Cybercrime Awareness and Perception among Students of Saint Michael College of Caraga

BRYL P. ARIOLA  
http://orcid 0000-0001-9288-7611  
brylariola94@gmail.com  
Saint Michael College of Caraga  
Nasipit, Agusan del Norte, Philippines

ETHEL RHONA FAYE O. LAURE  
http://orcid 0000-0002-4685-2079  
ethelrhonafaye@gmail.com  
Saint Michael College of Caraga  
Nasipit, Agusan del Norte, Philippines

MARK LEO A. PEROL  
http://orcid 0000-0001-5140-8098  
perolmark35@gmail.com  
Saint Michael College of Caraga  
Nasipit, Agusan del Norte, Philippines

PATRICK JORDAN T. TALINES  
http://orcid 0000-0002-4143-2083  
ptalines@yahoo.com  
Saint Michael College of Caraga  
Nasipit, Agusan del Norte, Philippines

Gunning Fog Index: 14.40   Originality: 99%   Grammar Check: 99%   Flesch Reading Ease: 40.88   Plagiarism: 1%

ABSTRACT

This study aimed to determine the level of Awareness among Students of Saint Michael College of Caraga Towards Cybercrime, their Perception, and the significant
difference on Awareness and Perception. Researchers used the Quantitative method of research utilizing a Descriptive Survey Questionnaire as the instrument in gathering the data. Frequency and percentage, weighted mean, and one way ANOVA are the statistical treatment used. The result showed that, awareness had a summary weighted mean of 2.72 with a verbal description of sometimes which means that the students have medium level of awareness towards cybercrime, while perception had a summary weighted mean of 3.03 with a verbal description of agree which means that as to the students the statements are illegal/immoral but can also be legal/moral as to the purpose. Meanwhile, the result of the one way ANOVA test accepted the hypothesis that there is no significant difference between the Cybercrime Awareness and Perception of the students.

KEYWORDS

Cybercrime, awareness, perception, students, quantitative, Philippines

INTRODUCTION

Cybercrime is a term used to describe broadly criminal activities in which computers or computer networks are a tool, a target, or a place of illegal activity including everything from electronic cracking to denial of service attacks. It is also used to incorporate traditional crimes in which computers or networks are used to enable illegal activities (Gupta, 2014). The Cybercrime can halt any railway where it is, it may misguide the planes on its flight by misleading with wrong signals, it may cause any delicate military data to fall into the hands of foreign countries, and it may halt e-media, and every system can collapse within a fraction of seconds (Bhatia, 2016).

Moreover, Cybercrime is “any illegal, unethical and unauthorized behavior in a system which processes information automatically or transfers data” (Akgün, Keskin, & Byrne, 2009). Cybercrime can be divided into two main categories where the computer is used as a tool or as a target. Harassing and threatening people on the internet or mobile phones, and publishing music or books without having the copyrights are two examples of cybercrime. The authorities prefer to extend the scope of the punishments for classic crimes instead of adding cybercrime clauses to the present codes. On the other hand, acts like distorting, replacing data, and blocking access to a system are crimes where the information systems are targeted directly, and there are independent codes and regulations in the law defining the scope of these crimes (Solak & Topaloglu, 2014).

The Philippines had been in the revolutionary stage of information technology since e-commerce law also known as Republic Act 8792 – E-Commerce Law of the Philippines has been established in the year 2000. Currently, a blog from rappler
reported that Senator Nancy Binay wants students to learn cyber ethics. According to the interview, Binay explained that the proposal she made in Senate Resolution 474 aims to promote responsible use of the Internet through education instead of laws that may restrict free speech (Macaraig, 2013). The Philippines is experiencing computing ethical dilemma regarding moral values, privacy, and other norms that affect an individual's whole being. Among those were reported in different news organizations such as cyber-sex, pornography, cyber stalking, identity thief, financial thief, and alike (Verecio, 2016).

Further, the researchers undertake this study to determine the level of Awareness and Perception among Students of Saint Michael College of Caraga.

**FRAMEWORK**

This study is anchored on the Space Transition Theory of Cybercrimes by Jaishankar & Ronel (2013). Space Transition Theory by Jaishankar & Ronel (2013) is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming Demeanor in the physical space and cyberspace. Space Transition postulates the movement of people from one space to another (e.g., from physical space to cyberspace and the other way around). Space Transition Theory contends that people act differently when they move from one space to another.

Virtual space allows an individual with so much space where he can convey his feelings and even vent out his outrage against anyone. Cyber stalking and Cyber defamation are examples where offenders use cyberspace because of its anonymity and widespread approach. The significant postulates of the theory are: (1) Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position; (2) Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime; (3) Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well; (4) Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape; (5) Strangers are likely to unite together in cyberspace to commit crime in the physical space, Associates of physical space are likely to unite to commit crime in cyberspace; (6) Persons from closed society are more likely to commit crimes in cyberspace than persons from open society; (7) The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes (Jaishankar & Ronel (2013).

Since criminology has begun viewing the outgrowth of cyberspace as a fresh locus of unlawful activity, a new theory is needed to expound why cybercrime occurs. The space transition theory presented above explains the criminal behavior in the cyberspace.
OBJECTIVES OF THE STUDY

This study was conducted to determine the level of Awareness and Perception among Students of Saint Michael College of Caraga Towards Cybercrime. Specifically, it answers the following questions:
1. What is the profile of the respondents;
2. What is the level of awareness of the respondents towards Cybercrime;
3. What is the perception of the respondents towards Cybercrime; and
4. Is there a significant difference in the Cybercrime Awareness and Perception of the students of Saint Michael College of Caraga?

METHODOLOGY

Research Design
The Researchers used the Quantitative method of research utilizing a Descriptive Survey Questionnaire as the instrument in gathering the data.

Research Locale
The study was conducted at Saint Michael College of Caraga, located at Atupan Street, Barangay 4, Nasipit Agusan Del Norte. Saint Michael College of Caraga is a Catholic School in Nasipit Agusan del Norte under the Ramon Diocese of Butuan in the Philippines. As cited from Saint Michael College of Caraga student's handbook (2017), the school was founded on July 1, 1948, as a Secondary School, with Fr. Francisco Van Dyke as the first Director.

Research Respondents
The respondents of this study were the College Student of Saint Michael College of Caraga. The College which is comprised of all the Departments except the Unit Earners has a total population of 1154 students with a sampling size of 297 students.

The College Students who were enrolled in Saint Michael College of Caraga for the 2nd Semester School Year 2017 – 2018 were the respondents of this study. The Sampling is evenly distributed using frequency and percentage. The Researchers used the Slovin Formula to determine the sampling size.

Research Instrument
The study utilized a set of survey questionnaires to gather the needed information relevant to the study. The survey questionnaire that was used in this study has three parts to obtain the personal profile of the respondent, to assess the level of Awareness and Perception of the Students. The first part includes personal information, such as Age, Gender, Course, Year level, Frequency in Cyber Networking, and Methods of Internet Usage. In the second part, it aims to assess the level of Cybercrime Awareness of the
students in terms of cyber culture, knowledge of victimization, and legal rights with four-point Likert scale with “Never (1), Rarely (2), Sometimes (3), Always (4)”. The last part aims to assess what is the Cybercrime Perception of the students in terms of Legal grounds and Moral grounds with a four-point Likert scale with “Strongly disagree (1), Disagree (2), Agree (3), Strongly agree (4)”.

The second part of the questionnaire form was taken from the journal “Awareness Regarding Cyber Victimization among Students of University of Sindh, Jamshoro” by MA Avais et al. (2014) and the last part of the questionnaire form was taken from the journal “The Perception Analysis of Cyber Crimes In view of Computer Science Students” by Solak & Topaloglu (2014).

**Ethical Standard**

The researchers itself observed the utmost privacy of their subject and consent to their subject, the information was protected, and the researchers asked permission to conduct the study, and it will remain confidential.

Upon the floating day of the survey questionnaires, the researchers approached the respondent in a friendly manner with good ethics to make them comfortable and to build rapport with the respondents. Afterward, the researchers discussed to the respondents in a vernacular manner what was the study all about and inform them the benefits that they will receive in this study. The researchers answered all the quarries of the respondents regarding the study and the researchers let them answer the survey questionnaire on their own without interference. The researchers also inform the respondents that the data or information that will be gathered is confidential and the researchers will follow protocol to keep the confidentiality. After the data is tabulated, analyzed and interpreted all the survey questionnaires were kept and stored by one of our group member for the confidentiality of the respondent’s data. Lastly, before answering the survey questionnaire, the respondents were given informed consent for them to answer and to let them sign at the bottom for the approval and conduct of the study.

**Data Gathering Procedure**

To gather the files needed for this study, the following steps were done:

The first step, the researchers sent a letter of request to the school registrar office to give us the list of all college students enrolled in second semester school year 2017 – 2018.

The second step, a letter was sent addressing to the Deans of all College Departments as to their students are the respondent in the research study entitled Cybercrime Awareness and Perception among Students of Saint Michael College of Caraga.

The third step, the researchers distribute and discuss to the respondents what was the content of the informed consent and also deliberate the possible questions they would encounter in answering the instrument. Upon the distribution of the instrument,
some of the respondents are hesitant and reluctant to answer the instrument especially the first year students. While answering the instrument, some of the respondents ask questions with regards to the definition of some words they are unfamiliar.

The fourth step, after floating of the questionnaire, the researcher gathered the instrument, and the data that was taken from the survey was tally for the data interpretation.

The fifth step, after the data gathered, the result was checked, evaluated, analyze, and interpreted with the use of statistical tools that seek to answer the problem 1, 2, 3, and 4.

Statistical Treatment

In treating the data statistically, the following statistical tools were used by the researchers:

Frequency and Percentage – was used to determine the percentage of the group to the total number of respondents. It is used to answer problem 1.

Weighted Mean – was used to determine the level of Awareness and Perception of the respondents towards Cybercrime. It is used to answer problem 2 and 3.

One Way Anova – was used to determine the significant difference among the Cybercrime Awareness and Perception of the students of Saint Michael College of Caraga. It is used to answer problem 4.

RESULTS AND DISCUSSION

Profile of the respondents

As to age, the majority of the college respondents of Saint Michael College of Caraga belong to the age bracket 20 – 24 years old. The majority of the respondent is between the age bracket of 20 – 24 years old. It must be noted that the appropriate year level for the mentioned age bracket is the fourth year, but the majority of the respondents are the third year. Therefore, the researchers infer that the respondent had to stop school for a year after graduating high school before enrolling college. Moreover, being in the mentioned age bracket makes the respondent less of a victim of cybercrime due to experience and level of education. As stated by Oksanen & Keipi (2013), young people are more likely to become victims of cybercrime even when other factors were adjusted, young cybercrime victims were more likely to be worried about future victimization.

As to Gender, The majority of the college respondents of Saint Michael College of Caraga are females who make up 54.21% of the total sample population. The majority of the respondents are females this is because of the courses offered in this institution especially in the College of teacher’s education (CTE) where the majority of the students are female. Therefore, the researchers infer that females are less likely to become a victim of cybercrime because they are more cautious and aware than male. According to Prabu (2015), male and female students differ significantly in their awareness about
cybercrime, but female student’s awareness towards cybercrime is far better than their counter-part.

As to Course, the majority of the college respondents of Saint Michael College of Caraga are from Bachelor of Elementary Education (BEED). The results infer that the majority of the respondents are Bachelor of Elementary Education (BEED) students this is because of the popularity of the said program, in which the students aspire to become teachers to impart their knowledge to others and because the tuition fee is not that costly. As students enter college, they must be educated about cybercrime because cybercrime is not limited only to those out of school youth, but also to the students who are pursuing to achieve their goals and dreams. As stated by Daigle (2016), when students come to pursue their educational interests, they believe they are entering a safe environment. But while colleges are thought of as “ivory towers,” they can also be places where students could become victims of a crime.

As to Year Level, the majority of the college respondents of Saint Michael College of Caraga are the third year who make up 40.07% of the total sample population. The results infer that the majority of the students are the third year this is because first year and second year students are busy, while the fourth year students are undergoing on the job training (OJT). On the other hand, students with higher year level are more ware due to experience and level of education. According to Hasan, Rahman, Abdillah, & Omar (2015), students with knowledge of cyber offenses and high level of education have high perceptions and awareness of cybercrime.

As to the Frequency of Internet Usage, the majority of the college respondents of Saint Michael College of Caraga use the internet for 2 – 3 hours per day. The results infer that the majority of the respondents use the internet for 2 – 3 hours per day. Access to the internet happens during their vacant time in school and when they are still at home. Frequency of internet usage contributes to cybercrime victimization because as an individual spend more time on the internet he/she will likely encounter cybercrime. As stated by Marcum (2015), people spending extensive amounts of time online are also placing themselves at risk for victimization, cyber bullying and cyber stalking are two main ways people can be victimized.

As to Methods of Internet Usage, the majority of the college respondents of Saint Michael College of Caraga use a mobile phone to access the internet. The results infer that the majority of the respondents use a mobile phone to access the internet, this is because the mobile phone is fairly cheap to purchase than desktop, laptop, and tablet. The mobile phone is popular, almost everyone owns a mobile phone because this is also a method of communication. Having this gadget as a method to access the internet will make an individual susceptible to cybercrime. Nonetheless, every device poses a great risk of becoming a victim. The computer is rapidly becoming the new crowbar says DI Smith, just another means by which to commit a crime. Anyone who has a desktop computer, laptop, tablet or mobile device/phone could be at risk of being a victim.
Level of awareness of the respondents towards Cybercrime

Cyber culture has a weighted mean with a total average of 2.79 and a verbal description of sometimes. The results infer that students are highly aware regarding the minimum age requirement to join social media sites because upon joining they read the policy guidelines of the social media sites, but the age restriction provided by the social media sites can easily be bypassed by providing fake birthdays. Not allowing others to use your personnel account will greatly help in your privacy in cyberspace. Knowing and following the ethics of cyber culture contributes to an individual of becoming less of a victim of cybercrime. Establishing cyber ethics means providing norms and values that an individual can follow on the cyber space that can greatly help the cyber space users to live in harmony while freely exchanging information and ideas. According to Jaishankar & Ronel (2013), Cyber culture is a conglomeration of cyber rules, norms, cultures, and principles generally provided by the Internet Service Providers (inclusive of website hosts, chat line providers, and email providers) and those rules and cultures which may or may not have legal sanction, but which are generally to be followed by the common internet users.

Knowledge of victimization has a weighted mean with a total average of 1.93 with a verbal description of rarely. The results infer that students rarely received abusive/dirty emails in inboxes from known/unknown sources. On the other hand, the students rarely seen their morphed pictures in the cyberspace, this can be the result of being aware of the victims and the aspiring offenders on cybercrime offenses. As stated by Van de Weijer, & Leukfeldt (2017), the prevalence of cybercrime has increased rapidly over the last decades and has become part of the everyday life of citizens. It is, therefore, of great importance to gain more knowledge on the factors related to an increased or decreased likelihood of becoming a cybercrime victim.

Legal rights have a weighted mean with a total average of 3.44 with a verbal description of always. The results infer that students are highly aware that there is a government department to control cybercrime victimization in the Philippines which is the Philippine National Police Anti-Cybercrime Group (PNP-ACG). Hacking, creation of pornography/distributing the same, distribution obscene materials, etc. are criminal offences by the law in which some of the students are unaware that those acts are punishable. It is alarming and must be addressed immediately by conducting extensive cyber ethics campaign. According to Osborne & Russo (2011), the best way to deal with legal challenges is to prevent them from occurring. The best way to prevent legal challenges in the school environment is for all to be aware of their legal responsibilities.

Perception of the respondents towards Cybercrime

Legal grounds have a weighted mean with a total average of 3.02 with a verbal description of agree. The results infer that students strongly agree that it is illegal to code and spread viruses and Trojans. On the other hand, student’s agreement on providing and obtaining old-dated movies and music albums via sharewares is illegal but can
also be legal as to the purpose. Whatever the purpose of such acts it is prohibited and punishable by the law and by that it is always illegal. Students as internet users must be fully aware of the cybercrime offenses, for them to perceive the legality and illegality of such acts. As stated by Solak & Topaloglu (2014), police and governments alone are not likely to prevent and solve cybercrimes that have become one of the biggest problems in the modern world. For that reason, individuals as internet users should be informed and aware of cybercrime by perceiving cybercrimes as classic crimes and social phenomena.

Moral grounds have a weighted mean with a total average of 3.03 with a verbal description of agree. The results infer that students agree that it is immoral but can also be moral as to the purpose to decrypt and change an e-mail account password that belongs to another and to forward offensive e-mails insulting individuals or companies. On the other hand, student’s agreement on using software to monitor and control children’s internet use, providing and obtaining old-dated movies and music albums via sharewares is immoral but can also be moral as to the purpose. Whatever the purpose, such acts mentioned is immoral, this misperception is a result of conflicting norms and values, which leads to such acts to be morally acceptable. According to stated Bele, Dimc, Rozman, & Jemec (2014), the findings are alarming, since they point to the fact that certain types of cybercrime are so widely performed that they have become socially acceptable.

**Significant difference on the Cybercrime Awareness and Perception of the students of Saint Michael College of Caraga**

The null hypothesis is accepted, where a p-value of 0.63 is greater than the significance level of 0.05 and that there is no significant difference on the cybercrime awareness and perception of the students of Saint Michael College of Caraga. It is necessary for the respondents to be highly aware and at the same having the right perception towards cybercrime for the prevention and protection. As stated Bele, Dimc, Rozman, & Jemec (2014), it is of crucial importance to raise the awareness and understanding among the general public and increase the knowledge of the members of law enforcement agencies regarding cybercrime and its consequences in our everyday life.

**CONCLUSION**

The result showed that, awareness had a summary weighted mean of 2.72 with a verbal description of sometimes which means that the students have medium level of awareness towards cybercrime, while perception had a summary weighted mean of 3.03 with a verbal description of agree which means that as to the students the statements are illegal/immoral but can also be legal/moral as to the purpose. Meanwhile, the result of the one way anova test accepted the hypothesis that there is no significant difference between the Cybercrime Awareness and Perception of the students. According to Bele, Dimc, Rozman, & Jemec (2014), the awareness of the general public is of crucial
importance for successful prevention and protection against cybercrime. Further, as to Solak & Topaloglu (2014), there was no significant difference between the legal and moral perspectives of the students. As most of the students reported disagreement with gathering personal information of internet users and leaking them to third persons, they are responsive to privacy on legal grounds.

**RECOMMENDATIONS**

Based on the findings of the study the researchers will endorse to the school through the administration to implement Cybercrime awareness intervention program in all courses or department in this institution. To educate the student regarding cybercrime, cyber ethics, computer, and network security, for them to know the positive and negative effects of using the internet and the ill-effects of cybercrimes and promote cyber security awareness.

Further, the researcher will also recommend to the Commission on Higher Education (CHED) and the Department of Education (DepEd) to implement that all schools with in the Philippines must establish its own cybercrime committee that will become an instrument for the prevention, protection, and to further raise cybercrime awareness on a national level.

The results are showing the importance of awareness as a method to decrease or prevent Cyber-Crime. We can condemn unethical Cyber Culture with partnership and collaboration of both individuals and authorities. The government can do more to safe and secure cyber space. Although we cannot make free cyber space from attacks, it is possible to combat and check Cyber-Crime.

**LITERATURE CITED**


