International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 4 (2019) pp. 900-907
© Research India Publications. http://www.ripublication.com

Preemptive Evaluation through Information Security Awareness: Perception of Information Technology Students in a Philippine State University

Lowell A. Quisumbing

Leyte Normal University, Tacloban City, Philippines.

Abstract

Objectives: Studies show that Filipino college students today employ the Internet exceedingly to find data, and gain general knowledge. Thus, the Internet has become a data superhighway where students propel their ideas and social experiences. However, utilizing the Internet routinely opens up students to various dangers like cybercrime, identity theft, and malware infections. Therefore, it is essential to know the Information Security practices and the level of awareness that college students possess to assess and prevent them from harm's way. **Methods:** The research employed a Descriptive Correlational Method which involved the use of online questionnaires delivered through Google form, interviews and observations. The respondents of the study were four hundred eleven (411) students enrolled during the second semester of school year 2016-2017. Simple Random Sampling was the method used for choosing the respondents. **Findings:** Outcomes indicate that there was a significant positive association between respondents Year level with the level of Information Security Awareness (ISA), (r (411) =. 451, p < .001). The result shows that the higher the Year Level of the respondents, the higher the comprehension and awareness in Information Security (IS). Students improve their experience, knowledge, and awareness on the protection and dissemination of information when they progress to a higher year in study. This implies that the program curriculum successfully meet the knowledge requirements of the learners in the university. **Application/Improvements:** The result of this study can serve as basis for policy measures on the use of Computer Networks in the University. It may also serve as a guide for developing inclusive and beneficial Information Security Awareness (ISA) training programs for the students.

Keywords: Information Security Awareness, Case Study, Descriptive Correlational Design, State University, Social Sciences, Computer Networking

INTRODUCTION

The Internet has become a data superhighway where students propel their ideas and social experiences (Chou, C., and Peng, H., 2011). The new direction requires administrations to allow their community members (faculty, students, and staff) to utilize their mobile devices in addition to computer systems to perform tasks. Such activities have led to an increased number of attacks and information security breaches. Electronic data, mobile devices, knowledge, behaviors and unintentional mistakes caused by users seemed to have contributed to this predicament (Khan, H. U., & Gadhoum, Y., 2018). Literature reviews about information security support the importance of research in measuring information security where possible (D'Arcy and Herath, 2011; Crossler et al., 2013). Thus, instead of opposing prohibitive approaches, it is better to cultivate a culture of appropriate use and raise awareness about information security among students (Vicks, M., 2013).

Indeed, prioritizing knowledge over policies that restrict or limit students to educational resources is a must (Datar, T. D., Cole, K. A., & Rogers, M. K., 2014). However, since there are varying levels of information security awareness (ISA) that differ from country to country; therefore, a need to conduct a study demonstrating particular profiles of the students in a specific context (Yilmaz, R., Karaoglan Yilmaz, F. G., Özturk, H. T., & Karademir, T., 2017) is encouraged. Lisman (2002) suggests performing research studies on the safe internet, and computer usage awareness at a national level. A study conducted on Students Information Security Behavior at the University of Dhaka, Bangladesh revealed unintentional disclosure of data and financial malware attacks has the highest incidence among students. (Nowrin, S., & Bawden, D., 2018). Similarly, a study on the security incidents experienced by students from Universities in the Western Region of the United States stated that hacking of personal and financial information were most common. Additionally, infection of viruses and malware programs were also a problem (Pawlowski, S. D., & Jung, Y. (2015). Another research (Rezgui, Y., & Marks, A. (2008) suggest conscientiousness, cultural assumptions, beliefs, and social conditions affect students behaviour and attitude towards ISA, Hence, this goes to show that Information security awareness (ISA) is a universal concern and it stems from different motivating factors.

In the Philippines, (ISA) is a growing concern as it involves the protection of online data due to web collaborations. The Commission on Higher Education (CHED) and the National Privacy Commission (NPC) mandates the compliance of Higher Education Institutions (HEI's) to the Data Privacy Act of 2012 (DPA) more commonly known as Republic Act No. 10173. The DPA is an act protecting individual personal data in ICT systems in both government and private sector. The law is crucial to help prevent cybercrimes by ensuring information are protected to prevent fraud. However, despite good intentions the study of (Ching, M. R. D., & Celis, N. J. 2018) on CHED's Information Systems Strategic Plan (ISSP) revealed that the Information Security policies of the Organization is partially compliant. Similarly, a case study on Bukidnon State University level of compliance (Flores, R. T. G., & Ching, M. R. D., 2018) to the provisions of R.A 10173 and NPC's five pillars Data Privacy Accountability also presented the same results. Moreover, the study of (Ching, M. R. D., Fabito, B. S., & Celis, N. J. 2018) revealed factors such as lack of awareness, budget, and time constraints as barriers to the DPA. This only proves that although the government and Universities are trying its best to implement Information Security Awareness among HEI's still there are several factors that hinder its abilities to abide. Thus, it is now the responsibility of institutions to implement ISA programs to its own clients.

The most recent study concerning ISA in the Philippines is that of Internet Subscribers in Iriga City Camarines Sur where findings show that despite existing cyber security laws (RA 8792 Electronic Commerce Act) and (RA 10173 The Data Privacy Act), users still are most vulnerable to phishing and malware attacks. And majority of the respondents' Internet security perception is derivative- meaning they practice online measure but with limited understanding of the purpose (Omorog, C. D., & Medina, R. P. (2018). Consequently, there are no literatures that describe the ISA of IT College students in a Philippine University. It is on this premise that the study deemed necessary to disclose the level of knowledge that students possess about Information Security Awareness and promote responsible use of computers to protect valuable information.

THEORETICAL FRAMEWORK

The study anchors on the Information Security theory **(**Horne, C. A., Ahmad, A., & Maynard, S. B., 2016) which posits that Information security is a conscious or subconscious process in which people and organizations attempt to create sustainable-viable resources for information. The method works by using controls that protect data from threats, based on goals for the use of that information. Those goals, then result in sustainable resources. Therefore, the focus of Information security is to identify the level of protection given to data, and what use that protected data can offer organizations.

The theory supports the study by providing a concept which can identify the different motivations behind an organization or an individual to secure information against threats. These motivations include goals, purpose, wants and needs. Information security thus appeals to an individual understanding of how necessary and vital is the protection of valuable data from threats. This perception determines the steps that individuals take or apply to meet their desired outcomes.

Moreover, the theory explains the need to create information security resources that can later improve organizational performance. These information security resources may be training, education, and policy development. Likewise, it formulates risk identification and data quality assurance through the application of security technology and management processes (Ernest Chang and Ho, 2006).

Finally, the theory of information security originates from the area of information systems, constructed entirely from ideas that identify with data and the expansiveness of the frameworks that it can dwell on. It applies to different levels, including strategies to protect information used by individuals, groups, organizations, and laws that safeguard information shared between organizations.

RESEARCH OBJECTIVES

This study aimed to determine the Information Security Awareness of BSIT students in a Philippine State University. Specifically, it seeks to:

1. Describe the demographic profiles of the BSIT students regarding Age, Sex and Year level.
2. Identify the level of proficiency of the BSIT students regarding Computer Networking and Information System usage according to their perception.
3. Identify the Information Security awareness level of the BSIT students.
4. Identify the extent of use of the BSIT students on the Computer Systems of the University.
5. Find the significant relationship between the profile of the respondents and the following:
   a) Level of Proficiency in Computer Networking
   b) Level of Awareness to Information Security
   c) The extent of use on the Computer Systems of the University

METHODOLOGY

Design

This study utilized a Descriptive Correlational research design. Using this method, the researcher described the current practice and behaviors of the respondents relevant to Information Security. The Descriptive method was used to identify the demographic profile, Level of proficiency, Level of Awareness and the extent of use of the respondents to the subject Information security. The Correlational method was utilized to identify the relationship between two or more relevant variables.

Respondents of the Study

Four hundred eleven (411) randomly selected Bachelor of Science in Information technology (BSIT) students from four (4) year levels were the respondents of the study. The students were officially enrolled in the university during the second semester of school year 2016-2017.

Research Instrument

This study aimed to describe the Information Security Awareness of BSIT students at Leyte Normal University. An online survey questionnaire developed using Google forms was the main instrument used in the study. The instrument was first face validated by experts in the field. Afterwhich it was classified into four areas. First part, the demographic profiles of the BSIT student to determine Age, Gender, Year Level and the Level of Proficiency relative to Computer Networking. Second part, the level of Information Security Awareness and the Extent of use of Computer Systems at the University to determine Computer network usage and identification of risks and threats. A 5-point Likert scale was utilized to gather responses.

Research Procedure

In obtaining the desired results, the researcher sought first the approval of the respondents. Then the planning and designing of the procedure for data gathering followed. The researcher conducted interviews and observations of the respondents in the network setting. The researcher asked the students about security practices, procedures and the extent of their compliance with the University security policies. The answers to the interview were classified and examined then revised for the drafting of the questionnaire. The survey questionnaire was finalized and then distributed for fielding after which the collection and tabulation of data followed.

The Statistical Analysis of Data

The researcher directly retrieved the responses of the electronic questionnaires through Google form then converted it to the prescribed excel format using Google Sheets. The Excel data was then feed into the Statistical Package for Social Sciences (SPSS) software and descriptive statistics was applied. In obtaining the Demographic profile, the researcher made use of frequency counts and percentages. Then, in the identification of Information Security awareness level of the students and the extent of use of the students the weighted mean of each item in the form was determined using simple descriptive statistics. Pearson, R Correlation using SPSS determined and analyzed the relationships between the Demographic profile and the variables; Level of Security Awareness and Extent of Use of Network Computer Systems in the University.

The following scale used in the evaluation of Information Security Awareness of the BSIT students,

Rating Scale	Limits of Scale	Qualitative Description
5	4.21 – 5.0	Strongly Agree
4	3.41 – 4.2	Agree
3	2.61 – 3.4	Moderately Agree
2	1.81 – 2.6	Disagree
1	1.0 – 1.8	Strongly Disagree

The following scale used in the evaluation of the BSIT Students Extent of Use of Network Computer Systems in the University,

Rating Scale	Limits of Scale	Qualitative Description
5	4.21 – 5.0	Strongly Agree
4	3.41 – 4.2	Agree
3	2.61 – 3.4	Moderately Agree
2	1.81 – 2.6	Disagree
1	1.0 – 1.8	Strongly Disagree

RESULTS AND DISCUSSION:

Table 1 illustrates the breakdown of respondents by age. Of the total number of respondents, the majority (215 or 52.31%) of the respondents were 18 years of age, followed by the students aged 19 years old at (79 or 19.22%). This was followed by respondents aged 17 (57 or 13.87%), 20 (44 or 10.71%), 21 (6 or 1.46%), 22 (5 or 1.22%), and 16 (2 or 0.49%). The student age that had the lowest number of respondents were 24, 25 and 27 at (1 or 0.24%) respectively. The results show that the majority of the respondents were 18 years and older. The age of the respondents is the legal age. The students understand the survey questions and can relate their user experiences with their ISA. Cognitive growth and the amount of academic and life experience at their ages prove useful for the study. Justice & Dornan, (2001) state that older learners perform better than younger learners. Hence, the ISA of the respondents are derived from their lifelong experiences and educational growth, which has a positive effect on the conduct of the study.

Table 1 presents the gender profile of the respondents. Out of the total number of respondents (188 or 45.7%) were Male and (223 or 54.3%) were Female. The result shows that the majority of the students in the BSIT program are female. The result has also roped previous studies which show that among those with academic degrees in the Philippines; there are more female enrollees than male enrollees in IT. Male individuals previously dominate the majority of enrollees in ICT and Engineering courses in the Philippines (Statistics on Filipino women and men's education. (2014, May 13). Retrieved August 13, 2017, from http://www.pcw.gov.ph/statistics /201405/statistics-Filipino-women-and-men-education). Instead, the result shows that both male and female individuals are equally interested in pursuing ICT courses. Hence, the gender is not a significant factor in information security awareness. Being male or female is not an assurance that an individual is performing safe online practices. Instead the key to safe computing is to educate and sharpen your IT security skills to keep up with the times (Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016).

Also, Table 1, below, shows the distribution of respondents regarding their course and year level. Out of the total population of 411 BSIT students, the majority came from the second year level with (167 or 40.53%) respondents, the third year level with (119 or 28.88%), the fourth year level with (89 or 21.60%) respondents and the first year level with (36 or 9.46%) respondents. The demographics show a lower enrollment in the first year level during Academic Year (A.Y. 2015-2016) in the University compared with the previous year, of which there was a lower percentage if not a decline in the number of new enrollees of the BSIT program.

Table 1 further illustrates the self-perceived proficiency of the respondents in Computer Networking and Information System usage which contributes significantly to information security awareness. In the data presented, (259 or 64.1 %) of the respondents described themselves as Intermediate users, while (134 or 33.2%) considered themselves as Basic users. A minimal number of respondents (11 or 2.7%) identified themselves as advanced users. The data exemplifies the knowledge of the respondents in the subject Computer

Networking and Information systems. The respondents knowledge of computer systems and Networks is the product of blended learning thru the CCNA Technology Certificate Program and classroom instruction. In classifying the appropriate user- levels of the respondents, we look at their Computing skills. According to (Cashion & Palmieri, 2002; Thompson & McGrath, 1999), skills are vital since it enables students to learn more effectively in information security. The more extensive the knowledge, the more likely they will be able to secure information. Hence, the Proficiency level of the respondents are very important in determining the ISA that they have currently.

Table 1. Age, Gender, Year Level and the Student Perceived Level of Proficiency in Computer Networking and Information Systems

Profile	Frequency	Percentage
Age		
27 Years Old	1	0.24
25 Years Old	1	0.24
24 Years Old	1	0.24
22 Years Old	5	1.22
21 Years Old	6	1.46
20 Years Old	44	10.71
19 Years Old	79	19.22
18 Years Old	215	52.31
17 Years Old	57	13.87
16 Years Old	2	0.49
Total ***(N)***	**411**	**100%**
Sex		
Male	188	45.7
Female	223	54.3
Total ***(N)***	**411**	**100%**
Year Level		
First Year	36	8.76
Second Year	167	40.63
Third Year	119	28.96
Fourth Year	89	21.65
Total ***(N)***	**411**	**100%**
Level of Proficiency in Computer Networking and Information Systems		
Advanced User	18	4.38
Intermediate User	259	63.02
Basic User	134	32.6
Total ***(N)***	**411**	**100%**

Table 2 illustrates the Information Security Awareness of the respondents in the university with a qualitative description of *Agree* having a total mean of 3.68. The findings described the level of Information security awareness of the respondents towards the information that they sent and received thru the Network Information System (NIS) of the University. The outcomes show that the highest qualitative description was *Strongly Agree* based on the following indicators. (I am aware that there are security risks in using computers = 4.94, I know that there are security software’s that protect information = 4.75, Information Security is an essential part of my education = 4.74).

The results show that students put more attention to risk, protection, and education as primary indicators of information security awareness. These characteristics are both preventive and protective. According to Albrechtsen (2007) when individuals are knowledgeable as to what to watch for, what to protect, and how to respond, this alone could prevent potential problems that could affect the infrastructure as a whole. Also, one of the most central mechanisms of individual security behavior is the identification of risks (Stoneburner, G., Goguen, A. Y., & Feringa, A., 2002). Recognizing threats, as well as managing those threats by learning protective methods will lessen the possibility of a security problem. Therefore, student's technical abilities should be at par with their level of awareness as it is equally important to know how to prevent and thwart attacks using hardware or software configurations.

Table 2. Information Security Awareness

Information Security Awareness	**Rating**	**Qualitative description**
Information Security is an integral part of my education.	4.74	Strongly Agree
I am aware that there is an existing Information Security policy and regulations of the University.	2.81	Moderately Agree
I have received Information Security awareness training at the University.	2.62	Moderately Agree
My study involved the use of research information.	4.65	Strongly Agree
My study involved the use of personal information	2.68	Moderately Agree
My study involved the use of confidential information	2.40	Disagree
My study involved the use of financial information	2.81	Moderately Agree
I am aware that there are security risks in using computers.	4.94	Strongly Agree
I am aware that there are threats in the university computer network.	4.44	Strongly Agree
I know that there are security software’s that protect information.	4.75	Strongly Agree
TOTALMEAN	**3.68**	***Agree***

Table 2 also illustrates the average responses of the students. With a qualitative description of *Moderately Agree* (I am aware that there is an existing Information Security policy and regulations in the University = 2.81, my study involves the use of financial information = 2.81, my study includes the use of personal information = 2.68). The lowest rated item in the table is (My study involves the use of confidential information) with a qualitative description of ***Disagree*** and a mean of **2.4**.

These results illustrate that the respondents are aware of the type of data that they distribute in the network. Furthermore, it shows that the respondents are mindful that certain kinds of information such as financial and personal are attractive targets for the online scam, identity theft, and hacking (Omorog, C. D., & Medina, R. P., 2018). Respondents also exercise caution in providing information, especially in the network of the University where hundreds of individuals communicate at any given time. Thus, results imply that respondents are familiar with the existing policies of the university in the use of the system.

As explained by Newman, G., & McNally, M. M. (2005), financial and personal information are the most common motivation of attackers due to the prospect of financial gain. Hence, the student's awareness of the value of user information and the importance of policies are beneficial in the operation and management of the network as it provides a certain level of protection such as confidentiality of data. Finally, user Behavior is a significant factor in the domain of Information Security (Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T., 2015). Negligence, ignorance, lack of awareness, and resistance to policies are the main factors in security breaches so respondents must focus to maintain adequate information security behavior for minimizing if not reducing it.

The table below (table 3) illustrates the Extent of use of the respondents in the Network Computers of the University with a qualitative result of **Agree** having a total mean of **3.43**. The findings show the degree to which the respondents utilize the computers in the Network of the University. The majority of the items rated ***Moderately Agree*** (I used the computer two to three hours a day=**3.0**, I used and exchanged information with Social Media sites =**3.29**, I searched the Network for different kinds of Information=**3.18,** and I acquired data from other users in the network computers =**3.2**).

The findings suggest that the respondent's extent of use of computers in the network have a more than average frequency involved. These findings also indicate that the regularity of using computers as well as the applications that were utilized such as social media poses a threat to its security. Darmawan, Chong, et al., (2009) explains that the only safe system is the system that disconnects from a network. However, with the value placed on connectivity, it is almost impossible to abstain from using the Internet. Hence, there is no way of avoiding a potential attack from both internal and external threats. Thus, a

Other indicators in Table 3 rated ***Strongly Agree (***I downloaded different material on the University Network=**4.5,** and I copied different file types to the computers in the Network=**4.67**). These findings indicate that the students do not exercise caution when downloading or reproducing data to and from the Internet. The indicators used in Table 3 present a significant threat to the integrity of the Computer Network likewise students responses exhibit complete disregard of University policies, controls, and restrictions.

Chin, A. G., Etudo, U., & Harris, M. A. (2016) explains, while some of these actions may be harmless, a potential for a security breach possibly with devastating consequences always lurks in the background due to computers being susceptible to diverse forms of malicious IT infringements. Furthermore, in a study conducted by Mylonas, (2013) users who downloaded applications from various application repositories were found to have exhibited a blind trust in such deposits and did not necessarily exercise caution when selecting, downloading, and installing apps. Finally, the lowest rated item in table 2, was (I shared my password and other log-in information with other people) with a qualitative result of ***Strongly Disagree*** and a mean of **1.9.** The finding suggests that the respondents knew how to secure their mail and online accounts from possible intrusions. They were aware of the risk of sharing their email and social media accounts and were cautious about divulging critical information to other people.

Table 3. The extent of use of Students in the Network Computers of the University

The Extent of use of Students in the Computer Systems of the University	**Rating**	**Qualitative description**
I used the computer for two to three hours a day.	3.0	Moderately Agree
I used and exchanged information with Social Media sites.	3.29	Moderately Agree
I searched the Network for different kinds of Information.	3.18	Moderately Applicable
I shared my password and other log-in information with other people.	1.9	Strongly Disagree
I downloaded different material on the University Network.	4.5	Strongly Agree
I copied different file types to the computers in the Network.	4.67	Strongly Agree
I acquired data from other users in the network computers.	3.2	Moderately Agree
I accessed the network server remotely.	3.5	Agree
I visited untrusted and underground websites using the network.	3.7	Agree
TOTALMEAN	**3.43**	**Agree**

The results show, depicted in the Table below (Table 4), there is a significant positive association between respondents Year level with the level of Information Security Awareness (ISA), (r (411) =. 451, p < .001). The result shows that the higher the Year Level of the respondents, the higher the comprehension and awareness in IS of the respondents. When students progressed to a higher year level in the BSIT program, they learn more advanced topics in IT, and even more, their experience, knowledge, and awareness on the protection and dissemination of Computer Information grew. The study of (Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., &

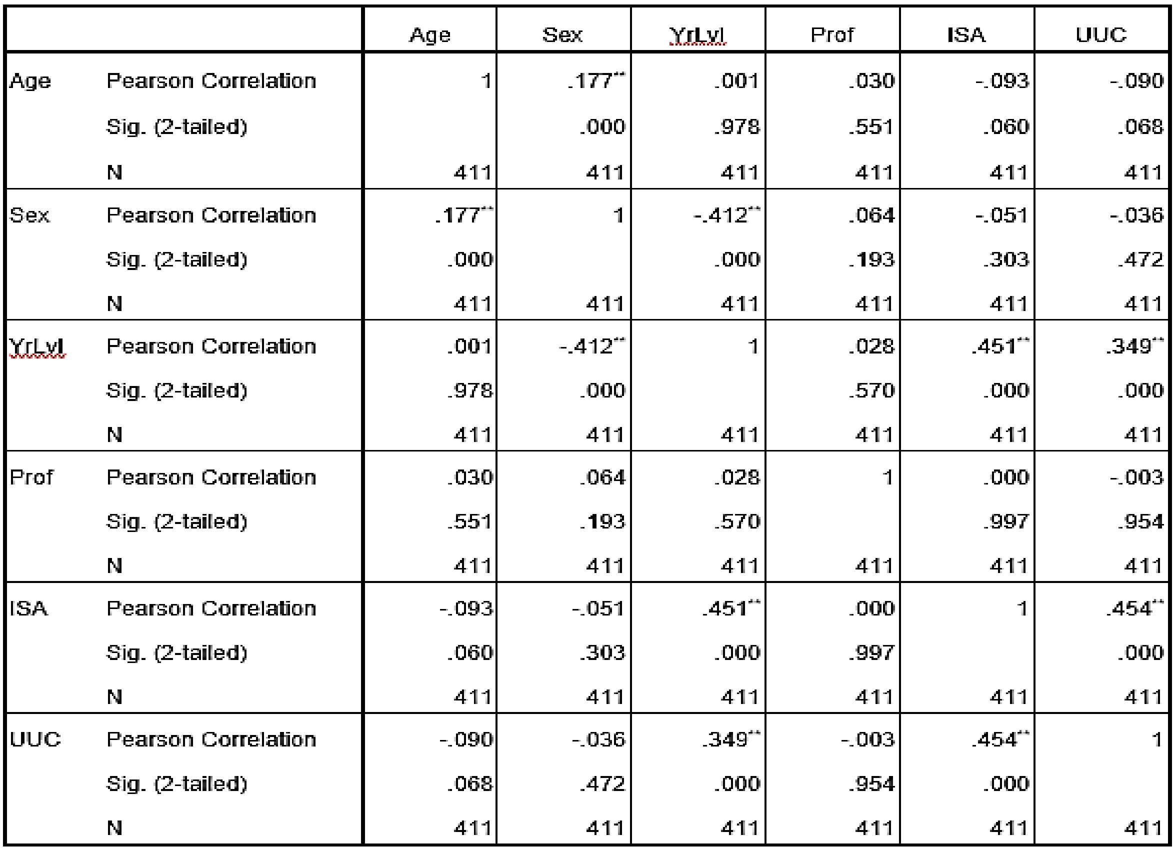
Omar, N., 2015) on Malaysian student's perception on cybercrime proved that those with higher academic qualifications are more mindful of what cybercrime and its hazards are. Similarly, Asokhia (2010) found that the level of training contributes significantly to Ghanian students' perception of cybercrime. The results infer that knowledge thru higher learning contributes to a widened and holistic view of students' understanding of IS consciousness. Therefore, this implies that education plays an imperative role in acquiring a conscious and constructive knowledge of IS.

The Table below (Table 4) also showed there was a significant relationship between Year Level and the Extent of Use of the Computer Systems by the respondents (r (411) =.349, p < .001). These means that the higher the year level of the respondents, the higher the extent of use of Computer Systems that they observe relative to IS. The result indicates that the respondents require more hours as they progress in their academic levels to master, secure, and protect their information. Further, it proves that even in an ideal workplace, ISA requires more time, focus and expertise for students. Likewise, the respondents needed vast amounts of practice and study to further improve their skills in securing information and protecting valuable data. Thus, the time necessary for them to sharpen and hone their craft progressively increases as they move to a higher level in their course.

Table 4. also disclosed a significant positive relationship between the students Level of ISA and the Extent of Use of the Computer Systems by the respondents (r (411) =.454, p < .001). It means that the higher the students Level of ISA the higher the Extent of Use of the Computer Systems by the respondents. The findings state that students increase and grow their ISA through constant and frequent use of computer and internet-based systems. The study of Findley, M. R. (2011) assert that students learn only 20% of what they hear and read, but can learn 90% of what they have practiced. Furthermore, Human knowledge directly affects our attitudes; this effect comes from our direct personal experience or the result of our observations (Albrechtsen, E., & Hovden, J., 2010). Hence, the result implies that students learn ISA not only through instruction and lessons but moreover from hours and days spent using computer systems. Individuals have different personalities and attitudes and may develop positive or negative effects based on what they experienced.

The result of the correlation process also showed a negative correlation between Year Level and Gender on the level of Information Security Awareness (r (411) = -.412, p < .001). The finding suggests merely that there is no significant relationship between the gender and the year level of the students relative to ISA. The gender does not determine the level of ISA.

Table 4. Correlates between the demographic profile of the respondents and the Level of Proficiency in Computer Networking; Level of Awareness to Information Security and Extent of use of the Computer Systems of the University.



		Age	Sex	YrLvl	Prof	ISA	UUC
Age	Pearson Correlation	1	.177**	.001	.030	-.093	-.090
	Sig. (2-tailed)		.000	.978	.551	.060	.068
	N	411	411	411	411	411	411
Sex	Pearson Correlation	.177**	1	-.412**	.064	-.051	-.036
	Sig. (2-tailed)	.000		.000	.193	.303	.472
	N	411	411	411	411	411	411
YrLvl	Pearson Correlation	.001	-.412**	1	.028	.451**	.349**
	Sig. (2-tailed)	.978	.000		.570	.000	.000
	N	411	411	411	411	411	411
Prof	Pearson Correlation	.030	.064	.028	1	.000	-.003
	Sig. (2-tailed)	.551	.193	.570		.997	.954
	N	411	411	411	411	411	411
ISA	Pearson Correlation	-.093	-.051	.451**	.000	1	.454**
	Sig. (2-tailed)	.060	.303	.000	.997		.000
	N	411	411	411	411	411	411
UUC	Pearson Correlation	-.090	-.036	.349**	-.003	.454**	1
	Sig. (2-tailed)	.068	.472	.000	.954	.000	
	N	411	411	411	411	411	411

CONCLUSION:

Based on the outcome, the researcher concludes that the BSIT students of the University have an adequate level of Information Security Awareness. Their self-perceived proficiency in Computer Networking and Information systems, computing knowledge and practices suggest that they have an average understanding of the subject Information Security. The respondents are also somewhat knowledgeable of the risks, threats and the types of data they utilize for online processing or transactions. However, a need for regular orientation and enforcing effective methods for information and security awareness because of the student's unsafe practice of downloading data from different sources. The students are careless in their behavior of not being selective about the type of information that they share and obtain from online sites and other network sources. These actions indicate that the awareness level about the rules and knowledge-required issues is still low. Furthermore, the development of an efficient and well-planned Information Security Awareness Training program must be conducted for the students to maintain and protect their valuable information.

REFERENCES

[1] Statistics on Filipino women and men's education. (2014, May 13). Retrieved August 13, 2017, from http://www.pcw.gov.ph/statistics/201405/statistics-filipino-women-and-mens-education

[2] Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4), 276-289.

[3] Aloul, F. A. (2012). The need for adequate information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183

[4] Asokhia, M. O. (2010). Enhancing national development and growth through combating cybercrime/Internet fraud: a comparative approach. *Journal of Social Sciences*, *23*(1), 13-19

[5] Cashion, J., & Palmieri, P. (2002). *The secret is the teacher: The learner's view of online learning*. National Centre for Vocational Education Research.

[6] Chin, A. G., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235.

[7] Ching, M. R. D., & Celis, N. J. (2018, June). Data privacy act of 2012 compliance performance of Philippine government agencies: a case study approach. In *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government* (pp. 59-63). ACM.

[8] Ching, M. R. D., Fabito, B. S., & Celis, N. J. (2018). Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance. *Advanced Science Letters*, *24*(10), 7042-7046.

[9] Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education*, *14*(1), 44-53.

[10] Darmawan, N., Chong, A., Ooi, K. B., & Venggadasallam, V. A. (2009). Security Mechanism in Computer Network Environment: A Study of Adoption Status in Malaysian Company. *Journal of Applied Sciences*, *9*(15).

[11] Datar, T. D., Cole, K. A., & Rogers, M. K. (2014, January). Awareness of scam e-mails: an exploratory research study. In *Proceedings of the Conference on Digital Forensics, Security and Law* (p. 11). Association of Digital Forensics, Security, and Law.

[12] De Leon, J. A. V., & Tarrayo, V. N. (2014). Cyber Reading in L2: Online Reading Strategies of Students in a Philippine Public High School. *i-Manager's Journal on English Language Teaching*, *4*(2), 8.

[13] D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

[14] Ernest Chang, S., & Ho, C. B. (2006). Organizational factors in the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361.

[15] Findley, M. R. (2011). The relationship between student learning styles and motivation during educational video game play. *International Journal of Online Pedagogy and Course Design (IJOPCD)*, *1*(3), 63-73.

[16] Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, *11*(4), 395.

[17] Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). Information Security Strategy in Organisations: Review, Discussion, and Future Research Directions. *arXiv preprint arXiv:1606.03528*.

[18] Implementing Rules and Regulations of the Data Privacy Act of 2012. (2016, August 24). Retrieved April 26, 2018, from https://privacy.gov.ph/implementing-rules-and-regulations-of-republic-act-no-10173-known-as-the-data-privacy-act-of-2012/

[19] Justice, E. M., & Dornan, T. M. (2001). Metacognitive differences between traditional-age and nontraditional-age college students. *Adult education quarterly*, *51*(3), 236-249.

[20] Lisman, J. (2002). Administrator complacency: a real threat to network Security. SANS Institute. Retrieved from http://www.giac.org/paper/gsec/1690/administrator-complacency-real-threat-network-security/103067. Retrieved on January 8, 2015.

[21] Nowrin, S., & Bawden, D. (2018). Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh. *Information and Learning Science*, *119*(7/8), 444-455.

[22] Khan, H. U., & Gadhoum, Y. (2018). MEASURING INTERNET ADDICTION IN ARAB BASED KNOWLEDGE SOCIETIES: A CASE STUDY OF

SAUDI ARABIA. *Journal of Theoretical & Applied Information Technology*, *96*(6).

[23] Newman, G., & McNally, M. M. (2005). Identity theft literature review.

[24] Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

[25] Omorog, C. D., & Medina, R. P. (2018). Internet Security Awareness of Filipinos. *International Journal of Computing Sciences Research*, *1*(4), 14-26.

[26] Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education*, *26*(4), 281.

[27] Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7-8), 241-253.

[28] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, *53*, 65-78.

[29] Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems.

[30] Thompson, M. M., & McGrath, J. W. (1999). Using ALNs to support a complete educational experience. *Journal of Asynchronous Learning Networks*, *3*(2), 54-63.

[31] Vicks, M. E. (2013). *An Examination of Internet Filtering and Safety Policy Trends and Issues in South Carolina's K–12 Public Schools* (Doctoral dissertation, Nova Southeastern University).

[32] Yilmaz, R., Karaoglan Yilmaz, F. G., Özturk, H. T., & Karademir, T. (2017). Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartin Province= Lise Ögrencilerinin Güvenli Bilgisayar ve Internet Kullanim Farkindaliklarinin Incelenmesi: Bartin Ili Örnegi. *Online Submission*, *7*(1), 83-114.