Journal of Pedagogical Sociology and Psychology
Volume 3, Issue 1, 2021
http://www.doi.org/10.33902/JPSP.2021167595

Research Article

Does threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid COVID-19 crisis?

Erwin Rotas[1] and Michael Cahapay[2]

[1]Department of Education, General Santos City, Philippines; [2]College of Education, Mindanao State University, Philippines

Correspondences should be addressed to Erwin Rotas erwinemperadorotas@gmail.com

Received 17 December 2020; Revised 10 February 2021; Accepted 1 March 2021

Amid the current period of massive migration to remote learning, it can be practically assumed in the context of cyber security that giving students threat knowledge will increase their protective behaviors. An emerging stance in behavior theories, however, offer an interesting ground on the dissociation between knowledge and behavior. This article is a preliminary study with the aim to test if threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid the COVID-19 crisis. Gathering data from a sample of students from a teacher education department of a Philippine university, modified questionnaires were used in online surveys. The results revealed that the students are somewhat knowledgeable about the possible threats and they sometimes practice protective behaviors in remote learning. This indicates a practical need to heighten the cyber security of the students. This study further found no significant relationship between threat knowledge and protective behaviors of the students. While this outcome contributes a piece of evidence in the current debate in behavior theories, further validation in other contexts is necessary.

Keywords: Threat knowledge, protective behaviors, cyber security, remote learning, COVID-19 crisis

1. Introduction

During the last decade, technologies have tremendously made human affairs more effective and efficient. The rise of information and communications technology has made almost all materials around the world readily accessible on the internet for a comprehensive and convenient search. It is expected that continuous innovations in the years to come will make it even possible to have a digital application for every human concern. This massive change has substantially transformed the lives of people across the world.

From the current global perspective, most people have engaged and developed dependence on information and communications technology (Akhilesh & Möller, 2020) owing to the COVID-19 crisis. The current situation which resulted in a "social recession" made most transactions be done online using different technologies. Within the context of the sudden migration of schools to remote education, the increasing demand for internet connectivity and even technology by students has widened opportunities for internet usage. The students in the process have become vulnerable to cyber threats and hazards (Zwilling et al., 2020). A review stresses that since COVID-19 spread, there has been an alarming increase in the number of cybercrime incidents (Hajj & Rony, 2020). Since remote learning is an internet-based platform, it is also open to cyber security attacks (Furnell & Karweni, 2001; Bandara et al., 2014).

Cyber security attacks are commonly performed by "bad hackers" who are capable of committing a cybercrime (Zwilling et al., 2020). It may be in a form of phishing attacks, conference bombing, and ransomware attacks (Curran, 2020). It may also be in a form of malware, malicious websites, and business email compromise (Khan et al., 2020). The criminals use hacking devices and malicious software to damage technology infrastructure, mobile devices, and computers (Abawajy, 2012). Within the remote learning context, cyber security threats are a possible event especially for higher education institutions that use different electronic management systems and video conferencing programs to conduct classes. According to studies (e.g. Schultz, 2005; Parsons et al., 2014), though protective tools are already built in technological devices, they do not fully dissolve cyber security threats.

Crucial factors in the context of cyber security towards a safe remote learning environment amid the current crisis are threat knowledge and protective behavior. Threat knowledge is linked to cyber security hazard awareness (Reid & van Niekerk, 2016). Many people experience information security hazards from multiple threats, and this includes students involved in remote learning. Since students are in the field of education and are not technology experts, they may fail to protect themselves (Bandara et al., 2014). Consequently, it has also been recognized that knowledge is a contributory factor to protective behavior (Safa et al., 2015). When certain knowledge is applied, a desired preventive measure is gained. Since majority of cyber incidents are due to lack of knowledge, it raises the issue that people remains a major cause of unintentional cyber breaches (Ahola, 2019). Students who just started remote learning are most possibly prone to commit these errors. It may be further exacerbated by the poor technology security system condition especially common in developing countries (Burgess & Sievertsen, 2020).

In the context of cyber security amid global health crisis, there is a practical need to equip students the necessary threat knowledge in remote learning. Cain et al. (2018) emphasized that end users, which in this case are students, are often characterized as the weakest link in cyber security. This is especially true within personal cyber environments which became target of 95% of the attacks (Talib et al., 2010) since home technological devices are not protected by information security staffs. Attackers look for vulnerabilities and these may come to students who perform poor cyber hygiene, such as those who are not following good practices of protection. So, it is assumed that once students are knowledgeable of the cyber-attacks, they will increase their protective behaviors. Cybersecurity personalities (e.g. Cain et al., 2018; Zwilling et al., 2020) supports such argument that threat knowledge affects people to engage in cyber protection behaviors.

Several global scholarly works reported the possible influence of knowledge on protective behaviors in different disciplines particularly on health domain (Schlueter, 1982 on breast self-examination; Hobfoll et al., 1993 on safer sex behavior; Sheeran & Taylor, 2006 on condom use; Paige et al., 2017 on diabetes control; Cahapay & Ramirez, 2020 on disaster preparedness; Guerra et al., 2005 on cancer screening; Ananth & Koopman, 2004 on HIV-AIDS protection; Silver Wallace, 2002 on osteoporosis prevention; and Spirito et al., 2007 on regimen compliance and metabolic control). These studies attempted to test whether knowledge plays a major role on people to comply the desired protective behaviors. Furthermore, a large body of literature also tested the levels of threat knowledge (e.g. Luminita, 2011; Cain et al., 2018; Affia et al., 2020) and extent of protective behaviors (e.g. McCormac et al., 2018; Malecki, 2018; Cain et al., 2018; Akhilesh & Möller, 2020; Curran, 2020; Zwilling et al., 2020) to foster cyber security in the practice of distance education. Drawing gaps from these studies, however, it can be significantly noted that in the context of cyber security, few studies looked into the possible influence of threat knowledge on protective behaviors of students beginning remote learning. When looking into the Philippine context, previous scholarly initiatives focused on cyber security awareness (e.g. Dela Cruz, 2016; Umali, 2018; Natonton, 2018) and the role of this acquired awareness on the tendency to perform the desired behavior is still unknown.

This paper is hinged on two important issues. First, at the practical level, when designing a remote learning program, it is important to put into the equation the threat knowledge and the extent of protective behaviors of the students. An accurate report of these concerns may open opportunities for relevant actions. Second, at the theoretical level, there is a new debate in behavior theories on the dissociation between knowledge and behavior. The researchers saw this problem as another opportunity to investigate in this paper such an emerging position. Thus, this article attempted to test if threat knowledge influence protective behaviors of Filipino students in the context of cyber security in remote learning amid the COVID-19 crisis.

1.1. Theoretical Framework

Behavior theories support the relationship between knowledge and behavior. One of the widely known theories is the social cognitive theory by Bandura (2014). His theory posits that, for education to promote change in behavior, it should improve knowledge. Thus, it underpins the common assumptions in the educational field that knowledge is a related variable to behavior. The conceptual notion of this theory is applied in the current study. It can be assumed that threat knowledge is expected to promote protective behavior in the context of cyber security. Thus, it can be hypothesized that there is a direct and positive relationship between threat knowledge and protective behavior of the students.

This assumed linear association has been confirmed in the different contexts including education. Ajzen et al. (2011) explained that several educational campaigns are focused on knowledge of a general nature. It is expected that once people have acquired this knowledge, the learners will engage in the desired behavior. However, scholarly reports on the dissociation between knowledge and behavior have emerged, calling to further probes on the classical assumption on the connection between behavior theories. For example, a review of selected studies over the past decades (e.g. Lancaster, 1990; Guerra et al., 2005, Cahapay & Ramirez, 2020) indicates a propensity towards disconnection between knowledge and behavior.

Thus, this paper, hinged on behavior theories, is also an extension of the continuing debate in the field of behavior theories. It is related to most of the studies attempting to relate knowledge and behavior. However, it is unique in the sense that it is conducted within the context of cyber security in remote learning amid the COVID-19 crisis.

2. Method

The methods employed in this study are discussed in this section. It includes the research design, participants, context, instrumentation, research procedure, and data analysis.

2.1. Research Design

A correlational research design was entailed in this study. This research design measures the association between two or more variables without manipulating them. It aims to find out whether there is either correlation between or among them (McCombes, 2019). It is considered suitable for the study as it aimed to determine the relationship between threat knowledge and protective behavior of the pre-service teachers in the context of cyber security in remote learning.

2.2. Participants

The respondents of this study were 31 students currently enrolled in an undergraduate teacher education program in a Philippine university. They were selected based on their engagement in remote learning program, thus have considerable experience to cyber security considerations. A large majority (74.19%) of the respondents use mobile phone while a few (25.81%) use either mobile phone, laptop computer, or desktop computer in remote learning. When it comes to internet connection, most of them (61.29%) connect thorough prepaid data while the rest (38.71%) through Wi-Fi. The availability and connectivity of the respondents at the time of the conduct of the study were also considered in the process. They were chosen regardless of age, gender, course standing, socioeconomic status, and geographical location.

2.3. Context

This study was conducted in a state university in Mindanao, Philippines. The Commission on Higher Education, through its COVID Advisory No. 7 series of 2020, encouraged higher education institutions to consider their delivery mode subject to compliance with minimum standards and the situation on the ground. As a response after considerations, the university opened its classes through remote learning program last September this year.

2.4. Instrumentation

This study used two survey questionnaires developed from various sources. Furthermore, the two survey questionnaires were electronically designed through the Google Form.

The first instrument is called “Cyber Security Threat Knowledge Scale.” It consists of 12 items designed to gauge the level of knowledge of pre-service teachers on cyber security threats. These items were adapted from the study of Zwilling et al. (2020) from which they were content validated by experts in the field. These items were further complemented with other items from the article of Freedman (2020). The instrument was framed according to the proposed four-point scale of Brown (2010) with 1 as “Not knowledgeable at all” and 4 as “Knowledgeable to a great extent.” The Cronbach’s alpha of the scale was found to be .834 which is adequate.

The second instrument is titled “Cyber Security Protective Behavior Scale.” It also has 12 items intended to determine the extent of protective behavior employed by the pre-service teachers as regards cyber security. The items were mostly adapted from the study of Zwilling et al. (2020). These items were added a few more items from an article by Tunggal (2020). The instrument was also framed according to the four-point scale suggested by Brown (2010) with 1 as “Never” and 4 as “Often.” It generated a satisfactory Cronbach alpha of .756.

2.5. Procedure

This study was conducted by initially securing the consent of the target respondents. The researchers explained the goal of the study as well the process of gathering the data. It was made clear that their participation is optional. Furthermore, they were informed of the confidentiality of their identities once they participate. After obtaining their consent, a link to the electronic survey was posted in the online discussion board of the class. The students accessed and answered the survey and their responses were automatically recorded. Finally, the researchers generated the data.

2.6. Data Analysis

The researchers employed descriptive statistics such as frequency count, percentage rate, and weighted mean to interpret the gathered data. Furthermore, considering the small sample size but ensuring that the assumption of normality is complied, the parametric tool of Pearson Product Moment Coefficient Correlation was used to ascertain the direction of association between the variables involved in this study. The test was done at 0.05 level of significance.

3. Results and Discussion

This study aimed to test if there is a significant relationship between the threat knowledge and protective behaviors of Filipino students in the context of cyber security in remote learning amid the COVID-19 crisis. This section presents the results.

This study initially surveyed the threat knowledge of the students. Table 1 shows the result.

Table 1
Threat knowledge of the students

Items	Mean	Description
1. loss of data	3.35	To a great extent
2. violation of privacy	3.29	To a great extent
3. changing of data	3.06	Somewhat
4. corrupted data	2.97	Somewhat
5. stealing of personal data	2.93	Somewhat
6. stealing intellectual property	2.81	Somewhat
7. loss of money	2.77	Somewhat
8. device damage	2.77	Somewhat
9. spying on organizations	2.74	Somewhat
10. takeover of devices	2.74	Somewhat
11. spying on people	2.71	Somewhat
12. block access to information	2.61	Somewhat
TOTAL	**2.90**	**Somewhat**

The result indicated that the students are knowledgeable to a great extent as regards cyber security threats such as loss of data (M=3.35) and violation of privacy (M=3.29). On the other hand, they are somewhat knowledgeable on cyber security threats like changing of data (M=3.06), corrupted data (M=2.97), and stealing of personal data (M=2.93).

On the other hand, the students are somewhat knowledgeable on cyber security threats in terms of stealing intellectual property (M=2.81), loss of money (M=2.77), device damage (M=2.77), spying on organizations (M=2.74), takeover of devices (M=2.74), spying on people (M=2.71), and block access to information (M=2.61).

Overall, the cyber security threat knowledge of the students obtained a weighted mean described as somewhat knowledgeable. This implies that they have an average level of awareness of the possible cyber security risks in the context of remote learning using online modalities. This study finds a parallel result with previous studies of Imgraben et al., (2014) and Hadlington (2017). They found out that students generally have an average level of threat knowledge.

When looking into the items, it can be gleaned from the results that two items that stand out as obtaining the highest scores of threat knowledge relate to the loss of data and violation of privacy. Bandara et al. (2014)

explained that students at this stage have developed a strong understanding of the security hazards that may affect their privacy. It includes the ability to secure a safe virtual learning space and safe storage of their personal data.

It can be further noted that most of the items that garnered high scores of threat knowledge pertain to data such as loss of data, changing of data, and corrupted data. This pattern can be attributed to the fact that, as Malecki (2018) described, the participants have gone through early exposure to computers with improved awareness of common threats that may harm their identity, information as well as their devices.

Furthermore, this study looked into the cyber security protective behavior of the students. Table 2 presents the result.

Table 2

Protective behaviors of the students

Items	Mean	Description
1. using strong passwords	3.64	Often
2. turning off Bluetooth when not used	3.71	Often
3. not sharing passwords	3.52	Often
4. ignoring spam messages and links	3.10	Sometimes
5. logging off all apps or programs	3.10	Sometimes
6. installing apps from known sources	2.93	Sometimes
7. updating software, browser, and apps	2.84	Sometimes
8. installing antivirus software	2.71	Sometimes
9. avoiding open networks or Wi-Fi	2.58	Sometimes
10. making regular data backup	2.58	Sometimes
11. creating different passwords	2.55	Sometimes
12. changing passwords regularly	2.19	Seldom
TOTAL	**2.95**	**Sometimes**

The result disclosed that the students often demonstrate cyber security protective behavior like turning off Bluetooth when not used (M=3.71). They also often display demonstrate cyber security protective behavior by using strong passwords (M=3.64), and not sharing passwords (M=3.52).

Moreover, it was found out that they sometimes exhibit protective behavior such as logging off all apps or programs (M=3.10), installing apps from known sources (M=2.93), updating software, browser, and apps (M=2.84), installing antivirus software (M=2.71), avoiding open networks or Wi-Fi (M=2.58), and making regular data backup (M=2.58). However, one protective behavior stands out as being seldom observed by the students; they seldom practice changing passwords regularly (M=2.19).

Overall, the cyber security protective behavior of the students generated a weighted mean described as sometimes. This suggests that they display measures to protect themselves in the context of cyber security in remote learning to a moderate extent. This finding corroborates with the result of the study of Chen and Zahedi (2016) where students generally employ an acceptable level of compliance to security protective behaviors.

It can be further noticed that two of the items with the highest scores refer to passwords like using strong passwords and not sharing passwords. These are common protection activities regularly practiced by students in remote learning (May & George, 2011). They added that students regularly update their passwords for privacy protection and to maintain confidentiality over their sensitive personal data. Colby and Profis (2020) also strongly suggested that students should make it a top priority to select a reliable password manager and use a secured password to avoid financial fraud and exploitation of data.

On the other and, one item that noticeably generated the lowest score was related to the password as changing passwords regularly. Chen and He (2013) warned that protective behaviors like changing passwords from time to time is one of the vital practices to be secured in remote learning. These practices also include installing antivirus software in computers and making regular data backup.

Lastly, this study investigated if threat knowledge is related to the protective behaviors of the students. Table 3 presents the result.

Table 3
Relationship between threat knowledge and protective behaviors of students

Variables	Protective behaviors
Threat knowledge	.287 (p=.365)

The correlation result revealed that there is no significant relationship between threat knowledge and protective behaviors of students (r=.287, p=.365). This means that threat knowledge does not influence the protective behaviors of the students in the context of cyber security in remote learning amid COVID-19 crisis. Reviewing ahead the current arguments put forward by different camps in behavior theories, this result is not surprising.

An emerging body of related studies in the field of medical research demonstrates that knowledge about diseases do not or may not necessarily affect the intention to perform the desired protective behaviors. For example, in the study of Lancaster (1990), it was found that knowledge on perceived susceptibility and benefits does not have significant relationship on the practice of breast examination. An instance of the same result in the field of education is that of Cahapay and Ramirez (2020). They uncovered that there is a negative and weak correlation between science literacy and disaster preparedness. Following the arguments in previous studies, they attributed this result to the kind of knowledge that students are taught which are more conceptual than practical. As a result, students generally show low level of compliance to required preparedness behavior. Thus, it can be assumed that, from both studies, the participants may lack the requisite knowledge to support the desired protective behaviors. Azjen et al. (2011) supported that most people focus on sharing accurate knowledge of a general nature. We expect that once people have acquired this knowledge, they will practice the desired behavior. On the other hand, this approach has often caused disappointments because people continue not to practice the desired behavior.

Applying those arguments in the context of this study, it can be anticipated that threat knowledge may not promote the practice of students of the desired protective behaviors. It may be attributed to the fact that the threat knowledge in cyber security may be unfamiliar to most of the students who were just obliged to quickly adapt to the remote learning in emergency situation. This context may have caused discrepancies in their responses as evidenced in the results for most items. Abawajy and Kim (2010) explained that possessing even the minimum required knowledge may not lead to accurate and appropriate behavioral responses to cyber security hazards. It should be recalled also that, in the Philippines, most initiatives have focus on cyber security awareness (Dela Cruz, 2016; Umali, 2018) but particular knowledge on unique cyber threats has not been formally taught in schools or considered as part of training of students. It can be further argued that awareness alone cannot change behavior nor lead to action (Richard, 2019). Cyber security is a complex thing, thus needs reinforcement. Hence, it implies that threat knowledge in this case is not enough to influence protective behaviors of students.

4. Conclusions

There is a need to investigate the level of awareness of the students on the possible hazards and the ways they protect themselves amid the sudden shift to remote education during the COVID-19 crisis. Exploring further the new debate in behavior theories on the dissociation between knowledge and behavior, the researchers also saw the opportunity to probe such an emerging position. Thus, the goal of this research was to describe the threat knowledge and protective behaviors of students in the context of cyber security in remote learning amid the COVID-19 crisis.

Based on the results, this article concludes that the students have an average level of threat knowledge and a moderate extent of protective behavior. It can be further highlighted that there is no significant relationship between threat knowledge and protective behaviors of students in the context of cyber security in remote learning amid the COVID-19 crisis. This study explained that threat knowledge in cyber security may be unfamiliar to most of the students who were just obliged to quickly adapt to the remote learning in emergency situation, thus not adequate to create change in their protective behaviors in cyber security.

This paper offers several significant points. On the practical level, some steps on awareness campaigns should be conducted to increase the cyber security threat knowledge and protective behavior of the students. This can be done by incorporating online information drives about possible hazards and the ways to prevent them. The administrators can also include discussing threat knowledge and protective behavior during college and department student orientations while the teachers enforce these points in their course policies and regulations. Moreover, at the theoretical level, this paper contributes a piece of evidence as regards the dissociation between threat knowledge and protective behaviors of students in the context of cyber security in remote learning amid the COVID-19 crisis. As a preliminary study, however, there is a need to replicate the study to involve more diverse samples. It is important to validate the results drawn from this study in other contexts given the different variations that may be possible.

Disclosure Statement. The authors confirm that there are no relevant financial or non-financial competing interests to report for this paper.

References

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behavior and Information Technology, 33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Abawajy, J. & Kim, T. (2010). Performance analysis of cyber security awareness delivery methods. *Communications in Computer and Information Science, 122,* 142-148. https://doi.org/10.1007/978-3-642-17610-4_16

Affia, A. A. O., Nolte, A. & Matulevičius, R. (2020). Developing and evaluating a hackathon approach to foster cyber security learning. *International Conference on Collaboration Technologies and Social Computing,* 3-19. https://doi.org/10.1007/978-3-030-58157-2_1

Ahola, M. (2019, October 18). The Role of Human Error in Successful Cyber Security Breaches. *Usecure*. Retrieved from https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Ajzen, I., Joyce, N., Sheikh, S., & Cote, N. G. (2011). Knowledge and the prediction of behavior: The role of information accuracy in the theory of planned behavior. *Basic and Applied Social Psychology, 33*(2), 101-117. https://doi.org/10.1080/01973533.2011.568834

Akhilesh, K. B. & Möller, D. P. F. (2020). Smart technologies: Scope and applications. *Springer.* https://doi.org/10.1007/978-981-13-7139-4

Ananth, P., & Koopman, C. (2003). HIV/AIDS knowledge, beliefs, and behavior among women of childbearing age in India. *AIDS education and prevention: Official publication of the International Society for AIDS Education*, *15*(6), 529–546. https://doi.org/10.1521/aeap.15.7.529.24049

Bandara, I., Ioras, F. & Maher, K. (2014). Cyber security concerns in E-learning education. *ICERI2014 Conference,* 0728-0734.

Bandura A. (2004). Health promotion by social cognitive means. *Health Education Behavior, 31*(2):143–164. https://doi.org/10.1177/1090198104263660

Brown, S. (2010). *Likert scale examples for surveys.* Retrieved from https://www.extension.iastate.edu/Documents/ANR/LikertScaleExamplesforSurveys.pdf

Burgess, S. & Sievertsen, H. H. (2020, April 01). Schools, skills, and learning: The impact of COVID-19 on education. Retrieved from https://voxeu.org/article/impact-covid-19-education

Cahapay, M. B. & Ramirez, R. P. B. (2020). Relationship between Science Literacy and Disaster Preparedness: The Possible Role of Curriculum in Behavior Theories. *Asian Journal of Science Education, 2*(2), 78-86. https://doi.org/10.24815/ajse.v2i2.16803

Cain, A. A., Edwards, M. E. & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security, 42,* 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

CHED COVID Advisory No. 7. Guidelines for the prevention, control and mitigation of the spread of Coronavirus Disease 2019 (COVID-19) in higher education institutions (HEIs). Retrieved from https://ched.gov.ph/

Chen, Y. & He, W. (2013). Security risks and protection in online learning: A survey. *International Review of Research in* Open and Distance Learning, *14*(5), 108-127. https://doi.org/10.19173/irrodl.v14i5.1632

Chen, Y. & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Poly-contextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222. https://doi.org/10.25300/MISQ/2016/40.1.09

Colby, C. & Profis, S. (2020). *9 rules for strong passwords: How to create and remember your login credentials*. Retrieved from https://www.cnet.com/how-to/9-rules-for-strong-passwords-how-to-create-and-remember-your-login-credentials/

Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud and Security, 2020*(6), 11-12. https://doi.org/10.1016/S1361-3723(20)30063-4

Dela Cruz, R. T. (2016, July 9). How to ecome a cybersecurity expert. Retrieved from https://manilastandard.net/mobile/article/210365

Freedman, M. (2020, October 14). 18 ways to secure your devices from hackers. *Business News Daily*. https://www.businessnewsdaily.com/

Furnell, S. M. & Karweni, T. (2001). Security issues in online distance learning. *VINE, 31*(2), 28-35. https://doi.org/10.1108/03055720010803998

Guerra, C. E., Dominguez, F., & Shea, J. A. (2005). Literacy and knowledge, attitudes, and behavior about colorectal cancer screening. *Journal of Health Communication, 10*(7), 651–663. https://doi.org/10.1080/10810730500267720

Gummesson, E. (1991). *Qualitative methods in management research*. London: SAGE.

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. https://doi.org/10.5281/zenodo.1467909

Hajj, A. A. & Rony, M. (2020). Cyber security in the age of COVID-19: An analysis of cyber-crime and attacks. *International Journal for Research in Applied Science & Engineering Technology, 8*(8), 1476-1480. https://doi.org/10.22214/ijraset.2020.31216

Hobfoll, S. E., Jackson, A. P., Lavin, J., Britton, P. J., & Shepherd, J. B. (1994). Reducing inner-city women's AIDS risk activities: a study of single, pregnant women. *Health Psychology: Official journal of the Division of Health Psychology, American Psychological Association*, *13*(5), 397–403. https://doi.org/10.1037/0278-6133.13.5.397

Imgraben, J., Engelbrecht, A. & Choo, K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour and Information Technology, 33*(12), 1347-1360. https://doi.org/10.1080/0144929X.2014.934286

Khan, N. A., Zaman, N. & Brohi, S. N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. *TechRxiv*. https://doi.org/10.36227/techrxiv.12278792.v1

Lancaster, C. (1990). *Personal practices of and beliefs about breast self-examination m students of nursing* (Unpublished honours dissertation) Western Australia College of Advanced Education, Perth.

Luminita, D. C. (2011). Information security in E-learning platforms. *Procedia- Social and Behavioral Sciences,* 15, 2689-2693. https://doi.org/10.1016/j.sbspro.2011.04.171

Malecki, A. (2018). Cybersecurity in the classroom: Bridging the gap between computer access and online safety. *Cyber Security Capstone Research Project Reports,* 1. Retrieved from https://scholar.valpo.edu/cscrpr/1/

May, M. & George, S. (2011). Privacy concerns in e-Learning: Is using a tracking system a threat? *International Journal of Information and Education Technology*, *1*(1). Available: http://liris.cnrs.fr/Documents/Liris-5266.pdf

McCombes, S. (2019). *Correlational research*. Retrieved from https://cacb.ca/

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M. & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security, 26*(3). Available: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2018-0032/full/html

Natonton, O. R. R. (2018). Cybersecurity awareness among selected educational institutions in Butuan City PH. *Mindanao Peace Studies & Conference 4,* 1-14.

Paige, S. R., Bonnar, K. K., Black, D. R., & Coster, D. C. (2018). Risk factor knowledge, perceived threat, and protective health behaviors: Implications for type 2 diabetes control in rural communities. *The Diabetes educator*, *44*(1), 63–71. https://doi.org/10.1177/0145721717747228

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computer and Security, 42,* 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Reid, R. & van Niekerk, J. (2016). Decoding audience interpretations of awareness campaign messages. *Information and Computer Security, 24*(2), 177-193. https://doi.org/10.1108/ICS-01-2016-0003

Richard, K. (2019, September 16). Changing People's Behavior: Awareness Alone Is Not Enough. *Design and Critical Thinking*. Retrieved from https://medium.com/human-centered-thinking-switzerland/changing-peoples-behavior-awareness-alone-is-not-enough-8de3b3204e35

Safa, N. S., von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organisations. *Computers and Security, 56*, 1-13. https://doi.org/10.1016/j.cose.2015.10.006

Schlueter L. A. (1982). Knowledge and beliefs about breast cancer and breast self-examination among athletic and nonathletic women. *Nursing research*, *31*(6), 348–353. https://pubmed.ncbi.nlm.nih.gov/6924219/

Schultz, E. (2005). The human factor in security. *Computer and Security, 24*(6), 425-426. https://doi.org/10.1016/j.cose.2005.07.002fle

Sheeran, P., & Taylor, S. (1999). Predicting intentions to use condoms: A meta-analysis and comparison of the theories of reasoned action and planned behavior. *Journal of Applied Social Psychology, 29*(8), 1624–1675. https://doi.org/10.1111/j.1559-1816.1999.tb02045.x

Silver Wallace, L. (2002). Osteoporosis prevention in college women: Application of the expanded health belief model. *American Journal of Health Behavior, 26*(3), 163–172. https://doi.org/10.5993/AJHB.26.3.1

Spirito A, Esposito-Smythers C, Wolff J, Uhl K, Cognitive-behavioral therapy for adolescent depression and suicidality, *Child and Adolescent Psychiatric Clinics of North America*. https://doi.org/10.1016/j.chc.2011.01.012

Tunggal, A. T. (2020, October 20). What is a cyber threat? *Cybersecurity & Risk Management Blog*. https://www.upguard.com/

Umali, T. (2018, November 12). Cybersecurity in the Philippine academe to bridge skills gap. *Open Government.* Retrieved from https://opengovasia.com/cybersecurity-in-the-philippine-academe-to-bridge-skills-gap/

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems.* https://doi.org/10.1080/08874417.2020.1712269