Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 7, Issue 2, Pages 160-176, April-June 2023

Cybercrime Awareness Among Senior High School Students

Christian Hygeia S. Toso*, Arnel Joey A. Jumalon, Jaderus Anfernee R. Magadan, Angelita B. Alvarico & Jose F. Cuevas Jr.

College of Criminology, Misamis University, Ozamiz City, Philippines.
*Corresponding Author Email: jingkyut1@gmail.com**

DOI: https://doi.org/10.46382/MJBAS.2023.7218

Article Received: 25 April 2023 *Article Accepted: 17 June 2023* *Article Published: 27 June 2023*

ABSTRACT

Over the past few years, Cybercrime has been increasing rapidly which gives a huge impact on the lives of the people especially the growing youth in the community. This study was conducted to determine the level of Cybercrime awareness among Senior High School students at Misamis University. This study uses quantitative research as its descriptive design. It has 253 respondents which are Senior High School students of Misamis University. Random sampling was used to identify the respondents from Grades 11 and 12 from the five (5) different strands namely: General Academic Strand (GAS), Pre-Baccalaureate Maritime, Science, Technology, Engineering and Math (STEM), Accountancy, Business and Management (ABM) and Humanities and Social Sciences (HUMMS). The adopted questionnaire survey was conducted to collect data regarding the students' awareness of Cybercrime. The findings of the study revealed that the level of Cybercrime awareness among the respondents was Very Aware, particularly in Cyberbullying, Cyberpornography, and Identity Theft. Therefore, the respondents are aware enough to avoid becoming a victim or from doing such acts of Cybercrime at all costs. On the other hand, circumstances may appear unexpectedly which is why we must be vigilant at all times to give guidance, safety, and security whenever they need it hence they have a good understanding of some types of cybercrime, such as cyberbullying, hacking, and phishing, but they have a limited understanding of other types, such as identity theft and online scams. Overall, this study provides insights into the level of awareness of cybercrime among senior high school students. The findings suggest that there is a need for increased or maintained education, information drive, and awareness-raising activities to help students develop a better understanding of the various forms of cybercrime and the risks associated with them. By enhancing the awareness of cybercrime among senior high school students, we can help them to use the internet more safely and responsibly, and protect them from falling victim to cybercrime. By implementing these recommendations, educators and policymakers can help senior high school students develop a better understanding of the risks associated with the use of technology, and equip them with the knowledge and skills to stay safe online.

Keywords: Awareness; Cybercrime; Cyber security; Online; Senior High School students.

1. Introduction

Cybercrime has emerged as a critical global concern with the increased use of technology in daily life. We use the Internet for various things, including communication, entertainment, education, and work. It has become essential (Adinya & Obono, 2021). However, the Internet exposes us to several threats, such as Cybercrime. Senior high school kids are particularly susceptible to online crime. They are accustomed to spending much time online since they are digital natives who grew up in a society where technology is pervasive. However, studies have shown that many young people are unaware of the dangers of using technology, making them more vulnerable to Cybercrime (Rajasekharaiah et al., 2020).

People's attitudes on one's dignity have always been crucial since they shape a person's mindset and morals, especially those of young people (Telo, 2023). The Internet, the world's largest anarchist experiment, is the first invention that humanity has made that it does not comprehend, according to Eric Schmidt 2021. Any behavior using a computer network or networked device for illegal purposes is called Cybercrime (Deora & Chudasama, 2021). In other words, the crime in question is committed by someone while using any digital device. This subject will make young people aware of the extent and limitations of Cybercrime, enabling them to forge solid bonds with their families, peers, and society. This idea is crucial because, if overlooked, it may encourage young people to commit crimes of this nature and veer from the proper path. Due to the effect of the environment, providing young people with adequate knowledge is a difficult responsibility for the government (Lee et al., 2021). Cybercrime has

emerged globally due to the advancement of science and technology (Lee, 2019). The first notable increase in Cybercrime happened in the late 1980s, along with email development. It has succeeded by disseminating various infections and scams (Dada et al., 2019). As web browser technology advanced in the 1990s, the second phase emerged. Because of their curiosity, many users were vulnerable to infections. When browsing dubious websites, viruses were spread via Internet connections (Thakral and Kalghatgi 2022). As social media took off in the 2000s, cybercrime cases also emerged, involving the straightforward hacking of personal data. Hackers typically try to acquire private data to advance their tactics and plans (Holt, 2020).

Social media is a tool that has both constructive and destructive uses. According to Mundt et al., (2018), social media comprises any digital technology that allows users to create and share content easily. A computer, smartphone, iPad, or other internet-connected device can access it. Some popular social media networks include Twitter, Instagram, Facebook, WhatsApp, and Messenger. Due to its ability to bring people together by exchanging pictures, feelings, and films that cause major security problems, it has become increasingly popular (Pianese and Belfiore, 2021). Nowadays, young individuals who feel comfortable and confident enough to share personal information on social networking platforms make up the majority of users. Internet scammers can register as many social media accounts as they wish under different aliases and exploit them for unlawful activities because social networking sites are so widely used (Umejiako and Uzoka, 2022). Remember that maintaining safety is essential when utilizing social media platforms. However, your name, phone number, and even your address could be taken and used for identity theft or the creation of false identities if you do not take the necessary safeguards. The full power of the leading social media platforms can be shown by observing their extensive influence (Gawer, 2022).

According to Jing et al., (2019), the ICT sector in the Philippines is one of the countries in Southeast Asia with the quickest economic development. However, because of its large population of internet users, the nation is also among the most susceptible to Cybercrime. Due to youngsters' greater access to technology and the Internet, Cybercrime is an issue that is getting worse in the Philippines (Szymkowiak et al., 2021). Due to the large number of internet users in the Philippines and the lack of knowledge and education regarding Cybercrime, there have been several instances of kids becoming involved in Cybercrime, either as perpetrators or victims (Abuda et al., 2020). The Philippines has a sizable young population, making them vulnerable to Cybercrime.

Knowledge is easily accessible to us thanks to modern technology. Threats to computer security are always present and always changing to keep up with and surpass new and developing technology (Lavorgna, 2020). At the very least, the perpetrators of these threats continuously devise new ways to annoy and disturb us; at worst, they are trying to steal our identity, money, and property (Bambacht and Pouwelse, 2022). The Philippines has never lagged in adopting new technologies, particularly regarding the Internet. On September 12, 2012, the Philippine Congress passed Republic Act No. 10175, often known as the "Cybercrime Prevention Act of 2012," which covers crimes against and perpetrated using computer systems. It consists of substantive and procedural penal laws and laws governing international cooperation. It has been described as "a crime committed with or through the use of information and communication technologies such as radio, television, cellular phones, computers and networks,

and other communication device or application," according to the Department of Justice (DOJ) (2021, Primer on Cybercrime Law. According to this definition, it appears that the term "cybercrime" has a broad definition in our nation and is not just limited to felonies committed using computers or the Internet. Two measures approved by the Philippine Senate and House of Representatives in June 2012 resulted in Republic Act 10175, often known as the Cybercrime Prevention Act of 2012. The final consolidated form of the measures above was signed into law by President Benigno Aquino III in September of the same year.

According to a recent study on peer influence, teenagers are more likely to participate in cybercrimes like hacking and online bullying if their friends do. It is crucial to know what your children are doing online and whom they are interacting with, both offline and online (Towner et al., 2022). Today's digital world has evolved into a similar way of existing. The general people can now do things that were unthinkable just a few years ago. Because of the increasing dependence and reliance of mankind on these computers, the Internet is quickly becoming a way of life for millions of people. Email, websites, and others are used anytime, everywhere I.T. solutions have been made possible via the Internet for the benefit of humanity. The Internet has many positive social effects and provides criminals with new, highly sophisticated technological tools. To prevent engaging in it or unintentionally creating illegal and punishable activities, they should be informed of the extent and restrictions of Cybercrime. Due to this, policymakers, law enforcement, and international organizations face new issues due to the emerging types of Cybercrime (Stansberry and Anderson, 2019). People's daily lives are significantly impacted by technology because it improves convenience in all facets of existence.

Although there has been research on cybercrime awareness among different age, groups, there needs to be more research on cybercrime awareness among senior high school students and in this particular locale setting. Most existing research focuses on college students or young adults, but there needs to be more research examining the level of cybercrime awareness among senior high school students. Furthermore, many existing studies on cybercrime awareness have been conducted in Western countries, with few studies in Asian countries, where internet usage and culture may differ significantly. Thus, there is a need for research that focuses on the specific context of senior high school students at Misamis University, Ozamiz City, where the use of technology is prevalent. However, awareness of Cybercrime may be limited or lacking.

Therefore, the study "Cybercrime Awareness Among Senior High School Students" aims to address this gap by examining the level of cybercrime awareness among senior high school students in an Asian country, specifically in the context of the Philippines. This study provides insights into the level of awareness among senior high school students, which can help educators and policymakers to develop appropriate programs and policies to enhance cybercrime awareness and ensure that young people are safe online.

2. Methods

In this study, a descriptive research design was employed. This investigation prefers this method because it emphasizes fact-finding with a proper interpretation. The descriptive technique was created to research a specific subject to learn about existing conditions or circumstances. The nature of a scenario or condition, as it exists from the moment of occurrence to the current occurrences, makes this methodology the most suitable tool.

The Senior High School Department of Misamis University, located in H.T. Feliciano St. Ozamiz City, Philippines' is where this research study was carried out. A progressive and dynamic education is promoted by Misamis University, which upholds the principle that God is the center of its existence and that education its service offering to God and country. Det Norske Veritas, a Dutch company, has awarded its first and only ISO certification in Mindanao for its high-quality instruction and services. With its current location, Misamis University has developed into an urban and contemporary institution that contributes to the area's success, progress, and development while enhancing its standing as a top institution of higher learning. The agricultural and fishing industries are major contributors to Ozamis City's economy. Additionally, it produces fisheries goods from fishpond and marine fishing operations in the Panguil Bay region. In the northwest region of Mindanao, most business establishments are evolving into hubs of trade, commerce, and education. Additionally, Ozamiz City is the ideal harbor position for Lanao Del Norte and Misamis Occidental to exploit as a production outlet. There are 51 barangays in Ozamiz City; 28 are in rural areas, and 23 are in urban areas.

In addition, the school provides senior high school instruction in the following strands: General Academic Strand (GAS), Pre-Baccalaureate Maritime, Science, Technology, Engineering, and Math (STEM), Accounting, Business, and Management (ABM), and Humanities and Social Sciences (HUMMS). It features a mix of Catholic and Muslim pupils, which piqued the researchers' interest in using it as the site for the study.

The study's respondents will be two hundred fifty-three (253) Senior High academic Students who are officially enrolled at Misamis University's academic year 2022-2023. 253 Senior High School Students participated out of a total of 1,268 students. They were chosen at random from their respective grade levels and strands using a random sampling process. Five strands will be required in each grade level to produce relevant results and truly determine the level of awareness of senior high pupils toward cybercrime. The demographic profile of the respondents was also gathered such as age, sex, grade level and academic strand of the students.

3. Results and Discussions

This part integrates the results of the study after data gathering. The data tables are prepared with their corresponding frequency, mean, and percentages. The researchers presented it in a table format.

Demographic Profile of the Respondents

First, the researchers divided the respondents' ages into three (3) groups. Table 1 reveals that the majority of respondents are between the ages of 15 and 17, with a frequency of 129 and a percentage of 51%, followed by the one with a frequency of 124 and a percentage of 49%. There are, however, no students over the age of 21. The Sex of the Respondents. According to the statistics, males outnumber females by 144 to a percentage of 56 percent, while females outnumber males by 109 to a percentage of 43.1 percent. As these students are still in high school, there is an opportunity for educational interventions to be implemented to increase their awareness of cybercrime and how to protect themselves online. Schools and educators can work to develop and implement programs to educate students on the risks associated with cybercrime and ways to stay safe online.

Respondents' Grade Level. According to the findings, the majority of respondents are in Grade 11, with 127 in total and a percentage of 50.2 percent, while there are only 126 in Grade 12, with a percentage of 49.8 percent. The

implication of the results was, the majority of respondents being in Grade 11 is that interventions and educational programs related to cybercrime awareness can be targeted towards this grade level. Since Grade 11 students comprise the largest group of respondents, it may be an effective strategy to provide them with age-appropriate information and training on how to stay safe online and avoid becoming victims of cybercrime. Additionally, educators can design and implement interventions that cater to the specific needs and preferences of Grade 11 students, considering that they may have different perspectives and experiences with technology compared to younger or older students. Overall, the findings suggest that there may be an opportunity to strengthen cybercrime awareness and prevention efforts among Grade 11 students, which could potentially benefit the wider student population.

Respondents' Academic Background. The statistics show that the majority of respondents are from Pre-Baccalaureate Maritime, with a frequency of 53 and a percentage of 20.9 percent, while others have a frequency of 50 and a percentage of 19.8 percent. The implication of the result that the majority of the respondents are from Pre-Baccalaureate Maritime is that this group may have unique perspectives or experiences related to cybercrime awareness and prevention. This could be due to the nature of their field of study or career aspirations, which may involve more frequent use of technology and exposure to cyber threats.

Additionally, the fact that a significant percentage of respondents (19.8%) come from other programs suggests that cybercrime awareness and prevention is a relevant topic for a broad range of students, not just those in technology-related fields. This highlights the importance of promoting cyber safety and education across different academic disciplines and fields of study. These findings emphasize the need for tailored and inclusive approaches to cybercrime awareness and prevention, taking into account the diverse backgrounds and perspectives of students from different programs and fields of study.

Table 1. Demographic Profile of the Respondents

(Frequency and Percentage Distribution of Respondents Demographic Profile)

Profile		**Frequency**	**Percentage**
Age			
	15-17	129	51
	18-20	124	49
	21-Up		
Sex			
	Male	144	56
	Female	109	43.1
Grade Level			
	Grade 11	127	50.2
	Grade 12	126	49.8

Academic Strand			
	ABM	50	19.8
	GAS	50	19.8
	HUMSS	50	19.8
	STEM	50	19.8
	Pre- Baccalaureate Maritime	53	20.9
		253	100

Table 2. Level of awareness of Cyberbullying among Senior High School Students

Variables	Mean	SD	Interpretation
Cyberbullying	4.46	0.27	Very Aware

Note: Awareness Scale: 4.24-5.00 (Very Aware); 3.43-4.23 (Aware); 2.62-3.42 (Neutral); 1.81-2.61 (Less Aware); 1.0-1.80 (Least Aware).

Cyberbullying may take place on social media posting and messaging platforms that are aimed at spreading or posting embarrassing photos and videos and sending hurtful, abusive, and threatening messages via messaging platforms (Thukral, 2022).

Table 2 presents the data on cyberbullying. It shows that the majority of the respondents with the highest mean 4.76 are very aware, particularly in the statement (10) Cyberbullying can happen anytime in the online world. I should be vigilant to avoid getting involved in it. The outcome reveals that the students are very vigilant to avoid getting involved and being one of the victims of cyberbullying. Therefore, the students are very aware enough that cyberbullying can happen anytime in the online world and must be vigilant anytime. The table also receives the lowest rating, with a mean of 3.84. Respondents are aware in a statement (5) they will tell their parents/guardians if someone bullied them online. In this response, they are not confident enough to tell their parents/guardians if someone bullied them online. For this reason, they may think that their parents experience a range of negative sensations, including annoyance, anger, and worry about the harmful consequences that bullying and victimization can have for their kids. In the only previous study of parental fear of bullying of which we are aware, (Stives et al., 2019) assessed the extent to which parents were fearful of their child becoming a victim of bullying. In the study of 54 parents, they found parents were evenly divided on whether they were fearful of their child becoming a victim (Stives et al., 2019).

The implication of the study for the result that the majority of respondents are “Very Aware” of the potential for cyberbullying and the need to be vigilant is and education and awareness-raising campaigns around this issue may have been effective. This suggests that efforts to educate students about the risks of cyberbullying and how to prevent it may have been successful in raising awareness and promoting safe online behavior. On the other hand, the finding that students are less confident in telling their parents or guardians if they are being cyberbullied

highlights the need for further support and resources for students who may be experiencing online harassment. This could include providing safe spaces for students to report incidents of cyberbullying and ensuring that there is a clear protocol for addressing such incidents. The study's results suggest that while efforts to raise awareness about cyberbullying may have been successful, there is still room for improvement in terms of supporting students who may be experiencing this type of harassment.

Table 3. Level of awareness of Cyberpornography among Senior High School Students

Variables	Mean	SD	Interpretation
Cyberpornography	4.71	0.09	Very Aware

Note: Awareness Scale: 4.24-5.00 (Very Aware); 3.43-4.23 (Aware); 2.62-3.42 (Neutral); 1.81-2.61 (Less Aware); 1.0-1.80 (Least Aware).

Cyber Pornography means publishing, distributing, or designing pornography by using cyberspace. The technology has its pros and cons and cyber pornography is the result of the advancement of technology (Wulandari, 2021).

Table 3 presents the data on cyberpornography. It shows that the majority of the respondents with the highest mean 4.90 are very aware, particularly in the statement (7) I will not share pornographic photos and videos on social media sites. With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online.

The outcome reveals that they are not fun engaging in sharing pornographic photos and videos online, they are very aware that the display of offensive photographs, particularly those showing sexual activity, is known as cyberporn. On the other hand, all of the statements on cyberpornography interpret “Very Aware”. This implies that even though they are born in a digital age they are very aware enough of what may be a consequence if they will be engaged in cyber pornography activities.

The implication of the study the result that the majority of respondents are very aware of the risks associated with sharing pornographic photos and videos on social media sites is that there may have been effective educational and awareness-raising campaigns around this issue. This suggests that efforts to educate students about the dangers of cyberpornography and the legal consequences of sharing such content may have been successful in promoting responsible online behavior.

Furthermore, the fact that all statements related to cyberpornography were interpreted as "Very Aware" indicates that students are highly sensitive to the risks associated with this type of online content. This highlights the importance of continued education and awareness-raising around the issue, as well as the need for ongoing efforts to prevent the dissemination of cyberpornography and to protect minors from exposure to inappropriate content online. The study's results suggest that efforts to educate students about the risks associated with cyberpornography may have been successful, but continued efforts are needed to promote responsible online behavior and protect students from exposure to inappropriate content online.

Table 4. Level of awareness of Identity Theft among Senior High School Students

Variables	Mean	SD	Interpretation
Identity Theft	4.71	0.09	Very Aware

Note: Awareness Scale: 4.24-5.00 (Very Aware); 3.43-4.23 (Aware); 2.62-3.42 (Neutral); 1.81-2.61 (Less Aware); 1.0-1.80 (Least Aware).

Identity theft is defined as the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases (Ma & McKinnon 2022).

Table 4 presents the data of the responses of the respondents on Identity Theft. It shows that the majority of the respondents with the highest mean 4.85 are very aware, particularly in the statement (10) I do not leave my social media accounts open in a computer shop. Due to the trend of the internet, many business establishments open an internet café. By this genre, students who can't afford to buy gadgets may still have or create their own social media accounts by going into an internet café and opening their social media accounts in it. The aforementioned availability has a time limit which sometimes ought them to forget about logging out of their accounts. All of the statements on Identity Theft interpret Very Aware. It implies that the respondents are truly aware of what they must have to do particularly the logging out of their social media accounts.

The result of the study indicating that the majority of respondents are very aware that they should not leave their social media accounts open in a computer shop has significant implications in terms of preventing identity theft. By being aware of the risks associated with leaving their accounts open, students can take appropriate measures to protect their personal information and prevent unauthorized access to their social media accounts. This awareness can also be extended to other online accounts and transactions, such as online banking, email, and e-commerce. The findings of the study highlight the importance of educating students on the proper use of technology and the potential risks and dangers associated with online activities.

Table 5. Test of significant differences between the level of awareness of cybercrime when the respondents are grouped according to profile

Profile	P-value	X^2	Decision
Age	.000305	21.08	Significant
Sex	.00001	57.47	Significant
Grade Level	.043928	6.25	Significant
Academic Strand	.029748	17.03	Significant

Table 5 presents the test of significant difference between the level of awareness of cybercrime when they are grouped according to their profile.

It is evident that there is a significant difference in terms of the level of awareness of cybercrime when the students are grouped according to their age. When senior high school students are grouped according to their age, there can

indeed be a significant difference in their level of awareness about cybercrime. Generally, older students may have more exposure to technology and online platforms, leading to a higher level of familiarity with potential risks and threats. However, it is important to note that individual experiences, interests, and prior education can also influence their level of awareness (Neubauer et al., 2019).

For younger senior high school students, who may be new to social media and online interactions, there could be a need for more foundational education on topics such as online privacy, safe internet practices, and responsible social media use (Fox et al., 2019). These students may require more guidance in understanding the potential risks and consequences associated with their online activities.

On the other hand, older senior high school students might have had more exposure to cybercrime incidents or have witnessed the consequences of online threats (Cheng et al., 2020). They may be more aware of issues like cyberbullying, scams, and phishing attempts. However, it is still crucial to provide them with advanced knowledge on topics such as sexting, digital reputation, media literacy, and reporting cybercrime incidents.

On the other hand, it is evident that there is a significant difference in terms of the level of awareness of cybercrime when the students are grouped according to their sex.When senior high school students are grouped according to their sex, there may be differences in their level of awareness about cybercrime due to varying online experiences and socialization. Females often display a higher level of caution and privacy awareness, being more mindful of their online activities and interactions. They may have a greater understanding of the risks associated with sharing personal information and be more proactive in protecting their online privacy. Additionally, females may be more likely to seek help or support when facing cyberbullying or online harassment situations (Zhu Huang et al., 2021).

On the other hand, males might exhibit different patterns of behavior and risk perception when it comes to cybercrime. They may be more prone to engaging in risky online activities or taking part in confrontations or cyberbullying incidents. It is essential to address these tendencies and provide education that emphasizes responsible online behavior, empathy, and respectful communication to ensure a safe and inclusive digital environment for all students (Cortesi et al., 2020). By recognizing and addressing the unique challenges and needs of each gender, we can promote a comprehensive understanding of cybercrime and empower all senior high school students to protect themselves and others online.It is important to note that these differences should not be generalized to every individual, as individuals' experiences and awareness levels can vary regardless of gender. A holistic and inclusive approach to cybercrime awareness should take into account individual differences and provide education that is relevant and beneficial to all students (Mohammad et al., 2022).

It is evident that there is a significant difference in terms of the level of awareness of cybercrime when the students are grouped according to their grade level. When senior high school students are grouped according to their grade level, there can be notable differences in their level of awareness about cybercrime. Younger students in the lower grades may have less exposure and experience with the online world, requiring more foundational education on basic cybercrime awareness (Venter et al., 2019). They may need guidance on topics such as online privacy, safe internet practices, and responsible social media use. These students may be less familiar with potential risks and may benefit from targeted education to build a strong foundation of digital literacy.

In contrast, older students in the higher grades may have already developed a higher level of awareness about cybercrime due to their increased online presence and longer exposure to digital platforms. They may have encountered or witnessed various online threats, such as cyberbullying or phishing attempts. For these students, it is important to provide more advanced education on topics like identity theft, online fraud, and protecting personal information (Makkonen et al., 2019). Focusing on critical thinking, media literacy, and the long-term consequences of online actions can help them navigate the digital landscape more safely and responsibly as they approach adulthood.By recognizing the unique needs and knowledge levels of students in different grade levels, educators can tailor cybercrime awareness programs to effectively address their concerns and equip them with the necessary skills to protect themselves and make informed decisions in the digital world (Ahmad 2020).

It is evident that there is a significant difference in terms of the level of awareness of cybercrime when the students are grouped according to their academic strand. When senior high school students are grouped according to their academic strand, there can be significant differences in their level of awareness about cybercrime due to the unique focus and subject matter of each strand. For instance, students in the STEM strand may have a more advanced understanding of technology and digital systems, making them more aware of cybersecurity threats and measures. They may have a greater familiarity with concepts like coding, encryption, and network security (Chong et al., 2021). Educators can further enhance their cybercrime awareness by delving into topics such as ethical hacking, data protection, and emerging cyber threats relevant to their STEM-focused studies.

In contrast, students in the ABM strand may benefit from targeted education on cybercrime in the context of business and finance. They may be exposed to concepts such as online fraud, financial scams, and data breaches that can impact organizations and individuals. Understanding the importance of secure financial transactions, data privacy, and compliance with legal regulations related to cybersecurity can be particularly valuable for these students (Tao et al., 2019).

Similarly, students in the HUMSS strand can explore cybercrime awareness from a sociocultural and ethical perspective. They may delve into topics like cyberbullying, online harassment, digital rights, and the impact of technology on society. Educators can emphasize media literacy, responsible digital citizenship, and the ethical considerations of online behavior in their cybercrime education. By tailoring cybercrime awareness programs to each academic strand, educators can effectively engage and equip students with knowledge and skills that align with their specific interests and future career paths (Franklin et al., 2019). This approach ensures a comprehensive understanding of cybercrime, empowering students to navigate the digital world safely and responsibly regardless of their chosen academic focus (Zubala et al., 2021).

4. Conclusion and Recommendations

In the digital environment, technology plays an important role for students. These technologies provide both advantages and disadvantages. Technology led to the emergence of Cybercrime around the globe and may be a risk to every individual. Young Internet users should be made aware of the threats to their lives if they may become a victim. Based on the findings of this study, the following conclusions were arrived at (1) The profile of the Senior High School students is different from each other in many aspects. However, according to the range of their ages,

they are aware of what Cybercrime is and its possible outcomes due to their maturity level. (2) even though the Internet is rampant nowadays, they must act responsibly. (3) The result gathered from the students in the questions they had answered was a good reminder that they were interested and could relate fully to the topic.

Senior High School students are aware of what Cybercrime is and its possible outcomes due to the level of maturity they have. However, they still need to act responsibly when using the Internet to prevent themselves from being victims of Cybercrime. The students showed good interest and understanding of the topic, indicating that it is important to continue educating young internet users about the risks and threats of Cybercrime.

Overall, the study highlights the importance of cybercrime awareness among Senior High School students and the need for continuous education to help them protect themselves and stay safe in the digital environment.

In light of the conclusions made in this study, the researchers recommend the following:

To the administrators- Administrators can organize seminars or workshops to educate students on cybercrime and its potential consequences. These events can also provide students with the necessary skills and knowledge to identify and prevent cybercrime. Implement strict policies - Schools can implement strict policies on the use of the internet and social media to prevent cybercrime. These policies should include guidelines on what students can and cannot do online and the consequences of violating these rules. Encourage reporting - Administrators should encourage students to report any cybercrime incidents they encounter or witness. This will enable the school to take the necessary steps to prevent further incidents and provide support to victims. Collaborate with parents/guardians - Schools should collaborate with parents/guardians to educate students about cybercrime. This can be achieved through parent-teacher conferences, newsletters, or workshops. Regularly update and monitor security measures - Administrators should ensure that the school's security measures, such as firewalls and anti-virus software, are up-to-date and functioning properly. They should also monitor the school's network regularly to detect and prevent any cyber threats.

To the faculty- The faculty can collaborate with the school administration to include cybercrime awareness as a topic in their curriculum. This will ensure that students are well-informed about the dangers of cybercrime and how to protect themselves from being victimized. Conduct regular workshops and seminars: The faculty can organize regular workshops and seminars for students to increase their awareness and knowledge of cybercrime. Inviting experts in the field to speak on the topic can also be beneficial. Promote responsible Internet use: The faculty can also play a role in promoting responsible Internet use among students. They can remind students to be mindful of their online behavior and the content they share. Encourage students to speak up: It is important for students to know that they can speak up if they have been victimized by cybercrime. The faculty can encourage students to report any instances of cybercrime to the appropriate authorities or school personnel. Monitor students' online activities: Finally, the faculty can monitor students' online activities to ensure that they are not engaging in risky behavior that could make them vulnerable to cybercrime. This can be done through the use of monitoring software or by having regular check-ins with students.

To the parents - Educate themselves about the dangers of cybercrime and the various ways in which it can affect their children. Monitor their children's internet activities and be aware of the sites they visit and the people they

interact with online. Encourage their children to talk to them if they experience any form of cybercrime, such as cyberbullying or identity theft. Teach their children how to protect themselves online, such as by using strong passwords and avoiding sharing personal information online. Advocate for the inclusion of cybercrime awareness and prevention programs in their children's school curriculum. Set rules and guidelines for their children's internet use, such as limiting screen time and not allowing access to certain sites or apps. Seek professional help if they suspect that their child has been a victim of cybercrime or is exhibiting concerning behavior online. By implementing these recommendations, parents can help ensure the safety and well-being of their children in the digital world.

Declarations

Source of Funding

This study did not receive any grant from funding agencies in the public or not-for-profit sectors.

Competing Interests Statement

The authors have declared no competing interests.

Consent for Publication

The authors declare that they consented to the publication of this study.

References

Abuda, B.F., Rivera, K.D., & Noroña, R.V. (2020). Predictive Validity of a Cybercrime Awareness Tool: The Case of Senior High School Students in a Philippine Secondary School. Abuda, BF, Rivera, K., & Noroña, Pages 18-26. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007646 on September 26, 2022.

Adams, B. (2020). "I Didn't Feel Confident Talking About This Issue... But I Knew I Could Talk About a Book": Using Young Adult Literature to Make Sense of# MeToo. Journal of Literacy Research, 52(2): 209-230. Retrieved from: https://tinyurl.com/5n79anty on April 17, 2023.

Adinya, O.J., Ele, B.I., & Obono, I.O. (2021). The impact of emerging wireless network system and cybersecurity in a global community. Computer, 9(3).

Afaq, S.A., Husain, M.S., Bello, A., & Sadia, H. (2022). A Critical Analysis of Cyber Threats and Their Global Impact. In Computational Intelligent Security in Wireless Communications, Pages 201-220, CRC Press. Retrieved from: shorturl.at/behlZ on November 3, 2022.

Agnew, R. (2019). The rise of Social Control Theory, Fall of Classic Strain Theory, and Reconciliation between Social Control and General Strain Theories. Fifty Years of Causes of Delinquency, Pages 29-44. Retrieved from: shorturl.at/brFLU on October 8, 2022.

Alenezi, M.N., Alabdulrazzaq, H., Alshaher, A.A., & Alkharang, M.M. (2020). Evolution of malware threats and techniques: A review. International journal of communication networks and information security, 12(3): 326-337. Retrieved from: https://tinyurl.com/ywk3mj2u on April 17, 2023.

Ahmad, T. (2020). Corona virus (covid-19) pandemic and work from home:Challenges of cybercrimes and cybersecurity. Available at SSRN 3568830.

Bekkers, L., Van't Hoff-de Goede, S., Misana-terHuurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E.R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers & Security, 127: 103099.

Behl, A., Pal, A., & Tiwari, C. (2019). Analysis of effect of perceived cybercrime risk on mobile app payments. International Journal of Public Sector Performance Management, 5(3-4): 415-432.

Benaraba, C.M.D., Bulaon, N.J.B., Escosio, S.M.D., Narvaez, A.H.G., Suinan, A.N.A., & Roma, M.N. (2022). A comparative analysis on the career perceptions of Stourism management students before and during the COVID-19 pandemic. Journal of Hospitality, Leisure, Sport & Tourism Education, 30: 100361. Retrieved from: https://shorturl.at/zBGKV on April 17, 2023.

Bluhm, K. (2023). Ready, set, know: the race against cybercrime and the importance of actual knowledge. The relationship between actual and perceived knowledge of cybercrime and the Intentions to Engage in Self-Protective Behaviour to Prevent Cybercrime Victimisation (Master's thesis, University of Twente).

Bowins, B. (2022). Sliding Scale Theory of Attention and Consciousness/Unconsciousness. Behavioral Sciences, 12(2): 43. Retrieved from:https://www.mdpi.com/2076-328X/12/2/43 on November 3, 2022.

Brown, B. (2021). Atlas of the heart: Mapping meaningful connection and the language of human experience. Random House. Retrieved from: https://shorturl.at/jwUW9 on April 17, 2023.

Cheng, C., Chan, L., & Chau, C.L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108: 106311.

Climie, R.E., Park, C., Avolio, A., Mynard, J.P., Kruger, R., & Bruno, R.M. (2021). Vascular ageing in youth: a call to action. Heart, Lung and Circulation, 30(11): 1613-1626. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S1443950621011124 on November 3, 2022.

Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). Youth and digital citizenship+ (plus): Understanding skills for a digital world. Berkman Klein Center Research Publication, (2020-2).

Cuizon, M.C.A., Garcines, A.A., Villantes, G.M., Engracia, J.R.L., Allianic, E.A., & Cuevas Jr, J.F. (2022). Generating the Trends and Forecast of Crime Rates in Ozamiz City, Philippines. Retrieved from: https://tinyurl.com/5aa2bz32 on May 17, 2023.

Dada, E.G., Bassi, J.S., Chiroma, H., Adetunmbi, A.O., & Ajibuwa, O.E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. Heliyon, 5(6): e01802. Retrieved from: https://www.sciencedirect.com/science/article/pii/S2405844018353404 on September 26, 2022.

Dearden, T.E., & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. American Journal of Criminal Justice, 46(6): 935-955.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8): 1796-1808.

Deora, R.S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. Journal of Communication Engineering & Systems, 11(1): 1-6. Retrieved from: shorturl.at/DIJQS on September 26, 2022.

Dirsehan, T., & Van Zoonen, L. (2022). Smart city technologies from the perspective of technology acceptance. IET Smart Cities, 4(3): 197-210.

Fox, A.K., & Hoy, M.G. (2019). Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers. Journal of Public Policy & Marketing, 38(4): 414-432.

Gawer, A. (2022). Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age. Innovation, 24(1): 110-124. Retrieved from: shorturl.at/nOPQ9 on September 26, 2022.

Giri, S. (2019). Cyber crime, cyber threat, cyber security strategies and cyber law in Nepal. Pramana Research Journal, 9(3): 662-672. Retrieved from: https://tinyurl.com/muzkc56p on September 26, 2022.

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice, 46(6): 837-842.

Holt, T.J. (2020). Computer hacking and the hacker subculture. The palgrave handbook of international cybercrime and cyberdeviance, Pages 725-742. Retrieved from: shorturl.at/abqy3 on September 26, 2022.

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In F. Schmalleger & M. Pittari. (Eds.), Crimes of the Internet, Pages 283-301, Upper Saddle River, NJ: Prentice Hall. Retrieved from https://www.jaishankar.org/theory.html on January 04, 2023.

Jayaraman, G., Venkatachalam, V.M., Ahmed, H.M.S., & Hussien, M.A. (2022). Adoption of Online Banking Security Measures by customers–Evaluation through Extended Technology Acceptance Model (TAM) and Structural Equation Model (SEM).

Jing, A.H.Y., Ab-Rahim, R., & Ismail, F. (2019). Information and communication technology (ICT) and income inequality in ASEAN-5 countries. International Journal of Academic Research in Business and Social Sciences, 9(9): 359-373. Retrieved from: shorturl.at/bmpu4 on September 26, 2022.

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

Lee, C.D., White, G., & Dong, D. (2021). Educating for Civic Reasoning and Discourse. Executive Summary. National Academy of Education. Retrieved from: shorturl.at/drSY4 on September 26, 2022.

Lee, J.M., Kim, J., Hong, J.S., & Marsack-Topolewski, C.N. (2021). From bully victimization to aggressive behavior: Applying the problem behavior theory, theory of stress and coping, and general strain theory to explore potential pathways. Journal of interpersonal violence, 36(21-22): 10314-10337. Retrieved from: https://journals.sagepub.com/doi/abs/10.1177/0886260519884679 on October 8, 2022.

Lee, L. (2019). Cybercrime has evolved: it's time cyber security did too. Computer Fraud & Security, 2019(6): 8-11. Retrieved from:shorturl.at/ekltz on September 26, 2022.

Ma, K.W.F., & McKinnon, T. (2022). COVID-19 and cyber fraud: emerging threats during the pandemic. Journal of Financial Crime, 29(2): 433-446. Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/JFC-01-2021-0016/full/html on May 1, 2023.

Makkonen, P., Lampropoulos, G., & Siakas, K. (2019, November). Security and privacy issues and concerns about the use of social networking services. In E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, Pages 457-466, Association for the Advancement of Computing in Education.

Maesaroh, S., Permana, H.J., Febrianaga, P.D., & Pardosi, R.A. (2022). Blockchain Technology in the Future of Enterprise Security System from Cybercrime. Blockchain Frontier Technology, 2(1): 1-8.

Mijwil, M., Unogwu, O.J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. Mesopotamian journal of cybersecurity, 2023: 57-63. Retrieved from: https://shorturl.at/drxY8 on April 17, 2023.

Mundt, M., Ross, K., & Burnett, C.M. (2018). Scaling social movements through social media: The case of Black Lives Matter. Social Media+ Society, 4(4), 2056305118807911. Retrieved from: https://journals.sagepub.com/doi/full/10.1177/2056305118807911 on September 27, 2022.

Mustofa, M.B., Dwiandrini, E.L., Agustin, I, Esyarito, M.A, Anggraeni, M & Wuryan, S. (2022). Media Massa dan Cyber Crime di Era Society 5.0. At-Tanzir: JurnalIlmiah Prodi KomunikasiPenyiaran Islam, Pages 77-98.

Navarro, J.N., & Marcum, C.D. (2020). Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime. The Palgrave Handbook of Int. Cybercrime and Cyberdeviance, Pages 527-545.

Nazir, M.A., & Khan, M.R. (2022). Identification of roles and factors influencing the adoption of ICTs in the SMEs of Pakistan by using an extended Technology Acceptance Model (TAM). Innovation and Development, Pages 1-27.

Neubauer, B.E., Witkop, C.T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. Perspectives on medical education, 8: 90-97.

Odoyo, J.A., Abeka, S., & Liyala, S. (2020). Exploring a Social Learning Perspective on Computer Forensics Barriers and Factors Affecting Cybercrime Investigation in Kenya.

Pianese, T., & Belfiore, P. (2021). Exploring the social networks' use in the health-care industry: a multi-level analysis. International Journal of Environmental Research and Public Health, 18(14): 7295. Retrieved from: https://www.mdpi.com/1660-4601/18/14/7295 on September 27, 2022.

Rai, M., & Mandoria, H. (2019). A study on cyber crimes cyber criminals and major security breaches. Int. Res. J. Eng. Technol, 6(7): 1-8. Retrieved from: https://shorturl.at/gjvw2 on April 17, 2023.

Rajasekharaiah, K.M., Dule, C.S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. In IOP Conference Series: Materials Science and Engineering, 981(2): 022062.

Rianawaty, I., Dwiningrum, S.I.A., & Yanto, B.E. (2021). Model of Holistic Education-Based Boarding School: A Case Study at Senior High School. European Journal of Educational Research, 10(2): 567-580. Retrieved from :https://shorturl.at/eDEQ0 on April 17, 2023.

Shadmanfaat, S.M., Howell, C.J., Muniz, C.N., Cochran, J.K., Kabiri, S., & Fontaine, E.M. (2020). Cyberbullying perpetration: An empirical test of social learning theory in Iran. Deviant Behavior, 41(3): 278-293.

Shari, A.M.J. (2023). Knowledge, Attitude, and Practices Towards Internet Safety and Security Among Generation Z in Malaysia: A Conceptual Paper.

Sulaiman, N.S., Fauzi, M.A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, 13(9): 413.

Stives, K.L., May, D.C., Pilkinton, M., Bethel, C.L., & Eakin, D.K. (2019). Strategies to combat bullying: Parental responses to bullies, bystanders, and victims. Youth & Society, 51(3): 358-376. Retrieved from: https://shorturl.at/mpIMO on April 17, 2023.

Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G.S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. Technology in Society, 65: 101565. Retrieved from: shorturl.at/disX0 on September 27, 2022.

Tao, H., Bhuiyan, M.Z.A., Rahman, M.A., Wang, G., Wang, T., Ahmed, M.M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, 98: 660-671.

Telo, J. (2023). Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing, 6(1): 31-45.

Thakral, M., Singh, R.R., & Kalghatgi, B.V. (2022). Cybersecurity and Ethics for IoT System: A Massive Analysis. In Internet of Things, Pages 209-233, Springer, Singapore. Retrieved from: shorturl.at/AIJUZ on September 27, 2022.

Thukral, P., & Kainya, V. (2022). How social media influence crimes. Indian Journal of Law and Legal Research, 4(2): 1-11. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4107673 on April 30, 2023.

Tus, J. (2020). Self–concept, self–esteem, self–efficacy and academic performance of the senior high school students. International Journal of Research Culture Society, 4(10): 45-59. Retrieved from: https://shorturl.at/uDTZ6 on April 17, 2023.

Chong, N., Cook, B., Eidelman, J., Kallas, K., Khazem, K., Monteiro, F. R., & Tuttle, M.R. (2021). Code-level model checking in the software development workflow at Amazon web services. Software: Practice and Experience, 51(4): 772-797.

Umejiaku, N., & Uzoka, N. (2022). An overview of social media related cybercrimes and its legal remedy. Law and social justice review, 2(2). Retrieved from: https://nigerianjournalsonline.com/index.php/LASJURE/article/view/2226 on September 27, 2022.

Venter, I.M., Blignaut, R.J., Renaud, K., & Venter, M.A. (2019). Cyber security education is as essential as "the three R's". Heliyon, 5(12): e02855.

Wamsler, C. (2020). Education for sustainability: Fostering a more conscious society and transformation towards sustainability. International Journal of Sustainability in Higher Education, 21(1): 112-130. Retrieved from: https://shorturl.at/orP06 on April 17, 2023.

Wolters, F. (2022). Resilience and behavior change in cybercrime victimization: usefulness of nudges in preventing individuals to mindlessly accept third-party tracking cookies (Bachelor's thesis, University of Twente).

Wulandari, C. (2021). Internet Blocking Policy in Indonesia: Between Realities, Pros and Cons?. In ICILS 2020: Proceedings of the 3rd International Conference on Indonesian Legal Studies, ICILS 2020, July 1st 2020, Semarang, Indonesia, Page 82, European Alliance for Innovation. Retrieved from: https://tinyurl.com/2ue625v7 on April 30, 2023.

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. Frontiers in Public Health, 9: 634909.

Zubala, A., Kennell, N., & Hackett, S. (2021). Art therapy in the digital world: An integrative review of current practice and future directions. Frontiers in Psychology, 12: 595536.