

Cybersecurity Awareness and Online Risk Exposure Among Senior High School Students: Implications for a School-Based Digital Safety Protection Program

Annie May L. Abrera^{1*}; Loida A. Cailipan²; Isamie P. Javarez³; Gener Nepomuceno⁴; Elmer L. Tapaya⁵; Angelyn Q. Tabianan⁶

^{1,2,3,4,5,6} University of Perpetual Help System Laguna, Philippines

Corresponding Author: Annie May L. Abrera^{*}

Publication Date: 2026/08/05

Abstract: The increasing use of digital technologies among adolescents has heightened their exposure to various online risks, underscoring the importance of cybersecurity awareness and school-based digital safety initiatives. This study examined the relationship between cybersecurity awareness and online risk exposure among senior high school students in Laguna, Philippines, as a basis for developing a School-Based Digital Safety Protection Program. A descriptive-correlational research design was employed involving 249 senior high school students selected through convenience sampling. Data were collected using a validated researcher-developed questionnaire measuring digital engagement, awareness of online risks, exposure to cyber threats, and perceived effectiveness of school-based digital safety measures. Descriptive statistics and Spearman's rho correlation analysis were used to analyze the data. The findings revealed high digital engagement ($M = 3.12$), very high awareness of online risks ($M = 3.38$), high exposure to cyber threats ($M = 2.57$), and effective school-based digital safety measures ($M = 2.85$). A strong positive and statistically significant relationship was found between digital engagement and awareness of online risks ($r_s = .743, p < .001$), while a very weak but statistically significant relationship was observed between awareness of online risks and exposure to cyber threats ($r_s = .134, p = .034$). The findings indicate that although increased digital engagement enhances cybersecurity awareness, awareness alone is insufficient to reduce online risk exposure, highlighting the need for school-based digital safety programs that strengthen practical cybersecurity skills and responsible online behavior.

Keywords: Cybersecurity Awareness; Digital Engagement; Online Risk Exposure; Cyber threats; Digital Safety Protection Program.

How to Cite: Annie May L. Abrera; Loida A. Cailipan; Isamie P. Javarez; Gener Nepomuceno; Elmer L. Tapaya; Angelyn Q. Tabianan (2026) Cybersecurity Awareness and Online Risk Exposure Among Senior High School Students: Implications for a School-Based Digital Safety Protection Program. *International Journal of Innovative Science and Research Technology*, 11(7), 2973-2980. <https://doi.org/10.38124/ijisrt/26jul1436>

I. INTRODUCTION

The rapid expansion of digital technologies has transformed education by enabling students to access information, communicate, and participate in learning through various online platforms. Increased digital engagement has broadened educational opportunities and improved access to diverse learning resources. However, greater online participation has also increased adolescents' exposure to cybersecurity threats such as phishing, identity theft, malware, cyberbullying, privacy breaches, misinformation, and online

scams (Quayyum et al., 2021; Moreno et al., 2021; Smahel et al., 2022). As students spend more time in digital environments, the need to strengthen their ability to recognize and respond to cyber risks has become increasingly important (Livingstone & Stoilova, 2021; Trinidad et al., 2025).

Cybersecurity awareness is recognized as an essential component of responsible digital citizenship. It encompasses knowledge of cyber threats, understanding of safe online practices, and the ability to make informed decisions when using digital technologies. Previous studies have shown that

students with higher cybersecurity awareness are more likely to protect personal information, recognize suspicious online activities, use privacy settings effectively, and critically evaluate online content (Antunes et al., 2021; Zhuo et al., 2021). Nevertheless, research also indicates that awareness does not always translate into safe online behavior, as many adolescents continue to engage in risky digital practices despite understanding potential consequences (Machimbarrena et al., 2022; Marciano et al., 2023). This suggests that effective cybersecurity education should emphasize not only knowledge acquisition but also the development of practical digital safety skills and responsible online behavior.

Educational institutions play a crucial role in equipping learners with the competencies needed to navigate increasingly complex digital environments. While digital technologies have become integral to teaching and learning, cybersecurity education remains inconsistently integrated into many school curricula (Antunes et al., 2021; Vandoninck et al., 2022). Existing school-based initiatives have demonstrated positive effects in improving students' awareness of online safety, cyberbullying prevention, and coping strategies (Yurdakul & Ayhan, 2022; Wisniewski et al., 2024). However, the implementation of these initiatives varies considerably across educational settings, leaving many students insufficiently prepared to address emerging cyber threats.

In the Philippines, the rapid adoption of digital technologies in secondary education has accelerated the use of online learning platforms, social media, and internet-based communication among students. Although these technologies have enhanced learning opportunities, they have also heightened concerns regarding cyberbullying, online scams, privacy violations, misinformation, and other forms of online victimization. Reports of increasing cyber-related incidents involving Filipino youth underscore the importance of strengthening cybersecurity education and establishing school-based programs that promote responsible digital behavior and student protection. As schools continue integrating technology into instruction, understanding students' cybersecurity awareness and exposure to online risks has become increasingly important for developing evidence-based educational interventions.

Despite the growing body of literature on adolescent cybersecurity, limited studies have simultaneously examined digital engagement, cybersecurity awareness, and online risk exposure among senior high school students while using empirical findings to inform the development of school-based digital safety interventions (Quayyum et al., 2021; Lui et al., 2025). This research gap is particularly evident in the Philippine context, where empirical evidence remains limited despite the increasing reliance on digital technologies in education. Addressing this gap is essential for providing educators and policymakers with evidence that can guide the design of comprehensive digital safety programs tailored to the needs of Filipino learners.

Accordingly, this study examined the cybersecurity awareness and online risk exposure among senior high school students as a basis for developing a School-Based Digital Safety Protection Program. Specifically, it assessed students'

levels of digital engagement, awareness of online risks, and exposure to cyber threats; examined the relationships between digital engagement and cybersecurity awareness, and between cybersecurity awareness and online risk exposure; and identified implications of the findings for the development of a school-based digital safety protection program. The study contributes to the growing body of knowledge on adolescent cybersecurity and provides empirical evidence to support educational interventions that strengthen digital resilience, responsible online behavior, and student safety in technology-enhanced learning environments.

II. THEORETICAL FRAMEWORK

This study is primarily grounded in Digital Literacy Theory, which posits that effective participation in digital environments requires individuals to possess a range of technical, cognitive, and critical competencies that enable them to access, evaluate, and utilize digital information responsibly. Beyond functional technology use, digital literacy encompasses the ability to recognize online risks, protect personal information, and engage in safe and ethical digital practices. Within the context of the present study, digital engagement represents students' participation in and interaction with digital technologies, while cybersecurity awareness reflects an essential dimension of digital literacy that facilitates the recognition and management of online threats. Consistent with the assumptions of Digital Literacy Theory, greater engagement in digital environments is expected to contribute to higher levels of cybersecurity awareness among senior high school students.

The study is further informed by Social Cognitive Theory (Bandura, 1986), which emphasizes that learning and behavior are shaped through the dynamic interaction of personal factors, environmental influences, and experiential processes. According to this perspective, individuals acquire knowledge and develop behavioral competencies through observation, social interaction, and direct experience. In digital contexts, students' engagement with online platforms exposes them to diverse sources of information, social influences, and technological experiences that contribute to the development of cybersecurity-related knowledge and awareness. Consequently, Social Cognitive Theory provides supporting justification for the proposed relationship between digital engagement and cybersecurity awareness.

To further explain the relationship between cybersecurity awareness and online risk exposure, the study draws on selected principles of Protection Motivation Theory (Rogers, 1975). The theory posits that individuals are more likely to adopt protective behaviors when they perceive a threat to be significant and believe that effective coping responses are available and within their capability to perform. Applied to cybersecurity contexts, heightened awareness of cyber threats and preventive measures may encourage students to engage in safer online practices, thereby reducing their vulnerability to online risks. Accordingly, Protection Motivation Theory provides supplementary theoretical support for the proposition that cybersecurity awareness influences the degree of online risk exposure experienced by students.

These theoretical perspectives provide a coherent foundation for examining the relationships among digital engagement, cybersecurity awareness, and online risk exposure. Specifically, the framework proposes that digital engagement contributes to the development of cybersecurity awareness, which subsequently influences students' exposure to online risks. This theoretical foundation guides the investigation of the mechanisms through which digital experiences and cybersecurity knowledge shape students' online safety outcomes.

III. CONCEPTUAL FRAMEWORK

The conceptual framework of the study posits that digital engagement influences students' awareness of online risks, which in turn affects their exposure to cyber threats. Digital engagement refers to students' participation in online activities, while awareness of online risks pertains to their knowledge and understanding of cybersecurity threats and safe online practices. Exposure to cyber threats refers to students' encounters with risks such as phishing, cyberbullying, privacy breaches, identity theft, and online scams.

The framework assumes that greater digital engagement increases students' awareness of online risks. Increased awareness may help students adopt safer online behaviors and reduce vulnerability to cyber threats. The findings on digital engagement, awareness of online risks, and exposure to cyber threats serve as the basis for developing a School-Based Digital Safety Protection Program aimed at strengthening students' cybersecurity competencies and promoting responsible online behavior.

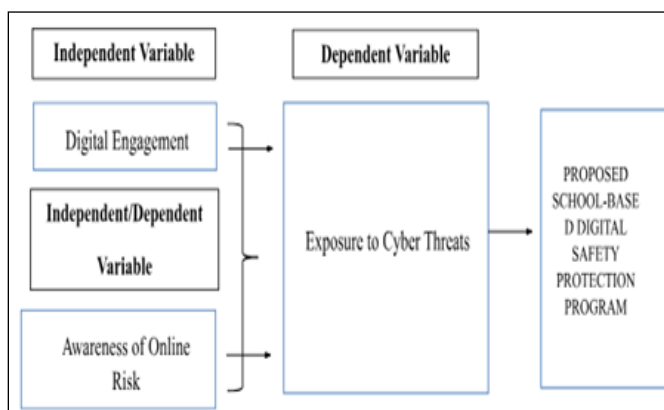


Fig 1 Conceptual Framework of the Study

IV. METHODOLOGY

This study employed a descriptive-correlational research design to examine cybersecurity awareness and online risk exposure among 249 senior high school students in Laguna, Philippines, as the basis for a School-Based Protection Program. It specifically assessed digital engagement, awareness of online risks, exposure to cyber threats, and perceived effectiveness of school-based digital safety measures, as well as the relationships among these variables. Respondents were selected through convenience sampling, with inclusion limited to currently enrolled senior high school students who are active users of digital technologies; incomplete responses were excluded.

Data were gathered using a researcher-developed structured questionnaire based on relevant literature, consisting of four sections measured on a 4-point Likert scale. Content validity was ensured through expert review, while reliability testing yielded Cronbach's alpha coefficients of .89 (Digital Engagement), .91 (Online Risk Awareness), .87 (Cyber Threat Exposure), and .90 (School-Based Digital Safety Measures), indicating good to excellent reliability. Ethical procedures were observed through voluntary participation, informed consent, and strict confidentiality, with no identifying information collected.

Data were analyzed using descriptive statistics (weighted mean and standard deviation) and inferential statistics using Spearman rho correlation to determine relationships among variables at a 0.05 level of significance.

V. RESULTS

This section presents the key findings of the study entitled "Cybersecurity Awareness and Online Risk Exposure among Senior High School Students: Basis for a School-Based Protection Program". It discusses the respondents' level of digital engagement, level of awareness of online risks, level of exposure to cyber threats, and perceived effectiveness of school-based digital safety measures among senior high school students. The study also explores the variations in students' digital engagement, awareness of online risks, exposure to cyber threats, and perceived effectiveness of school-based digital safety measures. Furthermore, the analysis examines the relationships among these variables to determine how digital engagement, awareness of online risks, exposure to cyber threats, and perceptions of school-based digital safety measures are associated with one another in understanding students' digital experiences and online safety practices.

Table 1 Respondents' Level of Digital Engagement

Indicators	Weighted Mean	Standard Deviation	Interpretation
1. I use the internet for academic purposes (research, assignments).	3.40	.888	Very High
2. I spend more than 3 hours per day online.	3.23	1.000	High
3. I actively use social media platforms (e.g., Facebook, TikTok, Instagram).	3.21	.903	High
4. I participate in online learning platforms and digital classrooms regularly.	2.90	.915	High

5. I engage in online gaming or entertainment activities frequently.	2.68	.995	High
6. I use digital tools to communicate with classmates and teachers.	3.38	.935	Very High
7. I enjoy learning new digital tools, apps, or platforms.	3.10	.954	High
8. I feel that being online is an important part of my daily routine.	2.93	.931	High
9. I can easily adapt to new technologies or digital platforms.	3.06	.865	High
10. I use the internet to learn skills or topics beyond my classroom lessons.	3.31	.836	Very High
Average Weighted Mean	3.12	.675	High

Table 1 presents the respondents' level of digital engagement. Findings revealed that the highest-rated indicators were the use of the internet for academic purposes ($M = 3.40$), communication with classmates and teachers ($M = 3.38$), and learning skills beyond classroom lessons ($M = 3.31$). These results suggest that students primarily utilize digital platforms as tools for learning, collaboration, and self-development rather than solely for entertainment. The prominence of educational and communication-related activities reflects the increasing role of technology in supporting flexible and student-centered learning environments.

On the other hand, online gaming and entertainment obtained the lowest mean score ($M = 2.68$), although it

remained within the high category. This indicates that recreational use, while common, is less dominant than academic and productivity-oriented digital engagement.

Overall, students demonstrated a high level of digital engagement ($M = 3.12$, $SD = 0.68$), indicating that digital technologies are deeply embedded in their daily academic and social activities. This finding is consistent with Lui et al. (2025), who emphasized that adolescents' active participation in digital environments contributes to greater exposure to digital learning opportunities and cybersecurity-related experiences.

Table 2 Respondents' Level of Awareness of Online Risk

Indicators	Weighted Mean	Standard Deviation	Interpretation
1. I am aware of the risks of sharing personal information online.	3.54	.879	Very High
2. I know how to identify phishing emails or suspicious messages.	3.15	.969	High
3. I understand the dangers of communicating with strangers online.	3.44	.873	Very High
4. I am familiar with privacy settings on social media.	3.36	.889	Very High
5. I know how to report harmful or inappropriate online content.	3.27	.936	Very High
6. I understand what cyberbullying is and its effects.	3.55	.953	Very High
7. I am aware of common online scams..	3.60	.822	Very High
8. I know how to secure my passwords and accounts	3.33	.974	Very High
9. I verify information before sharing it online	3.44	.879	Very High
10. I understand the concept of digital footprint.	3.16	1.043	High
Average Weighted Mean	3.38	.799	Very High

Table 2 shows that respondents demonstrated a very high level of awareness of online risks ($M = 3.38$, $SD = 0.80$). The highest-rated indicators were recognizing online scams ($M = 3.60$), understanding cyberbullying ($M = 3.55$), and identifying risks in sharing personal information online ($M = 3.54$), indicating strong awareness of commonly encountered online threats in social media and digital communication contexts.

Lower but still high ratings were observed in identifying phishing messages ($M = 3.15$) and understanding digital footprints ($M = 3.16$), suggesting comparatively weaker awareness in more advanced cybersecurity concepts that

require critical evaluation and long-term understanding of online behavior.

Taken together, the results indicate that students possess strong foundational cybersecurity awareness but require further development in advanced areas such as phishing detection and digital footprint management. These findings support Marciano et al. (2023), who reported that while adolescents generally demonstrate awareness of common online risks, gaps remain in higher-level digital media literacy and cyber risk prevention competencies.

Table 3 Respondents Level of Exposure to Cyber Threats

Indicators	Weighted Mean	Standard Deviation	Interpretation
1. I have experienced cyberbullying or online harassment.	2.40	1.081	Low
2. I have received suspicious or phishing messages.	2.69	1.071	High
3. I have accidentally shared personal information publicly.	2.13	1.006	Low
4. I have encountered fake or misleading information online.	2.99	1.023	High
5. My online account has been hacked or compromised.	2.22	1.190	Low
6. I have witnessed others being harassed online.	2.98	.983	High
7. I feel unsafe when using some online platforms.	2.66	.887	High
8. I have encountered online scams.	2.72	1.135	High
9 I have interacted with strangers who made me uncomfortable.	2.70	.962	High
10. I have experienced unauthorized access to my accounts.	2.18	1.059	Low
Average Weighted Mean	2.57	.618	High

As shown in Table 3, respondents reported a high level of exposure to cyber threats ($M = 2.57$, $SD = 0.62$), indicating that while direct victimization is relatively limited, students frequently encounter various forms of online risk.

The most common exposures were fake or misleading information ($M = 2.99$), online harassment ($M = 2.98$), and online scams ($M = 2.72$), suggesting that misinformation and unsafe online interactions are among the most prevalent cyber threats experienced by senior high school students. In contrast, lower exposure was reported for compromised accounts ($M = 2.22$), unauthorized access ($M = 2.18$), and accidental

disclosure of personal information ($M = 2.13$), indicating that students are less frequently affected by direct or technical forms of cyberattacks.

These findings are consistent with Machimbarrena et al. (2022), who found that adolescents commonly experience cybervictimization, misinformation, and risky online interactions, even when severe forms of cyber incidents occur less frequently. Similarly, Trinidad et al. (2025) reported that adolescents continue to encounter negative online experiences despite increased awareness of online risks.

Table 4 Perceived Level of Effectiveness of School-Based Digital Safety Measures

Indicators	Weighted Mean	Standard Deviation	Interpretation
1. My school provides enough information about online safety.	2.97	.908	High
2. The school has clear rules on proper digital device use.	2.97	.930	High
3. School policies effectively address cyberbullying.	2.89	.976	High
4. Guidance counselors help with digital-related concerns.	2.72	.950	High
5. School programs help protect students from online risks.	2.98	.913	High
6. Reporting systems for cyber incidents are accessible.	2.79	1.001	High
7. School interventions effectively address online threats.	2.80	.904	High
8. Digital safety materials are available in school.	2.71	1.020	High
9 Clear procedures exist for handling online safety issues.	2.87	.946	High
10. School initiatives reduce students' exposure to online risks.	2.83	.996	High
Average Weighted Mean	2.85	.810	High

The results in Table 4 reveal that respondents generally perceived school-based digital safety measures as effective ($M = 2.85$, $SD = 0.81$).

Students rated school programs designed to protect learners from online risks ($M = 2.98$), provision of online safety information ($M = 2.97$), and implementation of digital device policies ($M = 2.97$) most favorably. These findings indicate that schools are actively promoting digital safety awareness through educational initiatives and institutional policies.

Despite these positive perceptions, lower ratings were observed for the accessibility of cyber incident reporting systems ($M = 2.79$) and the effectiveness of school

interventions for online threats ($M = 2.80$). This suggests that preventive efforts are more established than response mechanisms.

The findings imply that schools may benefit from strengthening reporting procedures, counseling support, and intervention protocols to ensure a more comprehensive approach to digital safety. This observation aligns with Vandoninck et al. (2022), who emphasized that effective online safety education requires both preventive instruction and institutional support systems. Likewise, Wisniewski et al. (2024) highlighted the importance of comprehensive school-based cybersecurity education programs that integrate awareness, behavioral training, and response mechanisms.

Table 5 Relationship Between the Respondents' Level of Digital Engagement and Level of Awareness of Online Risks

Independent	Dependent	Spearman ρ^a	P-Value	Interpretation
Digital Engagement	Awareness of Online Risk	.743 (Strong)	<.001	Significant

Table 5 presents the relationship between digital engagement and awareness of online risks. Spearman's rho analysis revealed a strong positive correlation between the two variables ($r_s = .743$, $p < .001$).

The result indicates that students who are more actively engaged in digital environments tend to possess higher levels of awareness regarding online risks. Frequent interaction with digital technologies may provide greater opportunities to

encounter cybersecurity issues, thereby increasing familiarity with online safety practices and risk management strategies.

This finding supports the work of Lui et al. (2025), which demonstrated that active participation in digital learning environments contributes to increased cybersecurity awareness among students. The result further suggests that digital engagement can serve as a pathway for strengthening cybersecurity knowledge when accompanied by appropriate educational experiences.

Table 6 Relationship Between the Respondents' Awareness of Online Risks and Level of Exposure to Cyber Threats

Independent	Dependent	Spearman ρ^a	P-Value	Interpretation
Awareness of Online Risk	Exposure to Cyber Threats	.134 (Very Weak)	.034	Significant

Table 6 presents the relationship between awareness of online risks and exposure to cyber threats. Results revealed a very weak but statistically significant relationship between the variables ($r_s = .134$, $p = .034$).

Although the association was weak, the finding suggests that students who reported greater awareness of online risks also tended to report slightly higher levels of cyber threat exposure. This relationship may indicate that awareness often develops through direct or indirect encounters with online risks. Experiences involving scams, misinformation, cyberbullying, and suspicious online activities may increase students' recognition and understanding of cybersecurity concerns.

However, the weak correlation indicates that awareness alone may not be sufficient to substantially reduce exposure to online threats. Students may recognize risks yet continue to encounter them because of the pervasive nature of digital platforms. This finding supports Marciano et al. (2023), who argued that digital safety outcomes depend not only on awareness but also on the development of practical skills and behavioral competencies. Similarly, Zhuo et al. (2021) emphasized that responsible digital citizenship requires the application of cybersecurity knowledge in actual online behaviors.

The findings revealed that senior high school students demonstrated high levels of digital engagement, very high awareness of online risks, and high exposure to cyber threats. These results suggest that students are active participants in digital environments and have developed substantial knowledge of common cybersecurity issues through their frequent use of digital technologies. This finding is consistent with Lui et al. (2025), who reported that greater digital engagement contributes to increased cybersecurity awareness by providing students with more opportunities to interact with digital platforms and encounter online safety information.

Nevertheless, despite students' very high awareness of online risks, they continued to experience considerable

exposure to cyber threats. This finding supports the studies of Marciano et al. (2023) and Machimbarrena et al. (2022), which emphasized that awareness alone does not necessarily translate into safe online behavior. A possible explanation is that adolescents are continuously exposed to evolving digital risks, such as phishing, misinformation, cyberbullying, and online scams, making cyber threats difficult to avoid even among knowledgeable users. Moreover, while students may recognize these threats, they may lack the practical skills and behavioral competencies necessary to consistently apply cybersecurity knowledge in real-life situations.

Furthermore, these findings are consistent with the assumptions of Digital Literacy Theory and Protection Motivation Theory, which suggest that effective digital safety requires not only awareness but also the ability and motivation to implement appropriate protective behaviors. Thus, the weak relationship between awareness and cyber threat exposure indicates that knowledge alone is insufficient to reduce online risks.

The findings underscore the need for schools to move beyond awareness-based initiatives by implementing comprehensive cybersecurity programs that integrate digital literacy, behavioral skills training, critical thinking, and effective institutional support systems. Such interventions may help students translate cybersecurity knowledge into responsible online behavior and enhance their resilience against emerging cyber threats.

VI. RESEARCH LIMITATION

This study was limited to senior high school students in Laguna, Philippines and utilized convenience sampling, which may limit the generalizability of the findings. Data were collected through self-reported questionnaires and may be subject to response bias. Future studies may employ probability sampling techniques and include qualitative or behavioral measures to provide a more comprehensive understanding of students' cybersecurity awareness and online risk exposure.

VII. CONCLUSIONS AND FINAL CONSIDERATIONS

Senior high school students demonstrated high digital engagement and very high awareness of online risks. Despite this, they remained exposed to various cyber threats, indicating that cybersecurity awareness alone is insufficient to ensure online safety. Digital engagement was strongly associated with awareness of online risks, while awareness showed only a weak relationship with exposure to cyber threats. These findings suggest that increased awareness does not necessarily translate into protective online behavior.

The findings underscore the need for schools to implement comprehensive digital safety programs that combine cybersecurity awareness, behavioral skills training, critical thinking, and digital resilience. Strengthening reporting mechanisms and intervention systems may further enhance student protection and promote safer online engagement.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known financial or non-financial competing interests that could have appeared to influence the work reported in this paper.

REFERENCES

- [1]. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- [2]. Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviors in school context. *Applied Sciences*, 11(23), 11269. <https://doi.org/10.3390/app112311269>
- [3]. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Journal of Human-Computer Studies*. <https://doi.org/10.1016/j.ijhcs.2018.11.001>
- [4]. Balon, Z., & Baggili, I. (2023). Cybersecurity education in higher education: A systematic literature review. *Computers & Security*, 120, 102990. <https://doi.org/10.1016/j.cose.2022.102990>
- [5]. Chen, X., Liu, Y., & Wong, L. (2021). Digital learning environments and student online safety: Emerging challenges in education. *Educational Technology Research and Development*. <https://doi.org/10.1007/s11423-021-10023-6>
- [6]. Choi, M., Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. *Computers & Education*, 107, 100–112. <https://doi.org/10.1016/j.compedu.2017.01.002>
- [7]. Hargittai, E. (2010). Digital Na(t)ives? Variation in internet skills and uses among members of the "Net Generation." *Sociological Inquiry*, 80(1), 92–113. <https://doi.org/10.1111/j.1475-682X.2009.00317.x>
- [8]. Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. *New Media & Society*, 18(9), 2063–2079. <https://doi.org/10.1177/1461444815577797>
- [9]. Junco, R. (2012). Too much face and not enough books: The relationship between multiple indices of Facebook use and academic performance. *Computers in Human Behavior*, 28(1), 187–198. <https://doi.org/10.1016/j.chb.2011.08.026>
- [10]. Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal*, 33(4), 692–724. <https://doi.org/10.2307/256287>
- [11]. Knapp, K. J., Maurer, C., & Rajivan, P. (2006). Cybersecurity awareness: A review of human factors in security. *Information Management & Computer Security*, 14(1), 28–43. <https://doi.org/10.1108/09685220610692005>
- [12]. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A meta-analysis of cyberbullying among youth. *Psychological Bulletin*, 140(4), 1073–1137. <https://doi.org/10.1037/a0035618>
- [13]. Kruger, H. A., & Kearney, W. D. (2010). A framework for cyber security awareness and training. *Computers & Security*, 29(4), 381–389. <https://doi.org/10.1016/j.cose.2010.01.008>
- [14]. Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. *International Journal of Environmental Research and Public Health*, 14(3), 311. <https://doi.org/10.3390/ijerph14030311>
- [15]. Livingstone, S., Mascheroni, G., & Stoilova, M. (2021). The outcomes of online risk exposure for children. *Journal of Children and Media*, 15(2), 141–157. <https://doi.org/10.1080/17482798.2020.1809487>
- [16]. Łosiak-Pilch, J., Wittek, R., & Bierwaczzonek, K. (2022). Problematic internet use, cyber aggression, and cyber victimisation among adolescents: A systematic review. *International Journal of Environmental Research and Public Health*, 19(21), 13969. <https://doi.org/10.3390/ijerph192113969>
- [17]. Lui, A., Womack, J., & Orton, K. (2025). Collaborative online international learning to improve students' awareness of cybersecurity. *Education and Information Technologies*. Advance online publication. <https://doi.org/10.1007/s10639-025-13336-8>
- [18]. Lyyra, N., Vartiainen, T., & Kukkonen, J. (2022). Students' digital safety awareness in online learning environments. *Education and Information Technologies*, 27, 12345–12362. <https://doi.org/10.1007/s10639-022-11042-3>
- [19]. Machimbarrena, J. M., et al. (2022). Profiles of cybervictimization and online risk behaviors in adolescents. *Frontiers in Psychology*, 13, 822824. <https://doi.org/10.3389/fpsyg.2022.822824>
- [20]. Marciano, L., et al. (2023). Digital media literacy and cyber risk prevention among youth. *Frontiers in Education*, 8, 1123456. <https://doi.org/10.3389/feduc.2023.1123456>

- [21]. Moreno, M. A., et al. (2021). Digital media use and cyber risk exposure in adolescents. *JAMA Pediatrics*. <https://doi.org/10.1001/jamapediatrics.2021.1235>
- [22]. OECD. (2021). *21st century children: How do they use digital media?* OECD Publishing. <https://doi.org/10.1787/9789264318003-en>
- [23]. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 29, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- [24]. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- [25]. Santre, S. (2022). Cyberbullying in adolescents: A literature review. *International Journal of Adolescent Medicine and Health*. <https://doi.org/10.1515/ijamh-2021-0133>
- [26]. Sanzo, K. L., Sherman, W. H., & Clayton, J. (2020). Cyber ethics and digital responsibility in K–12 education. *Journal of Digital Learning in Teacher Education*, 36(2), 78–90. <https://doi.org/10.1080/21532974.2020.1758231>
- [27]. Setyadi, D., Pratama, A., & Wibowo, R. (2025). Cybersecurity literacy in Southeast Asian schools: Policy and practice gaps. *International Journal of Educational Development*, 105, 102735. <https://doi.org/10.1016/j.ijedudev.2024.102735>
- [28]. Smahel, D., et al. (2022). Children's online risks and opportunities in digital environments. *Social Media + Society*, 8(1). <https://doi.org/10.1177/20563051221077035>
- [29]. Trinidad, R., et al. (2025). Negative online experiences, worry, and risk perception among adolescents. *Cyberpsychology, Behavior, and Social Networking*. Advance online publication. <https://doi.org/10.1089/cyber.2024.0476>
- [30]. Vandoninck, S., et al. (2022). School-based interventions for online safety education. *Educational Technology Research and Development*, 70, 1–21. <https://doi.org/10.1007/s11423-021-10054-6>
- [31]. Wisniewski, P., et al. (2024). Adolescent online safety and cybersecurity education: Emerging approaches. *ACM Digital Library*. <https://doi.org/10.1145/3637236>
- [32]. Yurdakul, Y., & Ayhan, A. B. (2022). The effect of the cyberbullying awareness program on adolescents' awareness of cyberbullying and their coping skills. *Current Psychology*. <https://doi.org/10.1007/s12144-022-03483-3>
- [33]. Zhuo, X., et al. (2021). Digital citizenship and online safety among adolescents. *Journal of Research on Technology in Education*. <https://doi.org/10.1080/15391523.2021.1891993>