CYBERCRIME AWARENESS AMONG DORSU-CEC STUDENTS IN CATEEL, DAVAO ORIENTAL

Wilmie T. Gandela[1], Loydjay D. Damiar[2], Randy M. Pajo[3]

Bachelor of Science in Criminology, Davao Oriental State University, Mahan-ob, Cateel, Davao Oriental, Philippines

ABSTRACT

As cybercrime continues to rise globally, understanding and preventing it has become critical for educational institutions. This study aimed to investigate the level of cybercrime awareness among students at Davao Oriental State University – Cateel Extension Campus (DORSU-CEC) during the School Year 2023-2024. The research examined the demographic profile of respondents, their awareness of cybercrime laws, and the relationship between demographic characteristics and awareness levels. Utilizing a quantitative-descriptive research design, data were collected from 310 students via stratified random sampling, employing a survey questionnaire based on the Cybercrime Act of 2012. The analysis revealed a diverse respondent profile across academic programs, year levels, and gender, with most respondents showing high levels of cybercrime awareness, particularly in content-related offenses. Significant differences in awareness were observed across academic programs and year levels, though not by gender. Recommendations include developing tailored educational programs and awareness campaigns, continuing and expanding current initiatives, and implementing targeted measures to address awareness gaps. These actions aim to foster a more informed and secure digital environment for all students.

Keyword: *cybercrime, law, awareness, students*

1. INTRODUCTION

Cybercrime has become a pressing concern recently, with significant implications for individuals, organizations, and society (Gillespie, 2019). As technology advances and internet usage expands, the risks and vulnerabilities associated with cybercrimes have multiplied (Goodman, 2015). According to Smith and Mount (2019), the rise of cybercrimes has led to substantial financial losses, data breaches, identity theft, and other detrimental consequences. Furthermore, geographical boundaries do not limit cybercrimes, as they can be carried out from anywhere worldwide, making it a global issue (Lavorgna, 2020). In the educational context, many students are exposed to the digital world but need to be adequately informed about the potential dangers and legal consequences of their online activities (Voogt et a., 2013). This gap in knowledge leaves students vulnerable to both becoming victims and perpetrators of cybercrime (Jones & Parks, 2019; Soylu et al., 2021).

The ICT sector in the Philippines is one of the fastest growing in Southeast Asia, leading to significant economic development (Jing et al., 2019). However, the country's large population of internet users makes it particularly susceptible to cybercrime. This issue is exacerbated among the youth, who have greater access to technology and the Internet (Szymkowiak et al., 2021). Due to a lack of awareness and education regarding cybercrime, there have been numerous instances of young individuals in the Philippines becoming involved in cybercrime, either as perpetrators or victims (Abuda et al., 2020) Any behavior using a computer network or networked device for illegal purposes is termed cybercrime (Deora & Chudasama, 2021) This is particularly

concerning for students, who are heavy internet users and thus highly exposed to cybercrime victimization (Pontes, 2015).

The convergence of communication and the exponential growth of digital technology have brought enormous benefits to modern society (Wang, 2017). However, along with these benefits come greater risks. Lone offenders can now inflict catastrophic loss or damage on individuals, companies, and governments from anywhere globally at negligible cost to themselves (Grabosky, 2019). This awareness has led to the understanding that 'information security' is not just for technical specialists but for millions of everyday users engaging with these new media for business, communications, and leisure (Arora, 2019). The prosperity of industrial nations and the economic development of less affluent societies increasingly depend on electronic commerce (Yeager, 2018). Cybercriminal activity undermining public confidence in e-commerce threatens economic well-being (Jamshed, 2022). Although there is an extensive body of research on cybercrime and cybercrime awareness, there is a notable gap in studies specifically conducted within universities. The unique environment of universities, which includes a high concentration of young adults, extensive use of technology, and significant amounts of sensitive data, makes it an essential yet under-explored area for such research.

The need to conduct a study on cybercrime awareness among students is underscored by the rapid digitalization of education and social interactions, which exposes young individuals to an array of cyber threats (Erkomaishvili & Gillies, 2023). Despite increased connectivity, there is a significant gap in students' understanding of complex cyber threats such as phishing, ransomware, and social engineering, as highlighted by recent studies (Reyadul & Reyad, 2023; Garba et al., 2020). Due to the higher recurrence of hacking assaults on data frameworks in schools and colleges, students must be aware of the consequences and challenges of cybersecurity and cybercrime. Therefore, it is essential to determine the aspects surrounding students' levels of awareness of cybercrime and to address this research gap proactively.

The Philippines is experiencing a 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). Evidence suggests that cybercrimes are rising in the country, posing significant threats to individuals, organizations, and even national security (Cajes, 2020; National Privacy Commission, 2021). Thus, this study is of great importance in today's digital age. This study aims to address the problem using understanding the level of cybercrime awareness specifically among students. By focusing on this specific population, the study's findings can contribute to enhancing the curriculum and educational interventions to equip students with the necessary knowledge and attitudes to combat cybercrimes effectively. Further, the researchers undertake this study to determine the level of cybercrime awareness among students of DORSU.

1.1 Theoretical Framework

This study is anchored on Republic Act No. 10175, also known as the Cybercrime Prevention Act of 2012, a comprehensive legislation designed to combat cybercrimes in the Philippines.

This act focuses on the pre-emption, preventing, and prosecuting cybercrimes, such as offenses against the privacy, confidentiality, integrity, and availability of computer data and systems, computer-related offenses, and content-related offenses. It targets offenses against computer data and systems, such as illegal access, unauthorized interference, and data interference, as well as content-related offenses like cybersex, child pornography, and libel. Additionally, the act penalizes unsolicited commercial communications and cybersquatting, which is defined as acquiring domain names with malicious intent. Offenses committed through information and communications technologies are subject to penalties one degree higher than those in the Revised Penal Code, without prejudice to other legal liabilities.

Furthermore, the act ensures that crimes committed via information and communications technologies are covered by relevant provisions of the Revised Penal Code, with penalties increased by one degree. Prosecution under the Cybercrime Prevention Act does not exempt individuals from liability under other laws. The act aims to address and deter cybercrimes by providing legal frameworks for pre-emptive measures, prevention strategies, and prosecution guidelines.

According to Gravino and Villanueva (2021), in the Philippines, as many as 87 percent of Filipinos were identified as victims of malicious activities committed online, as stated by the DOJ. These include victims of malware

invasion, sexual predation, and online or phishing scams. Van de Weijer & Leukfeldt (2017). The prevalence of cybercrime has increased rapidly over the last decades and has become part of the everyday life of citizens. As stated by Marcum (2015), people spending extensive amounts of time online also place themselves at risk for victimization.

Cyberbullying and cyberstalking are two main ways people can be victimized. It is, therefore, essential to learn more about the factors related to an increased or decreased likelihood of becoming a cybercrime victim (Van de Weijer & Leukfeldt, 2017). Ariola et al. (2018) emphasized the importance of awareness to decrease or prevent cybercrime. Cybercrime law underscores the importance of cybersecurity awareness, computer systems, and data protection. It promotes initiatives to educate the public, including students, about cybersecurity best practices, such as safeguarding personal information, using strong passwords, and avoiding malicious websites and emails. According to Hasan et al. (2015), students with knowledge of cyber offenses and a high level of education have high perceptions and awareness of cybercrime. Republic Act No. 10175 emphasizes cybercrime awareness as critical to creating a safer online environment. It recognizes that young individuals are particularly vulnerable to cyber threats due to their frequent use of digital devices and platforms. Therefore, the act promotes initiatives to educate individuals about cybersecurity best practices.

By prioritizing cybercrime awareness among students, Republic Act No. 10175 equips such individuals in the Philippines with the knowledge and skills to navigate the virtual world safely and responsibly, contributing to a more secure digital environment.

2. METHODOLOGY

2.1 Research Design

This study utilized a quantitative-descriptive research design. According to Creswell (2013), quantitative research employs inquiry strategies such as experimental and surveys and collects data on predetermined instruments that yield statistical data. Further, as emphasized by Sirisilla (2023), descriptive research provides a comprehensive picture of the characteristics and behaviors of a particular population or phenomenon, allowing researchers to gain a deeper understanding of the topic. The goal of descriptive research is to provide a comprehensive and accurate picture of the population or phenomenon being studied and to describe the relationships, patterns, and trends that exist within the data. The approach is deemed appropriate for this study because it aims to measure cybercrime awareness among students in DORSU-CEC. The quantitative approach allows for using a standardized instrument for data collection. This means the data collected will be reliable and can be replicated in future studies.

2.2 Respondents and Sampling Procedures

The respondents in this study were from the Davao Oriental State University-Cateel Extension Campus. Specifically, the survey included only students enrolled in the second semester of the academic year 2023-2024. They were chosen through stratified random sampling to ensure that the sample is representative of the population of students in DORSU-CEC. According to Babbie (2017), stratified random sampling is a probability sampling technique that involves dividing the population into subgroups or strata based on specific characteristics and selecting a random sample from each stratum. This method can increase the precision and accuracy of the estimates for each stratum and the overall population. Further, this method is deemed appropriate since students are divided by departments, which serve as the strata indicated in the sampling procedure.

The population sample was calculated using Slovin's formula, which had a confidence level of 95% and a margin of error 0.05. Furthermore, the total population of DORSU-CEC students enrolled in the academic year 2023-2024 is 1,378. As calculated using the given formula, the sample generated is 310 respondents. More specifically, there are 19 respondents chose from the Bachelor of Agricultural Technology, 28 from the Bachelor of Elementary Education, 14 from BS Agriculture-Animal Science, 62 respondents from the Bachelor of Science in Agribusiness Management, 123 from the Bachelor of Science in Business Administration, and 64 respondents from the Bachelor of Science in Criminology Program.

Profile of respondents

Programs	Frequency	Percentage
BAT/BSA	39	12.58
BEED	28	9.03
BSAM	56	18.06
BSBA	123	39.68
BSC	64	20.65
Total	**310**	**100.00**

2.3 Research Instrument

This study employed a self-made survey questionnaire based on Republic Act No. 10175, the Cybercrime Act 2012. The questionnaire will be composed of two sections: the demographic profile of the respondents and the cybercrime awareness scale.

This study developed a self-made questionnaire that underwent validity and reliability tests. The validity criteria were met through factor analysis, with a KMO of 0.850 and Bartlett's Test of Sphericity showing a significance level of 0.000. This indicates that the questionnaire is valid. The reliability test was performed using Cronbach's alpha, which yielded a coefficient of 0.935, indicating that the questionnaire is highly reliable. Therefore, the survey instrument used in this study is both valid and reliable.

2.4 Data Gathering Procedure

The following are the aspects that the researcher considered throughout this study.

1. Seek ethical clearance. Researchers sought ethical clearance from the Davao Oriental State University-Cateel Extension Campus Research Ethics Office (REO).

2. Requesting permission to conduct the study. A formal letter requesting permission was sent to the School Dean of Davao Oriental State University-CEC, who subsequently communicated with each department's program heads and instructors for their approval regarding student participation in the study.

3. Administration of survey questionnaires. Before answering the questionnaire, respondents were given an informed consent form signifying their voluntary participation. They received detailed information about the study's objectives, methods, and potential risks and benefits. Only after obtaining consent were the survey questionnaires distributed.

4. Retrieval of questionnaires. After survey administration, completed questionnaires were collected, organized, and analyzed meticulously and professionally, with the assistance of a statistician.

2.5 Analysis of Data

Before the analysis, the responses were tallied on an MS Excel application. The statistician then utilizes the following statistical tools to analyze and interpret the data gathered.

Frequency Counts and Percentages were utilized to determine the demographic profile of the respondents. This further answered the statement of problem number 1.

Weighted mean was utilized to determine the cybercrime awareness of DORSU-CEC students. This will also answer the statement of problem number 2.

Table 2. Interpretation on the level of awareness of cybercrime law

Interval	Interpretation	Description
1.00 – 1.80	Not Aware	Not aware of most provisions of the cybercrime law.
1.81 – 2.60	Slightly Aware	Have a basic awareness of some provisions of cybercrime law.

2.61 – 3.40	Moderately Aware	Have a moderate awareness of provisions of cybercrime law and can follow them when reminded
3.41 – 4.20	Aware	Well aware of provisions of cybercrime law and understand their importance
4.21 – 5.00	Extremely Aware	Highly aware of provisions of the cybercrime law.

ANOVA was utilized to determine the significant difference between students' cybercrime awareness and their profiles. This will also answer the statement of problem number 3.

3. RESULTS AND DISCUSSION

3.1 Profile of the Respondents

Table 2 provides an overview of the distribution of respondents across various academic programs at Davao Oriental State University - Cateel Extension Campus.

Table 2. Profile of respondents in terms of programs

Programs	Frequency	Percentage
BAT/BSA	39	12.58
BEED	28	9.03
BSAM	56	18.06
BSBA	123	39.68
BSC	64	20.65
Total	**310**	**100.00**

The largest group of respondents is from the Bachelor of Science in Business Administration (BSBA) program, which accounts for 39.68% (123 out of 310) of the total sample. This suggests that a significant portion of this study's student population is pursuing a business administration degree, reflecting its popularity and more significant enrollment numbers at the university. Contrarily, the Bachelor of Elementary Education (BEED) program accounts for 9.03% (28 out of 310) of the respondents, showcasing the smallest group among the programs listed. This highlights a relatively lower but still significant enrollment in elementary education, emphasizing the importance of training educators for the foundational levels of the education system.

Overall, the distribution of respondents across these programs provides a comprehensive representation of the student body, ensuring that the study captures a wide range of perspectives and experiences related to cybercrime awareness.

Table 3. Profile of respondents in terms of their year level

Year Level	Frequency	Percent
1st Year	94	30.32
2nd Year	87	28.06
3rd Year	93	30.00
4th Year	36	11.61
Total	**310**	**100.00**

The data presented in Table 3 illustrates the distribution of respondents according to their year level at Davao Oriental State University-Cateel Extension Campus. The largest group of respondents consists of first-year students, accounting for 30.32% (94 out of 310) of the total sample. This substantial representation of first-year students indicates a strong engagement with the study among new university entrants, highlighting their interest in participating in research activities and their potential exposure to cybercrime awareness initiatives early in their academic journey.

Fourth-year students represent the smallest group, comprising 11.61% (36 out of 310) of the respondents. This lower percentage can be attributed to heightened academic and professional commitments. Despite their smaller representation, fourth-year students' participation is valuable, as they bring more extensive academic experience and potentially deeper insights into the study's focus on cybercrime awareness.

The distribution across year levels provides a balanced representation of the student population, ensuring that the study captures perspectives from various stages of academic progression. This comprehensive demographic profile is crucial for understanding the differences in cybercrime awareness and tailoring educational interventions accordingly.

Table 4. Profile of respondents in terms of their gender

Gender	Frequency	Percent
Male	142	45.81
Female	168	54.19
Total	**310**	**100.00**

The data presented in Table 4 shows the distribution of respondents based on their gender at Davao Oriental State University - Cateel Extension Campus. The table indicates that a slight majority of the respondents are female, accounting for 54.19% (168 out of 310), while male respondents constitute 45.81% (142 out of 310) of the total sample. This gender distribution suggests a balanced representation of male and female students, with a slight predominance of females.

The near-equal gender distribution ensures that the study captures both male and female students' perspectives and experiences regarding cybercrime awareness. This balance is crucial for analyzing potential gender-specific differences in awareness and attitudes towards cybercrime laws. Understanding these differences can help in designing targeted educational interventions that address the specific needs and concerns of each gender group, ultimately fostering a more inclusive and practical approach to cybercrime education.

3.2 Level of Cybercrime Awareness

Level of Cybercrime Awareness

Table 5 presents the level of cybercrime awareness in terms of offenses against confidentiality, integrity, and availability of computer data and systems. The result demonstrates a high awareness of various offenses in the current category. The category mean score is 4.12, which indicates that the students are well aware of cybercrime provisions and their importance. This high awareness suggests that students are well-prepared to recognize and respond to cyber threats, contributing to a safer online community. This finding aligns with the increasing importance of cybersecurity education and awareness initiatives worldwide (AlDaajeh et al., 2022). The emphasis on cybersecurity in corporate training and public awareness campaigns has likely contributed to this relatively high level of awareness (Zwilling et al., 2021). Moreover, the proliferation of cybercrime incidents has heightened individuals' consciousness about safeguarding digital information (Chen et al., 2021).

Table 5. Level of cybercrime awareness in terms of offenses against confidentiality, integrity, and availability of computer data and systems

No.	Descriptions	Mean	Std. Deviation	Interpretation
1	Awareness that accessing any part of a computer system without authorization is considered illegal.	4.32	0.81	Extremely Aware
2	Awareness that is intercepting non-public transmission of computer data without proper authorization is prohibited.	4.09	0.88	Aware
3	Awareness that intentionally altering, damaging, or deleting computer data without authorization breaches cybercrime laws.	4.20	0.89	Aware
4	Awareness that is intentionally hindering or interfering with the functioning of a computer or computer network without authority is an offense.	4.00	0.89	Aware
5	Awareness that unauthorized use, production, sale, or distribution of devices designed for cybercrime is illegal.	4.06	0.88	Aware
6	Awareness that acquiring a domain name over the Internet in bad faith, intending to profit or mislead, constitutes cyber-squatting.	4.04	0.84	Aware
	Average	4.12	0.67	Aware

Awareness that accessing any part of a computer system without authorization is illegal garnered the highest mean score, at 4.32. This implies that respondents are "extremely aware" of the prohibition of such offenses. This heightened awareness can be attributed to the widespread coverage of hacking incidents and unauthorized access cases in the media, reinforcing the understanding of its illegality (Adel, 2023). Studies have shown that media exposure significantly influences public perception and awareness of cybercrimes (Reik et al., 2016). Additionally, many organizations have implemented stringent policies and training programs to prevent unauthorized access, further bolstering awareness levels (Anderson et al., 2017).

Awareness that intentionally hinders or interferes with the functioning of a computer or computer network without authority is an offense that has the lowest mean score, at 4.00, but is still interpreted as "aware." Despite being the lowest, this score still reflects a strong understanding of cybercrime laws, though it may suggest a need for more targeted education in this area (Lee & Kim, 202). Research indicates that while general awareness is high, the general public needs to understand specific technical details of cybercrimes better (Johnson, 2016; Aswathnarayanan, 2024). Enhancing detailed knowledge through focused training could help bridge this gap (Martin, 2022).

Table 6 shows the level of cybercrime awareness in terms of computer-related offenses. The result demonstrates a substantial understanding among respondents. The data reveals a high level of awareness among respondents regarding various computer-related crimes. The category mean score is 4.05, which indicates that respondents are generally well aware of cybercrime provisions and their importance. This average suggests that most individuals have a solid grasp of the legal implications associated with computer-related offenses, reflecting the increasing emphasis on cybersecurity education (Mountrouidou et al., 2019). This awareness is crucial in mitigating the risks and prevalence of such crimes (Bandari, 2023; Aldawood & Skinner, 2019). Sarkar and Shukla (2023) noted that public understanding of such offenses is critical in combating digital fraud. Similarly, Wika and Suchi (2021) emphasized the role of awareness in preventing digital financial crimes.

Table 6. Level of cybercrime awareness in terms of computer-related offenses

No.	Descriptions	Mean	Std. Deviation	Interpretation
1	Awareness that unauthorized manipulation of computer data to create inauthentic information for legal purposes is considered computer-related forgery.	4.07	0.87	Aware
2	Awareness that unauthorized alteration or interference with computer data or systems with fraudulent intent constitutes computer-related fraud.	4.00	0.83	Aware
3	Awareness that intentional acquisition, use, or alteration of someone else's identifying information without authorization is a form of computer-related identity theft.	4.08	0.87	Aware
	Average	4.05	0.75	Aware

Awareness that intentional acquisition, use, or alteration of someone else's identifying information without authorization is a form of computer-related identity theft garnered the highest mean score, at 4.08, indicating that respondents are particularly aware that the intentional acquisition, use, or alteration of someone else's identifying information without authorization is a form of computer-related identity theft This high awareness can be attributed to the frequent occurrence and widespread reporting of identity theft cases in the media, which has heightened public consciousness about this specific crime (Norse, 2018; Anderson et al., 2017) Studies have highlighted that identity theft remains one of the most common and damaging forms of cybercrime, necessitating robust awareness and preventive measures (Smith & Noain-Sánchez, 2016; Mphatheni & Maluleke, 2022).

Conversely, awareness that unauthorized alteration or interference with computer data or systems with fraudulent intent constitutes computer-related fraud garnered the lowest mean score, at 4.00. Despite being the lowest, this score still reflects a strong understanding, interpreted as “aware.” This result suggests that while awareness is high, there may be a slight gap in the depth of understanding of computer-related fraud compared to other cybercrimes (Tsakalidis & Vergidis, 2019). Research indicates that fraud awareness can be enhanced through more detailed and targeted educational initiatives, which could help bridge this minor gap (Latif et al., 2021). Grabosky (2016) also advocated comprehensive cybercrime prevention strategies through public awareness and education.

Table 7 shows the level of cybercrime awareness in terms of content-related offenses. The result reveals a high degree of understanding among the respondents. The overall average indicates that the respondents are generally "aware" of these offenses, with most mean scores above 4.0. This indicates that respondents are generally well aware of cybercrime provisions and their importance. This high level of awareness suggests that students are well-informed about content-related cybercrime offenses, which can help them make safer choices online. The findings are in corroboration with the study of Sari et al (2024) which emphasizes the importance of comprehensive education on digital ethics and legal boundaries, as understanding the legal consequences of online behavior can deter individuals from engaging in illegal activities (Kala, 2024. Studies have shown that awareness campaigns and legal frameworks are crucial in mitigating such behaviors (Sarkar & Shukla, 2023. This finding suggests that awareness campaigns and legal education efforts around content-related cybercrimes have been relatively effective (Nzeakor et al., 2020).

Table 7. Level of cybercrime awareness in terms of content-related offenses

No.	Description	Mean	Std. Deviation	Interpretation
1	Awareness that engaging in a lascivious exhibition of sexual organs or sexual	4.21	0.88	Extremely aware

	activity using a computer system for personal gain or benefit is prohibited.			
2	Awareness that committing unlawful acts defined by the Anti-Child Pornography Act of 2009 through a computer system is punishable by law.	4.19	0.84	Aware
3	Awareness that sending commercial electronic communications without prior consent or violating specific conditions is prohibited.	4.19	0.72	Aware
4	Awareness that committing acts of libel through a computer system or similar means is illegal under cybercrime laws.	4.10	0.84	Aware
	Average	4.17	0.69	Aware

Awareness that engaging in a lascivious exhibition of sexual organs or sexual activity using a computer system for personal gain or benefit is prohibited has the highest mean score, at 4.21, indicating that respondents are "extremely aware" that engaging in a lascivious exhibition of sexual organs or sexual activity using a computer system for personal gain or benefit is prohibited Accordingly, engagement in a lascivious exhibition of sexual organs or sexual activity using a computer system for personal gain or benefit is a significant concern within the realm of cybercrime (Cruz & Sajo, 2015. The heightened awareness can be attributed to the extensive media coverage and public discussions around cyber sex crimes, which have significantly raised public consciousness about the legal and ethical implications of such actions (Henry and Powell, 2015). Studies have shown that increased visibility of these issues leads to greater public awareness and understanding (Ragusa & Crampton, 2017). Furthermore, stringent laws and actively prosecuting such offenses have likely contributed to this high awareness level (Hui et al., 2017). Educating the public about the legal provisions enhances their understanding of these laws' importance and promotes responsible online behavior (Walter et al., 2020).

Awareness that committing acts of libel through a computer system or similar means is illegal under cybercrime had the lowest mean score, at 4.10, about the, still interpreted as "aware." While this score is the lowest in the table, it still indicates a strong understanding among respondents. Research indicates that while general awareness is high, the general public might need help understanding specific legal nuances related to digital libel (Scott & O'Shea, 2022). Enhancing detailed knowledge through focused training and public education could help bridge this gap (Alwan, 2019). This lower score underscores the need for ongoing efforts to educate the public about the legal consequences of online defamation (Asam & Samara, 2016).

Table 8 shows the level of cybercrime awareness in terms of commission offenses. The result reflects a considerable understanding among respondents regarding their liability in assisting or attempting cybercrime offenses. The mean scores for these indicators range from 4.04 to 4.10. The overall average mean score is 4.07, indicating that respondents are generally "aware" of these offenses. This indicates that respondents are generally well aware of cybercrime provisions and their importance. In line with the results, studies have emphasized the increasing awareness of cybercrime laws and the legal implications of aiding or attempting to commit cyber offenses (Sarkar & Shukla, 2023). The importance of understanding the legal ramifications of cybercrime cannot be overstated, as it plays a crucial role in preventing these offenses and ensuring individuals are well-informed (Blunt, 2022) Smith et al. (2019) found that individuals are becoming more knowledgeable about the legal ramifications of cyber activities, reflecting a growing recognition of the importance of cybersecurity education Johnson (2016) highlights that public awareness campaigns and educational programs have significantly contributed to this heightened understanding, underscoring the role of proactive measures in combating cybercrime Additionally, Lee et al. (2023 observed that such educational efforts are vital in reinforcing the public's understanding of the severity of cybercrime and the importance of legal compliance.

Table 8. Level of cybercrime awareness in terms of commission offenses

No.	Descriptions	Mean	Std. Deviation	Interpretation
1	Awareness that anyone intentionally assisting or supporting the commission of cybercrime offenses is considered liable under the law.	4.10	0.76	Aware
2	Awareness that one is trying to commit any offenses listed in cybercrime laws, even if unsuccessful, renders the individual liable under the law.	4.04	0.83	Aware
	Average	4.07	0.72	Aware

The highest mean score, at 4.10, indicates that respondents are "aware" that anyone intentionally assisting or supporting the commission of cybercrime offenses is considered liable under the law. This high awareness may be attributed to the increasing emphasis on the comprehensive nature of cybercrime laws, which hold the primary offenders and their accomplices accountable (Caixia, 2022). The widespread dissemination of information regarding the legal consequences of aiding and abetting cybercrimes has likely contributed to this heightened awareness (Smith et al., 2019). Additionally, legal frameworks and educational programs often highlight the importance of understanding the broad scope of accountability in cybercrime (Amoo et al., 2024). Furthermore, Baker and Robinson (2022) argue that increased public understanding of these legal nuances helps build a more resilient and law-abiding digital community.

Conversely, the lowest mean score, at 4.04, relates to the awareness that attempting to commit any offenses listed in cybercrime laws, even if unsuccessful, renders the individual liable under the law. Although this is the lowest score, it still indicates a strong understanding, interpreted as "aware." This result conforms with the study of Williams et al. (2017), which indicates that awareness of cybercrime laws extends to understanding the liability of unsuccessful attempts to commit cyber offenses. This aligns with findings by Brown (2015), which show that legal frameworks effectively deter potential offenders by clarifying that even attempts at cybercrime carry legal consequences. Andronache (2021) emphasizes that such awareness is crucial for fostering a culture of compliance and deterring cybercriminal activities.

Table 9 shows the level of cybercrime awareness regarding the legal implications of cybercrime legislation. The data reveals a high level of awareness among respondents about the legal consequences of cybercrime, with mean scores ranging from 4.04 to 4.09, indicating that respondents are generally well aware of cybercrime provisions and their importance. The result demonstrates a significant understanding among respondents. The average mean score is 4.06, indicating respondents are generally "aware" of these offenses. This awareness reflects effective public education on cybercrime laws and the importance of understanding these offenses' legal framework (Chen, 2021). High awareness levels are crucial in ensuring compliance with cybercrime laws and fostering a secure digital environment (Tambo & Kazienga, 2017).

Table 9. Level of cybercrime awareness in terms of legal implications on cybercrime legislation

No.	Descriptions	Mean	Std. Deviation	Interpretation
1	Awareness that crimes committed using information and communications technologies fall under the provisions of this R. A. 10175, with penalties one degree higher than those in the Revised Penal Code or special laws.	4.09	0.83	Aware

2	Awareness that prosecution under R. A. 10175 does not exempt individuals from liability for violating provisions of the Revised Penal Code or special laws.	4.04	0.86	Aware
	Average	4.06	0.77	Aware

Awareness that crimes committed using information and communications technologies fall under the provisions of this R. A. 10175, with penalties one degree higher than those in the Revised Penal Code or special laws, garnered the highest mean score, at 4.09, indicating that respondents are "aware" that crimes committed using information and communications technologies fall under the provisions of R. A. 10175, with penalties one degree higher than those in the Revised Penal Code or special laws Recent studies have highlighted the growing awareness of the legal implications of cybercrime, particularly under R. A. 10175, which imposes enhanced penalties for offenses involving information and communications technologies (Serzo, 2021) According to Hui et al. (2017), the public's understanding of the stricter penalties associated with cybercrimes under this legislation is crucial for deterrence and compliance Shillair et al. (2022) Emphasize that educational initiatives and legal reforms have significantly raised awareness of these heightened penalties, contributing to a more informed populace.

Conversely, awareness that prosecution under R. A. 10175 does not exempt individuals from liability for violating provisions of the Revised Penal Code or special laws has the lowest mean score, at 4.04, still interpreted as "aware." Oville et al. (2024) found that awareness of R. A. 10175 has increased vigilance and adherence to cybercrime laws among internet users. This is supported by findings from Tsakalidis & Vergidis (2019), which show that individuals recognize the potential for being held accountable under multiple legal frameworks for cybercrime offenses (Fichman et al., 2014) argue that this comprehensive awareness is essential for ensuring that individuals are fully informed of the legal repercussions of their actions in the digital realm.

Awareness that crimes committed using information and communications technologies fall under the provisions of R. A. 10175, with penalties one degree higher than those in the Revised Penal Code or special laws, scored a mean of 4.09. This indicates that respondents know the enhanced penalties for cybercrime offenses under this legislation. Awareness that prosecution under R. A. 10175 does not exempt individuals from liability for violating provisions of the Revised Penal Code or special laws achieved a mean score of 4.04. This demonstrates respondents' understanding that they can be held accountable under multiple legal frameworks for cybercrime offenses.

3.3 Level of Awareness Cybercrime Laws

Table 10 summarizes the level of awareness of cybercrime law across various factors. The data reveals a consistently high level of awareness among respondents regarding different aspects of cybercrime law, with mean scores ranging from 4.05 to 4.17, indicating that respondents are generally well aware of cybercrime provisions and their importance.

Table 10. Summary on the level of awareness of cybercrime law

	Factors	**Mean**	**Std. Deviation**	**Interpretation**
A	Confidentiality, integrity, and availability of computer data and systems	4.12	0.67	Aware
B	Computer-related offenses	4.05	0.75	Aware
C	Content-related offenses	4.17	0.69	Aware
D	Commission offenses	4.07	0.72	Aware
E	Legal implications of cybercrime legislation	4.06	0.77	Aware
	Overall Awareness	4.09	0.57	Aware

The mean score for the factor related to confidentiality, integrity, and availability of computer data and systems is 4.12, indicating that respondents know the importance and provisions related to these aspects. The standard deviation of 0.67 suggests relatively consistent responses. The factor addressing computer-related offenses

has a mean score of 4.05, demonstrating respondents' awareness of computer-related crimes, such as forgery, fraud, and identity theft. The standard deviation of 0.75 shows some variation in responses.

Content-related offenses score a mean of 4.17, the highest among all factors, indicating that respondents are highly aware of offenses related to the content, such as lascivious exhibitions, child pornography, unauthorized commercial communications, and libel. The standard deviation of 0.69 indicates consistency. In responses, Commission offenses, including assisting or attempting cybercrimes, have a mean score of 4.07, showing respondents are aware of their legal responsibilities and liabilities. The standard deviation of 0.72 suggests some variability in responses. The legal implications of the cybercrime legislation factor have a mean score of 4.06, reflecting awareness among respondents about the enhanced penalties and multiple legal liabilities associated with cybercrime. The standard deviation of 0.77 indicates some variation in responses.

The overall awareness score is 4.09, with a standard deviation of 0.57, indicating that respondents generally have a high level of awareness about cybercrime law and its various provisions. This suggests that respondents understand the legal framework surrounding cybercrime and recognize the importance of compliance with these laws.

Recent studies have emphasized the growing awareness of the legal implications of cybercrime, particularly regarding the confidentiality, integrity, and availability of computer data and systems. According to De Bruijn & Janssen (2017), the public's understanding of the significance of these aspects is crucial for maintaining cybersecurity. Shillair et al. (2022) highlight that educational initiatives have significantly raised awareness of these critical factors, contributing to a more informed populace. Nwankpa and Datta (2023) found that awareness of cybercrime policies and provisions has increased vigilance and adherence to cybersecurity practices among internet users.

Moreover, research by Clough (2015) indicates a strong public understanding of computer-related offenses, such as forgery, fraud, and identity theft. This aligns with findings by Tsakalidis and Vergidis (2019), which show that individuals recognize the seriousness of these crimes and the legal consequences involved.

3.4 Significant Difference in the Level of Awareness of Cybercrime Law in Terms of Profile

Significant Difference in terms of Program. Table 11 compares the level of awareness of cybercrime law across different academic programs, examining five factors: confidentiality, integrity, and availability of computer data and systems; computer-related offenses; content-related offenses; commission offenses; and legal implications on cybercrime legislation.

Table 11. Mean comparison of the level of awareness of cybercrime law across different programs

	Factors	F-value	p-value	Interpretation	Post Hoc Test
A	Confidentiality, integrity, and availability of computer data and systems	7.722	0.000	Differs significantly	BEED & BSAM BEED & BSBA BSAM & BSC BSBA & BSC
B	Computer-related offenses	4.604	0.001	Differs significantly	BAT/BSA & BSC BSAM & BSC BSBA & BSC
C	Content-related offenses	8.443	0.000	Differs significantly	BAT/BSA & BEED BAT/BSA & BSC BEED & BSAM BEED & BSBA BSAM & BSC BSBA & BSC

D	Commission Offenses	10.148	0.000	Differs significantly	BAT/BSA & BEED BAT/BSA & BSAM BAT/BSA & BSC BEED & BSBA BSAM & BSC BSBA & BSC
E	Legal Implications of Cybercrime Legislation	6.843	0.000	Differs significantly	BAT/BSA & BSC BSAM & BSC BSBA & BSC
Overall Awareness of Cybercrime Law		10.927	0.000	Differs significantly	BAT/BSA & BEED BAT/BSA & BSC BEED & BSAM BEED & BSBA BSAM & BSC BSBA & BSC

The analysis reveals significant differences in awareness levels across all factors and overall cybercrime law awareness, as indicated by the F-values and p-values (all p-values = 0.000 or 0.001). The post hoc tests identify specific program pairs with significant differences, notably with Bachelor of Science in Agriculture (BAT/BSA) often showing higher awareness compared to other programs like Bachelor of Science in Computer Science (BSC), Bachelor of Elementary Education (BEED), Bachelor of Science in Agriculture Management (BSAM), and Bachelor of Science in Business Administration (BSBA) Overall, students in different programs exhibit varying levels of awareness of cybercrime laws, with specific programs showing notably higher or lower awareness compared to others.

Significant Difference in Gender. Table 12 presents the mean comparison of the level of awareness of cybercrime law between genders, precisely according to five factors**.**

Table 12. Mean comparison of the level of awareness of cybercrime law between genders

	Factors	t-value	p-value	Interpretation
A	Confidentiality, integrity, and availability of computer data and systems	-0.469	0.639	Do not differ significantly
B	Computer-related offenses	-0.911	0.363	Do not differ significantly
C	Content-related offenses	-0.973	0.331	Do not differ significantly
D	Commission Offenses	-1.476	0.141	Do not differ significantly
E	Legal Implications of Cybercrime Legislation	-1.284	0.200	Do not differ significantly
	Overall Awareness of Cybercrime Law	-1.301	0.194	Do not differ significantly.

The analysis reveals that there are no significant differences between genders in the level of awareness of cybercrime law across various factors, including confidentiality, integrity, and availability of computer data and systems, computer-related offenses, content-related offenses, commission offenses, and legal implications on cybercrime legislation Additionally, the overall awareness of cybercrime law also shows no significant difference between genders Therefore, the study concludes that gender does not significantly influence the level of awareness of cybercrime law across all the factors examined.

Significant Difference in terms of Year Level. Table 14 presents the mean comparison of the level of awareness of cybercrime law across different year levels, revealing significant differences among students from various academic years.

Table 13. Mean comparison of the level of awareness of cybercrime law across different year levels

	Factors	F-value	p-value	Interpretation	Post Hoc Test
A	Confidentiality, integrity, and availability of computer data and systems	5.907	0.001	Differs significantly	1st Year & 3rd Year 1st Year & 4th Year
B	Computer-related offenses	6.652	0.000	Differs significantly	1st Year & 3rd Year 2nd Year & 3rd Year
C	Content-related offenses	5.367	0.001	Differs significantly	1st Year & 3rd Year 2nd Year & 3rd Year
D	Commission Offenses	5.047	0.002	Differs significantly	1st Year & 3rd Year 1st Year & 4th Year 2nd Year & 3rd Year
E	Legal Implications of Cybercrime Legislation	6.175	0.000	Differs significantly	1st Year & 2nd Year 1st Year & 3rd Year 1st Year & 4th Year
Overall Awareness of Cybercrime Law		9.155	0.000	Differs significantly	1st Year & 3rd Year 1st Year & 4th Year 2nd Year & 3rd Year

The analysis of awareness levels of cybercrime law across different year levels indicates significant differences for all examined factors: confidentiality, integrity, and availability of computer data and systems; computer-related offenses; content-related offenses; commission offenses; and legal implications on cybercrime legislation. Significant differences are predominantly found between 1st Year and upper-year students (3rd and 4th Year) and, in some cases, between 2nd Year and 3rd Year students. The overall awareness of cybercrime law also shows significant differences among year levels, emphasizing that awareness increases as students' progress through their academic programs. This highlights a notable variation in awareness of cybercrime laws between lower and upper-year students.

3.5 Implications to Higher Education Institutions

Awareness and understanding of cybercrime law among students are critical in today's digital age, where cybersecurity threats are prevalent. The demographic profile of students, their level of cybercrime awareness, and the significant differences in awareness based on their profiles are essential factors to consider.

This study focuses on the outside factors of an ideal cybercrime awareness program. It is designed to investigate how students' demographic profiles, such as their academic programs, year levels, and gender, influence their awareness of cybercrime laws.

Results show that higher education institutions need to tailor their awareness campaigns and educational content to address the specific needs and gaps identified in each demographic group to maximize the awareness of cybercrime law. Programs such as BSBA and BSC demonstrate higher awareness than others like BAT/BSA and BEED. Additionally, implementing targeted awareness programs early in the student's academic journey, possibly during orientation or first-year seminars, and reinforcing these topics in subsequent years will solidify their understanding and awareness. Workshops, seminars, and training sessions should be designed to engage all genders, addressing any specific concerns or misconceptions they may have about cybercrime and its legal implications.

Lastly, leveraging technology in their teaching methods can enhance the effectiveness of cybercrime awareness education. Online modules, virtual simulations, and interactive platforms can provide students with hands-on experience dealing with cyber threats and understanding cybercrime laws. Developing and implementing policies that support continuous learning and awareness of cybercrime laws, such as mandatory cybercrime awareness courses and regular updates to the curriculum, will further enhance students' preparedness to navigate the complexities of cybercrime in the digital age.

4. CONCLUSIONS

This section interprets the research findings, drawing meaningful insights from the analyzed data. It discusses the implications of the respondents' diverse demographic distribution, the high levels of cybercrime awareness observed, and the significant differences in awareness across various groups.

1.The diverse demographic distribution of the respondents across various academic programs, year levels, and genders indicates a well-rounded and representative sample. The higher enrollment in the BSBA program and the balanced mix of year levels suggest a broad interest and engagement in business administration education. The slight female majority in gender distribution reflects the gender dynamics within the student population. This diversity ensures comprehensive insights into the awareness and perceptions studied in this research.

2. The high mean scores across all dimensions of cybercrime awareness demonstrate that the respondents understand cybercrime laws and their implications. Content-related offenses show. The highest awareness, indicating that respondents are particularly well-informed about this area. The overall high level of awareness, with an average mean score of 4.09, suggests that educational efforts to inform students about cybercrime laws have been practical. This comprehensive understanding is crucial for fostering a secure and informed digital environment.

3. Significant differences in cybercrime awareness levels across academic programs and year levels highlight the variability in how different student groups perceive and understand cybercrime laws. These disparities, particularly between specific academic programs and year levels, underscore the need for tailored educational initiatives. By addressing these gaps, institutions can ensure a more uniform level of awareness and understanding across all student demographics, thereby enhancing the overall effectiveness of cybercrime law education and compliance.

5. ACKNOWLEDGEMENT

First and foremost, we express our heartfelt gratitude to the Almighty God. Your unwavering presence has provided us with strength and direction throughout this journey. We are immensely grateful for the wisdom and blessings you bestowed upon us, which enabled us to accomplish this thesis.

We sincerely thank our parents, Liza T. Gandela, Jose C. Gandela, Lotche A. Cabang, Virgenito C. Damiar, Geralyn D. Damiar, and other loved ones. Your unwavering love and support served as the foundation that Made everything possible. Thank you for acknowledging every milestone, big or small, and lending a listening ear during difficult times. Your unflinching belief in us spurred our determination throughout the process.

We are truly grateful to our thesis adviser, Sir Randy M. Pajo. Your great help, experience, and encouragement were vital in shaping this thesis. We also thank the panel's chair, Sir Jade S. Cervantes, and the esteemed panel members, Ma'am Leneth Pearl S. Pingot and Sir Bryan L. Susada, for their contributions. Thank you for taking the time and expertise to review our thesis. We respect your intelligent comments and recommendations, which will help refine our research.

Additionally, we appreciate our friends and colleagues. We appreciate your unwavering support, late-night discussions, and diligent effort and help throughout our journey. Your kindness and companionship made this journey even more rewarding.

Finally, we express our profound gratitude to the study participants, whose efforts served as the foundation for this thesis. Your willingness to contribute your experiences and insights is much appreciated and has significantly enhanced our research.

.6. REFERENCES

[1] Adel, S. a. H. (2023, September 15). Cyber hacking: building a harmonised criminal legal framework for addressing cyber hacking in the Arab convention on combating information technology offences: a comparative study between Jordanian & Saudi cyber laws. Figshare. https://aru.figshare.com/articles/thesis/Cyber_hacking_building_a_harmonised_criminal_legal_framework_for_addressing_cyber_hacking_in_the_Arab_convention_on_combating_information_technology_offences_a_comparative_study_between_Jordanian_Saudi_cyber_laws/24147432

[2] Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1), tyy006.

[3] Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1–12.

[4] Alazab, M., & Broadhurst, R. (2016). An analysis of the nature of spam as cybercrime. In Springer eBooks (pp. 251–266).

[5] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754k3

[6] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73.

[7] Alexandrou, A. (2021). Cybercrime and information technology: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices. CRC Press.

[8] Al-Nomani, D. N. S., Al Nabhani, S. A. M., & Ahmed, S. T. (2021). Creating Mass Cyber Security Awareness Among Children, Parents And Teachers Through Appropriate Training And Campaign Mechanism. Journal of Student Research.

[9] Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. Sustainability, 15(15), 11512.

[10] Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. Sustainability, 15(15), 11512.

[11] Alwan, H. B. (2019). National Cyber Governance Awareness Policy and Framework. International Journal of Legal Information, 47(02), 70–89.

[12] Amoo, N. O. O., Atadoga, N. A., Abrahams, N. T. O., Farayola, N. O. A., Osasona, N. F., & Ayinla, N. B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205–217.

[13] Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. Journal of Management Information Systems, 34(4), 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

[14] Andronache, A. (2021). Increasing Security Awareness through Lenses of Cybersecurity Culture. Journal of Information Systems & Operations Management, 15 (1), 7-22.

[15] Ariola, B. P., Laure, E. R. F. O., Perol, M. L. A., & Talines, P. J. T. (2018). Cybercrime Awareness and Perception among Students of Saint Michael College of Caraga.

[16] Ariola, B. P., Laure, E. R. F. O., Perol, M. L. A., & Talines, P. J. T. (2018). Cybercrime Awareness and Perception among Students of Saint Michael College of Caraga.

[17] Arora, P. (2017). The next billion users: Digital life beyond the West. Harvard University Press. Retrieved from: https://books.google.com.ph/books?hl=tl&lr=&id=W6ODDwAAQBAJ&oi=fnd&pg=PP1&dq=info:k_Cc0UH

YoKMJ:scholar.google.com/&ots=4MHIMLbiC0&sig=eXfROoU72asL8vaX44nQF0hkmpE&redir_esc=y#v=onepage&q&f=false

[18] Asam, A. E., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. Computers in Human Behavior, 65, 127–141.

[19] Aswathnarayanan, K. (2024). Assessing Cybercrime Awareness and Internet Usage among Students: Implications for Policy and Education Section A -Research paper Assessing Cybercrime Awareness and Internet Usage among Students: Implications for Policy and Education". 1147-1153.

[20] Atta Ul Haq, Q. (2021). Cyber Crime and Their Restriction Through Laws and Techniques for Protecting Security Issues and Privacy Threats. In: Mahalle, P.N., Shinde, G.R., Dey, N., Hassanien, A.E. (eds) Security Issues and Privacy Threats in Smart Ubiquitous Computing. Studies in Systems, Decision and Control, vol 341. Springer, Singapore. https://doi.org/10.1007/978-981-33-4996-4_3

[21] Baker, D. & Robinson, P. (2022). Artificial intelligence and the Law: Cybercrime and Criminal Liability. Routledge & CRC Press.

[22] Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11.

[23] Bandura, A. (2009). Social cognitive theory of mass communication. In Media effects (pp. 110-140). Routledge.

[24] Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & security, 68, 145-159.

[25] Bhat, A. (2023). Descriptive Correlational: Descriptive vs Correlational Research. QuestionPro. https://www.questionpro.com/blog/descriptive-research-vs-correlational-research/

[26] Blunt, S. A. (2022). Understanding information security awareness in the American workforce – ProQuest.

[27] Braiker, Harriet B. (2014).Whos pulling Your Strings ? How to Break the Cycle of

[28] Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55.

[29] Brush, K., & Cobb, M. (2024). Cybercrime. Security. https://www.techtarget.com/searchsecurity/definition/cybercrim

[30] Bure, R. D. (2022). A cybersecurity governance framework for broadband expansion projects in the Western Cape (Doctoral dissertation, Cape Peninsula University of Technology).

[31] Caixia, Y. (2022). Research on the system reconstruction of the pluralistic paths of criminal regulation of cyber accomplices. In Edward Elgar Publishing eBooks (pp. 119–144).

[32] Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. Information Technology & People, 32(5), 1130-1152.

[33] Campbell, L. (2023). The Philippines: Cyber Threats.

[34] Canlas, R. B., & Fajardo, R. Q. (2023). Psychology behind Cyber Ethical behavior among Digital Natives: The Case of Higher Education Students in a State University in the Philippines. Journal of Namibian Studies: History Politics Culture, 34, 202-213.

[35] Charan, J. K. (2019) Safety First in the Cyber Universe: Shielding Students and Vulnerable Groups from Online Crime. Cyber Crime &, 112.

[36] Chaudhary, S. (2016). The use of usable security and security education to fight phishing attacks.

[37] Chen, L. (2021). Improving digital connectivity for e-commerce: A policy framework and empirical note for ASEAN.

[38] Collins-Camargo, C., Buckwalter, N., & Jones, B. (2016). Perceptions of state child welfare administrators regarding federally-mandated citizen review panels. Children and Youth Services Review, 62, 83–89.

[39] Cruz, E.M., Sajo, T.J. (2015). Cybersex as Affective Labour: Critical Interrogations of the Philippine ICT Framework and the Cybercrime Prevention Act of 2012. In: Chib, A., May, J., Barrantes, R. (eds) Impact of Information Society Research in the Global South. Springer, Singapore.

[40] Drew, J. M. (2020). A study of cybercrime victimisation and SOLAK: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research, Policy and Practice, 6(1), 17-33.

[41] Erkomaishvili, D., & Gillies, A. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security. Digitální Repozitář UK. https://dspace.cuni.cz/handle/20.500.11956/187353
[42] Fehske, A., Fettweis, G., Malmodin, J., & Biczok, G. (2011). The global footprint of mobile communications: The ecological and economic perspective. IEEE communications magazine, 49(8), 55-62.
[43] Fichman, R. G., Santos, B. L. D., & Zheng, Z. (2014). Digital innovation as a fundamental and powerful concept in the information systems curriculum. Management Information Systems Quarterly, 38(2), 329–343.
[44] Ford, R. A. (2019). Data scams. Hous. L. Rev., 57, 111.
[45] Forouzan, H., Jahankhani, H., & McCarthy, J. (2018). An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the Metropolitan Police Service. Cyber Criminology, 307-323.
[46] Garba, A., Sirat, N. M. B., Hajar, N. S., & Dauda, N. I. B. (2020). Cyber security awareness among university students: a case study. Science Proceedings Series, 2(1), 82–86. https://doi.org/10.31580/sps.v2i1.1320
[47] Ghonge, M. M., Pramanik, S., Mangrulkar, R., & Le, D. N. (Eds.). (2022). Cyber security and digital forensics: Challenges and future trends. John Wiley & Sons.
[48] Gillespie, A. A. (2019). Cybercrime: Key issues and debates. Routledge.
[49] Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Anchor.
[50] Grabosky, P. (2007). Requirements of prosecution services to deal with cybercrime. Crime, law and social change, 47, 201-223.
[51] Grabosky, P. (2016). The Evolution of Cybercrime, 2006-2016. In Cybercrime Through an Interdisciplinary Lens (pp. 29–50).
[52] Gravino, E. & Villanueva, M. C. (2021). R.A. No. 10175: The Cybercrime Prevention Act: The Net Commandments. Philippine Legal Research.
[53] Gravino, E. & Villanueva, M. C. (2021). R.A. No. 10175: The Cybercrime Prevention Act: The Net Commandments. Philippine Legal Research.
[54] Green, L. (2010). The internet: an introduction to new media. Berg.
[55] Henry, N., & Powell, A. (2015). Embodied harms. Violence Against Women, 21(6), 758–779.
[56] Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
[57] Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
[58] Horgan, S. L. (2019). Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder.
[59] Horgan, S. L. (2019). Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder.
[60] Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. MIS Quarterly, 41(2), 497–524.
[61] Ibrahim, H. (2022). A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. Wasit Journal of Computer and Mathematics Science, 1(3), 76-108.
[62] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177.
[63] Jain, A., & Gupta, N. (2020). Cyber crime. National Journal of Cyber Security Law, 2(2), 152-158.
[64] Jamshed, J., Rafique, W., Baig, K., & Ahmad, W. (2022). Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. International Journal of Business and Economic Affairs, 7(1), 10-22.
[65] Johnson, M. (2016). Cyber crime, security and digital intelligence. Routledge.
[66] Jones, R., & Sparks, R. (2019). Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder. https://era.ed.ac.uk/handle/1842/35869
[67] Kala, E. M. (2024). Influence of online platforms on criminal behavior. International Journal of Research Studies in Computer Science and Engineering, 10(1), 25–37.

[68] Kharat, S. (2017). Cyber crime–a threat to persons, property, government and societies. Property, Government and Societies (March 1, 2017).

[69] Kilag, O. K. T., Indino, N. V., Sabagala, A. M., Abendan, C. F. K., Arcillo, M. T., & Camangyan, G. A. (2023). Managing cybersecurity risks in educational technology environments: strategies and best practices. American Journal of Language, Literacy and Learning in STEM Education (2993-2769), 1(5), 28-38.

[70] Kittichaisaree, K. (2017). Cyber Crimes. In Law, governance and technology series (pp. 263–293). https://doi.org/10.1007/978-3-319-54657-5_7

[71] Latif, N. W. A., Hasnan, S., Hussain, A. R. M., & Ali, M. M. (2021). The influence of fraud prevention mechanisms on fraud awareness in the federal ministries in Malaysia. Asia-Pacific Management Accounting Journal/Asia-Pacific Management Accounting Journal, 16(3), 191–220.

[72] Lavorgna, A. (2020). Cybercrimes: Critical issues in a global context. Bloomsbury Publishing.

[73] Lee, C. S., & Kim, J. H. (2020). Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. Computers & Security, 97, 101995.

[74] Lee, C. S., & Kim, J. H. (2023). How victims perceive fear of cybercrime: importance of informed risk. Criminal Justice Studies, 36(3), 206–227. (2023). How victims perceive fear of cybercrime: importance of informed risk. Criminal Justice Studies, 36(3), 206–227.

[75] Liwur, S., Takyi, S., Amponsah, O., & Quagraine, V. (2023). Spatio-temporal analysis and level of awareness of Ghana's buffer regulations on ecologically sensitive areas: lessons from the Kumasi Metropolis. African Geographical Review. 1-22. 10.1080/19376812.2023.2250329.

[76] Lošonczi, P. (2018). Importance of dealing with cybersecurity challenges and cybercrime in the senior population. Security Dimensions, 26, 173-186.

[77] Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. IEEE transactions on professional communication, 57(2), 123-146.

[78] Manipulation (psychology). (2024, February 6). Wikipedia. Ayyagari, R. (2020). Data breaches and carding. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 939-959.

[79] Manipulation. ISBN 0-07-144672-9.

[80] Martin, E. V. (2022). The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training (Doctoral dissertation, Walden University).

[81] Martin, E. V. (2022). The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training (Doctoral dissertation, Walden University).

[82] Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. Media and Communication, 8(2), 258-269.

[83] Morse, B. A., Carman, J. P., & Zint, M. T. (2019). Fostering environmental behaviors through observational learning. Journal of Sustainable Tourism, 27(10), 1530-1552.

[84] Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the Human. Proceedings of the Working Group Reports on Innovation and Technology in Computer Science EducationDecember.

[85] Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. International Journal of Research in Business and Social Science, 11(4), 384–396.

[86] Noain-Sánchez, A. (2016). "Privacy by default" and active "informed consent" by layers. Journal of Information, Communication & Ethics in Society, 14(2), 124–138.

[87] Norse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624.

[88] Nzeakor, O. F., Nwokeoma, B. & Ezeh, P-J. (2020). Pattern of cybercrime awareness in Imo State, Nigeria: an empirical assessment – ProQuest.

[89] Okutan, A. (2019). A framework for cyber crime investigation. Procedia Computer Science, 158, 287-294.

[90] Oville, J. M., Dodelon Sabijon, Yolanda Sayson, Maricar G. Cañedo, Christine B. Salem, & and Renato C. Sagayno. (2024). Sentry of the Cyberspace during Covid-19 Pandemic: Experiences of Philippine National Police Cyber Cops. International Journal of Law and Politics Studies, 6(3), 54–65.

[91] Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. J. Nat'l Sec. L. & Pol'y, 10, 487.

[92] Petrosyan, A. (2024). Worldwide digital population 2024. Statista.

[93] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic sciences, 2(2), 379-398.

[94] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022, April 16). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379–398.

[95] Pontes, H. M., Szabo, A., & Griffiths, M. D. (2015). The impact of Internet-based specific activities on the perceptions of Internet addiction, quality of life, and excessive usage: A cross-sectional study. Addictive Behaviors Reports, 1, 19-25.

[96] Ragusa, A., & Crampton, A. (2017). Environmental campaign awareness, participation, and media visibility. ˜ the œInternational Journal of Social Sustainability in Economic, Social and Cultural Context/International Journal of Social Sustainability in Economic, Social and Cultural Context, 13(2), 51–66.

[97] Reinhardt, W., Mletzko, C., Sloep, P., and Drachsler, H. (2012). Understanding the Meaning of Awareness in Research Networks. Journal of Educational Technology & Society. 931.

[98] Reyadul, M. & Reyad, M. (2023). Awareness of Social Engineering in the Educational Sector in Bangladesh. Retrieved from: https://www.researchgate.net/publication/376265387_Awareness_of_Social_Engineering_in_the_Educational_Sector_in_Bangladesh

[99] Richards, N. M., & Hartzog, W. (2015). Taking trust seriously in privacy law. Social Science Research Network.

[100] Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. IEEE Transactions on Dependable and Secure Computing/IEEE Transactions on Dependable and Secure Computing, 13(2), 261–273. https://doi.org/10.1109/tdsc.2015.2410795

[101] Sabillon, R., Cano, J., Cavaller Reyes, V. & Serra Ruiz, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security, 4(6), 165-176.

[102] Sari, H. B., Ningsih, N. M. a. P. C., Kristina, N. M. Y., Rismayanti, N. P. I., Thalib, E. F., Meinarni, N. P. S., & Julianti, L. (2024). DIGITAL ETHICS AND CITIZENSHIP CHALLENGES IN CYBERSPACE: AN OVERVIEW FROM PERSPECTIVE MORALS AND LAWS.

[103] Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 2, 100034.

[104] Saul, B., & Heath, K. (2021). Cyber terrorism and use of the internet for terrorist purposes. In Research Handbook on International Law and Cyberspace (pp. 205-230). Edward Elgar Publishing.

[105] Scott, J., & O'Shea, J. A. (2022). TRANSLATION IN LIBEL CASES: REPUTATIONS AT STAKE! Comparative Legilinguistics, 50, 123–179.

[106] Serzo, A. L. O. (2021). Philippine Regulations for Cross-Border Digital Platforms: Impact and reform Considerations – ProQuest.

[107] Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756.

[108] Sirisilla, S. (2023). Bridging the Gap: Overcome these 7 flaws in descriptive research design. Enago Academy.

[109] Sirisilla, S. (2023). Bridging the Gap: Overcome these 7 flaws in descriptive research design. Enago Academy.

[110] Smith, K.T., Jones, A., Johnson, L. and Smith, L.M. (2019), "Examination of cybercrime and its effects on corporate stock value", Journal of Information, Communication and Ethics in Society, Vol. 17 No. 1, pp. 42-60.

[111] Solak, D., & Topaloglu, M. (2014). The Perception Analysis of Cyber Crimes in View of Computer Science Students. Procedia: Social & Behavioral Sciences, 182, 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787

[112] Soylu, D., Medeni, T. D., Andekina, R., Rakhmetova, R., & Ismailova, R. (2021). Identifying the cybercrime awareness of undergraduate and postgraduate students: Example of Kazakhstan. 2021 IEEE

International Conference on Smart Information Systems and Technologies (SIST). https://doi.org/10.1109/sist50301.2021.9465995

[113] Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: towards a'digital criminology'?. International Journal for Crime, Justice and Social Democracy, 6(2), 17-33.

[114] Tambo, E. & Kazienga, A. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. International Journal of Cyber-security and Digital Forensics, 6(3), 126–138.

[115] Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. International Journal of Cyber-Security and Digital Forensics, 6(3), 126-138.

[116] Taylor, P. (2023). Forecast number of mobile users worldwide 2020-2025. Statista.

[117] Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management, 12(3), 1-23.

[118] Tomer, A., Gautam, J. K., Gupta, J. K., Singh, H., & Deshwal, A. (2023). Psychological, Economical, Privacy and Personnel Impacts of Cybercrime: Is Cyber Crime Exploits Technology and Digital Platforms. Journal for ReAttach Therapy and Developmental Diversities, 6(8s), 114-133.

[119] Tsakalidis, G., & Vergidis, K. (2019). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics. Systems, 49(4), 710–729.

[120] Tsakalidis, G., & Vergidis, K. (2019). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics. Systems, 49(4), 710–729.

[121] United Nations Office on Drugs and Crime. (2019). Cybercrime Module 3 Key issues: The role of Cybercrime Law.

[122] United Nations Office on Drugs and Crime. (2019). Cybercrime Module 3 Key issues: The role of Cybercrime Law.

[123] Veresha, R. (2018). Preventive measures against computer related crimes: Approaching an individual. Informatologia, 51(3-4), 189-199.

[124] Vieraitis, L. M., Copes, H., Powell, Z. A., & Pike, A. (2015). A little information goes a long way: Expertise and identity theft. Aggression and Violent Behavior, 20, 10–18.

[125] Vitus, E. N. (2023). Cybercrime and Online Safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users—A Case of African States. Tijer-International Research Journal, 10(9), 975-989.

[126] Voogt, J., Erstad, O., Dede, C., & Mishra, P. (2013). Challenges to learning and schooling in the digital networked world of the 21st century. Journal of Computer Assisted Learning, 29(5), 403–413. https://doi.org/10.1111/jcal.12029

[127] Walsh, J. P., & O'Connor, C. (2019). Social media and policing: A review of recent research. Sociology compass, 13(1), e12648.

[128] Walter, M., Kukutai, T., Carroll, S. R., & Rodriguez-Lonebear, D. (2020). Indigenous Data Sovereignty and Policy. In Routledge eBooks.

[129] Wang, S., Zhang, X., Zhang, Y., Wang, L., Yang, J., & Wang, W. (2017). A survey on mobile edge networks: Convergence of computing, caching and communications. Ieee Access, 5, 6757-6779.

[130] Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networking, 18(1), 3-7.

[131] Wika, P. M. & Suchi, P. N. (2021). Cybercrime and Terrorism Financing: Nigeriaâ€TMs Potential Vulnerabilities and Policy Options. Ideas.repec.org.

[132] Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. Computers in Human Behavior, 72, 412-421.

[133] Woodhams, S. (2021). Spyware: An unregulated and escalating threat to independent media. Center for International Media Assistance.

[134] Yadav, V. (2023). Tackling Non-Consensual Dissemination of Intimate Images in India's contemporary legal framework. Annales Internationales De Criminologie, 61(3–4), 355–383.

[135] Yeager, T. (2018). Institutions, transition economies, and economic development. Routledge.

[136] Zwilling, M. Lesjak, D., Natek, S., Phusavat, K. & Anussornnitisarn, P. (2019). How To Deal With The Awareness Of Cyber Hazards And Security In (Higher) Education. Thriving on Future Education, Industry, Business and Society; Proceedings of the MakeLearn and TIIM International Conference 2019. ToKnowPress.

[137] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.