Available online at ijci.wcci-international.org

International Journal of Curriculum and Instruction 16(1) (2024) 175–190

IJCI
International Journal of Curriculum and Instruction

Personal privacy and cyber security: Student attitudes, awareness, and perception on the use of social media

Jose Niño Sales [a] *, Ryan Tiongco [b], Simin Lu [a], Mary Jane Ruiz [c], Jocelyn Cruz [d], Maricar Prudente [e]

[a] *College of Educaiton, De La Salle Araneta University, Malabon City, Philippines*
[b] *Department of Dentistry, Centro Escolar University, Makati City, Philippines*
[c] *College of Arts and Letters, University of Makati, Makati City, Philippines*
[d] *Department of Commercial Law, De La Salle University, Manila, Philippines*
[e] *Department of Science Education, De La Salle University, Manila, Philippines*

Abstract

Students now a days are described as the generation that cannot live without using social media. It is patent that using social media platforms are already part of our daily activities to help provide for our needs, interests, leisure, and other purposes. Descriptive design using mixed method approach was utilized to examine the attitude, perception, and awareness of students (N=384) focused on personal privacy and cybersecurity with use of social media. The data collected from the students of different grade level from elementary up to college were organized, analyzed, and interpreted to understand how students' demographic profile and their experiences affect their attitude, perception, and awareness towards personal privacy and cybersecurity on the use of social media and to identify if there are differences between groups. The findings revealed that the students have a positive attitude towards the use of social media and perceive trust with social media providers. Students were expressed awareness on how to protect their personal privacy and utilize cybersecurity features available for their social media account. Further, this study found significant differences on students' level of awareness concerning personal privacy and security between age group and educational level. Those who are on higher educational level and with older age express higher level of awareness when using social media when personal privacy and cybersecurity is concern.

Keywords: Personal privacy; cyber security; awareness; perception; attitude; social media

* Jose Niño Sales. ORCID ID.: https://orcid.org/0000-0003-3330-3836
E-mail address: nino.sales@dlsau.edu.ph

1. Introduction

Students have become aware of the use of social media especially during this pandemic. Schools continue to see value in using video conferencing platforms and other applications including social media even remote learning restrictions have eased (Sander, 2022). Within the context of this study, social media is a form of electronic communication (as websites for social networking and microblogging) through which users create online communities to share information, ideas, personalized messages, and other content (as videos). Privacy is defined as the state of being alone or kept apart from others. Cyber Security is defined as being protected by internet-connected systems, including hardware, software, and data, from cyberattacks. In a computing context, security comprises cyber security and physical security. Both are used by enterprises to safe against unauthorized access to data centers and other computerized systems. The security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of cyber security (Seemma et al., 2018).

Digital devices and similar tools can enhance students' experience during their educational journey. While most teachers are concerned about students being distracted by phones and laptops, few think about data privacy and security (Llego, 2022). Given the increasing frequency of cybersecurity incidents among students, there are limited programs in school that teaches students how protect their data and privacy. As data security and privacy are inseparable (Sander, 2022), the purpose of the research is to describe the perception, awareness and attitudes of the students related to data privacy and cyber security in the use of social media. Using mixed method approach, the study will identify the differences between demographic variables and analyzes factors related to perception, attitude, and awareness of the students related to cybersecurity and personal privacy. Specifically, the study seeks to answer the following questions:

1. What are the students' attitude towards;
   1.1. cybersecurity?
   1.2. data privacy
2. What are the students' perceptions about;
   2.1. cyber security
   2.2. data privacy
3. What is the students' level of awareness about personal privacy?
4. Is there a significant difference in the students' level of awareness about data privacy when grouped according to;
   4.1. gender
   4.2. grade level

4.3. age

5. What are the factors that contribute to the students' attitudes on cybersecurity and personal privacy?
6. What are the factors that contribute to the students' perception about cybersecurity and personal privacy?

1.1. Data privacy trend

We are living in an era of big data, where the process of generating data has continuously been taking place with each coming second. The data structure is more diverse, and the data itself is more complex (Naeem et al., 2021). In the context of this era, digital information and the economy are closely linked and cannot be separated. After all, linking with economic interests will always increase the difficulty of supervision, and the frequent emergence of more new technologies also puts the protection of data privacy in a dilemma. According to Yang et al. (2020), traditional networks in cloud storage systems also have security threats such as data destruction, data theft, data tampering, and denial of service, which affect the secure storage of data. From overall view, Dimodugno et al. (2021) cites that a key issue with data privacy is that big data analytics methods allow users' data to be generated, stored, and processed illegally, and users have little control over their personal information. In addition, Liu et al. (2020) stated that new technological developments have also brought benefits to data privacy, such as Blockchain is a promising distributed ledger technology that prevents malicious data tampering and provides reliable data storage. As the amount of data generated increases and cloud usage becomes more and more mainstream, blockchain technology is expected to become an important presence in data privacy protection. Therefore, data privacy is very important. New technologies bring difficulties and improvements at the same time. Technicians must also keep up with the rhythm of technological updates. Otherwise, once data privacy is violated, it will bring huge risks and losses.

1.2. Cyber Security trend

Nowadays, both people's daily life and enterprises and governments are inseparable from the use of the Internet. While the Internet brings us convenience, danger also comes with it. Network security is a very important topic at present. Himanshu et al. (2022) says that protecting the security of data and information systems is the goal of network security, and there are many risks in the data network world that need to be vigilant. Today's prevalence of cybercrime based on smartphones and personal devices underscores the need for cybersecurity. With more technological innovations, Samtani et al. (2020) mentioned that it is important to be proactive in responding to emerging

cybersecurity issues. Artificial intelligence (AI) has quickly become a viable approach to sift through terabytes of heterogeneous cybersecurity data with extreme efficiency and effectiveness for threat detection, classification, control assignment, vulnerability management and other basic network security tasks, although artificial intelligence in cybersecurity disciplines is still in its infancy. Juneja et al. (2021) also said that AI is capable of accumulating, classifying and detecting large volumes of data and allowing organizations to extract more valuable utility from the data. These attributes have been used in cyber security sector. With the development of new technologies and market applications, the trend of network security has become increasingly complex and important, and the risks are also increasing, but at the same time, network security also has the application of various new technologies, and the overall trend of rapid development.

1.3. Perception of students in data privacy and cyber security

Students, as the most active users of the Internet, have a higher degree of acceptance of new technologies and new products. Their attitudes towards data privacy and network security are more important and have reference significance. The more complex the system, the more important and necessary it is to maintain data privacy, especially when students are mainly involved in the system interaction. In most cases, data breaches and digital misconducts occur among students due to lack of cyber security knowledge and awareness and consequences of cyber-crimes (Alharbi & Tassaddiq, 2021). Students' lack of knowledge about network security is one aspect, and their attitude towards data privacy is also worthy of attention,78% of the students indicated that they are currently using the security features on social media platforms to address potential technical risks, but 52% of the students indicated that they are willing to sacrifice personal privacy to obtain the functions of social platforms, which is worthy of vigilance. (Bhatnaga & Pry, 2020). Therefore, students attach great importance to data privacy and network security, and have a clear understanding, but they have insufficient knowledge of relevant knowledge, but they are enthusiastic enough to learn this knowledge, which also proves that data privacy and security are important in the minds of students.

1.4. Perception of students in data privacy and cyber security

Perceptions of online data privacy, whether in terms of concern, control, and confidence, are strongly related to the context in which the questions are asked. Attitudes towards data privacy are carefully explored in the literature through specific measures, which also contributes to the degree of variance in findings. Just like what was discovered in Petrova (2021) study found out that surveys among students show that very few students are willing to provide their private data for tailored training and possible referrals. Most students prefer to do this by providing information such as

academic background and study experience information, while remaining anonymous. Also, New Survey Research Conducted in Partnership with Freedom Pay and Cornell University Highlights Gen Z's Attitudes on Data Privacy and Sharing (2022), which surveyed 200 Cornell Generation Z students, – The perceived privacy security level of a piece of information was found to have a significant impact on participants' willingness to share it with third parties, such as financial institutions and telecommunications institutions, among others.

1.5. Perception of students in data privacy and cyber security

Many believe that students are increasingly aware of the use of technology. But only a few have knowledge about their security privacy. This is very worrying because most people in this age group spend most of their school and *lifetime* online. Today these students are not only users of data products and online platforms, students of online learning, but tomorrow may be software engineers, technology entrepreneurs, and professionals in other fields that are integral to privacy conversations. These students' attitudes toward data privacy will most likely influence the policies and practices that govern the Internet (Park &Vance, 2021). Brook (2016) EDUCAUSE Center for Analysis and Research (ECAR) survey found that one-third of undergraduate students were "concerned that technology advances may increasingly invade their privacy". Fleming & Adkins (2015) in Gallup poll in also found that 44 percent of Millennials believe their personal information is kept private "some of the time" and that 26 percent believe their personal information is kept private "little" or "none of the time." Studies and surveys indicate that students are wary of privacy risks and value privacy protections. As is widely reported in the media, cyber-attacks are increasing in quantity and sophistication. Students are also not exempt from this problem. Chandarman & Niekerk (2017) found in their study that the 56% of the respondents have a serious lack of knowledge about phishing, 56% of the respondents answered incorrectly or do not know at all, know very little about the use of antivirus software, and 43% of the respondents answered incorrectly or not at all Know. Respondents' knowledge of phishing and antivirus software is woefully inadequate. This lack of knowledge is very likely to lead to some unsafe practices and may be exploited by cybercriminals to carry out criminal activities. These are just a few studies to show that students' use of technology is indeed included in their daily activities.

2. Method

This section will narrate how the study was conducted in terms of its research design, participants, instrument used, data gathering procedure, and analysis.

2.1. Research design

This descriptive study utilized the mixed method research design wherein qualitative results were used to supplement the interpretation of the quantitative study. Quantitative research uses surveys and questionnaires to seek a precise analysis on the awareness of students on cybersecurity and data privacy thus quantifying the generated statistical data for more efficient delivery and analysis. Qualitative on the other hand investigates the attitudes and perception of the respondents' regarding data privacy and cybersecurity in the use of social media.

2.2. Research Participant

Different year levels were targeted as respondents. Three hundred eighty-four (384) students participated and answered the questionnaires. Informed consent and declaration of privacy were attached to the letter of invitation and questionnaires.

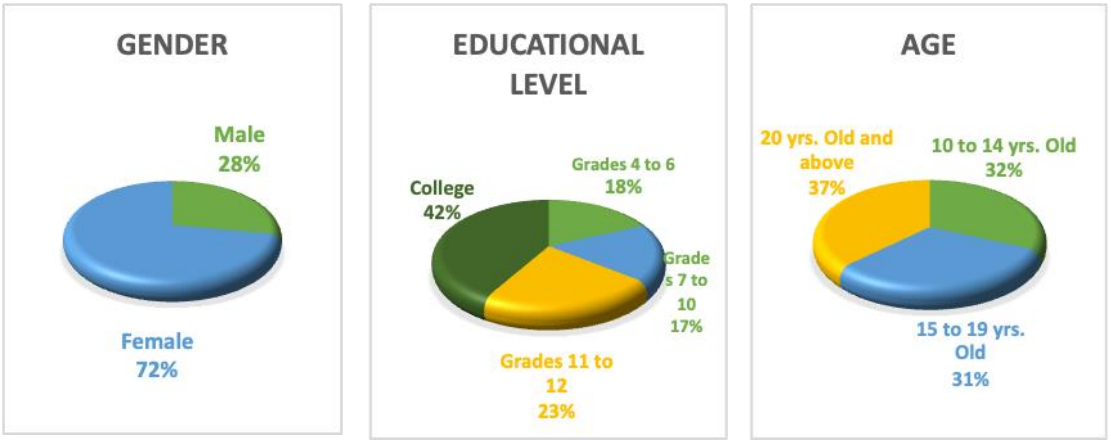

Figure 1. Distribution of respondents according to demographic profile

Figure 1 revealed that in terms of gender majority are female (72%) compared to male (28%). In terms of educational level, almost half were college (42%), nearly quarter of the respondents were from grades 11 to 12 (18%), the least were followed by grades 4 to 6 (18%) and grades 7 to 10 (17%) with closely equal distribution. Further, dis-attribution of the respondents according to the age group are closer to one another.

2.3. Research instrument

The researchers used and patterned the survey questionnaires for awareness level on data privacy conducted by Santos et.al (2017) and the students' attitudes and perception on privacy and cybersecurity from the initial study of Bhatnagar and Pry (2020). The

survey questionnaire was prepared using google forms and divided into four parts namely: Demographic profile of the respondents, attitudes, perception in cyber security, and awareness towards personal privacy in the use of social media.

2.4. Data gathering

Consent from school heads was secured before gathering data. The survey questionnaires in Google form were distributed with the help of subject teachers and accessed online by the students for 2 weeks across different level from grade 4 up to college. There were no exclusion criteria set. Each student was allowed to complete and answer the questionnaire once. All respondents were fully informed about the objectives of the study and agreed to voluntarily participate.

2.5. Data analysis

Data from the survey for students' attitudes, awareness and perception about personal privacy and cybersecurity in the use of social media were summarized and organized in tabular form using descriptive statistics. Frequency, percentage, mean and standard deviation per item were calculated to describe the identified variables. To identify if there is a significant difference between gender on personal privacy awareness of the respondents, independent sample t-test was used. One- way ANOVA was performed to compare if three age groups and four educational level groups differ on personal privacy awareness level with the use of social media. The answers on the open-ended questions that required a text response, a consolidation process was used to synthesize the responses and collaboratively read, coded, categorized, and thematically analyzed.

3. Results and Discussion

In the section, summary of the collected data and the analysis performed were presented and relevant results were discussed.

3.1. Students' attitude on cybersecurity

Table 1. Students' attitude towards

		Grades 4-6 (n = 70)		Grades 7-10 (n = 67)		Grades 11-12 (n = 87)		College (n = 160)		Total (N = 384)	
		f	%	*f*	%	*f*	%	*f*	%	*f*	%
1. Do you use social media?	Yes	70	100	67	100	87	100	160	100	384	100
	No	0	0	0	0	0	0	0	0	0	0
	Not applicable	0	0	0	0	0	0	0	0	0	0
3. Are you aware of security features offered	Yes	65	93	56	84	82	94	145	91	348	91
	No	2	3	10	15	5	6	15	9	32	8

by social media providers?	Not applicable	3	4	1	1	0	0	0	0	4	1
5. Do you see a risk with your social media profile being public?	Yes	48	69	57	85	73	84	119	74	297	77
	No	18	26	6	11	12	14	34	21	70	18
	Don't care	5	7	2	4	2	2	5	3	14	4
	Not applicable	1	1	2	4	0	0	2	1	5	1
6. Do you know how to navigate the social media system setting and set the security option that are available?	Yes	59	84	57	85	77	89	134	84	327	85
	No	9	13	9	13	9	10	24	15	51	13
	Not applicable	2	3	1	1	1	1	2	1	6	2
7. Have you been a victim of a cyber security attack, breach, or loss of privacy?	Yes	16	23	12	18	21	24	40	25	89	23
	No	51	73	55	82	65	75	119	74	171	45
	Not applicable	3	4	0	0	1	1	1	1	5	1

Results shows that all students participated in this study uses social media. Majority of the students indicate awareness of security features offered by social media providers (91%), that they see risk with their social media being public (77%), and that they know how to navigate system setting and security option for their social media account (85%). However, given these responses, there are still notable incidents (23%) of cyber security attack, breach, or loss of privacy among the students.

Table 2. Social media brand most frequently used by the students.

Social Media Brand	Grades 4-6 (n = 70)		Grades 7-10 (n = 67)		Grades 11-12 (n = 87)		College (n = 160)		Total (N = 384)	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%
Facebook	62	89	59	88	76	87	151	94	348	91
Instagram	1	1	2	3	1	1	4	3	8	2
Snap chat	2	3	2	3	1	1	1	1	6	2
Twitter	1	1	2	3	7	10	3	2	13	3
Others	4	6	2	3	2	3	1	1	11	3

Table 2 shows that majority (91%) of the students frequently use Facebook brand as social media platform among others. This supports the report of Statista Research Department (2022) that in the recent year 2020, 70 percent of the Filipino population are Facebook users.

Table 3. Current social media account profile status of the students.

Social media status	Grades 4-6 (n = 70)		Grades 7-10 (n = 67)		Grades 11-12 (n = 87)		College (n = 160)		Total (N = 384)	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%
Public	36	51	20	30	26	30	63	39	145	38
Private	28	40	46	69	60	69	89	55	223	58

Don't Know	4	6	1	1	1	1	6	4	12	3
Not Applicable	2	3	0	0	0	0	2	1	4	1

Shown in Table 3 is the distribution of the respondents' social media status according to educational level being public (28%), private (58%), Don't Know (3%), and not applicable (1%). Further it can be observed that the number of students having a public status in social media is higher among Grades 4-6 (51%) and lower among Grade 7-10 (30%) and Grade 11- 12 (30%) students.

3.2. Students' attitude on personal privacy

Table 4. Students' attitudes towards personal privacy in social media.

Indicators	Response	Grades 4-6 (n = 70)		Grades 7-10 (n = 67)		Grades 11-12 (n = 87)		College (n = 160)		Total (N = 384)	
		f	%	*f*	%	*f*	%	*f*	%	*f*	%
On a scale of 1-5 (1 - very important, 2 - important, 3 - moderately important, 4 - of little importance, 5 - unimportant), how important is privacy to you?	Very important	44	63	54	81	65	75	116	73	279	73
	Important	7	10	4	6	11	13	19	12	41	11
	Moderately important	6	9	0	0	3	3	6	4	15	4
	Of little importance	4	6	1	1	0	0	9	6	14	4
	Unimportant	9	13	8	12	8	9	10	6	35	9
Are you aware of the privacy policy of how your data is used by social media providers?	Yes	53	76	50	75	76	87	132	83	311	81
	No	15	21	16	24	10	11	26	16	67	17
	Not applicable	2	3	1	1	1	1	2	1	6	2
Do you care about how your data is being used by social media providers?	Yes	43	61	55	82	60	69	123	77	281	73
	No	9	13	3	4	2	2	6	4	20	5
	Haven't given it much thought	18	26	8	12	24	28	30	19	80	21
	Not applicable	0	0	1	1	1	1	1	1	3	1
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"?	Yes	34	49	31	46	40	46	82	51	187	49
	No	20	29	30	45	30	34	68	43	148	39
	Not applicable	16	23	6	9	17	20	10	6	49	13
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	19	27	8	12	11	13	33	21	71	18
	No	43	61	56	84	72	83	118	74	289	75
	Not applicable	8	11	3	4	4	5	9	6	24	6
Do you think training should	Yes	5	84	65	97	79	91	147	92	350	91

Indicators	Response	Grades 4-6 (n = 70)		Grades 7-10 (n = 67)		Grades 11-12 (n = 87)		College (n = 160)		Total (N = 384)	
		f	%	*f*	%	*f*	%	*f*	%	*f*	%
be offered on personal privacy and cyber security awareness?		9									
	No	6	9	1	1	3	3	9	6	19	5
	Don't care	5	7	1	1	5	6	4	3	15	4

To describe students' attitude on personal privacy questions were grouped according to educational level (Table 4). For the indicator "how important is privacy to you?", Most of the student (73%) responses fall under "very important" and highest among grade 7-10 students (81%). For other indicators related to giving importance to personal privacy, majority of students answers are "Yes" such as "Are you aware of the privacy policy of how your data is used by social media providers? (81%), Highest among grades 11-12, "Do you care about how your data is being used by social media providers? (73%)", highest among grades 7-10, and "Do you think training should be offered on personal privacy and cyber security awareness? (91%)", highest among grade 7-10. In addition, the advantage of having a free social media application is greater for the students (49%) than the risk of your information being used by the provider or a 3rd party as part of big data analytics while for others it is No (39%). However, majority of the students (75%) mostly from grades 7-10 expressed that they are not comfortable being tracked by social media providers for the purpose of having targeted advertising based on your likes and dislikes or preferences.

3.3. Students' perception on cyber security

Most of the students (98%) perceived the positive benefits of setting security features in social media. Giving importance to setting security features increase protection from cyber-attack and it make them feel safe. According to one student, "I believe that setting security features in my social media account will protect my account from being hacked and prevent other people from accessing information that I don't want to disclose in public." In addition, majority of the students (89%) perceived no disadvantage in setting security features. However, there are some students (6%) who expressed that they believed to be disadvantage of setting security features such as having a hard time to retrieve your password when you forgot, it limits the users network opportunity and the time it consumes in setting up the security features. According to one student "Setting security features can also mean setting boundaries, so it will start to limit the choices you have for being in a social media platform. What's more is that it will take a very long time to sign in through a different gadget since it has set so many boundaries". Students'

main purpose in setting security features is to protect their account from hackers while other tend to filter and customize the security features at their own preference.

3.4. Students' perception on personal privacy

On students' perception about personal privacy, only few students (16%) answered the question "Why are you willing to give up your privacy" this is pertaining as a follow-up question related to "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"? which majority of the students (49%) answered "yes" and mostly college students. Students emphasize that they are not willing to just give up their privacy, but some also consider the benefit of tracking their activities just to have them more options in terms of their preferences.

3.5. Students' awareness on personal privacy

Table 4. Students' Level of awareness about data privacy (N=384).

	Indicators	Always		Sometimes		Seldom		Never		*M*	*SD*
		f	%	*f*	%	*f*	%	*f*	%		
1.	My parents check my social media account.	25	7	106	28	107	28	146	38	2.03	0.96
2.	I post informative matters on social media such us political issue.	38	10	137	36	76	20	133	35	2.23	0.03
3.	I browse social media to check on my relatives or friends' account.	92	24	184	48	79	21	29	8	2.89	0.86
4.	I stalk people by means of social media.	46	12	125	33	108	28	105	27	2.30	1.00
5.	I gossip by means of social media.	35	10	94	24	99	26	156	41	2.03	1.01
6.	I use social media only for educational purposes.	76	20	185	48	85	22	38	10	2.78	0.88
7.	I accept friend request/s from people that I don't know as long as there are mutual friends.	13	3	64	17	100	26	207	54	1.70	0.87
8.	I post criticisms pertaining to someone indirectly on social media.	6	2	28	7	63	16	287	75	1.36	0.70
9.	I argue with anyone on social media.	4	1	19	5	68	18	293	76	1.32	0.63
10.	I post malicious and scandalous images on social media.	3	1	10	3	9	2	362	94	1.11	0.46

Shown in Table 5 is the awareness level of the student described by the distribution of the students' responses on the given indicators. Results shown that the indicator "I browse social media to check on my relatives or friends (M = 2.89, SD = .86)" has the highest average rating followed by "I use social media only for educational purposes (M = 2.78, SD = .88)". This means that most of the main reason students use social media is to check on their relatives and friends and also to acquire information that can be useful in their studies. Further, indicators "I post malicious and scandalous images on social media (M = 1.11, SD = .46)" and "I argue with anyone in social media (M = 1.32, SD = .63)" has the lowest mean scores. This means that students' least priority in using social

media is making arguments with someone and posting malicious and scandalous contents.

3.6. Test for significance between gender, educational level, and age

Table 6. Independent sample t-test for student' level of awareness according to gender.

Gender	*n*	*M*	*SD*	*t*	*df*	*p*
Male	107	2.05	.40	2.31	382	.99
Female	277	1.94	.41			

To identify if there is a significant difference between gender in terms of awareness level of the student, an independent sample t-test was used. Results shown that there is no significant difference on the level of awareness about personal privacy in the use of social media of male (M = 2.05, SD =. 40) compared to female (M = 1.94, SD = .41), $t(382) = 2.31$, p = .99.

Table 7. Education level descriptive statistics.

	n	*M*	*SD*
Grades 4 to 6	70	1.92	.46
Grades 7 to 10	67	2.05	.37
Grades 11 to 12	87	2.06	.39
College	160	1.92	.40
Total	384	1.98	.41

Table 7 shows the descriptive data for educational level. Among the identified groupings of educational level, we can observe that highest awareness mean score are highest in the middle group of grades 7 to 10 (M = 2.05, SD = .37) and grades 11 to 12 (M = 2.06, SD = .39).

Table 8. One-way ANNOVA for students' level of awareness according to educational level.

	Sum of sq.	*df*	M^2	*F*	*p*
Between Groups	1.84	3	.613	3.77	.01
Within Groups	61.82	380	.163		
Total	63.66	383			

An analysis of variance showed that the educational level was significant, $F(3, 380) = 3.77$, p = .01, on students' level of awareness. Post hoc analyses using the Tukey post hoc criterion for significance indicated that the students' average level of awareness was significantly higher in high school level than in the college level (p = .04). There is no significance identified among other educational levels.

Table 9. Age descriptive statistics.

	n	*M*	*SD*
10 to 14 yrs. old	122	1.98	.43
15 to 19 yrs. old	119	2.06	.40
20 yrs. old and above	143	1.90	.38
Total	384	1.97	.41

Table 9 shows the descriptive statistics of the respondents according to age. We can observe that the age group with the highest mean score is the group of 15 to 19 years old (M = 2.06, SD = .40) and 20 years old and above (M = 1.90, SD = .38) with the lowest mean score. This indicates that those who are 20 years old and above are more aware of personal privacy and use social media accordingly compared to the other groups with the ages 15 to 19 years old as the least aware.

Table 10. One-way ANNOVA for student' level of awareness according to age.

	Sum of sq.	*df*	M^2	*F*	*p*
Between Groups	1.84	2	.810	4.976	.007
Within Groups	61.82	381	.163		
Total	63.66	383			

A one-way ANOVA revealed that there was a statistically significant difference in mean awareness level between age groups, $F(2, 381) = 4.98$, p = .007. Tukey's HSD Test for multiple comparisons found that the mean value of awareness level was significantly different between 15 to 19 yrs. old and 20 yrs. old and above, p = .05, 95% C.I. = [.040, .275]. There was no statistically significant difference in mean exam scores between 10 to 14 yrs. old and 15 to 19 yrs. old (p = .27) or between 10 to 14 yrs. old and 20 yrs. old and above (p = .27).

3.7. Factors that contribute to the students' attitudes on cybersecurity and data privacy

The shared personal experience of the students being a victim of cyber security attack, breach, or loss of privacy, they are now become aware of the different modus of cyber attackers. Here is one of the students shared experience; "I fell for clear fake links back then, claiming free gifts and such, but I learned to look at the links properly and sometimes I look at fishy looking websites better if something's off". Further, students started to realize the effects of not taking seriously their cyber security. One student shared "One time, I saw that I shared posts from which I did not share so I took drastic measures to upgrade my security". However, with regards to personal privacy, the students do not mind much whether social media providers track their habits and activities for the purpose of advertising based on their likes, dislikes and preferences.

According to the students, even if they are not really willing to give up their privacy as is, they express their trust to this social media provider to use their shared data properly and accordingly.

3.8. Factors that contribute to the students' perception about cybersecurity and data privacy

4. Conclusion

Being hacked and identity theft are the common reasons of the student that make them aware of risks of using social media. Students provided good examples their account being compromised by hackers and cyber secutiy issues that have occurred in the. Even students are not comfortable when social media provider tracked their activities for promotion, they are still using social media because of the greater benefits it offers than the risks of cyber-attacks which they believe can be minimize if proper security features has been set. The common reasons of the students when security features were not being used is the inconvenience when they need to retrieve their passwords and the time it consumes. Students also indicated that setting security features set boundaries on how they maximize social media especially connecting with other people. To give more protection on cyber-attacks and for students to become more aware of their personal privacy with the use of social media, trainings should be done at school and students feel this should occur as early as possible and strengthen on the preceding levels. This study also found significant differences in awareness level of the student where educational level and age are concerned. Surprisingly, results of this study found that high school students or those who are 15 to 19 years old reached higher awareness level in terms of data privacy and cyber security compared to those who were older to them or in college level. However, factors affecting this result were not included in this study and can be a subject for future research.

Acknowledgements

The researchers would like to extend their deepest gratitude to all the school administrators for allowing them to conduct survey on their students, to the teachers who helped them to facilitate the survey and to all the students who voluntarily participated in this important research endeavor, their sincerest and warmest appreciation..

References

Alharbi, T. & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University, https://www.mdpi.com/2504- 2289/5/2/23

Arora, H, Manglani, T., Bakshi, G., Choudhary, S. (2022), "Cyber Security Challenges and Trends on Recent Technologies," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 2022, pp. 115-118, https://doi.org/10.1109/ICCMC53470.2022.9753967.

Arora, H., Manglani, t., Bakshi, G., & Choudhary, S. (2022). Cyber Security Challenges and Trends on Recent Technologies, 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 2022, pp. 115-118, https://doi.org/10.1109/ICCMC53470.2022.9753967.

Brooks, C. (2016). ECAR Study of Undergraduate Students and Information Technology, EDUCAUSE, p. 22; https://er.educause.edu/- /media/files/library/2016/10

Chandarman R. & Niekerk B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution.Researchgate.net. https://www.researchgate.net/publication/322455127_Students'_Cybersecurity_Awareness_at_a_Private_Tertiary_Educational_Institution

Dimodugno, M., Hallman, S., Plaisent, M. & Bernard, P. (2021). The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach Conf. Ser. 2090 012017 https://iopscience.iop.org/article/10.1088/1742-6596/2090/1/012017

Fleming, J. & Adkins, A. (2015). Data Security: Not a Big Concern for Millennials, Gallup.

Juneja, A., Juneja, S., Bali, V., Jain, V.,. & Upadhyay, H.,. (2021). Artificial Intelligence and Cybersecurity: Current Trends and Future Prospects. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119761655.ch22

Liu,Y. & Zhang, J. (2021). Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Comput 24, 1331–1345 (2021). https://doi.org/10.1007/s10586-020-03190-3

Llego, M. A. (2022). The importance of student privacy in the education process. Teacher PH. https://www.teacherph.com/importance-student- privacy-education-process/

Naeem, M., Jamal, T., Martinez, D. J., Butt, S. A., Montesano, N., Tariq, I. M., De-La-Hoz-Franco, E., De-La-Hoz-Valdiris, E. (2022). Trends and Future Perspective Challenges in Big Data. In: Pan, JS., Balas, V.E., Chen, CM. (eds) Advances in Intelligent Data Analysis and Applications. Smart Innovation, Systems and Technologies, vol 253. Springer, Singapore. https://doi.org/10.1007/978-981-16-5036-9_30

New Survey Research Conducted in Partnership with FreedomPay and Cornell University Highlights Gen Z's Attitudes on Data Privacy and Sharing https://corporate.freedompay.com/press-release/new-survey-research-conducted-in-partnership-with-freedompay-and-cornell-university- highlights-gen-zs-attitudes-on-data-privacy-and-sharing/

Park, J. & Vance, A. (2021). Data Privacy in Higher Education: Yes, Students Care. EDUCAUSE. https://er.educause.edu/articles/2021/2/data-privacy- in-higher-education-yes-students-care

Petrova, A. (2021). Students' Attitudes towards Personal and Learning Data Usage in Aptitude Project Learner Taxonomy. http://ceur-ws.org/Vol- 2933/paper3.pdf

Samtani ,, S., Kantarcioglu, M.,. & Chen, H. (2020). Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap, Article.:17,pp1-19. https://dl.acm.org/doi/abs/10.1145/3430360

Sander, C. (2022). Student Data Security and Privacy Must Be Taken More Seriously. The Journal. https://thejournal.com/articles/2022/01/24/student- data-security-and-privacy-must-be-taken-more-seriously.aspx

Santos, S., Ege, L., & Cruz, I. T. (2017). Data privacy usage on facebook of college students in Metro Manila.w International Journal of Scientific & Engineering Research, 8(2), 1117-1128. https://www.ijser.org/researchpaper/Data-Privacy-Usage-on-Facebook-of-College-Students-in-Metro- Manila.pdf

Seemma, P., Nandhini, S. & Sowmiya, M. (2018). Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security

Yang, P., Xlong, N.,. & Ren, J.,. (2020). "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020, https://doi.org/10.1109/ACCESS.2020.3009876.
