the claim of asking whether they felt adequate or lacking theoretical/technical awareness to protect their privacy(14). About 2.7% had confidence in their scientific expertise, and only 1.8% had confidence in their technical abilities(14). On awareness advocacy, 129 respondents advocate security threats to other social media users, while 256 do not advocate. Furthermore, on responsiveness, 279 respondents are responsive to threats, while 106 are not.

Table 6. Frequency Table on the Respondent’s Security Awareness on Social Networking Sites per Classification

SOCIAL NETWORKING BASIC AWARENESS SURVEY	Yes	No
Aware of pretenders and are very vigilant (in adding them as your friend)	183	202
Share or post personal information such as phone numbers, home/work address in the profile	195	190
Do you think before posting photos (to avoid it from being exploited)	156	229
Share password with anyone	133	252
Add people as friends only if they are known	156	229
Meet someone whom you have first ’met’ on social networking site	125	260
Average	158	227
SOCIAL NETWORKING TECHNICAL AWARENESS	Yes	No
Use privacy setting of the social networking site	145	240
Install monitoring software to monitor online activities	72	313
Enable privacy setting to restrict who can post and access information on social networking sites	105	280
Enable privacy setting to restrict who can post and access information on sites	119	266
Average	110	274
SOCIAL NETWORKING AWARENESS ADVOCACY	Yes	No
Tell them information about someone who asks or talks about sensitive issues that make them uncomfortable	120	265
Tell them that information posted online cannot be taken back	138	247
Average	129	256
SOCIAL NETWORKING RESPONSIVENESS	Yes	No
Responds to harassing or threatening comments posted on profile?	97	288
Responds if with a reasonable belief that someone is a scam artist or sexual predator on the social networking site?	114	271
Average	106	279

Social Networking Sites users often share personal information that can be used to trace their movements and actions. Most people are unaware that their posts and alerts are public and readily accessible. It is vital to increase their privacy awareness to shield users from potential property loss or tracking [15].

It has been noted that security concerns are very low on social networking sites, and users' attempts to make reasonable improvements to their social media security are considerably low than other types of security operations. In comparison, many social media users lack technical knowledge and have a low degree of security concerns [16]. Thus according to He's findings, many companies lack an effective social media security policy and program and are unaware of how to implement effective social media security policies to mitigate social media security risks [17].

3. Multivariate Test on the responses of the respondents when grouped as to:

Table 7 shows the computed multivariate test on the responses of the respondents as to gender. As shown on the table under Wilks' Lambda, it is revealed that the value is 0.828 with an F-value of 5.488 and a probability value of 0.000, since the p-value is less than 0.05 margin of error. Hence, the null hypothesis is rejected. It means that a significant relationship is evident in the awareness of social networking security grouped as to gender. It further reveals that the responses of males are significantly correlated with the responses of females. Most respondents were also aware of the privacy features of social networking sites, irrespective of gender [11]. Female users are more aware than male users [11], but they are more susceptible to attacks [12]

Table 7. Gender

Multivariate Tests	Value	F	df	Error df	p-value
Pillai's Trace	.172	5.488(b)	14.000	370.000	.000
Wilks' Lambda	.828	5.488(b)	14.000	370.000	.000
Hotelling's Trace	.208	5.488(b)	14.000	370.000	.000
Roy's Largest Root	.208	5.488(b)	14.000	370.000	.000

Table 8 shows the computed multivariate test on the responses of the respondents as to age. As shown on the table under Wilks' Lambda, it revealed that the value is 0.865 with an F-value of 1.298 and a probability value of 0.099 since the p-value is more significant than the 0.05 margin of error; hence, the null hypothesis is accepted. It means that there is no significant relationship between social networking security awareness when the respondents are grouped according to age. It further revealed that respondents' responses to their age are insignificantly correlated to other respondents' age. However, Al Johani emphasized in his Masteral thesis that age has indicated a significant effect on privacy/security, such as self-disclosure habits and privacy setting applications [18].

Table 8. Age

Multivariate Tests	Value	F	Hypothesis df	Error df	Sig.
Pillai's Trace	.139	1.287	42.000	1110.000	.106
Wilks' Lambda	.865	1.298	42.000	1092.430	.099
Hotelling's Trace	.150	1.310	42.000	1100.000	.091
Roy's Largest Root	.103	2.712(c)	14.000	370.000	.001

Table 9 shows the computed multivariate test on the responses of the respondents as to Educational Attainment. As shown on the table under Wilks' Lambda, it revealed that the value is 0.834 with an F-value of 1.641 and a probability value of .007, since the p-value is less than 0.05 margin of error. Hence, the null hypothesis is rejected, resulting in a significant relationship on social networking security awareness when grouped according to educational attainment. According to Albladi & Weir, the educational level has no substantial effect on users' vulnerability, as shown by the regression study of the susceptibility to attacks [12].

Table 9. Educational Attainment

Multivariate Tests	Value	F	Hypothesis df	Error df	Sig.
Pillai's Trace	.175	1.633	42.000	1110.000	.007
Wilks' Lambda	.834	1.641	42.000	1092.430	.007
Hotelling's Trace	.189	1.649	42.000	1100.000	.006
Roy's Largest Root	.112	2.956(c)	14.000	370.000	.000

Table 10 the computed multivariate test on the respondents' responses to using social media. As shown on the table under Wilks' Lambda, it revealed that the value is 0.886with an F-value of 1.088 and a probability value of 0.970 since the p-value is higher than the 0.05 margin of error. Hence, the null hypothesis is accepted. It suggests no significant association with social networking security knowledge when grouped based on the years of using social media. It further revealed that respondents' responses to their years of using social media are insignificantly correlated to other respondent's years of using social media.

Table 10. Years of using social media

Multivariate Tests	Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power(a)
Pillai's Trace	.118	1.083	42.000	1110.000	.334	.039	45.470	.971
Wilks' Lambda	.886	1.088	42.000	1092.430	.325	.040	45.185	.970
Hotelling's Trace	.125	1.094	42.000	1100.000	.317	.040	45.940	.973
Roy's Largest Root	.082	2.174(c)	14.000	370.000	.008	.076	30.433	.967

4 Conclusion

Most of the respondents are vulnerable to threats due to low social networking security awareness, which is also evident in some researches. Also, it shows that the computed multivariate test on the respondents' responses has a significant relationship to social networking security awareness when respondents are grouped as to gender and educational attainment. On the other hand, age and years of using social media have no significant relationship. It is a manifestation of the need to strategize dissemination of knowledge to educate people about the necessity of being vigilant in securing their social networking platforms.

Further, the researchers will conduct information dissemination to capacitate social media users. It will be a collaboration between the government and private sectors.

References

1) &amp; Lawler J, Molluzzo J. A Study of the perceptions of students on privacy and security on Social Networking Sites (SNS) on the internet. *Journal of Information Systems Applied Research*. 2010.
2) Ben-Joseph EP. Teaching Kids to Be Smart About Social Media (for Parents) - Nemours KidsHealth. 2018. Available from: https://kidshealth.org/en/parents/social-media-smarts.html.
3) Krubhala P, Niranjana P, Priya GS. Online Social Network - A Threat to Privacy and Security of Human Society. *International Journal of Scientific and Research Publications*. 2015;5(4):1–6. Available from: http://www.ijsrp.org/research-paper-0415/ijsrp-p40119.pdf.
4) Raynes-Goldie K. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*. 2010;15(1). Available from: https://doi.org/10.5210/fm.v15i1.2775.
5) Alqubaiti ZY. The Paradox of Social Media Security: A Study of IT Students' Perceptions versus Behavior on Using Facebook. 2016. Available from: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1003&context=msit_etd.
6) Interpol. COVID-19 Cybercrime Analysis Report. 2020. Available from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
7) Milkovich D. 15 Alarming Cyber Security Facts and Stats. 2021. Available from: https://www.cybintsolutions.com/cyber-security-facts-stats/.
8) Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*. 2014;80(5):973–993. Available from: https://dx.doi.org/10.1016/j.jcss.2014.02.005.
9) Sanchez MJ. Social media usage in the Philippines - statistics & facts. Statista. 2020. Available from: https://www.statista.com/topics/6759/social-media-usage-in-the-philippines/.
10) Tankovska H. Number of worldwide social media users 2020, by region. Stastica. 2021. Available from: https://www.statista.com/statistics/454772/number-social-media-user-worldwide-region/.
11) Ishak I, Sidi F, Jabar MA, Sani NFM, Mustapha A, Supian SR. A survey on Security Awareness among Social Networking Users in Malaysia. *Australian Journal of Basic and Applied Sciences*. 2012;6(12):23–29.
12) Albladi SM, Weir GRS. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*. 2020;3(1):1–19. Available from: https://dx.doi.org/10.1186/s42400-020-00047-5.
13) Jordan K. Academicss Awareness, Perceptions and Uses of Social Networking Sites: Analysis of a Social Networking Sites Survey Dataset. *SSRN Electronic Journal*. 2014;p. 1–29. Available from: https://dx.doi.org/10.2139/ssrn.2507318.
14) Zolait AHS, Anizi RRA, Ababneh S, BuAsalli F, Butaiba N. User awareness of social media security: the public sector framework. *International Journal of Business Information Systems*. 2014;17(3):261–261. Available from: https://dx.doi.org/10.1504/ijbis.2014.064973.
15) Nyoni P, Velempini M. Privacy and user awareness on Facebook. *South African Journal of Science*. 2018;114(5/6):1–5. Available from: https://dx.doi.org/10.17159/sajs.2018/20170103. doi:10.17159/sajs.2018/20170103.
16) N SK, K S, K D. On Privacy and Security in Social Media – A Comprehensive Study. *Procedia Computer Science*. 2016;78:114–119. Available from: https://dx.doi.org/10.1016/j.procs.2016.02.019. doi:10.1016/j.procs.2016.02.019.
17) He W. A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*. 2012;14(2):171–180. Available from: https://doi.org/10.1108/13287261211232180.

18) Johani MA. Personal Information Disclosure and Privacy in Social Networking Sites. 2016. Available from: https://core.ac.uk/download/pdf/80334091.pdf.