CYBERCRIME AWARENESS AND CYBERCRIME PREVENTION ATTITUDE OF CRIMINOLOGY STUDENTS

Clark Roble Concoles

Nonalie Cristobal

Efren Felonia Jr.

Vanessa Mae Tadtad

Khryzzler Alrizon Villafuerte
Tommy Von D. Lucas

ABSTRACT

This study determined the cybercrime awareness and cybercrime prevention attitude of criminology students. The descriptive-correlational design was utilized in this study. Data were gathered through survey questionnaire from 100 criminology students in central Mindanao colleges. Mean was employed in analyzing cybercrime awareness of the students, and cybercrime prevention attitude of criminology students. Pearson-product moment correlation was used to analyze the relationships that exist between the variables. The results show that the levels of cybercrime awareness, and cybercrime prevention attitude are high among of Criminology students. Meanwhile, The Cybercrime awareness (r=.550, p<.05) and cybercrime prevention attitude (r=.489, p<.05) have significant relationship. Lastly, the hypothesis which state that there is a significant relationship between cybercrime awareness and cybercrime prevention attitude of criminology students in central Mindanao colleges (CMC)

INTRODUCTION

This study focused on the determinants factor of preventing cybercrimes that are getting more prevalent in cyberspace against the backdrop of the legal landscape. This cybercrime issue not also has become a viral in information system environment but knocks out as a general issue that could be harm national constitution. As national institution like Cyber Security use to help to face the challenges, but there is no agreed indicator to measures the success. According to Cyber Security Malaysia, a very challenging part in cybercrime investigation is the gathering of evidence and most of the cybercrime's issues are financially motivated. The impact of the economic downturn and financial crisis could potentially lead to the increase in cybercrime cases globally. With regards to this challenge, this research to be done to find a solution and model of prevention, if any, with some sort of recommendation to overcome such challenge. 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 misguiding 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 behaviour 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 Peer Reviewed Journal 21 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 cybersex, 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 central Mindanao colleges.

Statement of the Problem

This study determined the relationship between Cybercrime Awareness and Cybercrime Prevention Attitude. More specifically, it sought answers to the following questions:

1. What is the level of Cybercrime awareness?

2. What is the level of Cybercrime Prevention Attitude?

3. Is there a significant relationship between cybercrime awareness and Cybercrime Prevention Attitude?

4. Do cybercrime awareness significantly predict the Cybercrime Prevention Attitude?

FRAMEWORK

Researchers have determined ONE independent variable namely cybercrime. The researchers wanted to study the variables that had significant positive relationship commitment. Shows a theoretical framework on the relationship between the independent variables and their correlation with the dependent variable.

Social structure theories, this theory is applied to a variety of approaches within criminology in particular and in sociology more generally as a conflict theory or structural conflict perspective in sociology and sociology of crime. As this perspective is itself broad enough, embracing as it does a diversity of positions.

Cybercrime act on the other hand of social integrity related to the Strain theory, also known as Mertonian Anomie, advanced by American sociologist Robert Merton, suggests that mainstream culture, especially in the United States, is saturated with dreams of opportunity, freedom, and prosperity--as Merton put it. Most people buy into

this dream, and it becomes a powerful cultural and psychological motivation and that's why the liberty to use social networking sites as to rejects the stresses. Merton also used the term anomie, but it meant something slightly different for him than it did for Durkheim. Merton saw the term as meaning a dichotomy between what the society expected of its citizens and what those citizens could actually achieve. Therefore, if the social structure of opportunities is unequal and prevents the majority from realizing the dream, some of those dejected will turn to illegitimate means crime in order to realize it.

Following the Chicago school and Strain Theory, and also drawing on Edwin Sutherland's idea of differential associations, subcultural theorists focused on small cultural groups fragmenting away from the mainstream to form their own values and meanings about life.

METHOD

Research Design

This study used a descriptive-correlational research design. Quantitative research is the systematic empirical investigation of observable phenomena via statistical,mathematical, or computational techniques. The objective of quantitative research is to develop and employ mathematical models, theories, and hypotheses pertaining to phenomena. The process of measurement is central to quantitative research because it provides the fundamental connection between empirical observation and the mathematical expression of quantitative relationships (Lisa, 2008). Creswell (2013) states, quantitative research "employ strategies of inquiry such as experimental and surveys, and collect data on predetermined instruments that yield statistical data. The findings from quantitative research can be predictive, explanatory, and confirming. The next section focuses on quantitative research methodology.

Research Respondents

The students in Central Mindanao Colleges were the respondents of this study. A total of 100 respondents were needed and selected using non probability sampling, specifically the quota sampling technique. Quota samplingis defined as a non-probability sampling method in which researchers create asample involving individuals that represent a population. Researchers chosethese individuals according to specific course. In the selection ofrespondents only thosestudents who took Criminology course in Central Mindanao Colleges.

Instruments

Cybercrime Awareness Questionnaire. The scale is an Efficacy of Online Learning adopted from F Alotaibi, S Furnell, I Stenge - 2016 (2016). The tool was composed of 9 items that measures the levels of cybercrime awareness of criminology students. The tool is 9 items construct from 5 (Strongly Agree) to 1 (Strongly Disagree).

Cybercrime Prevention Attitude. This questionnaire was adopted from PA Amosun, OA Ige. The tool is composed of 10 items that measure the Cybercrime Prevention of Criminology students. The tool is a 10- itemconstruct from 5-Strongly Agree to 1-Strongly Disagree.

Statistical Tools

This study utilized the following statistical tools that are needed in the analysis and interpretation of the data gathered the frequency count and percentage distribution.

The weighted mean was used to determine the cybercrime awareness and cybercrime prevention attitude of criminology college students

Descriptive statistics of frequency counts and percentages were used in analysing demographic variables and research questions while the inferential statistics of Chi-square (x^2).

Mean. Ismeasured of central tendency and gives us an idea about where the data seems to cluster around. The weighted mean is calculated by multiplying the weight (or probability)

Standard Deviation.is ameasured dispersion of a dataset relative to its mean The standard deviation is calculated as the square root of variance by determining each data point's deviation relative to the mean. If the data points are further from the mean, there is a higher deviation within the data set; thus, the more spread out the data, the higher the standard deviation.

The Pearson product-moment correlation coefficient ismeasured of the strength and direction of association that exists between two variables measured on at least an interval scale.

RESULTS AND DISCUSSION

Level of Cybercrime awareness

Table 1 showed the level of Cybercrime awareness of criminology students.It garnered an overall mean of 3.44, and a standard deviation (SD) of 0.550with a

description of moderate. The SD results is less than 1 which denotes that respondent`s answers are not so dispersed from one another.

Table 1

Level of Cybercrime awareness

Cybercrime awareness	Mean	Std. Deviation	Description
1.I have heard about phishing	3.92	.916	High
2. I would click any link that Ireceive via email/SMS.	2.65	1.309	Moderate
3.I think that it is difficult to identifya fraudulent website	3.37	.996	Moderate
4. I think that a fraudulentemail/website/link is easy to identify.	3.26	1.006	Moderate
5. I would report being a victim of acybercrime if I had been a victim.	3.67	.993	Moderate
6. I have been the victim of fraudonline and lost money.	2.51	1.302	Moderate
7. I use other methods other than antivirussoftware to protect myself from cybercrimes.	3.53	1.100	Moderate
8. In general, I do not trust the websitesThat ask me to enter some details about my bankcard	4.19	1.075	High

Category Mean	**3.44**	**.550**	**High**

In terms of Cybercrime awareness, most of the item's scores are between the ranges of 2.51- 4.19, which is described moderate extensive. The highest mean score is 4.19 with a standard deviation of 1.075 in the *in general, I do not trust the websites that ask me to enter some details about my bankcard.* On the other hand, the lowest mean is2.51 with a standard deviation 1.305 in *I have been the victim of fraud online and lost money.* The category mean is 3.44, described as moderate extensive. This denotes that the criminology students are aware of cybercrimes

This supports the study of (National Cyber Security Policy, 2013). The policy plans to launch various national awareness programs across the country with a view to increase cybercrime awareness. The policy calls for a public and private partnership in order to tackle the cybercrimes. The evolution of digital technology has changed the way in which we, as a global society, socialize and conduct business. This growth has led to an increasing reliance on technology, much more interconnected ness and in turn, an expansion of criminal opportunities, Known now as "cybercrime". This study aims to explore the experience of victimization, perceptions of cybercrime and use of online crime prevention strategies.

This also supports the study (UNODOC 2013). The proportion of cybercrimes detected through investigation remains very low(According to the 2013 Study conducted by the United Nations Office on Drugs and Crime (UNODOC), responding countries estimated that the reporting of cybercrimes to the police by victims was in the range of slightly upwards of 1 per cent.

Lastly Supports the Study (2010 EU Communication)National governments should launch publicity campaigns to help people protect themselves against on-line crime. Simple security precautions, especially among youngsters, could considerably reduce cybercrime. Awareness raising via sustained media campaigns, television adverts and ad hoc websites is just one option to achieve this aim.

Cybercrime prevention attitude

Table 2 presented the cybercrime prevention attitude of criminology students. The overall mean is 3.91 while its standard deviation is 4.89 With an Interpretation of High. The standard deviation is less than 1 which denotes that respondents' scores are closer to the mean.

Table 2

Level of Cybercrime Prevention Attitude

Cybercrime Prevention Attitude	Mean	Std. Deviation	Description
1.I think that antiviruses are enoughto protect me from a cybercrime.	3.40	.968	Moderate
2. I use other methods other than antivirus software to protect myself from cybercrimes.	3.79	.918	Moderate

3.I would make people aware of how andwhat damage will viruses do to ourcomputers and files.	4.31	.616	High
4. I will report any obscure materials in the social media	3.93	.786	High
5. I would report being a victim of acybercrime if I had been a victim.	4.15	.694	High
6. I had a virus or other harmful software on one of my devices	3.02	1.229	Moderate
7. I will only use visited websites if I know and trust them.	4.28	.718	High
8. I will install anti-virus software on one or moreof my devices.	4.05	.842	High
9. I will check my browser history to see which sites I`ve visited	4.04 / 4.13	.781 / .804	High
10. I reduce the amount of personalinformation I disclose			High
Category Mean	**3.91**	**.489**	**High**

In terms of cybercrime prevention, it shows a highest mean 4.15 with a standard deviation of 6.94 in *I would report being a victim of a cybercrime if I had been a victim.* On the other hand, the lowest mean is 3.02 with a standard deviation of 1.229 in terms

of *I had a virus or other harmful software on one of my devices.* The category Cybercrime prevention 3.91describes as High. This means that cybercrime prevention is important among students.

This study supports the study. (M.L. Williams and M. Levi 2015) In organisational settings, there are issues of legacy systems that if left unpatched, create vulnerabilities such as those that led to the large data breaches at JP Morgan in 2014 and the US Office of Personnel Management in 2015, the latter leading to the 'theft' of information from the security clearance applications of 19.7 million people, plus 1.8 million spouses and partners of applicants.

Also proves the study (Drew, J.M. 2020) A Study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies.

Relationship between the variables

Table 3 showed the relationship between cybercrime awareness and cybercrime prevention attitude of criminology students. According to the data below mentioned, the data got .429 of multiple r with a P value of .000 And with an interpretation of Significant which means very low correlation, therefore, "there is a significant relationship between cybercrime awareness and cybercrime prevention attitude of criminology students in central Mindanao colleges (CMC)"

Table 3. Relationship between Cybercrime Awareness and Cybercrime Prevention Attitude

INDEPENDENT VARIABLES	Cybercrime Prevention Attitude		
	r	p-value	Remarks

Cybercrime Awareness	.429	.000	Significant

(Journal of Criminology research policy and practice 2019) This proves the study that Identifies key levers, In particfular perceived prevalence and harm of cybercrime, as critical in the use of online crime prevention strategies by potential victims. As such, this study provides an important evidence base on which to develop more effective online crime prevention education and awareness campaigns to reduce cybervictimisation.

(Drew, J.M. 2020) This research also proves takes different perspective from much of the previous research, seeking to be better understand how attitudinal factors (perceived prevalence of cybercrime) might motivate or influence the use of online crime prevention strategies by potential victims

(Brunton 2013) Educational researchers were celebrating the transformation the Internet hadbrought toeducation, when the criminal behaviours aided by the anonymity offered by the Internetwere confounding the many users across the globe.

CONCLUSION

That most criminology students of central Mindanao colleges who has moderate experience of cybercrime needs to make cybercrime prevention one of their priorities to prevent worse experiences with regards to it. The relationships between the variables show that there is a significant relationship between cybercrime awareness and cybercrime prevention.

REFERENCES

Akgün, A. E., Keskin, H., & Byrne, J. (2009). Organizational emotional capability, product   and process innovation, and firm performance: An empirical analysis. Journal of Engineering and Technology Management, 26(3), 1   03-130. Retrieved on February 7, 2019 from https://goo.gl/T4mve3

Brunton (2013). Awareness andPerception of Cyber Crimes and   Cyber Criminals, International Journal of Cybersecurity Intelligence &   Cybercrime, 2019, Vol 2, Issue 1, Page 1-3 (HannaraeLee 2019)

Creswell_(2013)https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/Referen cesPapers.aspx?ReferenceID=1485543

Drew, J.M. (2020)a Commentary on Officer Well-being During COVID-19 – NCBI

Gupta, G. K. (2014). Introduction to data mining with case studies. PHI Learning Pvt. Ltd. Retrieved on January 6, 2019 from https://goo.gl/PgbaxT

Journal of Criminology research policy and practice (2019) Journal of Criminological Research, Policy and Practice

(Lisa, 2008). https://methods.sagepub.com/reference/sage-encyc-qualitative-research-methods

Macaraig, J. M. R. (2013). Urban Greenspace, Civil Society and Science: The Creation and Management of the Rouge Park, Ontario, Canada (Doctoraln dissertation). Retrieved on February 7, 2019 from https://goo.gl/gkt4MB

M.L. Williams and M. Levi 2015https://orca.cardiff.ac.uk/95521/1/ Cyberfraud%20and%20the%20Implications%20for%20Effective%2 0Risk%20final.pdf

National Cyber Security Policy, 2013 https://en.wikipedia.org/wiki/National_

    Cyber_Security_Policy_2013

Recent (2010)EU Communication "A digital agenda for Europe"

    https://link.springer.com/article/10.1007/s12027-014-0333-4

Solak, D., &Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View

    ofComputer Science Students. Procedia-Social and Behavioral

    Sciences, 182,590-595Retrieved on February 7, 2019 from

    https://goo.gl/TUduib

United Nations Office on Drugs and Crime (2020) "Comprehensive Study on

    Cybercrime", February 2013, p. 117.

(UNODOC 2013https://www.unodc.org/documents/organizedcrime/

    UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_21021

    3.pdf