"Cybercrime Vulnerability of Saint Mary's University Students"

Esthyre Kate A. Bayangan

Faculty of the College of Advanced Education Ifugao State University Master of Arts in Criminal Justice with Specialization in Criminology

DOI: https://doi.org/10.47772/IJRISS.2026.100400324

Received: 11 April 2026; Accepted: 16 April 2026; Published: 08 May 2026

ABSTRACT

The commission of cybercrimes in the advent of technological advances, industrialization, and globalization is inevitable. This is one of the prevailing challenges in universities that must be addressed. Using a quantitative, descriptive, comparative method, this study endeavored to bring out baseline information on the vulnerability of SMU students as offenders of cybercrimes. The findings included profile variables such as gender, year level, school, and frequency of Internet use. This study was dominated by female respondents, with almost equal distribution in terms of year level and the considerable proportion concerning school, and most of the respondents had a frequency of Internet use between 4 – 8 hours. Further, findings showed that SMU students had a very low probability of committing cybercrime: 1) Offenses against confidentiality, integrity, and availability of computer data systems; 2) Content-related offenses; and 3) Computer-related offenses. Lastly, gender affects the responses of SMU students in terms of offenses against confidentiality, integrity, and availability of computer data systems and content-related offenses but not in computer-related offenses. Only the responses between First- and fourth-year students vary for the year level. Meanwhile, the school of the respondents influences the responses of students but not the frequency of Internet use. The researchers recommend enhancing and expanding policies and guidelines in Internet use and virtual learning to include safe browser systems. For future research, it is highly recommended to look at the side of the victims and not only the vulnerability of becoming offenders.

Keywords: Computer and Content-related Offenses, Cybercrime Act of 2012, Hacking, Phishing, Privacy Act of 2012

INTRODUCTION

The growth of computer technology is one of the goals of every country. Computer technology makes our tasks easier and allows people to communicate. It gives an advantage to an upgrading country like the Philippines. However, despite the positive effects that internet and computer technology could have, there are still negative effects that it could have, including the emergence of Cybercrimes. Cybercrimes are criminal acts that involve or use a computer, computer network, or network device. Cyberspace became a new target of criminals because it made it easier for them to fool other people.

As technology improved and almost everything relied on the Internet and technology, it also became easier for criminals to commit crimes with just a click of their hands. The online world or cyberspace is where people share their life and everyday being without thinking that a faceless criminal could be watching them. Crimes committed in cyberspace are termed cybercrimes which include Offenses against the confidentiality, integrity, and availability of computer data and systems, Computer-related Offenses, and Content-related Offenses that are provided by (Philippines) Republic Act No. 10175, known as the Cybercrime Prevention Act of 2012.

This is supported by Khiralla (2020) claiming that cybercrime became easier because computers and cellphones became affordable to the people. Another evident study premises the fact that cybercrime rates have increased in the past years up until now. According to the Department of Justice (DOJ), citing data from the US-based National Centre for Missing and Exploited Children (NCMEC), cases of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines increased by 264.6 percent. Reports escalated during the imposition of

community-enhanced quarantine almost three times that of cases reported in 2019. The number of cases from March-May in 2019 surged from 76,561 to 202 605 in the same period in 2020.

The online world's size expanded twice, and criminals will have a greater opportunity of victimizing innocent individuals. Now that the other universities and schools turned back to the normal mode of learning, the traditional face-to-face class, we cannot eradicate the fact that people still use computers and the Internet, especially young people. The evolution of technologies and today's essentials has driven the immersion unto these things. We are already in the digital world, which keeps us drawing nearer daily. Moreover, we are moving forward to the future and not backward. A study by Swansea University (2020) showed that about 25% of the students reported spending four hours online, with the rest indicating that they spent between one to three hours a day. In addition, to the surveyed study on Information Society Statistics - Households 2019, nearly 80% of people use the Internet daily. This can be supported by Burden (2023) who found significant relationship o level of self-control, time spent participating in routine online activities to cybercrime offending and being a victim-offender as well.

The Philippines, should not be relieved by the statistics result, as it is shown in the result of the survey of Statista (2022) "Countries with the highest number of internet users for February 2022" that the country is one of the biggest populations of online users in the world ranking number 11 globally. The Philippines is still prone to cybercrimes, especially today when almost everything relies on the Internet.

Emmanuel Tupas of the Philippine Star (2019) reported that according to the Philippine National Police Anti-Cybercrime Group (PNP-ACG), the number of cybercrime cases in the country increased by nearly 80 percent last year. In 2018, data from the ACG showed the recorded 4,103 cybercrimes higher by 79.64 percent compared to 2017, when 2,284 cases were reported. This report was before the pandemic happened.

This pandemic opened a new door for cybercriminals to commit cybercrimes. Cybercrimes continued to increase in the Philippines during this pandemic, involving students, teachers, and other personalities. According to Cudis (2021) in her report on Philippine News Agency (PNA), the general public should practice heightened vigilance against cyber criminals as reported online scams in the Philippines continue to go up, an official of the trade association of key players in the financial technology industry in the country.

The Police Regional Office of Region 2 employed an Anti-Cybercrime Unit at Santiago City Police Office because the issues of cybercrimes in the region increased since the pandemic started, and the citizens were engaged more in social media. The Anti-Cybercrime Group supported nearby provinces, including Nueva Vizcaya (Felina, 2021).

Government authorities in the country abstain from tolerating such crimes, thus setting statutes and regulations as preventive and punitive measures. Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, was enacted to regulate cyberspace access to and use. It punishes anyone who commits offenses stated from there, such as offenses against the confidentiality, integrity, and availability of computer data and systems, computer-related offenses, and content-related offenses. However, several of its provisions have been seriously challenged for their constitutionality in the case of Disini, Jr. et al. vs. The Secretary of Justice, G.R. No. 203335, February 11, 2014 (*En Banc*). The High Court ruled some provisions, such as Sections 4 (c) (3), Section 12, and Section 19, as void and unconstitutional.

Lastly, the Court resolved to leave the determination of the correct application of section 7 that authorizes prosecution of the offender under both the revised penal code and republic act 10175 to actual cases, except for the crimes of: (1) Online libel as to which, charging the offender under both Section 4(c)(4) of Republic Act 10175 and Article 353 of the Revised Penal Code constitutes a violation of the proscription against double jeopardy; and (2) Child pornography committed online as to which, charging the offender under both Section 4(c)(2) of Republic Act 10175 and Republic Act 9775 or the Anti-Child Pornography Act of 2009 also constitutes a violation of the same prescription. The rest of the challenged provisions were upheld to be valid and constitutional.

A study published by the Statistics Research Department (2021), by the year 2019 the National Capital Region of the Philippines had 2.7 million victims of cybercrime for those who had been sent fraudulent SMS or text scams and most of the cybercrimes committed in the Philippines is cyber bullying, hacking and phishing. Whereas, in a specific setting, cyber libel is leading particularly in Nueva Vizcaya, having 7 cases from January 2022 to May 2022, one case (1) is dismissed and six (6) are still pending, according to Regional Trial Court Branch 29 designated as Family Court and Specialized Commercial Court or "Cybercrime Court" of Nueva Vizcaya North District.

This study is being conducted to determine the involvement of students from the four schools of Saint Mary's University's in the various cybercrimes mentioned above. Also to determine the vulnerability of these students and to know some security measures to take to protect these students from being involved in these different crimes. The study's significance remains considering the return of a full face-to-face learning set-up. Internet use is still continuous as evidently students may refer to it for non-educational and educational purposes. Hence, students' vulnerability to cybercrimes is not yet relieved, thus a need to render attention to suppress further crimes.

As a result, the following people will benefit from the findings of this study: the students from the four school of Saint Mary's University, who are the primary respondents in this study. Herein, included as well the Senior High, Junior High, and grade school students, regardless of whether they experience online class still can't deny the fact that they are already using the Internet. Thus they are not excused from being vulnerable to cybercrime. With the study result of the study, they may be more aware and cautious of their actions towards internet discipline during online class, regular class, and in their daily use; the Saint Mary's University Administration may be more aware of their students' cyber security situation. They may be able to assist students in dealing with problems and situations that may arise in the online environment; parents, because they are the ones who should know about their child's situation, this study could raise awareness among parents that their children needed protection from them because the online world is a harsh environment; The PNP's cybercrime group, they could use the results of this study to give recommendations to the school and students on how to address these types of issues in online world; The researchers for this study will help them bring out their expertise in their future work as law enforcers and will also raise awareness about cybercrime. Future researchers will be able to use this study as their basis and reference as well as their Review of Related Study in conducting research related to the involvement and vulnerability of students in cybercrime.

Cybercrime Offenses

Section 4 of Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, was categorized into three acts constituting cyber offenses, namely: (a) Offenses against confidentiality, integrity, and availability of computer data and systems; (b) Computer-related Offenses; and (c) Content-related Offenses.

First, Offenses against confidentiality, integrity, and availability of computer data and systems include the crime of (1) Illegal access, (2) illegal interception, (3) data interference, (4) system interference, (5) device misuse, and (6) cyber-squatting. Pulta (2020) of the Philippine News Agency quoted the Department of Justice (DOJ) warning the public about emerging security threats during online classes. The DOJ has issued a public alert in response to the rising security threats connected with online classrooms amid the coronavirus disease (Covid-19) epidemic, as public schools resume blended learning, including online classes.

Students are vulnerable to these cybercrimes because they visit unknown websites and log in, entering their passwords and personal information. The abuse of passwords is one of the most common ways to compromise data confidentiality (Grivna & Drápal, 2018). Hackers would look for an easily guessed password (e.g., Password1) to attempt in a conventional Brute Force assault, wherein the attacker repeatedly guesses, or has a software guess, a range of different passwords until it is accurate (Grivna & Drápal, 2018).

Second, Computer-related offenses refer to crimes committed using a computer or through cyber space such as (1) fraud, (2) forgery, and (3) identity theft. All of these involve money which is the primary motivation of the perpetrators, and the same cannot be denied that students may involve in this type of cybercrime due to financial need for money.

The Federal Trade Commission (FTC) received 371,061 identity theft reports in 2017, accounting for 13.87 percent of all reports received that year. More than 133,000 reports were received about information being used to open a new credit card account or to misuse an existing one. According to a Tulane University blog, there was a 23 percent increase in credit card fraud and a 46 percent decrease in tax fraud.

According to the report, at least 200,000 people are addicted to internet sexual material. However, pornography and cybersex addiction are growing increasingly frequent. In a study of 339 students, 10.3 percent scored in the clinical range for cybersex addiction. Furthermore, we discovered substantial gender differences between the clinical and non-clinical range groups, with men scoring higher in the clinical range for cybersex addiction (Giordano & Cashwell, 2017).

Doring et al. (2015) conducted a study on Online Sexual Activity Experiences among College Students: A Four-Country Comparison, and the results are impressive. Most participants (89.8 percent) and sexual entertainment (76.5 percent) reported accessing sexual information and entertainment online. Almost half (48.5 percent) acknowledged looking for sexual products online, and a sizable minority admitted to cybersex (30.8 percent). Only 1.1 percent of participants paid or received money for online sexual services (0.5 percent). Individuals generally reported occasional encounters with all kinds of OSA in the previous three months. Men used sexually arousing content online at a higher rate and frequency than women.

Hackers broke into several lectures at a prestigious school in Kolkata, displaying filthy movies on the screen and threatening students and professors, prompting the school to abandon online education. The hackers used violent language and threatened students with rape and murder, according to a parent who spoke to Outlook. As a result, professors were forced to suspend online classes (Roy, 2020).

Students' involvement in cybercrimes

Undeniably, students may be involved in a wide range of cybercrimes in today's world. They may be victims, perpetrators, or both. The poll reveals some of the online activity habits among Maharasthra's children, according to a study conducted by Express Computer, (2020). Forty-six (46) percent of students surveyed said they were addicted to their devices (phones, tablets, and computers) which had a negative impact on their studies.

Furthermore, it was found that the attackers are sometimes the students themselves Hogdan, (2020). The Miami-Dade Schools Police Department (M-DSPD) has been arrested in connection with the cyber-attacks that have hampered teaching and learning since the beginning of the school year. An IP address linked to the attacks was traced to a 16-year-old junior at South Miami Senior High School, according to M-DSPD officers. The student admits to executing eight Distributed Denial-of-Service cyber-attacks, meant to overwhelm District networks, particularly web-based services needed for School Online.

In higher years, undergraduate students who visit browsing center participates more in cybercrime than those who do not. The main reason for this is that those who attend a browsing center will have no one to monitor their activity, therefore they are more likely to engage in undesirable behaviours such as cybercrime.

Screening down to gender differences in online participation, completed literature about engagement patterns of online learners found that women were more likely than men to collaborate Yaghmour, (2012). In the same context, a study by Prinsen et al. (2007) and Caspi et al. (2008) found that females posted more messages than males. These do not conclude that males are less engaged in cybercrimes as very few are committed by females Hutchings A and Chua Y T.

On the other hand, Prasad, (2016) showed that male undergraduate students have more internet addiction and cybercrime participation than female undergraduate students in a study on Internet Addiction and Cyber Crime Engagement of Undergraduate Students. The explanation for this is that male students have more access to the internet than female pupils. In addition, Taylor (1999) states that the gender ratio at hacking conferences is approximately one female to every hundred males and that often females are only transiently involved in the hacker subculture. They are more oriented in using the internet unlike males who prefer to look for newer technologies exposing them to be likely involved in cybercrimes. The idea is again supported by the conclusions

of Anderson and Haddad, (2005) that female students are less hesitant to engage in the online environment as they have more control over their learning.

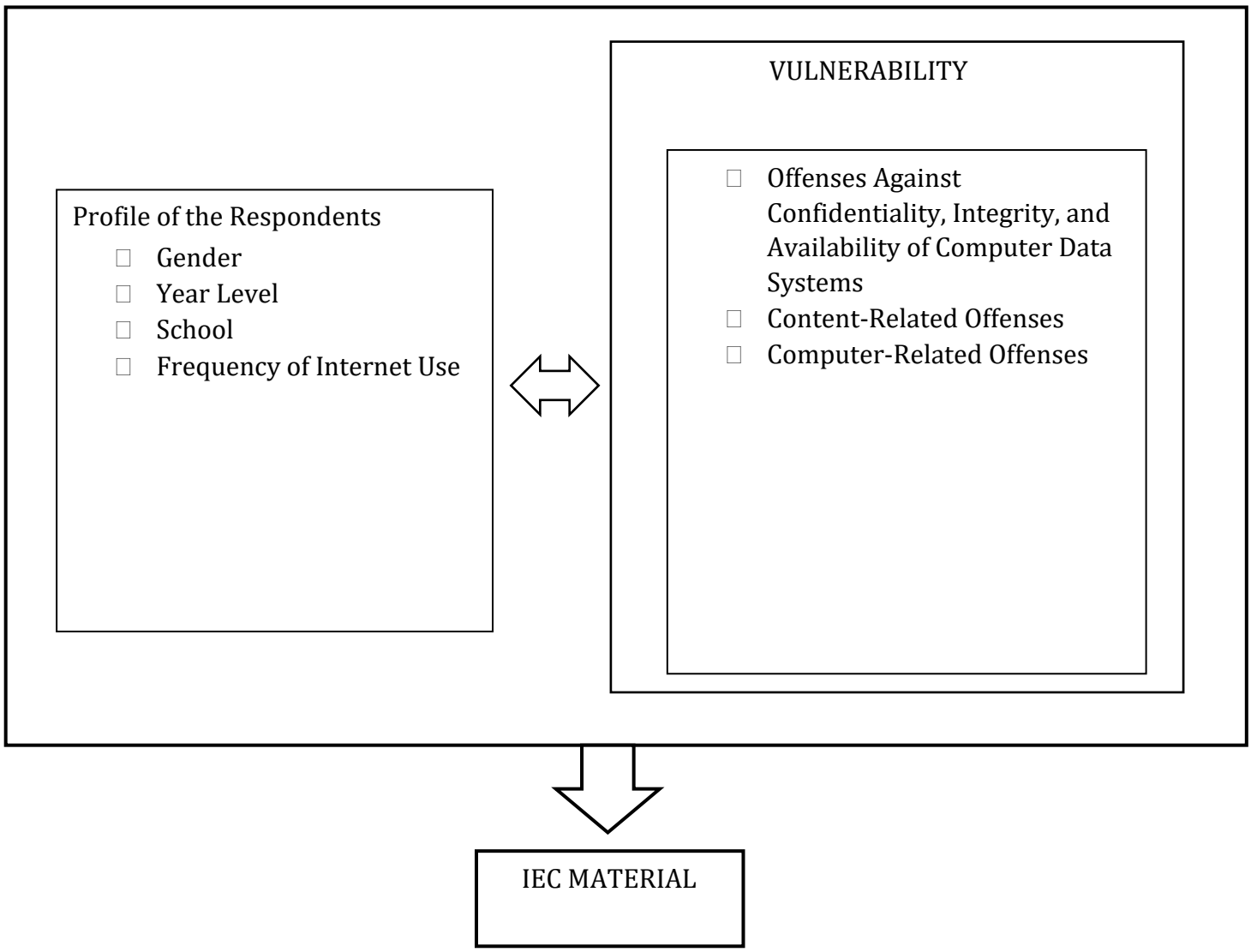
Conceptual and Analytical Framework

The concept of this study is important and unique for it will tell us if the Saint Mary's University students are vulnerable to committing cybercrime. It is important to know if there are factors that could affect their vulnerability and their significance in committing such crimes. Cybercrime is a common crime that should be given importance, especially today, because the generation is adapting more to technology.

The conceptual framework of this study illustrates the significant differences in the level of cybercrime vulnerability of Saint Mary's University students- as the dependent variable- when grouped according to profile- as the independent variable. The profile of the respondents – these were considered as these were perceived to affect the vulnerability of students to commit cybercrimes. Their gender, year level, school and their frequency of internet use were factors that are being considered to have an impact on students as they navigate and utilize the internet relative to their personal, academic and other undertakings.

The dependent variable focuses on the different offense categories provided by Section 4 of Republic Act No. 10175 These are Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems, Content-Related Offenses, and Computer-Related Offenses. The researcher will determine the level of vulnerability of the respondents to commit such crimes.

Figure 1 Research Paradigm



Statement of the problem

This study endeavored to find out the cybercrime vulnerability of the Saint Mary's University students in the first quarter of 2023. To be specific, the study aimed to answer the following problems:

What is the profile of the respondents according to:

1.1 Gender

1.2 Year level

1.3 School

1.4 Frequency of Internet Use

What is the level of cybercrime vulnerability of the Saint Mary's University students in terms of:

1.5 Offenses against Confidentiality, Integrity, and Availability of Computer

Data Systems

1.6 Content-Related Offenses

1.7 Computer-Related Offenses

Is there a significant difference in the level of cybercrime vulnerability of the Saint Mary's University Students when grouped according to profile?

What informational and educational campaign material could be crafted to provide relative information about cybercrime vulnerability?

Statement of Null Hypothesis

There is no significant difference in the students' cybercrime vulnerability level when grouped according to profile.

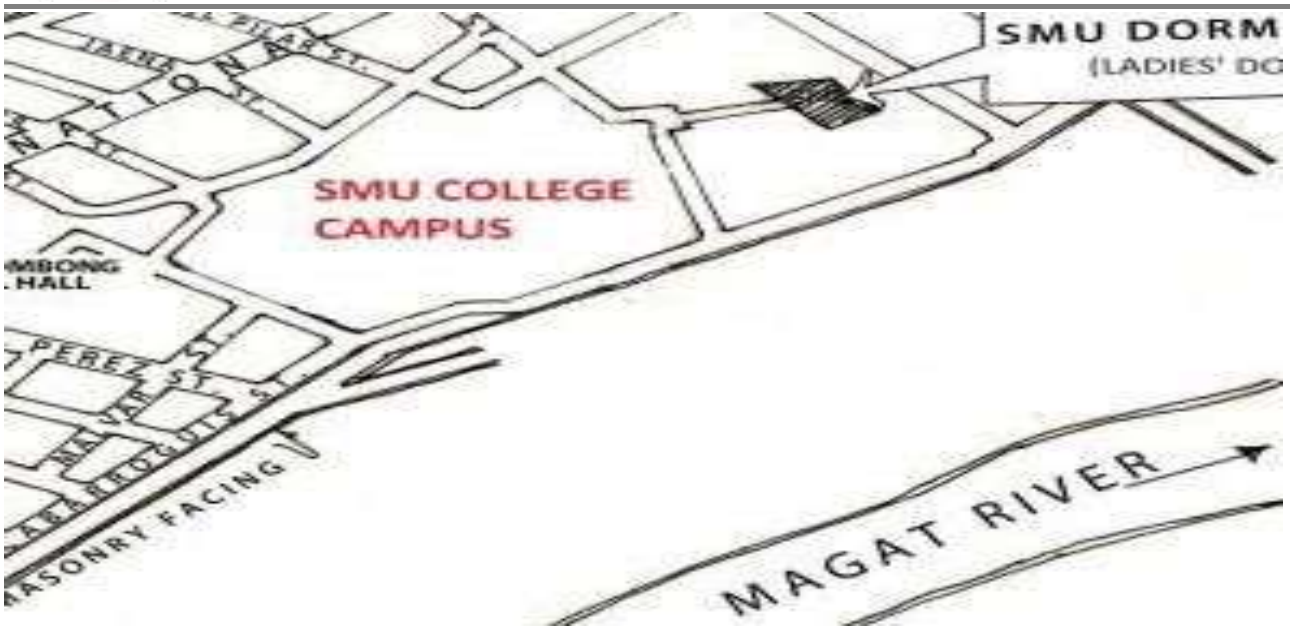
METHODOLOGY

Research Design

In the study, researchers utilized a descriptive comparative method which provides descriptive information concerning the vulnerability of students from Saint Mary's University to cybercrimes. The descriptive part was used for the profile, and level of vulnerabilities. At the same time, the comparative part was used in determining the significant differences in the level of vulnerability of Saint Mary's University students to cybercrimes when grouped according to profile. The data gathered from the respondents were quantitatively examined.

Research Locale

Figure 2 Map of Saint Mary's University College Campus (https://smu.edu.ph/home/maps-and-directions/*)*



The research was conducted at Saint Mary's University situated at San Vidal Corner Ponce Street, District 4, municipality of Bayombong, province of Nueva Vizcaya. Saint Mary's University is a Private Catholic School founded on June 1928 It is divided into four schools: the School of Health and Natural Sciences, the School of Engineering Architecture Information and Technology, the School of Accountancy and Business, and the School of Teacher Education and Humanities. This research was conducted at Saint Mary's University because the focus of the study is to determine the vulnerability of students and the target respondents are the students of the university from the four schools.

Research Respondents

The study respondents came from four (4) schools in all year levels: School of Teacher Education and Humanities, School of Health and Natural Sciences, School of Accountancy and Business, and School of Engineering Architecture Information Technology. Sample sizes were selected from the total population of Students using the Raosoft Calculator, and from the Sample Size, Sample Strata for each School were determined using proportionate sampling or stratified random sampling. The strata were equally divided to determine the number of respondents for each department in that certain school. Respondents were first- to fourth-year students of Saint Mary's University.

Research Instrument

To gather the data needed, the research instrument is a survey questionnaire made by the researchers based on the Statement of the problem and the provision of the Cybercrime Prevention Act of 2012 or the R.A. 10175 of the Philippine constitution. The research instrument is divided into different areas to address the concerns stated in the statement of the problem of the study.

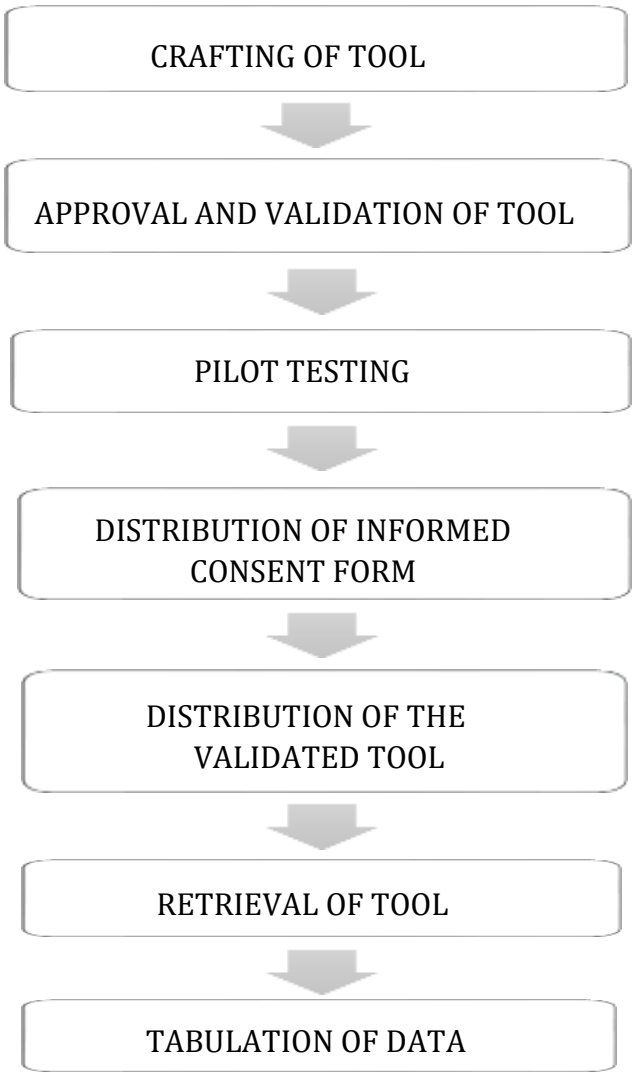
The first part of the questionnaire reflects the profile of the respondents. This was the independent variable of the study; it determines the gender, year level, School, and internet usage frequency of the respondents. The second part of the questionnaire determined students' vulnerability level to cybercrimes. They were asked to assess their vulnerability based on situations and again following a probability scale.

The research instrument made by the researchers was checked by the Panel of evaluators and Research Chair and underwent a series of validation by the experts and made sure that the questionnaire was reliable and served its goal of obtaining accurate data for determining the level of vulnerability of the students of Saint Mary's University. The results were the researchers' basis for drawing conclusions and determining the significant differences between the variables mentioned in the study. The instrument was pilot tested by students of Saint Mary's University with the help of the University statistician.

Data Gathering Procedure

The figure below demonstrates the flow chart of the researchers' procedures in Data Gathering.

Figure 3 Steps in the Gathering of Data.



The data gathering commenced with the crafting of tools by the researchers. After the tools had been crafted, they were subjected to the University Research Center for validation and approval by the University Research Ethics Board. After being issued clearances and approval certificates, the researchers sent letters to inform the School officials and other authorities of Saint Mary's University (SMU) to get their consent before the researchers gathered data. Data gathering commenced in January 2023.

Upon given consent by the authorities, the instrument was pilot tested to a smaller group from Saint Mary's University. This is to provide data about the feasibility of the instruments used in the study before it was launched on a larger scale which was implemented in the four schools (STEH, SHANS, SEAIT, and SAB) of Saint Mary's University. The questionnaires were administered to the respondents using a Survey Questionnaire. Action for the questionnaire distribution to the first participants for the pilot testing was done after the study's objective was explained to them that the same should be used to describe the cybercrime vulnerability of students.

The effectiveness of the pilot study accounts for the distribution of the informed consent form following the distribution of the validated tool to the target respondents. After the questionnaire had been answered, the researchers retrieved the same for the tabulation of data. The researchers followed the Minimum Health Protocol to avoid the risk of getting infected with the covid19 virus.

Treatment of Data

The data gathered in this were subjected through the following statistical treatment:

1. The frequencies and percent were presented for the profile variables of the respondents.

2. Mean ratings and standard deviations were used to determine the students' vulnerability to the identified cybercrimes. The following scale was used:

Table 1 Likert Scale for the Level of Cybercrime Vulnerability of SMU students.

Mean Range	Description	Interpretation
3.50 – 4.00	Very High Probability	Will always be involved in cybercrime
2.50 – 3.49	High Probability	Will be involved in cybercrime
1.50 – 2.49	Low Probability	Might be involved in cybercrime
1.00 – 1.49	Very low Probability	Will be less likely involved in cybercrime

T-test was used for the gender variable while One-way ANOVA was used for the year level, school and frequency of Internet use.

Ethical Considerations

The researcher ensures ethical protocols by initially informing all respondents and requesting their consent using a letter to participate in the research before distributing. The researcher emphasized that participation in the study will be voluntary, and respondents were under no obligation to answer the questionnaires if they chose not to. Privacy was of utmost importance, and the confidentiality of each respondent's information will be a primary concern. The researchers will ensure that all the personal data that is collected in this study will be gathered and treated with confidentiality. Since the researchers will strictly follow the ethical standards of conducting research, this study is intently for research and academic purposes only.

Conflict of Interest

There was no conflict of interest, and the researchers did not profit from the research. It is solely for the purpose of study and for the benefit of the entire SMU community.

Confidentiality and Data Protection

All collected data and each respondent's privacy remained confidential and shall be respected by the researchers. All data were collected through a survey questionnaire. Furthermore, the researchers used number codes instead of names or emails to protect the respondents' identities. All the information was entered into an excel spreadsheet in a number-coded style. No one, except the study's researchers, was allowed to do so.

Furthermore, all the data were only in our possession for the second semester of the academic year 2022-2023. Finally, after the study was completed, bounded in a book, saved on a CD, and sent to the Research Center and Library, all raw data, including questionnaire replies, were disposed of by burning and erasing softcopies. Only the overall results are stored in the Study Center and Library for future research.

Management of Vulnerability

To control the respondents' vulnerability, all the research details and the questions were kept private. They were instructed on how to complete the questionnaire in a manner and language that they will fully comprehend.

Respondents had the option to continue participating in the research or to pull out or withdraw from the research at any time after fully understanding the objective and nature of the study.

Risk/Benefit Ratio

There are no documented side effects from participating in this study. In the unlikely event that the respondents asked for greater information about the study, the researchers informed them of its significance for the study's benefit. Regardless of whether the hypotheses are accepted, the researchers will explain the significance of the study's findings. Furthermore, suppose they select to request a copy of the summary of the findings. In that case, the researchers can email them a copy of the synopsis. The volunteers were not paid for their involvement in this study. Still, the findings will benefit all participants by providing advice. The researchers will adhere to safety protocol in administering questionnaires to avoid the risk of getting infected with Covid19.

Informed Consent

After receiving approval from the SMU-REB for data collection, the researchers chose the respondents. All consent and questionnaire were disseminated personally within the school premises. The respondents have read and understood the informed consent form. If they agreed to participate in the study, they picked "yes," indicating their willingness to participate. After giving their approval to participate, the respondent began filling out the research instrument.

Terms of References

The researchers and the research adviser have owned the intellectual property of the study results. This survey does not include any insurances.

RESULTS AND DISCUSSIONS

Section 1. Profile of the respondents

This section presents the profile of the respondents. The profile variables included in this study are gender, year level, school, and frequency of Internet use. These are premised on have been affected by the level of cybercrime vulnerability of the respondents. Table 2 shows the frequency and percent of these variables.

Table 2 Profile Variables of the Respondents

Profile Variables	Frequency	Percent
Gender		
Male	124	34.9
Female	231	65.1
Year Level		
First	89	25.1
Second	89	25.1
Third	89	25.1
Fourth	88	24.8
School		
SAB	83	23.4
SEAIT	96	27.0
SHANS	116	32.7
STEH	60	16.9
Frequency of Use		
12 hours and above	78	22.0
Between 8 – 12 hours	126	35.5
Between 4 – 8 hours	140	39.4

Below 4 hours	11	3.1
Total	**355**	**100.0**

There were more female respondents, 231 or 65.1%, while 124 or 34.9%, male respondents. Regarding year level, 89 or 25.1% for First, Second, and Third while 88 or 24.8% for the Fourth year students. Concerning to school, the respondents' size was proportionate to their overall population; thus, 83 or 23.4% were from the School of Accountancy and Business (SAB), 96 or 27.0% from the School of Engineering, Architecture and Information Technology (SEAIT), 116 or 32.7% were from the School of Health and Natural Sciences, and 60 or 16.9% were from the School of Teacher Education and Humanities. For the frequency of use, most of the respondents had a frequency of use *between 4 – 8 hours* having 140 or 39.4%, followed by between *8 – 12 hours* having 126 or 35.5%, *12 hours and above* having 78 or 22.0% while only 11 or 3.1% of the respondents had *below 4 hours.*

Section 2. Level of Cybercrime Vulnerability of Saint Mary's University Students

This section presents the level of cybercrime vulnerability of SMU students in terms of: 1) Offenses against confidentiality, integrity and availability of computer data systems; 2) Content-related offenses; and 3) Computer-related offenses. Tables 3 to 5 present the responses in these three aspects.

Table 3 Level of Cybercrime Vulnerability on Offenses Against Confidentiality, Integrity, and Availability of Computer Data Systems

Offenses against Confidentiality, Integrity and Availability of Computer Data Systems	Mean	SD	Qualitative Description
1. Hacking someone's account to see their activities.	1.07	.25	Very Low Probability
2. Stealing information of my other classmate for personal gain.	1.04	.23	Very Low Probability
3. Illegal processing of personal and private information	1.04	.22	Very Low Probability
4. Inputting malicious software that can threaten the integrity or use of data or programs.	1.03	.20	Very Low Probability
5. Destroying the computer data of others.	1.04	.22	Very Low Probability
6. Distributing copyrighted software, music and film.	1.21	.43	Very Low Probability
7. Using the name of other brands to make profit.	1.02	.15	Very Low Probability
Mean	1.07	.15	Very Low Probability

Legend: 1:00 – 1:49: Very Low Probability; 1:50 – 2:49: Low Probability; 2:50 – 3.49: High Probability 3.50 – 4.0 Very High Probability

It is shown in the table that the respondents had an overall mean rating of (M=1.07; SD= .15) indicating that SMU students had a *very low probability* that they would commit cybercrime offenses. This means that they will be less likely to be involved in cybercrimes. Specifically, the respondents had a very low probability of: Hacking someone's account to see their activities (M=1.07; SD=.25); Stealing information of my other classmate for personal gain (M=1.04; SD=.23); Illegal processing of personal and private information (M=1.04; SD=.22); Inputting malicious software that can threaten the integrity or use of data or programs (M=1.03; SD=.20); Destroying the computer data of others (M=1.04; SD=.22); Distributing copyrighted software, music and film (M=1.21; SD=.43); and Using the name of other brands to make a profit (M=1.02; SD=.15).

The least that SMU students could do is *using the name of the brands to make profit* while the most probable cybercrime that they could perform is the *distribution of copyrighted software, music and film.* These findings imply the reflection of SMU students' values and attitudes. This is an optimistic embodiment of the Christian spirit that Marian students are known for. Committing cybercrime is very much enticing when students are so attached to the computer and the Internet. While the school has restrictions over these known cybercrimes, other computer shops around the campus and students' mobile phones could not be censored.

Likewise, the image SMU has depicted since its foundation by the CICM fathers must have been embraced and influenced by the students. Even before the pandemic, policies and guidelines already restricted students from committing these cybercrimes. When the university had to go through synchronous and asynchronous classes, pertinent rules and regulations were crafted to prevent students from these cybercrimes and protect students' privacy, as reflected in the Data Privacy Act of 2012.

In a similar study, Saidul (2018) revealed that in some exclusive universities, the commission of cybercrime could not be so much observed and experienced since there were measures to prevent these. Some schools have censored their Internet server and limited access on sites that could endanger the operating systems including nudity, violent content and websites that are not trusted. But in some cases, these were not being reported or covered by media outlets so as not to expose the school's identity and name.

Notwithstanding, the studies of Khan (2019), Alghamdi (2020) and Hawdon (2021) presented that students in the recent years are prone to cybercrimes due to the proliferation of undertakings in the digital world and the Internet. They presumed that this is inescapable as the whole World Wide Web enters globalization and industrialization. The COVID–19 pandemic has also contributed to virtually establishing many academic activities and transactions. The most common of these cybercrimes were hacking, computer fraud, viruses (Trojan), worms and numerous forms of scams and harassment.

Table 4 Level of Cybercrime Vulnerability on Content – Related Offenses

Content – Related Offenses	Mean	SD	Qualitative Description
1. Sending obscene pictures and videos.	1.08	.28	Very Low Probability
2. Selling child pornography to make money.	1.00	.07	Very Low Probability
3. Sending unsolicited emails (spam), newsletters, messages and links to my online friends.	1.05	.29	Very Low Probability
4. Posting about untruth about someone.	1.05	.23	Very Low Probability
Mean	1.05	.16	Very Low Probability

Legend: 1:00 – 1:49: Very Low Probability; 1:50 – 2:49: Low Probability; 2:50 – 3.49: High Probability 3.50 – 4.0 Very High Probability

Table 4 showed that regarding cybercrime on content-related offenses, the overall mean rating of the respondents is (M=1.05; SD= .16) meaning that they had a very low probability of committing content-related offenses. To be specific, the respondents had a *very low probability* of: Sending obscene pictures and videos (M=1.08; SD=.28); Selling child pornography to make money (M=1.00; SD=.07); Sending unsolicited emails (spam), newsletters, messages and links to my online friends (M=1.05; SD=.29); and Posting about untruth about someone (M=1.05; SD=.23). The least here that SMU students could do is *selling child pornography to make money* while the most probable that they could perform is *sending obscene pictures and videos*.

Again, with the very low probability description, the respondents will be less likely be involved in cybercrimes on content-related offenses such as sending obscene pictures and videos, selling child pornography and posting about untruth things on someone. Further, they are very much aware of the consequences of these actions, thus a very low commission of these. These just show that SMU students are not vulnerable to committing cybercrime and their lessons in various Christian Faith Education (CFE) and other classes must have resonated in these actions.

These findings corroborate the study of Deora and Chudasama (2021) that some schools were able to regulate the proliferation of cybercrimes; hence, a low probability of committing these. However, the authors believe that the reports from these schools do not actually picture the whole big picture of cybercrimes. According to them, some common forms of cybercrimes like phishing: fake mail messages to get personal information, child pornography, soliciting and spreading obscene pictures and videos, and hacking website or computer networks are very difficult to stop since the spread of technology and the Internet. Many government agencies and private

establishments have tried different strategies but these people who commit cybercrime will always have their ways.

Table 5 Level of Cybercrime Vulnerability on Computer – Related Offenses

Computer-Related Offenses	Mean	SD	Qualitative Description
Making or forging a document for financial gain.	1.05	.25	Very Low Probability
Pretending to be someone to gain access to another's funds.	1.01	.10	Very Low Probability
Using the identity of someone for financial gain.	1.01	.12	Very Low Probability
Mean	1.02	.13	Very Low Probability

Legend: 1:00 – 1:49: Very Low Probability; 1:50 – 2:49: Low Probability; 2:50 – 3.49: High Probability 3.50 – 4.0 Very High Probability

It was also evident for computer-related offenses that the respondents had a very low probability of committing these cybercrimes with an overall mean rating of (M=1.02; SD= .13). Specifically, the students had a very low probability of: Making or forging a document for financial gain (M=1.05; SD=.29); Pretending to be someone to gain access to another's funds (M=1.05; SD=.29); and Using the identity of someone for financial gain (M=1.05; SD=.29). This would tell us that the students of SMU are less likely to be involved in cybercrimes.

During the pandemic, SMU heightened its policies and guidelines in its Learning Management System (LMS) to prevent students from performing cybercrimes that could distract their studies and affect the privacy of the school and students. The adaption of these policies and guidelines including the tradition in SMU and the many subjects of instilling desirable values, must have reverberated in these results of the study.

Just like offenses against confidentiality, integrity, and availability of computer data systems and content-related aspects, these computer-related aspects forging and using the identity of someone for financial gains are very difficult to detect and resolve. The studies of Monteith et al. (2021), Hawdon (2021), and Alghamdi (2020) claimed that cybercrimes in todays time had taken their greatest heights. Banks, private mail, and even government websites have had shares of these various cybercrimes, particularly forging and identity faking. Even the government has tightened its security measure with a two-factor authentication system and various verification measures. Hackers of cybercrime violators have always had their ways of performing their offenses.

Section 3. Comparison of the Level of Cybercrime Vulnerability

This section presents the level of Cybercrime Vulnerability of Saint Mary's University students in terms of their gender, year level, school, and frequency of internet use.

Table 6 Level of Cybercrime Vulnerability when Grouped According to Gender

Mean	Sex	Mean	SD	t	df	Sig.(2-tailed)	Decision Action
Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems	Male	1.10	.21	2.468	160.305	**.015**	Reject Ho
	Female	1.05	.11				
Content – Related Offenses	Male	1.08	.20	2.031	173.47	**.044**	Reject Ho
	Female	1.04	.12				
Computer – Related Offenses	Male	1.04	.17	1.547	171.899	.124	Accept HO
	Female	1.01	.10				

Legend: Reject the null hypothesis (Ho) if p-value (Sig.) is less than 0.05 (95% confidence level): Accept null hypothesis (H0) if p-value (Sig.) is greater than 0.05 (95% confidence level).

As shown, the male and female respondents had different responses regarding offenses against confidentiality, integrity, and availability of computer data systems (P-value=.015) and content – related offenses (P-

value=.044). Based on the computed p-values of these two groups of cybercrimes, which were less than .05, these differences are significant; therefore, the null hypothesis is rejected. In both of these, the male respondents had higher mean ratings, which implies that they are more likely vulnerable to committing cybercrimes than the female respondents under these aspects. There is no significant difference, however, concerning computer-related offenses, which means that gender is not a factor when it comes to cybercrimes under this category.

These results were similar to previous studies regarding the gender gap and cybercrimes. From a sample of 522 college students, Donner (2016) claimed that men were likely to engage in online offenses, such as digital piracy, cyber-harassment, and hacking. The author also believed this was fairly constant across the variables relative to socialization and Involvement in the internet world. Wadhwa (2017) likewise related that crime and criminality have been greatly associated with men since immemorial. This was carried on in the cyber world, where men were known to be the most offenders. Though women today, were also apprehended committing cybercrimes, more males were being caught as offenders.

Meanwhile, Lazarus *et al.* (2022) had different findings. They found out that men and women vary in terms of their commission on cybercrimes. In socio-economic which relates to cybercrime that can be defined as the *computer or/and Internet-mediated acquisition of financial benefits by false pretense, impersonation, manipulation, counterfeiting, forgery, or any other fraudulent representation of facts such as online fraud, credit card fraud, online embezzlement and romance scams,* there is no difference between men and women. However, in terms of psychosocial cybercrime which refers to *digital crimes that are primarily psychologically driven to cause shock, distress or harm to a person, where monetary gain is not the primary objective. They include cyberstalking, cyberbullying, and online harassment,* they found out that women were worse than men.

These contradicting findings could be relative to the context in which the studies were conducted. The findings that men were more likely to commit crimes than men may relate to the idea that society is patriarchal and the nature of men being traditionally perceived as more straightforward and possessive than submissive women. Likewise, the condition where men held the most important positions in society; thus, a more probability of becoming offenders. Lazarus *et al.* (2022) pointed out, however, that women are worse than men since they generally recognize crime as more serious than men, especially those crimes that concern them unreasonably, such as harassment and online abuse, causing physical harm.

Table 7 Level of Cybercrime Vulnerability when Grouped According to Year Level

Mean	Year Level	Mean	SD	F	df	Sig.	Decision Action
1. Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems	First	1.03	.08	3.446	3	**.017**	**Reject HO**
	Second	1.07	.13				
	Third	1.06	.12				
	Fourth	1.10	.23				
	Total	1.07	.15				
2. Content – Related Offenses	First	1.03	.10	1.761	3	.154	Accept Ho
	Second	1.04	.12				
	Third	1.06	.17				
	Fourth	1.08	.21				
	Total	1.05	.16				
3. Computer – Related Offenses	First	1.01	.05	.928	3	.427	Accept HO
	Second	1.02	.12				
	Third	1.04	.18				
	Fourth	1.03	.14				
	Total	1.02	.13				

Legend: Reject the null hypothesis (Ho) if p-value (Sig.) is less than 0.05 (95% confidence level): Accept null hypothesis (H0) if p-value (Sig.) is greater than 0.05 (95% confidence level).

Table 7 reflected a significant difference in the responses on the offenses against confidentiality, integrity, and

availability of computer data systems with a p-value of .017 and less than .05, which rejects the null hypothesis. Meanwhile, there are no significant differences between content–related offenses (P-value=.154) and computer – related offenses (P-value=.427). Table 8 shows the Post Hoc result (LSD) of the significant difference in the aforestated cybercrime.

Table 8 Post Hoc for the Level of Cybercrime Vulnerability on the Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems

Mean of the Dependent Variable	(I) Year Level	(J) Year Level	Mean Difference (I-J)	Std. Error	Sig.	Decision Action
Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems	First	Second	-.04022	.02345	.087	Accept HO
		Third	-.03202	.02345	.173	Accept HO
		Fourth	-.07515*	.02352	**.002**	**Reject HO**
	Second	Third	.00820	.02345	.727	Accept HO
		Fourth	-.03493	.02352	.138	Accept HO
	Third	Fourth	-.04313	.02352	.068	Accept HO

Legend: Reject the null hypothesis (Ho) if the p-value (Sig.) is less than 0.05 (95% confidence level): Accept the null hypothesis (H0) if the p-value (Sig.) is greater than 0.05 (95% confidence level).

As shown, the difference exists only between First and Fourth-year students, meaning their responses vary. Further, it showed that Fourth-year students had a greater mean rating, meaning they are more likely to perform cybercrimes than Third, Second, and first-year students. First-year students are the least likely to commit cybercrimes.

The condition that fourth-year students were more likely to commit cybercrimes than the first year could be due to their age and exposure to the Internet. In a report by U.T. News (2021), millennial commit less crime than prior generations, and current conditions do not cause it but because of the life decisions of the younger generation. Since these students belong to the generation of computer and Internet natives, their difference was that fourth-year students were older and more exposed to the Internet. Hence, the result was the same as earlier findings that revealed the older population to be more prone to cybercrimes than the young ones. Munanga (2019) claimed that since higher-year students are now given more tasks to be searched on the Internet, they are more likely to be exposed to various attacks, including content and computer-related offenses.

Table 9 Level of Cybercrime Vulnerability when Grouped According to School

Mean	**School**	**Mean**	**SD**	**F**	**df**	**Sig.**	**Decion Action**
1. Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems	STEH	1.09	.17	1.437	3	.232	Accept HO
	SHANS	1.05	.18				
	SAB	1.05	.11				
	SEAIT	1.08	.15				
	Total	1.07	.15				
2. Content – Related Offenses	STEH	1.07	.18	.748	3	.524	Accept HO
	SHANS	1.04	.17				
	SAB	1.05	.12				
	SEAIT	1.06	.15				
	Total	1.05	.16				
3. Computer – Related Offenses	STEH	1.07	.24	3.571	3	**.014**	**Reject HO**
	SHANS	1.01	.10				
	SAB	1.00	.00				
	SEAIT	1.02	.12				
	Total	1.02	.13				

Legend: Reject the null hypothesis (Ho) if p-value (Sig.) is less than 0.05 (95% confidence level): Accept null hypothesis (H0) if p-value (Sig.) is greater than 0.05 (95% confidence level).

Table 9 shows that when grouped according to school, the responses only on computer – related offenses (P-value=.014) had significant differences because the p-value is less than 0.5 which rejects the null hypothesis while the offenses against confidentiality, integrity, and availability of computer data systems (P-value=.232) and content – related offenses (P-value=.524) has no significant difference in which it accepts the null hypothesis. Table 10 presents the Post Hoc result (LSD) of this comparison.

Table 10 Post Hoc for the Level of Cybercrime Vulnerability on Computer – Related Offenses

Mean of the Dependent Variable	(I) School	(J) School	Mean Difference (I-J)	Std. Error	Sig.	Decision Action
Computer – Related Offenses	STEH	SHANS	.06051*	.02146	**.005**	**Reject HO**
		SAB	.06971*	.02286	**.002**	**Reject HO**
		SEAIT	.05006*	.02221	**.025**	**Reject HO**
	SHANS	SAB	.00920	.01940	.635	Accept HO
		SEAIT	-.01045	.01862	.575	Accept HO
	SAB	SEAIT	-.01965	.02022	.332	Accept HO

Legend: Reject the null hypothesis (Ho) if p-value (Sig.) is less than 0.05 (95% confidence level): Accept null hypothesis (H0) if p-value (Sig.) is greater than 0.05 (95% confidence level).

Table 10 shows significant differences across all the schools, which implies that school is a factor that influences students' responses. Moreover, STEH students are more likely to commit cybercrimes, followed by SEAIT then SHANS. The school which least likely to commit cybercrime is SAB.

Students engage in various things on the Internet relative to their field of discipline. With the different disciplines, this means different exposure to cybercrimes. So this school becomes a factor that influences someone to offend or do various forms of cybercrimes. The study conducted by Fadara and Adegbola(2022) highlighted that most of their respondents with comprehensive knowledge of cybercrime and how it is being perpetrated would be most likely to commit it. School of Teachers Education and Humanities comprised courses on these various disciplines with a relatively conscious introduction and in-depth study of cybercrime subjects. Thus, further explains that the School of Teachers Education and Humanities students are more likely to commit cybercrimes

Notwithstanding, this finding is contrary to the studies of Lazarus *et al.* (2022), Deora and Chudasama (2021), and Khan (2019). In these studies, individuals' various disciplines or inclinations were not considered a factor in committing crimes. Cybercrime, according to them, is a worldwide phenomenon that does not distinguish and exempt people because they are studying Engineering, Business, Education, and the Humanities.

Table 11 Level of Cybercrime Vulnerability when Grouped According to Frequency of Use

Mean	**Frequency of Use**	**Mean**	**SD**	**F**	**df**	**Sig.**	**Decision Action**
Offenses against Confidentiality, Integrity, and Availability of Computer Data Systems	12 hours and above	1.07	.20	.016	3	.997	Accept HO
	Between 8 – 12 hours	1.07	.13				
	Between 4 – 8 hours	1.06	.15				
	Below 4 hours	1.06	.13				
	Total	1.07	.15				
Content – Related Offenses	12 hours and above	1.08	.20	1.608	3	.187	Accept HO
	Between 4 – 8 hours	1.04	.13				
	Between 4 – 8 hours	1.05	.15				
	Below 4 hours	1.00	.00				
	Total	1.05	.16				
Computer – Related Offenses	12 hours and above	1.05	.18	1.980	3	.117	Accept HO
	Between 4 – 8 hours	1.00	.05				
	Between 4 – 8 hours	1.03	.15				

	Below 4 hours	1.00	.00				
	Total	1.02	.13				

Legend: Reject the null hypothesis (Ho) if p-value (Sig.) is less than 0.05 (95% confidence level): Accept null hypothesis (H0) if p-value (Sig.) is greater than 0.05 (95% confidence level).

As shown in Table 11, all the groups of cybercrimes had p-values greater than .05, indicating no significant differences in the responses of SMU students. These are offenses against confidentiality, integrity, and availability of computer data systems (P-value=.997); content – related offenses (P-value=.187); and computer – related offenses (P-value=.117). This implies that the frequency of computer or Internet use does not affect the vulnerability of SMU students in committing cybercrimes. The null hypothesis is accepted in this indicator.

In some studies, however, the frequency of Internet or computer use greatly affects the probability of students in committing cybercrimes. In the study by Khan (2019) on senior college students, his analyses showed that there were only 10% of their respondents had less internet usage. There were more who spent 1-3 hours or more and according to the author, more time spent on the Internet means higher exposure and probability of encountering cybercrime. Likewise, Hawdon (2021) claimed that the frequency of use of the Internet, computer and other devices where students could access the cyberspace, the more that they could be exposed to cybercrimes such as viruses that could damage computer systems, hacking, piracy and other cyber threats.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Based on the findings of the study, the following conclusions were derived:

The profile variables included are gender, year level, school, and frequency of Internet use. This study was dominated by female respondents, with almost equal distribution in terms of year level, considerable proportion concerning school, and most of the respondents had frequency of Internet use between 4 – 8 hours having.

In terms of: 1) Offenses against confidentiality, integrity and availability of computer data systems; 2) Content-related offenses; and 3) Computer-related offenses, the students of Saint Mary's University had a very low probability of committing cybercrime.

It is to be concluded that gender affects the responses of SMU students in terms of offenses against confidentiality, integrity and availability of computer data systems and content-related offenses but not in computer-related offenses. The same with the year level but the responses vary only between first-year and fourth-year SMU students.

Meanwhile, the school of the respondents also influences students' responses regarding computer-related offenses specifically the STEH students differ from the other schools. The Frequency of Internet use does not affect the responses of the SMU students.

Recommendations

From the conclusions, the following are highly recommended:

For the profile variables, the comparison would be more reliable and valid if the respondents had a balanced number of males and females and those participants from the four schools. Other variables may also be considered in future research, like students' interests/habits and socio-economic and academic performance, as these may also affect their vulnerability to committing cybercrimes.

The study looked into the vulnerability of SMU students in committing cybercrime, and the results showed that they had a very low probability. For future studies, it would also be good to conduct another research that aims to reveal the vulnerability of certain respondents from the point of view of being victims of the various

enumerated cybercrimes. Knowing this may provide enlightenment and more explanations on why SMU students have a low probability of being an offender of cybercrimes.

To prevent future problems, the school may provide guidelines and precautions for using the Internet within the university, including the Learning Management System (LMS), corporate email, and other university portals containing the student's information. Sanctions should also be spelled in the Students' Manual aside from being generally stated as part of the Privacy Act of 2012. Programs. Seminars and workshops may also be conducted every semester for the students to learn and relearn about the policies and guidelines in the use of Internet and the pertinent laws governing each user.

To further prevent the commission of cybercrimes among SMU students, the researchers created a flyer (Information Education and Communication) to spread awareness and proper treatment. The IEC also contains suggestive actions to protect the students from any potential attacks it may bring to them as an effect of exposure to the Internet. Controlled measures were included to supplement the students' positive responses. This flyer shall be reviewed and utilized upon approval.

ACKNOWLEDGEMENT

The researcher, sincerely thanks her for supporting us morally and financially throughout our journey in this

study.

To Mrs. Jeanette Manuel, our research instructor, Attorney Jonathan Budaden as our research adviser, Mr. Erwin Naval as the Chairman of our Research Panelists, Mr. Kenneth Maslang as our Data Analyst and at the same time member of our research panelist, and to Mrs. Alona Costales as our Research Panelist, for sharing us their expertise that resulted to the success of this study. Especially to our Research Coordinator, Mr. Jonathan Vergara who guided us from the start up to the accomplishment of this paper.

I would also like to give thanks to our loved ones and friends, who gave comfort to us in times of troubles during the completion of this study.

Above all, God, for giving us the comfort, strength and provision that we needed throughout the accomplishment of this masterpiece.

Dedication

I dedicate this study to our parents and relatives, who always support us.

I also dedicate this to all the victims of cybercrime, especially the students, we hope that this study will bring comfort and relief to them.

REFERENCES

1. Abadilla (2021). Bank clients lose over P1 billion to cybercrime. *Inquirer. Net*. https://newsinfo.inquirer.net/1516546/bank-clients-lose-over-p1b-tocy bercrime
2. Adegbola & Fadara (2022). Cybercrime among mathematical science students: implications on their academic performance. https://www.researchgate.net/publication/363043649_CYBER_CRIME_AMONG_MATHEMATICAL_SCIENCE_STUDENTS_IMPLICATIONS_ON_THEIR_ACADEMIC_PERFORMANCE
3. Affi (2022). Effects of the Internet on students. https://digitalcommons.unl. edu/cgi/viewcontent.cgi?article=13409&context=lib philprac
4. Alghamdi, M. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. International Journal of Engineering Research & Technology (IJERT), 09 (06). **DOI : 10.17577/IJER TV9IS060565**

5. Bandara et. al (2014). Cyber security concerns in E-learning education. https:// ecesm.net/sites/default/files/ICERI_2014.pdf
6. Central Statistcs Office (2019). Information Society Statistics - Households 2019. https://www.cso.ie/en/releasesandpublications/ep/p-informationstatistics-
7. CHED (2020). Guidelines on the implementation of the flexible learning. https://ched.gov.ph/wp-content/uploads/CMO-No.-4-s.-2020-Guideline s-onthe-Implementation-of-Flexible-Learning.pdf
8. De Vera & Bautista (2022) Teachers lose savings to bank cyberscam. Inquirer.Net. https://newsinfo.inquirer.net/1544537/teachers-lose-savingsto-bank-cyber scam
9. Deora, R. & Chudasama, D. (2021). Brief study of cybercrime on an Internet. Journal of Communication Engineering and Systems, 11 (1). DOI:10.37591/JoCES
10. Donner, C. (2016). The gender gap and cybercrime: An examination of college students' online offending, victims & offenders, 11 (4) , 556-577, DOI: 10.1080/15564886.2016.1173157
11. Döring et. al (2015). Online Sexual Activity Experiences among College Students: A Four Country Comparison. CUNY Academic Works. https://academic works.cuny.edu
12. Express Computer (2020). 80% cybercrimes faced by school students in Maharashtra go unreported Study. https://www.expresscomputer.in/
13. Felina (2021). PRO2, naglagay ng anti-cyber crime unit sa Santiago City para matulungan ang mgabiktima ng cybercrime. Bombo Radyo Cauayan. https://www.bombo radyo.com/cauayan
14. Giordano and Cashwell (2017). Cybersex addiction among college students: A prevalence study. https://www.semanticscholar.org/paper/Cybersex Addiction-Among-Col lege
15. Grado (2005). Internet investigations: The crime scene of cybercrime. https://www.ojpgov/ncjrs/virtual-library/abstracts/internet-investiga-tionscrime-scene-cyber crime
16. Grivna & Drapal (2018). Attacks on the confidentiality, integrity, and availability of data and computer systems in the criminal case law of the Czech Republic. https://www.researchgate.net/publication/329500128_Attacks_on_the_confide ntiality_integrity_and_availability_of_data_and_computer_systems_in_the_crimin al_case_law_of_the_Czech_Republic
17. Harasim (1989). Online education.https://files.eric.ed.gov/fulltext/ED484990.pdf
18. Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *Am J Crim Just* 46, 837–842. https://doi.org/10.1007/s12103-021-09652-7
19. Hogan (2020). Cybercrime is on the rise during remote learning. *Market Scale*. https://marketscale.com/industries/education-technology/cybercrimeon-the-rise-during-remote-learning
20. Hutchings, A. & Chua, YT. The final publication is available in T. J. Holt (ed.), Cybercrime through an Interdisciplinary Lens (pp. 167-188). *Oxon: Routledge.* https:// www.cl.cam.ac.uk/~ah793/papers/2017gendering_ cybercrime.pdf
21. IGI Global. What is Vulnerability to Internet Crimes. https://www. igiglobal.com/ dictionary/vulnerability-to-internet-crimes/32072
22. Johnson (2022). Countries with the highest number of Internet users 2022. Statista.https://www.statista.com/statistics/262966/number-ofinternet -users-in-selec ted-countries/#
23. Johnson (2022). Cybercrime encounter rate in selected countries 2021. *Statista.* https:// www.statista.com/statistics/194133/cybercrime-rate-in-selectedcountries/
24. Khan, A, (2019). A study of awareness on cybercrime amongst senior college students of Pune City. International Journal of Research and Analytical Reviews, 6 (1), 167 – 172.
25. Lahcen, et.al (2020). Review and insight on the behavioural aspects of cyber securityhttps://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00050
26. Lazarus, S., Button, M. & Kapend (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. The Howard Journal of Crime and Justice, 61 (3). https://doi.org/10.1111/hojo.12485
27. Macdonald and Pittman (2010). Cyberbullying among college students: Prevalence and demographic differences. https://www.researchgate.net/ publication/24112 3159
28. Monteith, S., Bauer, M., Alda, M. (2021). Increasing cybercrime since the pandemic: Concerns for Psychiatry. Curr Psychiatry Rep **23**, 18. https://doi.org/ 10.1007/s11920-021-01228-w
29. Munanga, A. (2019). Cybercrime: A new and growing problem for older adults. Journal of Gerontological Nursing, 45 (2). https://doi.org/10.3928/ 00989134-20190111-01

30. Nagel et al. (n.d.) Findings on student use of social media at the collegiate, undergraduate, and graduate levels: Implications for post-secondary educators. https://files.eric. ed.gov/fulltext/EJ1173809.pdf
31. Pulta (2020). DOJ warns public on emerging security risks during online classes. Philippine News Agency. https://www.pna.gov.ph/articles/1116318
32. Republic Act No. 10175. Cybercrime Prevention Act of 2012. www. officialgazette.gov.ph
33. Roy (2020). Online classes disrupted by hackers; Schools fight flood of obscene and abusive messages. https://www.outlookindia.com/website/story/ india-news-online-classesdisrupted-by-hackers-schools-fight-flood-of-obscene-and-abusive-messages
34. Saidul, S. (2018). Cybercrime and its effects on youth. An empirical study on MBSTU students. https://www.academia.edu/9202289/Cyber_Crime_and_its_ef fects_on_youth_An_empirical_study_on_MBSTU_students
35. Save the Philippines (2019). Online sexual abuse of children rising amid COVID-19 pandemic.https://www.savethechildren.org.ph/our-work/ourstories/ story/online-sexual-abuse-of-children-rising-amid-covid-19-pandemic/
36. Seoane (2021). Two BHS students arrested for distribution of child pornography. *NRI now News*. https://nrinow.news/2021/07/03/two-bhs-studentsarrested-for-distri bution-of-child-pornography/
37. Swansea University (2020). Internet use reduces study skills in university students. https://www.sciencedaily.com/releases/2020/01/200117085 321.htm
38. Tulane University (n.d.). Students more at risk of identity theft: Tips and resources to stay Protected. https://sopa.tulane.edu/blog/student-loanidentity-theft
39. Tupas (2019).Cybercrimes up by 80% in 2018. *PhilStar Global*. https:// www. Phil star.com/headlines/2019/03/29/1905544/cybercrimes-802018
40. Tunngal (2022) What is vulnerability? https://www.upguard.com/ blog/ vulnerability
41. University Police (2021). U. of I. student arrested in child pornography investigation. https://blogs.illinois.edu/view/6221/1908687740
42. UT News (2021). Millenials commit less crime than prior generation. https://news.utexas.edu/2021/05/10/millennials-commit-less-crime-than-prior-generations/
43. Varga (n.d.). Global Cybercrime Report: Which countries are most at risk? Seon. https://seon.io/resources/global-cybercrime-report/
44. Wadhwa, A. (2017). A review on cyber crime- major threats and solutions. International Journal of Advanced Computer Research, 8(5):2217-2221

APPENDIX A

Research Instrument

Cybercrime Vulnerability of Saint Mary's University Students

Survey Questionnaire

PART I: Profile *(*Please check or provide the information)

1. **Name** (optional) _____

2. **Gender:** _____

3. **Year level**: 1st year _____2nd year_____3rd year_____ 4th year_____

4. **School:**

□ School of Teacher Education and Humanities

□ School of Health and Natural Sciences

□ School of Accountancy and Business

□ School of Engineering Architecture and Information Technology

Frequency of Internet use:

□ 12 hours and above a day

□ Between 8 to 12 hours a day

□ Between 4-8 hours a

□ Below 4 hours a day

PART II: level of vulnerability of Saint Mary's University students to cybercrimes

Based on your personal assessment may you personally determine the level of your vulnerability to be involved in the different cybercrimes using the following scale:

1 = Very Low Probability

2 = Low Probability

3 = High Probability

4 = Very High Probability

Cybercrime refers to any criminal activity or offenses committed through the use of computer or the computer.

Indicators	1	2	3	4
A. Offenses against Confidentiality, Integrity and Availability of Computer Data Systems				
1. Hacking someone's account to see their activities.				
2. Stealing information of my other classmate for personal gain.				
3. Illegal processing of personal and private information				
4. Inputting malicious software that can threaten the integrity or use of data or programs.				
5. Destroying the computer data of others.				
6. Distributing copyrighted software, music and film.				
7. Using the name of other brands to make profit.				
B. Content – Related Offenses				
1. Sending obscene pictures and videos.				
2. Selling child pornography to make money.				
3. Sending unsolicited emails (spam), newsletters, messages and links to my online friends.				
4. Posting about untruth about someone.				
C. Computer-Related Offenses				
1. Making or forging a document for financial gain				
2. Pretending to be someone to gain access to another's funds.				
3. Using the identity of someone for financial gain.				

Thank you very much!

Appendix B

RELIABILITY CLEARANCE

RELIABILITY CLEARANCE

Research Proponent:

ESTHYRE KATE A. BAYANGAN

Program:

Master of Arts in Criminal Justice

Research Title:

Cybercrime Vulnerability of Saint Mary's University Students

This is to certify that the tool has undergone reliability analysis at the University Research Center of Ifugao State University and by a duly accredited Quantitative Data Analyst.

MR. KENNETH L. MASLANG
Data Analyst

January 2023
Date

Appendix C

QUANTITAIVE DATA ANALYSIS CERTIFICATION

Research Proponent:

ESTHYRE KATE A. BAYANGAN

Program:

Master of Arts in Criminal Justice

Research Title:

Cybercrime Vulnerability of Saint Mary's University Students

This is to certify that the quantitative data analysis were done at the University Research Center of Ifugao State University and by a duly accredited Quantitative Data Analyst.

MR. KENNETH L. MASLANG
Data Analyst

February 27 2023
Date

Quantitative Analysis Clearance

Appendix D

COMMUNICATION LETTERS

December 14, 2022

DR. ARLENE L. TABAQUERO, LPT, MBS
Dean, SHANS

Dear Ma'am;

I, Esthyre Kate A. Bayangan, a 4th year Forensic Science student is currently conducting a research study entitled **"CYBERCRIME VULNERABILITY OF SAINT MARY'S UNIVERSITY STUDENTS"** as part of our academic requirement in Research 2.

Our respondents in the study are the stuydents of the four schools in your university. Hence, I would like to request from your good office to allow me conduct data gathering in your school. Rest assured that the data that will be gathered will be usd for academic purpose only.

Respectfully yours,

ESTHYRE KATE A. BAYANGAN
Researcher

Noted by:

JEANETTE D. MANUEL, RCrim
Research Instructor

December 14, 2022

DR. HENRY F. GAMBOA
Dean, STEH

Dear Ma'am;

I, Esthyre Kate A. Bayangan, a 4th year Forensic Science student is currently conducting a research study entitled **"CYBERCRIME VULNERABILITY OF SAINT MARY'S UNIVERSITY STUDENTS"** as part of our academic requirement in Research 2.

Our respondents in the study are the stuydents of the four schools in your university. Hence, I would like to request from your good office to allow me conduct data gathering in your school. Rest assured that the data that will be gathered will be usd for academic purpose only.

Respectfully yours,

ESTHYRE KATE A. BAYANGAN
Researcher

Noted by:

JEANETTE B. MANUEL, RCrim
Research Instructor

December 14, 2022

ENGR. CARINA S. MALLILLIN
Dean, SEAIT

Dear Ma'am;

I, Esthyre Kate A. Bayangan, a 4th year Forensic Science student is currently conducting a research study entitled **"CYBERCRIME VULNERABILITY OF SAINT MARY'S UNIVERSITY STUDENTS"** as part of our academic requirement in Research 2.

Our respondents in the study are the stuydents of the four schools in your university. Hence, I would like to request from your good office to allow me conduct data gathering in your school. Rest assured that the data that will be gathered will be usd for academic purpose only.

Respectfully yours,

ESTHYRE KATE A. BAYANGAN
Researcher

Noted by:

JEANETTE D. MANUEL, RCrim
Research Instructor

December 14, 2022

MRS. ELNORA V. ADALEM, CPA
Dean, SAB

Dear Ma'am;

I, Esthyre Kate A. Bayangan, a 4th year Forensic Science student is currently conducting a research study entitled **"CYBERCRIME VULNERABILITY OF SAINT MARY'S UNIVERSITY STUDENTS"** as part of our academic requirement in Research 2.

Our respondents in the study are the stuydents of the four schools in your university. Hence, I would like to request from your good office to allow me conduct data gathering in your school. Rest assured that the data that will be gathered will be usd for academic purpose only.

Respectfully yours,

ESTHYRE KATE A. BAYANGAN
Researcher

Noted by:

JEANETTE D. MANUEL, RCrim
Research Instructor