Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 8, Issue 2, Pages 208-217, April-June 2024

Measuring the Level of Cybersecurity Awareness among Senior High School Students

Jared U. Dapitan[1*], John Michael M. Butchayo[2], Jun Lloyd R. Palma[3], Marinella A. Arevalo[4], Angelita B. Alvarico[5] & Jose F Cuevas Jr.[6]

[1-6]*College of Criminology, Misamis University, Philippines. Email: jareddapitan886@gmail.com*[*]

DOI: https://doi.org/10.46382/MJBAS.2024.8216

Copyright © 2024 Jared U. Dapitan et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Article Received: 06 April 2024 *Article Accepted: 14 June 2024* *Article Published: 21 June 2024*

ABSTRACT

This study aimed to assess the level of cybersecurity awareness among senior high school students at one of the educational private institutions in Ozamiz City, focusing on their profiles in terms of age, gender, grade level, and academic strand. Using random sampling, 100 students were selected to ensure a representative distribution. The study sought to determine the demographic profile of the respondents, evaluate their level of cybersecurity awareness, and investigate significant differences in awareness levels based on demographic factors. The findings revealed that the majority of respondents were 17 years old, predominantly male, and mainly in Grade 11, with varied social media usage indicating diverse online exposure. The students exhibited a "Knowledgeable" level of cybersecurity awareness, showing a consistent understanding across the population but highlighting the need for further improvement. Significant differences in cybersecurity awareness were found based on age, gender, and grade level, suggesting the necessity for tailored education programs. The study concluded that demographic diversity necessitates customized cybersecurity education to address specific needs and vulnerabilities. Effective education should combine theoretical knowledge with practical skills and critical thinking, integrated into the high school curriculum. Tailored approaches for different age groups and gender-specific strategies are recommended to ensure comprehensive and relevant cybersecurity education. These findings underscore the importance of personalized instructional strategies in enhancing students' digital safety and preparedness. Consequently, schools and policymakers should prioritize robust cybersecurity education programs that cater to diverse student demographics, fostering a higher level of cybersecurity awareness and promoting safer digital habits among senior high school students.

Keywords: Cybersecurity education; Digital literacy; Digital safety; High school curriculum; Internet safety; Cybersecurity awareness; Senior high school students; Demographic profile; Academic strand; Social media usage.

1. Introduction

1.1. Rationale of the study

In today's digital world, cybersecurity is like a shield that protects computers and information from many different types of online dangers (George et al., 2023). Cybersecurity is super important because there are more and more online threats these days, and it helps keep digital lives and important systems safe (Choithani et al., 2022). As technology keeps growing, cybersecurity has to keep changing and getting better to stay ahead of the bad guys. And since people are all so connected online, cybersecurity is not just about personal stuff; it is also about making sure businesses, governments, and society can work smoothly and safely (Asaad & Saeed, 2022).

The importance of addressing cybersecurity in the modern digital age cannot be overstated. As the reliance on digital technology grows, it becomes more important than ever to address cybersecurity issues in order to protect not only the personal data but also the stability of the linked world (Michael et al., 2019). An incomplete approach to cybersecurity can have disastrous repercussions, including monetary losses, reputational harm, and even the compromise of vital services and national security. The multinational dimension of cyber threats emphasizes how crucial international cooperation is to successfully tackling cybersecurity concerns and reducing their global impact.

Preventing cybercrime means working together to keep people, organizations, and computer systems safe from online dangers. To do this, people need to keep learning and team up with others who care about cybersecurity. People use the latest technology and keep updating the security to stay ahead of cybersecurity bad guys. The key to

beating them is being able to change and adopt just like they do (Khadim et al., 2022). Furthermore, fostering a culture of cyber awareness and educating individuals about online threats is crucial in building a resilient defense against cybercriminals, and promoting cyber hygiene practices should be a top priority for all.

Knowing about cybersecurity is important to keep people, businesses, and the whole society safe from all the different online dangers. When people understand how to be safe online, it makes businesses stronger, gives power to individuals, and helps the whole society stay strong against online threats (Muneer et al., 2023). When everyone knows about cybersecurity, it is like having a big shield that defends the society from cyberattacks that keep changing. This makes the digital world safer for everyone and helps protect important information, important systems, and personal privacy in the connected world (Althibyani & Al-Zahrani, 2023). To remain ahead of cyber threats and unite everyone in the fight against them, collaboration across borders and information sharing are also essential.

Therefore, conducting study at one of the universities in Ozamiz City to gauge senior high school students' understanding of cybersecurity would not only close the broad research gap but also offer a localized perspective on the issue. Keeping in mind that different places and educational institutions may have different cybersecurity environments, this study will make an effort to explore topics relevant to the institution. Most of the time, focusing the research on a single academic context will enable an in-depth understanding of the cybersecurity awareness of senior high school students by allowing the exploration of the many advantages and problems that they encounter in this particular academic setting. The results can then be utilized to guide the development of customized educational interventions at the institution and serve as a model for the kind of intervention that could benefit other comparable institutions, thereby advancing cyber security education in the region.

1.2. Objectives of the Study

The study aimed to achieve the following:

(i) Assessment of Cybersecurity Awareness: To identify the stage of understanding by the chosen senior high school learners on cybersecurity. (ii) Impact of Demographic Factors: To establish the significant difference between demographic factors of age, gender, grade level, and academic strand when understanding cybersecurity. (iii) Correlation with Online Behavior: To determine how to show the correlation between students' usage of social media and security awareness of cybersecurity. (iv) Knowledge Gaps: To identify exactly what students, misunderstand or fail to understand about cybersecurity. (v) Recommendations for Education Programs: To make recommendations for designing and implementing such tailored programs in cybersecurity education, as are likely to address specific needs and vulnerabilities of various demographic groups.

2. Methods

This study utilized the descriptive survey research design. This research design was used to collect data on the current state of cybersecurity awareness among senior high school students. It is a quantitative research design that uses surveys to collect data from a sample of participants. The data collected from this descriptive survey research study is used to describe the characteristics of the population, identify trends, and make comparisons between

different groups. This research design is appropriate for assessing the level of awareness of senior high school students on cybersecurity because it allows for the collection of data from a large sample of students, which is necessary for a true representation of the population, and it provides a quantifiable assessment of cybersecurity awareness to identify areas that need more instruction.

This study was conducted in one of the universities in Ozamiz City. Ozamiz City, in the Philippines' Misamis Occidental region, offers an intriguing setting for a range of research projects because of its distinctive combination of natural, cultural, and economic features. Ozamiz, a port city in Northwestern Mindanao that faces Panguil Bay, is strategically important to the area's transportation and commercial networks. The city is known for its tropical weather, which has distinct wet and dry seasons that affect both urban growth and agricultural methods.

In this research study, one hundred (100) respondents from the senior high school were chosen by the researchers from one of the Universities in Ozamiz City. Understanding the mechanics of cybersecurity awareness within this specific educational context required their views and opinions on a variety of topics. Their involvement greatly enhanced the scope and applicability of the findings. These participants were conveniently and purposively chosen by the researchers.

3. Results and Discussions

The profile of respondents at Misamis University shows that most of the senior high school students are 17 years old, followed by 18 years at 31%, 16-year-olds at 19%, and those aged 19 years at 3%. There are more male respondents to the survey at 56% than females at 44%, which could skew the outcomes for gender-specific cybersecurity awareness differences. Most of the students are in Grade 11, numbering 63%, compared to Grade 12 students who form 37%. Hence the study shall be biased to the lower grade level of senior high. Thirty-seven percent of the sample has one social media account, 42% have two, and 21% have three, showing varied online presence. From such profiles, customization of the cybersecurity awareness programs to various levels of online activity and the concomitant practical measures contingent upon social media engagement may be perceived. Customization needs arise to address gender and grade level differences so that educators and policymakers can plan more appropriately concerning promoting digital safety and creating a culture of digital responsibility.

On average, senior high school students at Misamis University exhibit moderate to high knowledge of cybersecurity, as most items scored between 3.0 and 3.5, showing solid expertise of cybercrime, antivirus software, password protection, and online safety. Further support that their cybersecurity awareness is only moderate to high is the degree of their understanding of the differing access rights of various devices during downloads. However, there is an improvement margin, especially on the ability to discuss cybersecurity issues with friends and family, which had a mean average score of 2.96. One research study found that most students were unaware of cyber threats because their parents did not have the guidance or resources for it. The work framework the researcher uses has four steps between areas of the gaps: threat identification, current awareness assessment, forming an awareness approach, and efficacy assessment. More creative ways, such as using cybersecurity emojis, can enhance cybersecurity awareness among high school students.

These results indicate that high school students rank in the category of "Knowledgeable" when considering levels of cybersecurity awareness, based on a mean score of 3.21 with a standard deviation of 0.25. Consistency is needed at this level of grasp toward higher levels of awareness. In today's world, good knowledge of cybersecurity should be improved through holistic education and training. Research suggests that digital safety concepts should be introduced early and reinforced at intervals for an effective learning process. When students receive interactive, scenario-based cybersecurity education in high school, they significantly improve their digital habits and behaviors. The intense commitment to a robust educational program around cybersecurity will instill the ability in students to transit the digital world securely and safely, hence providing a better environment in our digital space.

The chi-square obtained for age (29.50), gender (34.04), and harmonized level in school (44.16) is significantly higher than the critical threshold, with highly significant p-values in all cases less than 0.00005; demographic factors affect cybersecurity awareness. Thus, the null hypothesis was rejected. These findings emphasize that age, gender, and grade level must be considered when designing educational programs in the area of cybersecurity. This necessitates tailored approaches, whereby younger students require foundational content and older students need advanced topics, in addition to gender-specific strategies to ensure that relevant education is provided to all. Research supports the fact that age and grade level affect awareness; hence, older students require a more sophisticated understanding. In addition, gender differences will dictate different guiding educational interventions for appropriate learning.

Table 1. Frequency and Percentage Distribution of Respondents According to their Profile

Profile		**Frequency**	**Percentage**
Age			
	16 years old	19	19.00
	17 years old	47	47.00
	18 years old	31	31.00
	19 years old	3	3.00
Gender			
	Male		
	Female	56	56.00
Grade		44	44.00
	Grade 11		
	Grade 12	63	63.00
		37	37.00
Number of Gadget			
	1	37	37.00
	2	42	42.00

3	21	21.00
Number of Social Media Account		
1	27	27.00
2	13	13.00
3	31	31.00
4	13	13.00
5	7	7.00
6	9	9.00

Table 1 presents the respondents' profile of senior high school students that most of them are 17, with 31% at 18 years, 19% at 16 years, and 3% at 19 years. The survey has more male respondents than females, with 56% and 44%, respectively, which may distort the results meant to show the difference in cybersecurity awareness between the sexes. Most pupils are in grade 11, which is 63%, and the rest 37% are in grade 12. Hence, the research will not be an accurate representation because its results and scope shall be based on a junior-level grade of the senior high section. Has one social media account, 42% have two, 21% have three, depicting a diverse online presence

Table 2. Frequency and Percentage Distribution of Respondents According to their Profile

Level of Cybersecurity Awareness among Senior High School Students Responses

Constructs	**M**	**SD**	**Remarks**
Cybersecurity Awareness	3.21	.25	Knowledgeable

Scale: 4.20-5.0 (Very Knowledgeable); 3.40-4.19 (Somewhat Knowledgeable); 2.60-3.39 (Knowledgeable) 1.80-2.59 (Less Knowledgeable); 1.0-1.79 (Not Knowledgeable).

Table 2 shows senior high school students' awareness of cybersecurity based on how they answered different questions. The table asks about knowledge of antiviral software, awareness of password protection, comprehension of internet safety, and familiarity with cybercrime, among other related subjects. To ascertain the students' overall degree of cybersecurity knowledge, a scale was used to score each question, and the average weighted results were computed. Students' knowledge of cybersecurity is indicated by the overall weighted mean.

Senior high school students have a moderate to high level of cybersecurity knowledge, according to Table 2 data. Students are usually informed or very knowledgeable about many elements of cybersecurity, as indicated by the average weighted values for most questions falling between 3.0 and 3.5. Given that they show a solid grasp of important ideas like cybercrime, antivirus software, password protection, and online safety, it appears that attempts to educate pupils about cybersecurity issues have been fairly successful. Additionally, Table 6 shows that senior high school students have a moderate to high level of awareness regarding cybersecurity. The average weighted value for the entire sample indicates that pupils have some level of cybersecurity expertise. Understanding the security of allowing device access rights during file/app downloads had the highest average weighted value (3.95),

demonstrating a high level of awareness in this area. Conversely, talking with friends or family about cybersecurity issues had the lowest average weighted value (2.96), indicating that these conversations should be given less importance. These results are corroborated by the literature, which suggests that in order to raise awareness and encourage students to use safe online practices, there should be more candid conversations about cybersecurity.

The results indicate that the level of cybersecurity awareness among senior high school students falls into the "Knowledgeable" category, with a mean score (M) of 3.21 and a standard deviation (SD) of 0.25. This suggests that while students have a reasonable understanding of cybersecurity concepts, there is still room for improvement to elevate their awareness to a higher level. The relatively low standard deviation indicates a consistent level of knowledge across the student population, implying that most students share a similar understanding of cybersecurity issues. Given the scale, where a score between 2.60 and 3.39 is classified as "Knowledgeable," it is evident that the students' awareness is not as high as it could be, especially considering the increasing importance of cybersecurity in today's digital age. Efforts to enhance this knowledge could focus on more comprehensive education and training programs tailored to high school students (Sanusi et al., 2022; Alam & Mohanty., 2023). Such initiatives could bridge the gap between their current level of awareness and the "Somewhat Knowledgeable" or "Very Knowledgeable" categories.

The findings suggest that while senior high school students have a foundational understanding of cybersecurity, there is a significant opportunity to deepen their knowledge. Schools and educators should prioritize the incorporation of more robust cybersecurity education into their curricula. By doing so, they can equip students with the necessary skills to navigate the digital world safely and responsibly. Moreover, fostering a higher level of cybersecurity awareness at this educational stage can contribute to a more secure digital environment in the broader community, as these students become more vigilant and proactive digital citizens (Al Daajeh et al., 2022; Sharma & Thapa., 2023).

Table 3. Significant difference on the level of awareness of the senior high school students towards cybersecurity when they are grouped according to their profile

Variables	**Chi-square value**	***p* value**	**Decision**
Conflict Management Strategy			
Age	29.50	0.00005	Reject Ho
Gender	34.04	0.00001	Reject Ho
Grade Level	44.16	0.00001	Reject Ho

Ho: There is no difference on the level of awareness of the senior high school students towards cybersecurity when they are grouped according to their profile.

*Note: Probability Value Scale: **p<0.01 (Highly Significant); *p<0.05 (Significant); p>0.05 (Not significant).*

The analysis of Table 3 reveals significant differences in the level of cybersecurity awareness among senior high school students when grouped according to their profile variables. The chi-square values for age (29.50), gender (34.04), and grade level (44.16) all exceed the critical threshold, and the corresponding p-values (0.00005, 0.00001, and 0.00001, respectively) indicate highly significant differences. Consequently, the null hypothesis (Ho) stating that there is no difference in cybersecurity awareness among students based on their profiles is rejected. This suggests that demographic factors such as age, gender, and grade level significantly influence students' cybersecurity awareness.

These findings underscore the importance of considering demographic variables when designing and implementing cybersecurity education programs. The significant differences suggest that tailored approaches might be necessary to address the specific needs and knowledge gaps of different student groups. For instance, younger students might benefit from more foundational and introductory content, while older students could be engaged with more advanced topics. Similarly, gender-specific strategies might be required to ensure that both male and female students receive adequate and relevant cybersecurity education (Bromall et al., 2023; McGill & Thompson., 2021). Research in the field of cybersecurity education often emphasizes the impact of demographic variables on awareness and knowledge levels. Age is a critical factor, as younger students generally have less exposure to complex digital environments compared to their older counterparts. As students' progress through grade levels, their interaction with technology and the internet increases, necessitating a more sophisticated understanding of cybersecurity threats and best practices. Studies also indicate that tailored educational strategies that evolve with students' cognitive and experiential development can significantly enhance their cybersecurity awareness (Shearer et al., 2020; Familoni & Onyebuchi., 2024).

Gender differences in cybersecurity awareness have also been widely documented. Males and females often exhibit different online behaviors and attitudes towards technology, which can influence their understanding and engagement with cybersecurity concepts. Educational interventions that acknowledge and address these differences are more likely to be effective (Webb Hooper et al., 2021). For instance, integrating examples and scenarios that resonate with both genders can help in making the learning process more inclusive and impactful. The significant differences in cybersecurity awareness based on age, gender, and grade level highlight the need for differentiated instructional strategies in cybersecurity education. Educators and policymakers should consider these demographic factors when developing curricula and educational resources. By adopting a more personalized approach, schools can ensure that all students, regardless of their demographic profile, receive the appropriate level of cybersecurity education. This not only helps in closing the awareness gaps but also promotes a more comprehensive understanding of digital security across the student population. Ultimately, such targeted educational efforts can contribute to building a more digitally secure and aware generation (Manoharan & Sarker., 2023; Brunetti et al., 2020).

4. Conclusions

The results of the study show that massive differences exist within the cybersecurity awareness level of senior high school students under demographic characteristics. However, the chi-square values for age (29.50), gender

(34.04), and grade level (44.16) easily surpass thresholds, whereby highly significant differences are interpreted by corresponding p-values. This serves as evidence that demographic factors are one of those variables that influence the level of cybersecurity awareness of the students. For example, based on the proportional data given, this stands as 47 percent for the 17-year-old respondents, followed by 31 percent for the 18-year-olds, 19 percent for the 16-year-olds, and a minimal 3 percent for the 19-year-olds — statistics that keep in line with the usual trend in the mention of senior high school students. Furthermore, gender distribution reflects slight male dominance, with males constituting 56% and females 44% of all respondents, which might affect the general findings regarding gender-specific cybersecurity practices. An additional fact that strikes a disparity in the grade levels is that 63% are in Grade 11, while 37% are in Grade 12. This distribution puts emphasis on the students within Grade 11 and likely holds more relevance for Grade 11 students' cybersecurity awareness and behaviors than it does for Grade 12 students. Moreover, questions on the number of accounts in social media showed that 37% have one account on a social network, 42% have two, and 21% have three, reflecting high variability for the specific factor within the students' digital footprints. This could influence risks related to potential susceptibility to cybersecurity threats. Generally, these results highlight the need to consider demographic variables in designing cybersecurity education programs to address diverse needs and knowledge gaps.

In conclusion, the significant differences in cyber-security awareness based on age, gender, and grade level underline the importance of tailored instructional strategies in teaching cyber-security. Such variations in the students' demographics have to be taken into account and provisions made to ensure that educational initiatives capture backgrounds and experiences. Such personalized approaches would not only bridge awareness gaps but enable a deeper understanding of digital security across student populations—a contribution to a safer, more informed generation well on its way toward confidently managing the complexities of the digital landscape.

5. Recommendations

Personalized strategies need to be developed in the study to recommend cybersecurity education programs for senior high school students, considering substantial age, sex, and grade-level differences in awareness. Attention should be given to issues of specific concern and knowledge gaps related to other variables, such as digital exposure and social media use. This should primarily target the Grade 11 level and include inclusive and targeted interventions to address awareness gaps to better understand digital security issues.

Declarations

Source of Funding

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

Competing Interests Statement

The authors declare no competing financial, professional, or personal interests.

Consent for publication

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

Authors' contributions

All the authors took part in literature review, analysis and manuscript writing equally.

References

[1] Alam, A., & Mohanty, A. (2023). Cultural beliefs and equity in educational institutions: exploring the social and philosophical notions of ability groupings in teaching and learning of mathematics. International Journal of Adolescence and Youth, 28(1): 2270662.

[2] Al Daajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.K.R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119: 102754.

[3] 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.

[4] Asaad, R.R., & Saeed, V.A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. Applied computing Journal, Pages 227–244.

[5] Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, crypto currency and banking system. Annals of Data Science, 11(1): 103–135.

[6] Bromall, N., Slonka, K., Draus, P., & Mishra, S. (2023). Factors and experiences that prepare students for a cyber career: a gender-based study. Issues in Information Systems, 24(1).

[7] Brunetti, F., Matt, D.T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. The TQM Journal, 32(4): 697–724.

[8] Familoni, B.T., & Onyebuchi, N.C. (2024). Augmented and virtual reality in us education: a review: analyzing the impact, effectiveness, and future prospects of ar/vr tools in enhancing learning experiences. International Journal of Applied Research in Social Sciences, 6(4): 642–663.

[9] George, A.S., George, A.H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4): 155–172.

[10] 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): 50–68.

[11] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. International Research Journal of Modernization in Engineering Technology and Science.

[12] Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In 2019 IEEE International Symposium on Technology and Society (ISTAS), Pages 1–13, IEEE.

[13] Muneer, S.M., Alvi, M.B., & Farrakh, A. (2023). Cyber Security event detection using machine learning technique. International Journal of Computational and Innovative Sciences, 2(2): 42–46.

[14] Sanusi, I.T., Oyelere, S.S., & Omidiora, J.O. (2022). Exploring teachers' preconceptions of teaching machine learning in high school: A preliminary insight from Africa. Computers and Education Open, 3: 100072.

[15] Sharma, R., & Thapa, S. (2023). Cybersecurity awareness, education, and behavioral change: strategies for promoting secure online practices among end users. Eigenpub Review of Science and Technology, 7(1): 224–238.

[16] Shearer, R.L., Aldemir, T., Hitchcock, J., Resig, J., Driver, J., & Kohler, M. (2020). What students want: A vision of a future online learning experience grounded in distance education theory. American Journal of Distance Education, 34(1): 36–52.

[17] Webb Hooper, M., Nápoles, A.M., & Pérez-Stable, E.J. (2021). No populations left behind: vaccine hesitancy and equitable diffusion of effective COVID-19 vaccines. Journal of General Internal Medicine, 36(7): 2130–2133.