International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:03, Issue:01 "January 2018"

VIEWS ON CYBERSECURITY PRINCIPLES AND PRACTICES: THE CASE OF BS INFORMATION TECHNOLOGY STUDENTS OF LNU, TACLOBAN CITY, PHILIPPINES

Las Johansen B. Caluza, Lowell A. Quisumbing, Rommel L. Verecio, Dennis S. Tibe

Leyte Normal University,Tacloban City, Philippines

INTRODUCTION

The use of the Internet and other computing technologies in the Philippine Universities has significantly increased in the last decade. While its purpose and aim is to promote communications and research in the academic field, it has become an integral part of a College student's life. Students use the Internet for locating information, and acquiring general knowledge (De Leon, J. A. V., & Tarrayo, V. N., 2014). The Internet today is not only an information superhighway serving teachers and students, but also a new interpersonal arena in which young people can enhance their opportunities and social experiences (Chou, C., & Peng, H., 2011). In many ways, the Internet can be used to access email, complete coursework, purchase books and negotiate online transactions that require the need for personal information. However, this kind of dependency on the Internet has its pitfalls and drawbacks. Using the Internet habitually, exposes students to different risks such as exposure to inappropriate or potentially dangerous information, disclosure of important and private information, online-purchase scams, and enticement by cyber-predators who want to meet them in person for detrimental purposes (Aftab, 2000). Hence, students who use the Internet are more vulnerable to different types of computer security threats such as pornography, hacking, copyright infringement, piracy, and abuse (Poftak, A., 2002).

As information security threats continue to be a critical concern, the importance of educating and re-orienting students on correct computer security practices continues to be important. According to Ng, Kankanhalli, and Xu (2009), information security education including security education, security training, and security awareness programs influence users to become more security conscious. (Arachchilage and Love, 2014; Shillair et al., 2015; Van Bruggen, 2014) believed that human factor is the most imperative factor in guaranteeing safe web and PC use. Parents, teachers and officials should provide the proper guidance and awareness to students so they never stray. Furthermore, (Chou & Peng, 2011; Cole, 2014) agreed that providing a high level of security awareness should be prioritized over policies that restrict or limit the access of students to educational resources. (Vicks, 2013) proposes that as opposed to actualizing prohibitive approaches, it is critical to cultivate a culture of appropriate use of the web and raise data security awareness to the students instead.

Similarly, studies have shown that there are varying influences that motivate individual's Cybersecurity practices. While technological controls are significant to the protection of computer information, Cybersecurity also relies on an individual's opinion on security. (Ng, B. Y., Kankanhalli, A., & Xu, Y. C., 2009). More so, minimal studies have been conducted on the adverse computing practices among students but few have tried to prove theoretically the explanation for the individual's actions. While the behavioral understanding of cybersecurity practices amongst university students remains a complex issue, it is undeniably important to study the causes that bring about this behavior. Aytes, K., & Connolly, T. (2004) on their study of public university students' computer security practices, aver that students who are knowledgeable about the critical consequences of risky computing practices, most likely committed frequent unsafe computing acts due to low level insecure behavior and poor rational choice. Rational choice means that the individual is assumed to take account of available information, probabilities of events, and potential costs and benefits in determining preferences, and to act consistently in choosing the self-determined best choice of action (Cornish, D. B., & Clarke, R. V., 1987). This means that students prefer security practices that are perceived best for them and therefore acts accordingly.

(White, G., & Nordstrom, G., 1996) believed that using computer science principles to teach security subjects tend to motivate positive computer security practice among university students. Lessons, assignments and research papers on subjects like public key encryption, malicious software, Hacking and Cracking provide ample opportunities to raise student's level of cybersecurity awareness thus, developing a positive foundation in cybersecurity practice. Furthermore, in the study of (Skinner, W. F., & Fream, A. M., 1997) findings reveal that social learning theory remains a significant factor in student's computer security habits. Their study sought to find the etiology of computing crimes by understanding why college students commit illegal computer acts. It was anchored on the idea that people learn through observing others' behavior, attitudes, and outcomes of those behaviors. Most human behavior is learned observationally through modeling. From observing others, one forms an idea of how new behaviors are performed, and on later occasions this coded information serves as a guide for action (Bandura, 1962). Therefore, the student's behavior in computing depends on reciprocal interaction between cognitive, behavioral, and environmental influences.

This study explored the cybersecurity habits, practice and experiences of selected Bachelor of Science in Information Technology (BSIT) students in a Philippine State University to disclose and evaluate hidden behaviors and motivations. It aims to reveal the hidden practices, current and past experiences, views and issues of IT students on cybersecurity that influences their behavioral practices in computing. Results of the study will be used as bases for pedagogical improvements in the university BSIT program. Moreover, the study envisions fostering the development of an adaptive cybersecurity policy for the University to enforce.

RESEARCH OBJECTIVES

This case study explored the perspectives of IT students at the University to unravel their sentiments and opinions towards cybersecurity.

Specifically, this study seeks the following questions:

1. How do IT students practice cybersesecurity in school?
2. What experiences have the IT students encountered that influenced their views on cybersecurity?
3. Why should IT students practice cybersecurity?
4. What are the pressing issues of IT students on cybersecurity in school?

FRAMEWORK OF THE STUDY

Today, the protection of every institutions critical infrastructure is conceived as a shared responsibility where the government itself cannot offer the necessary security alone (Eriksson, J., & Giacomello, G., 2004). Individuals cannot merely rely on laws or government policies to strengthen, secure or protect information. Educators and learners alike are inclined to practice security in order to protect not only their valuable data but as well as national and international interests. Bringing this to mind the study anchors on the Constructivist Theory of Securization (Baylis, J., Owens, P., & Smith, S., 2017). This theory posits that individual's reactions relative to cybersecurity are influenced by their perception of the environment, including the technological space and the outcomes or the results of their interactions with other individuals in the digital realm (Ciolan, I. M., 2014).

This means that students characterized as learners, are information constructors and have the ability to create their own subjective representations of objective reality. It implies that the knowledge of how to practice cybersecurity including threat identification and security solutions are constructed based on the student personal experiences and hypotheses of the environment in which they work on.

Furthermore, learners continuously test these hypotheses through social negotiation which are learned through experiences such as when they are subjected to online abuse, cyber bullied, or when there is a significant or similar situation. Thus, each person initiates a different interpretation and construction of the knowledge process. The learner is not a blank slate (tabula rasa) but brings past experiences and cultural factors to a situation which becomes the bases for their actions.

METHODOLOGY AND DESIGN

Research Design

This study is anchored on Collaizzi's phenomenological method of data analysis. As cited by Edward, K. L., & Welch, T. (2011), the Collaizzi's seven step method are: (1) transcribing all the subjects' description; (2) extracting significant statements; (3) creating formulated meanings; (4) aggregating formulated meanings into themes and clusters; (5) developing an exhaustive description; (6) identifying the fundamental structure of the phenomenon and (7) returning to participants for validation. Hence, the steps cited provides researchers an insights on how to present an auditable decision trail and explore issues of rigor and trustworthiness.

Research Procedure

The researchers sought approval from the University President for the determination of samples that will be involved in the study. This was confined to all BSIT students of the university who were currently enrolled during the first semester of school year 2017-2018. Purposive sampling was done with a total of 5 participants out of 321. Further, data was analyzed using categories and themes for the purpose of grouping the responses.

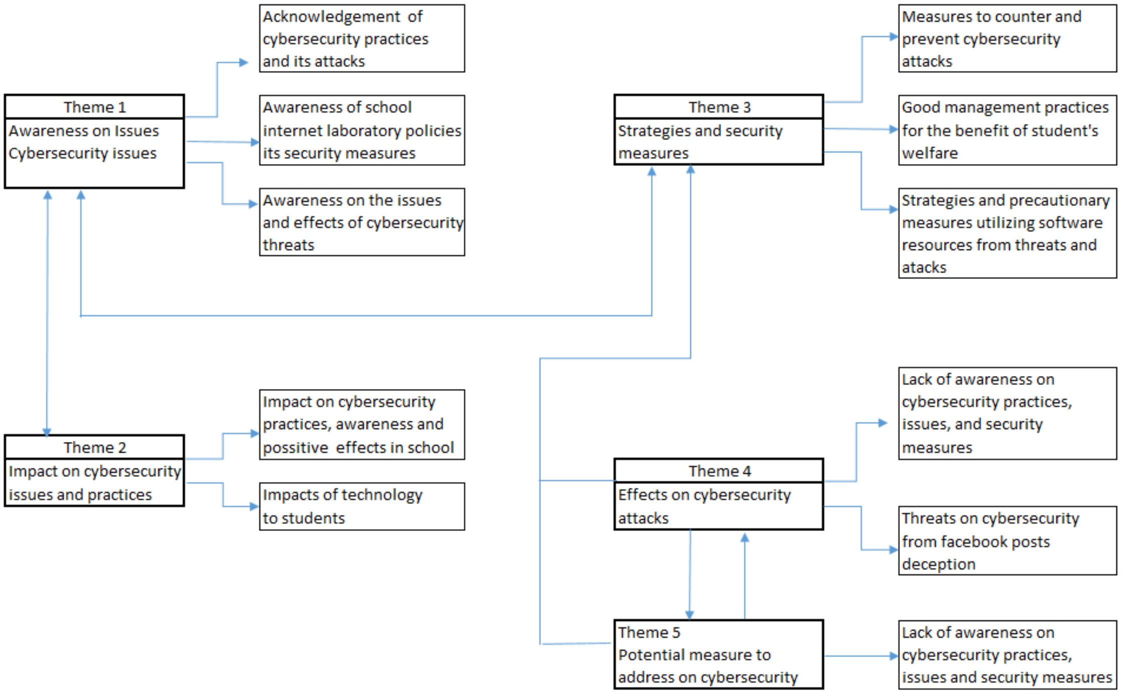
Research Reflexivity

The researcher's objectives of conducting this study is to explore, dig deeper and understand their views on cybersecurity principles and practices. A new framework or paradigms may be suggested to the administration for the improvement of its information and communication technology services particularly on cybersecurity based on the result of the study.

Ethical Issues

The information used in this research derived from participants were their own respective views on the issues in relation to the subject. Hence, in the interest of future predicaments that may arose based on the impressions and misconceptions of the readers, their identities were not be divulge in the study. The researchers reserved the right to protect against the participants and the name of the university in general.

RESULTS AND DISCUSSION


Theme 1
Awareness on Issues Cybersecurity issues
Acknowledgement of cybersecurity practices and its attacks
Awareness of school internet laboratory policies its security measures
Awareness on the issues and effects of cybersecurity threats
Theme 2
Impact on cybersecurity issues and practices
Impact on cybersecurity practices, awareness and possitive effects in school
Impacts of technology to students
Theme 3
Strategies and security measures
Measures to counter and prevent cybersecurity attacks
Good management practices for the benefit of student's welfare
Strategies and precautionary measures utilizing software resources from threats and atacks
Theme 4
Effects on cybersecurity attacks
Lack of awareness on cybersecurity practices, issues, and security measures
Threats on cybersecurity from facebook posts deception
Theme 5
Potential measure to address on cybersecurity
Lack of awareness on cybersecurity practices, issues and security measures

Qualitative data was processed through its methodology to gather reliable information and validation of the questions in terms of clarity, understandability, and appropriateness (Creswell 2013). The following presentations are the results and discussions by theme.

Theme 1: "Awareness on cybersecurity issues".

Responses of the participants:

- Acknowledgement of cybersecurity practices and its attack
- Awareness of school internet laboratory policies and its security measures
- Awareness on the issues and effects of cybersecurity threats

Most of the participants use the internet on a daily basis using their smart phones, tablets and computers, there are a large number of attacks on a daily basis. Cyber-attacks, hacks and security breaches on the internet are no longer an exception anymore (Arora, Nandkumar, & Telang, 2006). The participants are aware and understands the importance of cybersecurity. In these, the participant's practices cybersecurity to protect their personal data form hackers and crackers.

Theme 2: "Impact on cybersecurity issues and practices".

Responses of the participants:

- Impact on cybersecurity practices, awareness and positive effects in school
- Impact of technology to students

It is important to recognize that awareness does not equal lasting behavior change. Not only the impact of cybersecurity practices and awareness has positive effects on the students of the university but also the increasing growth of technology. The university should have good network policy for the benefit of every student.

Theme 3: "Strategy and security measures".

Responses of the participants:

- Measures to counter and prevent cybersecurity attacks
- Good management practices for the benefit of student's welfare
- Strategies and precautionary measures utilizing software resources from threats and attacks

In this new sphere of cyberspace, however, malicious activities are prevailing. Stealing personal, business, and organizational information and assets has been increasingly persistent. In light of such malicious activities, how to best counter these threats are a challenge to ensure and maintain the free flow of information that is the "backbone" of democracy, the safe and secure living environment of the people, economic and social prosperity, and peace, while protecting intellectual properties that are the fruits of the creativities and inspirations of individuals and businesses as well. Good internet management practices are being observed by the respondents. They use utility software, antiviruses to prevent attacks.

Theme 4: "Effects on cybersecurity attacks".

Responses of the participants:

- Lack of awareness on cybersecurity practices, issues, and security measures
- Threats on cybersecurity from facebook posts deception

The lack of awareness on cybersecurity practices, issues, and security measures are one of the major reasons why some internet users are a victim of hackers. The outcomes of an attack have different effects ranging from data theft, data decay or damage (wiping files) and exploring and interrupting systems or services.

Theme 5: "Potential measures to address on cybersecurity".

Responses of the participants:

- Lack of awareness on cybersecurity practices, issues and security

The lack of awareness on cybersecurity practices, issues and security measures on the part of the faculty, staff, and students of the university makes the network vulnerable to attacks and threats. Maintain an accurate inventory of control system devices and eliminate any exposure of this equipment to external networks. Network segmentation and firewalls should be implemented.

CONCLUSION AND RECOMMENDATION

Cybersecurity is not solely a technical endeavor, a wide range of education, training, and seminars should be conducted for the benefit of the faculty, staff, and students of the university. These are needed in an effective cybersecurity awareness. It is necessary that more attention to both the capacity and capability of the university in terms of cybersecurity should be addressed.

Further, if the university budget warrants, the researchers recommend the following measures;

1. maintain an accurate inventory of control system devices and eliminate any exposure of this equipment to external networks,
2. implement network segmentation and apply firewalls,
3. use secure remote access methods
4. use strong passwords, change default passwords, and consider other access controls,
5. Maintain awareness of vulnerabilities and implement necessary patches and updates,
6. develop and enforce policies on mobile devices,
7. implement cybersecurity training program,
8. implement measures for detecting compromises and develop a cybersecurity incident response plan.

REFERENCES

Arachchilage, N.A.G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. Journal of Organizational and End User Computing (JOEUC), 16(3), 22-40.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. Journal of research in crime and delinquency, 34(4), 495-518.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. Criminology, 25(4), 933-948.

Bandura, A. (1962). Social learning through imitation.

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.

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.

Aftab, P. (2000). The parent's guide to protecting your children in cyberspace. New York:McGraw-Hill.

Poftak, A. (2002). Net-wise teens: Safety, ethics, and innovations. Technology & Learning, 22(1), 36–45.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48, 199-207.

Van Bruggen, D.C. (2014). Studying the impact of security awareness efforts on user behavior. Unpublished doctorate dissertation, University of Notre Dame.

Eriksson, J., & Giacomello, G. (2004, March). International Relations Theory and Security in the Digital Age. In Montreal: International Studies Association Convention, Panel: Theorizing Information Age Security (also available at: http://www. threat-politics. net/docs/eriksson_isa. pdf, 24. 6. 2005).

Ciolan, I. M. (2014). Defining Cybersecurity As The Security Issue of The Twenty First Century. A Constructivist Approach. Revista de Administratie Publica si Politici Sociale, 12(1), 40.

Baylis, J., Owens, P., & Smith, S. (Eds.). (2017). The globalization of world politics: An introduction to international relations. Oxford University Press.