

CYBERSECURITY AWARENESS AMONG STUDENTS: A COMPARATIVE REVIEW OF RECENT STUDIES

Grace Llego and Jim Alves-Foss

Center for Secure and Dependable Systems, University of Idaho, Moscow, ID
USA

ABSTRACT

Since about 2010, there has been increased attention in gauging and improving digital citizenship across the world. One important aspect of digital citizenship is cybersecurity awareness. This paper reports on a review of 35 studies that have been conducted in this area, primarily consisting of surveys of students. The primary purpose of this review was to compare and evaluate the methods used in these studies to provide guidance towards future studies. The studies surveyed from 32 to over 3000 participants evaluated cybersecurity awareness and/or practice, with about half of them providing copies of the survey questions to allow for follow-on comparative studies.

KEYWORDS

Cyber security awareness, Surveys. Digital Literacy

1. INTRODUCTION

The prevalence of cybersecurity attacks is well documented, and there are worldwide efforts to help protect people from those attacks. In addition to the creation and deployment of enhanced cybersecurity technologies, people have developed training programs to increase cybersecurity awareness, and to also hopefully improve cybersecurity related behaviours.

Cybersecurity awareness is a general term that covers the concepts related to general user knowledge of computer/Internet security and privacy issues; for example, password management, account security, email attacks, fake websites, etc. Cybersecurity behaviour involves the users' actual use of good cybersecurity practices.

Training in cybersecurity awareness is common in most US and European Universities and businesses, as well as in many other countries. Unfortunately, we have noticed that much of the training makes some implicit assumptions about access to technology, or experience with the Internet. Especially more advanced training may assume access to tools such as antivirus software or assume use of specific social media platforms or technology, such as desktops or laptop computers. This access is not common in poorer regions, including rural communities in many of the "advanced economies" as well as wide portions of countries classified as developing economies.

For example, according to Our World in Data [1], there is quite a disparity in the share of a population using the Internet. According to their most recent report 90.9% of the population in the United States had Internet access, while in the Philippines, it is only 49.8%, and was under 30% in

Sub-Saharan Africa (see Table 1). What is separately interesting is that the data indicates multiple mobile subscriptions per person across all regions.

What this tells us, is that there are places in the world where people have initial limited or low access to the Internet. The question for these people, when they do eventually get access, if it is for limited times, or later in life, are they aware of cybersecurity problems? Were they taught to be careful, when using the technology, often just cell phones, they use to access the Internet?

We decided to look at several published surveys addressing cybersecurity awareness in students, primarily college students. We felt that this was a demographic that would likely be studied and should provide a guide to general cybersecurity awareness across the world. In the course of our review we found several papers that looked at parents and corporate workers. We decided to include those as well to make the report more inclusive.

There are of course several limitations with these studies, the first is the correlation between college students and the general public. College students are generally better educated, more informed of current threats and more technologically experienced than the general public. In addition, we need to look at whether these surveys address both awareness and practice, and do they provide any training as part of the study.

We are particularly interested in enabling others to create similar surveys in the future, to judge contemporary knowledge and also to potentially evaluate overall trends over time. To that end, we are asking the following research questions:

RQ1: What are the overall findings of these studies with respect to student awareness?

RQ2: What are the common questions asked in surveys of cybersecurity awareness of college students?

RQ3: Do these surveys make assumptions about student technology access?

Table 1. Adoption of Communications Technology per 100 people, 2020 [1]

Region/Country	Mobile Phone Subscriptions	Internet Users
North America	105.1	91.0
United States	107.3	90.9
Europe and Central Asia	128.7	83.8
Middle East and North Africa	117.0	75.5
Latin American and Caribbean	108.2	73.9
East Asia and Pacific	129.4	73.1
World	110.0	59.6
Philippines	143.4	49.8
South Asia	85.0	38.5
Sub-Saharan Africa	92.6	29.3

The remainder of this paper is organized as follows. Section 2 provides a summary of related research. Section 3 provides a summary of the surveyed papers and Section 4 discusses the results and potential future work.

2. RELATED WORK

During our survey, we found 3 other papers that discussed student awareness by looking at the literature. Each of these papers took a different approach to evaluating existing surveys and awareness studies.

Baadel et al. [2], also in 2021, provided a thorough exploration of the evolving landscape of phishing threats and the multifaceted approaches to counter them, ranging from technical solutions like Machine Learning to traditional measures such as legislation and education.

Mohammed and Bamasoud's [3] survey paper focused on the critical need to enhance cyber security awareness among university students in Saudi Arabia as a proactive measure to mitigate cyber threats. They state that cybersecurity awareness initiatives play a crucial role in educating students about cybersecurity risks, threats, and best practices, fostering a positive cybersecurity culture. By enhancing awareness, students are better equipped to protect critical information assets and navigate cyberspace safely, aligning with the goals outlined in Saudi Arabia Vision 2030. This proactive approach not only safeguards personal and technological assets but also contributes to broader national cybersecurity resilience and privacy protection efforts.

Qayyum et al. [4] conducted a systematic literature review of studies related to cybersecurity awareness in children in 2021. They focused on papers with empirical data published in academic venues since 2011. From an initial online search listing over 1500 papers, they were able to reduce the number of papers to 56 peer reviews papers that satisfied their selection criteria and then further evaluated what they covered, and how the studies were conducted.

3. AWARENESS STUDIES

We examined the literature and found 30 studies that examined student, parent and working adult cyber security awareness. We have broken these into categories of parental awareness, college student awareness. K-12 student awareness and worker awareness. If a study included college students and others, we only report it in the college student awareness section.

3.1. Parental Awareness

Ahmad et al. [5] surveyed 872 parents about awareness in Malaysia. This study's focus on parental awareness of cyber threats is highly relevant and timely, given the increasing digital engagement of adolescents and the associated risks. Parents play a crucial role in shaping their children's online behaviours and protecting them from potential dangers on the internet. The finding that parental awareness of cyber threats is at a medium level suggests there is room for improvement through targeted education and awareness programs. The following formatting rules must be followed strictly. This (.doc) document may be used as a template for papers prepared using Microsoft Word. Papers not conforming to these requirements may not be published in the conference proceedings.

3.2. College Student Awareness

Ahmed et al. [6] conducted a survey, both online and offline, of 802 Bangladehsi respondents. They found low to moderate awareness of cybersecurity practices and high experience of respondents being victims of phishing, identity theft and malware. The report did not include specific survey questions. It was followed in 2019 by another report that specifically looked at demographics tied to cybersecurity awareness [7].

Alotaibi, et al. [8] conducted an online survey of 629 Saudi nationals related to cybersecurity awareness and internet usage. Key findings of this survey found that almost 90% of the respondents

primarily used smartphones for internet access. Respondents used internet on almost a daily basis yet had low cybersecurity awareness. \

Al-Janabi and Al-Shourbaji [9] surveyed 760 college students in the Middle East with respect to cybersecurity awareness. The paper highlighted the crucial role of information security awareness in combating cyber-attacks within educational environments in the Middle East. By analysing the awareness levels among academic staff, researchers, undergraduate students, and employees, the study found a significant gap in their knowledge and understanding of information security principles and their practical application. This deficiency poses a risk to both institutional IT systems and personal data security. The paper suggested that comprehensive awareness and training programs, along with necessary safety measures at all institutional levels, are essential to address this gap. Such initiatives would help ensure that students, staff, and employees become more technology-savvy and capable of protecting their data. The findings underlined the need for immediate action to implement these recommendations, as neglecting information security training could lead to severe negative consequences for both institutional and personal cybersecurity.

Alves-Foss and Llego [10] surveyed 200 college students in the Philippines. Unlike many other studies, a large portion of their respondents were not from technical majors, and many had not used the Internet until they were teenagers. They found no significant correlation between several different demographics and differences in student awareness and behaviour. Overall the awareness and behaviour were average for these students.

Bernadas and Soriano [11] provided valuable insights into the online privacy behaviours of 300 urban poor youth in the Philippines, revealing that diversified Internet connectivity fosters more cautious online privacy practices. By utilizing a quantitative, interview-administered survey approach, the study highlighted that increased access through multiple Internet points enhance online privacy behaviours, with information literacy playing a key explanatory role. This research is significant as it contributes to the limited literature on online privacy in the Global South, emphasizing the importance of digital skills and connectivity diversity in promoting protective online behaviours. The findings underscore the need for targeted policy interventions to support vulnerable populations in navigating online privacy effectively.

Clemons and Wilson [12] addressed the critical issue of data mining in educational applications and its implications for young Internet users. By questioning 1453 individuals from Latin America, they examined parents' and students' attitudes across several countries, the research revealed a widespread preference for minimal data mining of students' online activities, contrasting sharply with current practices. Interestingly, aversion to data mining is not correlated with awareness of these practices, highlighting a disconnect that warrants attention. The findings underscore the need for regulatory interventions, ranging from enhanced transparency to stringent legal requirements for software providers, depending on the root causes of inappropriate online behaviour and the selection of educational software. This study paves the way for future research to develop suitable regulatory frameworks to protect students' privacy and ensure ethical data handling in educational contexts.

Garba et al. [13] aimed to assess the cybersecurity awareness among Computer Science students at Yobe State University in Nigeria. Using a quantitative approach and a set of questionnaires, the study surveyed 201 students during a period when universities were closed due to the COVID-19 pandemic, limiting participation to those in urban areas. The findings indicated that while the students' cybersecurity awareness is at a satisfactory level, more than half lack adequate knowledge on protecting their data. The study revealed the absence of an active cybersecurity awareness program and highlights that female students are more susceptible to cyber-attacks. Despite these challenges, the survey showed a high enthusiasm among students to learn more about

cybersecurity. These insights underline the urgent need for implementing comprehensive cybersecurity education programs to enhance students' ability to safeguard themselves against online threats.

Hong et al. [14], surveyed 852 year 1–3 students, 325 final-year students (age = 18–25) and 475 full-time employees (age = 18–50) in two cities of China. This study introduced an extended Knowledge-Attitude-Behavior (KAB) model to explore factors influencing Internet Security Awareness (ISA), particularly focusing on the moderating role of societal education levels through exposure to full-time work environments. The study employed the Human Aspects of Information Security Questionnaire (HAIS-Q). Results from MANOVA and PROCESS regression analyses revealed a significant negative moderating effect of work exposure on ISA, impacting all three dimensions of knowledge, attitude, and behavior related to cybersecurity.

Irfan et al. [15] surveyed 203 college students in Pakistan. The study's findings underscored a critical need for heightened cybersecurity awareness among university students in Pakistan, given the escalating frequency and severity of cyber-attacks. The identified lack of awareness among students highlighted vulnerabilities that could lead to exploitation in an increasingly interconnected digital landscape. The authors claim that organizing targeted cybersecurity education programs is imperative to equip students with essential knowledge and skills for protecting themselves online. The authors claim that by fostering a proactive approach to cybersecurity education, institutions can empower students to navigate the internet securely and contribute to building a safer digital environment in Pakistan and beyond.

Mollaem [16] reported on a survey of 247 college students from two California State Universities. Despite being in a highly tech-savvy environment, the research suggests that students are not sufficiently aware of cyber-attacks or how to protect their data effectively but were not very aware of how to protect themselves.

Muhirwe and White [17] surveyed 214 students in a college in the Pacific Northwest. The study underscores the significant role of cybersecurity awareness among college students, who are heavy users of Information Technology (IT) for personal and educational purposes. The authors claim that as students spend more time online, they face increased risks such as identity theft, fraud, and unintentional involvement in cybercrimes. Furthermore, entering the workforce without adequate cybersecurity awareness can perpetuate vulnerabilities in organizational cybersecurity defences. The research investigates how cybersecurity awareness influences students' cybersecurity practices, finding a clear correlation between awareness and practice. Although cybersecurity training alone may not predict awareness effectively, the study highlights its crucial role in enhancing cybersecurity awareness among the next generation of corporate technology users. These insights emphasize the importance of integrating robust cybersecurity education into college curricula to better prepare students for navigating digital environments safely and responsibly.

Peker et al. [18] developed cybersecurity training modules and evaluated student awareness both pre and post-test for 372 participants. The study showed that the training was effective.

Posa and Grossklags [19] conducted of student awareness of cybersecurity risk. They surveyed 798 university students across four categories: remote work and Wi-Fi settings, smart home devices, personal devices/BYOD/BYOS, and social engineering threats. Their analysis showed that work experience significantly enhanced cybersecurity risk awareness across various topics. However, some areas of risk awareness were less influenced by work experience, suggesting other contributing factors such as early formal education and longer employment periods. The study found that younger generations, like Generation Z and Generation Alpha, generally exhibit good security practices, potentially benefiting from cybersecurity education integrated into their early experiences.

Pratma and Alshaikh [20] surveyed 1681 undergraduate students from two Universities, one in Indonesia and one in Saudi Arabia. They enhanced the survey with a between-subject experimental design to test awareness of password strength after being exposed to different infographics.

Sarathchandra et al. [21] surveyed 498 college students in the US Northwest. The research addresses a significant gap in understanding college students' cybersecurity perceptions and behaviours by quantifying latent factors identified in previous qualitative research. The study explores factors such as routinization and ritualization of risk, optimistic bias, self-efficacy bias, and the 'Can-I-Live' syndrome. These factors are analysed alongside additional measures of cybersecurity awareness and behaviour through an online survey. The findings from this quantitative analysis provide valuable insights for cybersecurity scholars and practitioners, offering a nuanced understanding of what drives students' perceptions and practices in this critical domain. Senthilkumar and Easwaramoorthy [22] surveyed 379 students. The study aimed to assess the awareness of cyber security among college students in Tamil Nadu, focusing on various internet security threats such as email scams, viruses, phishing attacks, fake advertisements, popup windows, and other online threats. Cybercrime poses significant challenges across national security, public safety, and personal privacy domains, necessitating proactive measures to educate individuals on safeguarding themselves online. The research employs a well-structured questionnaire survey method conducted across major cities in Tamil Nadu to gauge students' awareness levels and understanding of cyber security issues. Recommendations will be formulated based on survey findings to enhance awareness and mitigate these cyber security challenges effectively among college students in the region.

3.3. K-12 Student Awareness

Choong et al. [23] investigated the password practices and perceptions of children, highlighting their early engagement with technology and the importance of cybersecurity education. Surveying 189 3rd to 8th graders from two Midwest schools, the research reveals that children generally maintain good password habits, with average password lengths increasing with age. However, only a small percentage of children create very strong passwords, indicating a need for further development of their cognitive and linguistic skills related to password creation. The study underscores the importance of reinforcing positive practices through cybersecurity education while adapting to the developmental stages of children. Recognizing the study's limited scope, future research aims to include a broader age range and more diverse school districts to enhance generalizability and provide deeper insights into children's cybersecurity behaviours.

Dempsey et al. [24] investigated children's understanding of online privacy, a crucial aspect for meeting GDPR obligations which mandate that privacy notices be child-friendly and age-appropriate. By surveying 32 children aged 8 to 10 from a UK primary school, the study reveals that while children grasp the importance of privacy for online safety, they often lack an understanding of the inherent value of their data and have misconceptions about what data should be protected. These findings underscore the challenges faced by technology designers in creating compliant, comprehensible privacy notices for children. It emphasizes the need for enhanced educational efforts and thoughtful design to help children better understand privacy issues in the digital age.

Hamdan et al. [25] surveyed 150 teenagers to explore the dual impact of technological advancements on modern teenagers, focusing on internet addiction and cyber security threats. By analysing the internet usage patterns of Emirati teenagers through both qualitative and quantitative methods, the study assesses their awareness of various cyber threats and their strategies for dealing with them. Based on these findings, the research proposes countermeasures to help teenagers and

their parents avoid or manage cyber security threats effectively. The recommendations aim to enhance cyber security awareness and promote safer internet practices among teenagers, addressing a critical aspect of modern digital life.

Hofstra et al. [26] investigated the predictors of privacy settings on Facebook among Dutch adolescents, focusing on peer influence, popularity, and trust. Using survey data from 3434 adolescents and their observed Facebook behaviours, the findings reveal that adolescents tend to imitate the privacy settings of their classroom peers, especially in highly connected classrooms. Popular adolescents are more likely to display their profiles publicly, while groups with lower trust levels—such as ethnic minorities, lower educated and younger adolescents, and girls—prefer private profiles. These insights underscore the importance of social dynamics and trust in shaping online privacy behaviours among youth.

Maoneke et al. [27] addressed the under-researched area of ICT use and associated risks among adolescents in the developing world, focusing on Namibia. Using a quantitative methodology with 729 respondents aged 13 to 17 from both urban and rural areas, the research identified common cyberspace activities and risks. Mobile phones are the primary means of internet access, with popular activities including social networking, watching movies, playing games, researching health issues, and schoolwork. Key risks identified are cyberbullying and sexual abuse, with a notable trend of adolescents befriending and sharing contact details with strangers online. While these risks are prevalent across all age and gender groups, female adolescents are more susceptible, and risk exposure increases with age. These findings highlight the urgent need for targeted policy frameworks to protect adolescents from cyberspace risks, tailored to the specific vulnerabilities identified in the study.

Zukifli [28] reported on a study of secondary students in Malaysia, along with their parents and teachers. They did not specify the number of respondents, only some of the statistics of the study. The study, conducted through both physical and online surveys, reveals that while there is a general awareness of cyber risks among the respondents, few take proactive security measures.

3.4. Worker Awareness

When we were collecting the list of studies, we found that some of them did not reference college students, but the information they presented was still relevant to our work. We summarize these studies in this section.

Ansari [29] evaluated risk scores from 200 industry participants who used an AI-based security awareness training program. More effective training resulted in better risk scores.

Daengsi et al. [30] reported on corporate training for about 20,000 employees in Thailand. They conducted a phishing exercise, followed it with training, and then retested the employees. This illustrates the kind of awareness training that many organizations offer.

Omorog and Ruji [31] surveyed 252 working Filipinos and found both strengths and serious weaknesses in their cybersecurity practices. It is concerning that many rely heavily on mobile and public WiFi for Internet access. At the same time, they implement security measures inadequately, despite understanding their importance.

Simonet and Teufel [32] surveyed 456 working adults in order to investigate the factors that affect cybersecurity awareness of home computer users. Their contribution brings into light the dynamics involved in personal cybersecurity practices. The results show how particularly important personal

initiative and information systems knowledge are to develop awareness and behaviour concerning cybersecurity at home.

Table 2. Summary of Surveyed Students and Their Content

Authors	Questions	Age	Awareness	Practice	Training	N
Ahmad et al. [5]	✓	Parents	✓			872
Ahmed et al. [6]		Adults	✓			802
Alotaibi. [8]	✓	Adults	✓	✓		629
Al-Janabi and Al-Shourbaji [9]	✓	College	✓	✓		760
Alves-Foss and Llego [10]	✓	College	✓	✓		208
Ansari [20]		Adults	✓	✓	✓	200
Bernadas and Sorianp [36]		College	✓			300
Choong [36]	✓	K-12	✓		✓	189
Clemons and Wilson [34]	✓	Teens and Parents	✓	✓		1453
Daengsi et al. [21]		Adults			✓	20,000
Dempsey et al. [33]		K-12	✓			32
Garba et al. [11]		College	✓			201
Hamdan et al. [31]	✓	K-12	✓	✓		150
Hofstra et al. [30]		K-12	✓			3434
Hong et al. [12]	✓	Adults	✓	✓		1652
Irfan et al. [13]	✓	College	✓	✓		203
Maoneke et al. [29]		K-12	✓	✓		789
Moallem et al. [14]	✓	College	✓	✓		247
Muhirwe and White [28]	✓	College	✓	✓		214
Omorog and Medina [22]	✓	Adults	✓	✓		252
Peker et al. [15]		HS & College	✓			372
Posa and Grossklags [16]	✓	College	✓			789
Pratama et al. [17]		College			✓	1681
Sarathchandra et al. [18]	✓	College	✓	✓		498
Senthilkumar and Easwaramoorthy [27]	✓	College	✓	✓		379
Simonet and Teufel [23]	✓	Adults	✓	✓	✓	456
Valli et al. [24]		Adults	✓			50
Zulkifli et al. [19]		HS & Adults	✓			N/A

Valli et al. [33] conducted a survey among 50 small to medium enterprise workers in Western Australia. SMEs, while an integral part of the economy, generally lack resources and expertise to protect themselves from cyber threats. Instead, what they have done is directly interact with SMEs in Joondalup and Wanneroo through surveys and interventions. In so doing, the researchers are not only filling a big gap in current cybersecurity research but also possibly improving the economic stability and security of these businesses. The output could be quite pragmatic, enabling the SMEs to better protect their systems and data from cyber attacks so that they can contribute to regional and national efforts toward cybersecurity.

4. DISCUSSION

When looking at the studies we categorized if they provided a list of the survey questions they used, the target audience, the number surveyed, if they looked at both awareness and behaviour of the participants, and if they provided or discussed training for the participants. The summary of this analysis is provided in Table 2.

Throughout these studies, there is a common theme, those surveyed are not aware enough of how to protect themselves, and often not aware of the existing threats.

For those wishing conduct their own studies in the future, we recommend looking at questions that address awareness of best cyber practices for desktop devices, mobile devices and general internet use. This includes passwords, backups, and awareness of phishing, malware and scams. In addition, the most thorough studies should look at actual behaviour and not just self-reported awareness or behaviour, although that requires significantly more resources.

The research highlights the need for future studies to explore additional factors influencing cybersecurity awareness and to use survey research alongside organizational risk measurements to better understand actual security practices in remote work environments.

REFERENCES

- [1] N. Ahmad, A. Arifin, U. Asma'Mokhtar, Z. Hood, S. Tiun and D. I. Jambari, "Parental awareness on cyber threats using social media," *Jurnal Komunikasi: Malaysian Journal of Communication*, vol. 35, no. 2, pp. 485-498, 2019.
- [2] H. Ritchie, E. Mathieu, M. Roser and E. Ortiz-Ospina, "Data Page: Share of the population using the Internet," 2023. [Online]. Available: <https://ourworldindata.org/grapher/share-of-individuals-using-the-internet>. [Accessed 20 May 2024].
- [3] J. Alves-Foss and B. G. Llego, "Internet Security and Privacy Awareness Among College Students in the Philippines," in *IEEE Cyber Science and Technologu Congree*, 2024.
- [4] Z. Zulkifli, N. N. A. Molok, N. H. Abd Rahim and S. Talib, "Cyber security awareness among secondary school students in Malaysia," *Journal of information systems and digital technologies*, vol. 2, p. 28-41, 2020.
- [5] R. Von Solms and S. Von Solms, "Cyber safety education in developing countries," *SYSTEMICS, CYBERNETICS AND INFORMATICS*, vol. 15, 2015.
- [6] C. Valli, I. C. Martinus and M. N. Johnstone, "Small to medium enterprise cyber security awareness: an initial survey of Western Australian business," in *Proceedings of International Conference on Security and Management*, 2014.
- [7] J. Simonet and S. Teufel, "The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users," in *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34*, 2019.
- [8] K. Senthilkumar and S. Easwaramoorthy, "A Survey on Cyber Security awareness among college students in Tamil Nadu," *IOP Conference Series: Materials Science and Engineering*, vol. 263, p. 042043, 2017.
- [9] D. Sarathchandra, K. Haltinner and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016.
- [10] H. Ritchie, E. Mathieu, M. Roser and E. Ortiz-Ospina, "Data Page: Share of the population using the Internet," 2023. [Online]. Available: <https://ourworldindata.org/grapher/share-of-individuals-using-the-internet>.
- [11] F. Quayyum, D. S. Cruzes and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, p. 100343, 2021.
- [12] A. R. Pratama, M. Alshaikh and T. Alharbi, "Increasing cybersecurity awareness through situated e-learning: a survey experiment," in *The 2nd Global Trends in E-Learning Forum (GTEL 2023)*, 2023.
- [13] T. Pósa and J. Grossklags, "Work experience as a factor in cyber-security risk awareness: A survey study with university students," *Journal of Cybersecurity and Privacy*, vol. 2, p. 490-515, 2022.

- [14] Y. Peker, L. Ray and S. Da Silva, "Online cybersecurity awareness modules for college and high school students," in 2018 National Cyber Summit (NCS), 2018.
- [15] C. D. Omorog and R. P. Medina, "Internet security awareness of Filipinos: A survey paper," International Journal of Computing Sciences Research, vol. 1, p. 14–26, 2017.
- [16] J. Muhirwe and N. White, "CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS," Issues in Information Systems, vol. 17, 2016.
- [17] M. Mohammed and D. M. Bamasoud, "The impact of enhancing awareness of cybersecurity on universities students: a survey paper," Journal of Theoretical and Applied Information Technology, vol. 100, p. 4756–4766, 2022.
- [18] A. Moallem, "Cyber security awareness among college students," in Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, 2019.
- [19] P. B. Maoneke, F. B. Shava, A. M. Gamundani, M. Bere-Chitauro and I. Nhamu, "ICTs use and cyberspace risks faced by adolescents in Namibia," in Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities, 2018.
- [20] H. Irfan, K. J. Akhter and R. Shakeel, "Cybersecurity and Multidisciplinary Students: A Survey," International Journal of Scientific & Engineering Research, vol. 11, p. 1786–1791, 2020.
- [21] W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N.-L. Lei and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," Education and Information Technologies, vol. 28, p. 439–470, 2023.
- [22] B. Hofstra, R. Corten and F. Van Tubergen, "Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust," Computers in Human Behavior, vol. 60, p. 611–621, 2016.
- [23] Z. Hamdan, I. Obaid, A. Ali, H. Hussain, A. V. Rajan and J. Ahamed, "Protecting teenagers from potential internet security threats," in 2013 international conference on current trends in information technology (CTIT), 2013.
- [24] M. Grobler, J. Jansen van Vuuren and J. Zaaiman, "Evaluating cyber security awareness in South Africa," in Proceedings of the 10th European Conference on Information Warfare and Security, 2011.
- [25] A. A. Garba, M. M. Siraj, S. H. Othman and M. A. Musa, "A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach," Int. J. Emerg. Technol, vol. 11, p. 41–49, 2020.
- [26] J. Dempsey, G. Sim and B. Cassidy, "Designing for GDPR-investigating children's understanding of privacy: A survey approach," in Proceedings of British HCI 2018, 2018.
- [27] T. Daengsi, P. Pornpongtechanich and P. Wuttidittachotti, "Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks," Education and Information Technologies, p. 1–24, 2022.
- [28] E. K. Clemons and J. S. Wilson, "Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications," Journal of Management Information Systems, vol. 32, p. 40–70, 2015.
- [29] J. M. A. C. Bernadas and C. R. Soriano, "Online privacy behavior among youth in the Global South: A closer look at diversity of connectivity and information literacy," Journal of Information, Communication and Ethics in Society, vol. 17, p. 17–30, 2018.
- [30] S. Baadel, F. Thabtah and J. Lu, "Cybersecurity awareness: A critical analysis of education and law enforcement methods," Informatica, vol. 45, 2021.
- [31] M. F. Ansari, "A quantitative study of risk scores and the effectiveness of AI-based Cybersecurity Awareness Training Programs," International Journal of Smart Sensor and Adhoc Network, vol. 3, p. 1, 2022.
- [32] F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, "A survey of cyber-security awareness in Saudi Arabia," in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016.
- [33] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," Journal of Information & Knowledge Management, vol. 15, p. 1650007, 2016.
- [34] N. Ahmed, U. Kulsum, I. B. Azad, A. Z. Momtaz, M. E. Haque and M. S. Rahman, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," in 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017.

- [35] N. Ahmed, M. R. Islam, U. Kulsum, M. R. Islam and E. Haque, “Demographic Factors of Cybersecurity Awareness in Bangladesh,” in International Conference on Advances in Electrical Engineering, 2019.
- [36] Y.-Y. Choong, M. F. Theofanos, K. Renaud and S. Prior, “Passwords protect my stuff—a study of children’s password practices,” Journal of cybersecurity, vol. 5, p. tyz015, 2019.

AUTHORS

Baby Grace Llego received her BS in Early Childhood Education in 2025 from the Golden State College of Malungon, Philippines. She is currently a Research Scholar at the University of Idaho, Moscow ID USA. Her research focuses on age-appropriate Internet Security and Privacy Awareness Education for K-12 students.



Dr. Jim Alves-Foss received his BS in physics, mathematics, and computer science in 1987, MS in computer science in 1989, and PhD in computer science in 1991, all from the University of California, Davis CA, USA. He is currently a Distinguished Professor of Computer Science at the University of Idaho, Moscow, ID USA. His research interests involve designing and analysing secure systems, including formal methods, automated vulnerability analysis and repair tools, and secure software development practices.

