Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 6, 2583-2590
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i6.8450

Development of an instructional package for enhancing e-safety awareness among secondary school students in Kerala, India

Asokan Vasudevan[1*], Sojia John[2], N. Raja[3], Hariharan N Krishnasamy[4], Suma Parahakaran[5], Rabindra Dev Prasad Prasad[6]
[1]Faculty of Business and Communications, INTI International University, Persiaran Perdana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia. asokan.vasudevan@newinti.edu.my (A.V.).
[2]Mount Tabor Training College, Pathanapuram, Kollam, Kerala, India; sojiajohn17@gmail.com (S.J.).
[3]Department of Visual Communication, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India; rajadigimedia2@gmail.com (N.R.).
[4,5,6]Faculty of Education and Liberal Arts, INTI International University, Persiaran Per-dana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia; hariharan.samy@newinti.edu.my (H.N.K.) suma.parahakaran@newinti.edu.my (S.P.) rabindra.prasad@newinti.edu.my (R.D.P.P.).

Abstract: The increasing early exposure of children to the internet, involving activities such as social networking, gaming, and shopping, has raised concerns about their vulnerability to cybercrimes. Children, particularly secondary school students in Kerala, are at significant risk due to their lack of understanding of online risks and safety measures. This has led to challenges for schools, as the rise in cyber threats poses severe national and social security risks. To address this, a study evaluated the effectiveness of an instructional package called 'e-SHIELD' in enhancing e-safety awareness among 90 secondary school students in Kerala. The experimental treatment involved pre- and post-tests to measure the impact of the instructional package on students' awareness of e-safety. The results demonstrated a significant improvement in e-safety awareness among students after the package's implementation, with no significant difference between male and female students. The study underscores educators' crucial and valued role in teaching students how to use technology safely, emphasizing the need for ongoing education to ensure proactive internet safety throughout their lives.

Keywords: *Cybercrimes, E- safety awareness, Education, Instructional package, Internet safety.*

1. Introduction

Technology is omnipresent in the modern world. It dominates our lives, since it continuously captivates our interest and provides enjoyment. A new type of civilization known as the information society is thought to have been produced by the development and emergence of new Information communication technologies (ICT) in the last few decades. Students are more likely to become disengaged from reality and neglect their obligations due to the plethora of readily available technology and networking. People today live in a new realm known as Cyberspace because of internet connectivity. Changes have been brought about in many areas of society by the massive expansion of Internet connectivity and the development of other electronic communication technologies. Over 500 million individuals worldwide access the Internet daily to purchase and sell products, exchange concepts, and convey exciting prospects and creative solutions. Despite all of ICT's advantages, there are drawbacks, such as security issues. A few predators have decided to turn cyberspace into a haven for crime and fraud even though billions of dollars pass over the Internet every day. Cybercrime is a general term for illegal activities in which a computer is a tool, a target, or both [1]. Among the many crimes where a computer is used as a weapon are financial crimes, the sale of illegal goods, pornography, online

History: Received: 1 April 2025; Revised: 6 June 2025; Accepted: 9 June 2025; Published: 30 June 2025
* Correspondence: asokan.vasudevan@newinti.edu.my

gambling, email spoofing, forgery, cyber stalking, cyber defamation, and crimes involving intellectual property.

Mobile phones are a common form of communication these days. Mobile phones are completely portable electronic communication devices that allow users to engage with one another by exchanging data, text, or audio over a cellular network of relay stations. Unlike personal PCs, mobile phones let users accomplish all those programs and activities anytime, anywhere. Students in secondary schools are increasingly using mobile phones, which are becoming more intelligent devices. Student use of mobile devices includes texting, calling, searching the internet, viewing movies, playing games, listening to music, and utilizing social media. According to the National Crime Records Bureau [2] India has the second-largest communications network globally in terms of the total number of phone subscribers. It is almost common for teenagers and young people in India to own a cell phone as their standard of life rises. In certain Indian states, a survey conducted among school-age children revealed that almost one-third had been victims of cybercrime. Adolescents' self-formation depends heavily on their ability to communicate and feel connected to their peers during adolescence. Teenagers' use of mobile phones serves as a conduit for this communication, allowing social interactions and connections to occur in context and time without being restricted. Thirty percent of Indian youngsters who access the internet in schools across states have suffered cyber damage [3]. This covers cyberbullying, privacy infringements, and Security threats, which are real concerns that affect our students [3]. The issue of cybercrime among children and young adults is on the rise as a result of fast globalization, inexpensive mobile phones, easy access to the internet, and essentially no laws to restrict friends from abusing their friends' children. Youngsters (8 to 18 years old) are the most vulnerable to the harmful impacts of electronic media.

Knowing the benefits, risks, and responsibilities of using information technology is therefore essential for teaching youth and adolescents. To give people control over their online experiences, e-safety raises awareness and provides protection. So, e-safety education and awareness should be raised to improve students' online behavior. The term 'e-Safety' is frequently used to describe security when using ICT resources. According to Vanderhoven, et al. [4] electronics like cell phones and wireless technologies are included in the definition of safety and internet technologies. Siyam and Hussain [5] refer to e-safety as preventing harm to children and adolescents; e-safety ensures that kids and teenagers are equipped to fully use emerging technology without endangering others or themselves. Hence, awareness activities should be scheduled regularly and spaced out for the year using formal and informal methods [6].

The internet usage habits of children are rapidly evolving due to significant advancements in technology, industry trends, and society. Children's internet use is generally pleasant, as seen by their regular interaction with online music, games, movies, texting, and searching. According to their parents, children between the ages of three and four are known to watch cartoons, short films, animations, or music on YouTube. As kids become older, they view different content. They watch more amusing videos, music videos, vloggers, and YouTube celebrities. Schools have a crucial role in educating kids about vital digital literacy and informing and advising parents about their children's internet use at home. Cybersecurity education aims to educate technology users about the threats they may encounter when utilizing online communication platforms, including social media, chat, online gaming, email, and instant messaging. Even though much research has been done in the past on cyber security, it has mostly been done in various domains. For instance, not many papers specifically address the actions schools should take to assist in fostering cybersecurity awareness. It emphasizes how crucial it is to instruct younger generations on the benefits, risks, and obligations associated with using technology. E-safety raises awareness and protects so that individuals can take control of their online experiences. More e-safety education and awareness campaigns are needed to influence people's online behavior.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 6: 2583-2590, 2025
DOI: 10.55214/25768484.v9i6.8450

1.1. Research Problem

Cyberbullying is the practice of harassing, intimidating, or causing harm to others via the use of electronic communication. It can come in a lot of different forms, such sending threatening messages, publishing embarrassing images or videos, or starting rumours. Cyber bullying victims may experience severe emotional and psychological impacts from the abuse, including anxiety, depression, and in severe situations, suicidal thoughts. When someone is subjected to control, manipulation, or emotional injury by words, deeds, or behaviors, it is referred to as emotional abuse. Cyberbullying, harassment, and gaslighting are examples of emotional abuse that occurs online. Low self-esteem, anxiety, and trauma are common among victims of emotional abuse. Phishing is a kind of cyber attack in which perpetrators deceive targets by sending phony emails, messages, or websites in an attempt to trick them into divulging personal information, including bank account information or login passwords. Financial loss, identity theft, or illegal access to personal accounts are all possible outcomes of phishing assaults. Cyber attacks known as "pharming" entail secretly sending people to phoney websites. In order to divert visitors to fake websites intended to steal confidential data, attackers can change DNS settings or install malicious software. Pharming attempts can result in identity theft and jeopardize users' sensitive data. Online exposure to unsuitable content: People, particularly kids and teenagers, might suffer severe consequences from this type of exposure. Violent, pornographic, or hateful speech that desensitizes viewers, encourages bad behavior, or has a detrimental effect on their mental health is considered inappropriate content. Children should be supervised in their online activities, and parents and teachers should offer advice on using the internet safely. Identity theft is a sort of fraud in which financial fraud or other crimes are committed using a victim's personal information, such as their name, Social Security number, credit card information, or other sensitive data. The information stolen by identity thieves can be used to open false accounts, make illegal transactions, apply for credit cards or loans, and even file false tax returns. Identity theft victims could suffer from severe emotional suffering, credit score ruin, and substantial financial losses. People must be aware of these online dangers and take preventative action to shield themselves from exposure to unsuitable content, phishing, pharming, cyberbullying, and emotional abuse. This entails using appropriate online conduct, exercising caution when disclosing personal information, and asking for assistance from authorities or reliable adults in the event that you become the target of abuse or harassment online.

1.2. Rationale of the Study

Many youngsters in Kerala utilise several accounts on social media platforms including Instagram, Facebook, WhatsApp, YouTube, Instagram, Telegram, and Snapchat, which makes them more susceptible to cyber abuse and exploitation. In Kerala the students in high schools are accustomed to seeing cyber dangers on their phones and computers [7]. Simple jokes about one's appearance, habits, or any other item that piques a child's curiosity are not inherently harmful, but when the same verbal comments cause a child to experience severe depression, withdrawal symptoms, or even worse academic difficulties, the issue is taken much more seriously than just for fun sake. Due to students' easy access to smart phones and the internet, the situation is more serious because a wider audience may learn the victim's identify. Bullying at school affects students of all ages and academic levels, and it is linked to major mental health problems like suicide, homicide, and other violent crimes. Teenagers are becoming increasingly concerned about the issue of cyber bullying via ICTs like smart phones and the internet. The pandemic has added greatly to the situation. According to Sebastian, et al. [8] the cyber helpline 1930 received 23,888 complaints last year, compared to 5,642 in 2021.Kerala is now ranked fifth nationally. Kerala also records 5% of the total number of cases. Cybercrimes are the most dangerous issues affecting pupils in higher secondary schools in Kerala. Students are becoming more vulnerable to cyber dangers, which is causing issues in the classroom. Both national security and social insecurity are seriously threatened by these issues. The world would be unimaginable without the internet, which is pervasive. Devils use the shadows to their advantage to move stealthily. With every button click, we get closer to them. According to recent polls, cybercrime has dramatically increased in Kerala in a short

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 6: 2583-2590, 2025
DOI: 10.55214/25768484.v9i6.8450

period. Teachers and parents at the upper secondary level are ill-equipped to monitor and shield their pupils from online dangers. Cybersecurity awareness is the only way to combat online scams [9]. *Schools must adopt education and awareness-based programs in order to combat cybercrimes.* One crucial element of cyber security education is e-safety education [10]. It has been argued that Elementary schools should teach students about cybersecurity when using computers. The research indicates that identifying phishing emails and websites is a topic that requires extra attention [11]. Thus, for children to live in a safer cyber world, a comprehensive intervention involving all the important players—children, parents, children's institutions, law enforcement, community-based organizations, and others entrusted with the responsibility of child development and protection is required [7]. Integrating cyber security education into school curricula safeguards their privacy and security and optimizes the internet's full potential [12]. The necessity to re-evaluate the educational factor's negligible significance highlights the existing cyber security education plan. More research is required to determine how successfully cyber security education achieves the stated goal of increasing awareness. Consequently, it is essential to provide Instructional materials that emphasize factors such as mindset and behavioral regulation that favorably impact intentions related to cyber security [11]. Students' e-safety abilities can be enhanced in both formal and informal learning environments with web-based learning environments, which are effective and highly motivating [13]. Previous studies highlight the requirement for an adequate educational intervention.

1.3. Research Aim and Research Questions

Thus, based on the context and rationale of the study, the initial questions raised by the investigator are:

- To what extent do secondary school students of Kerala aware of e-safety?
- To what extent can the instructional package enhance the e-safety awareness level of secondary school students?
- Does the awareness of e-safety among secondary school students differ significantly from one another based on subsamples-gender and locale?

In light of this, the primary goal of the research is to prepare and test an instructional package that edify secondary school students about cyber risks and helps them become responsible online users.

1.4. Research Objectives

1. To determine the effectiveness of the Instructional package for secondary school students in enhancing e-safety awareness

2. To compare the efficacy of the Instructional Package for enhancing e-safety awareness among secondary school students based on gender

3. To compare the efficacy of the Instructional Package in enhancing the e-safety awareness among secondary school students based on locale.

2. Methodology

The primary goal of the research is to create an instructional package to enhance e-safety awareness among secondary school students. The investigator classified this section into two steps by considering the sequential arrangement of research activities. I) Prepare materials for the instructional package on e-safety awareness, and II) Evaluate the prepared package's efficacy. An experimental approach was selected to assess the instructional package's efficacy. A pre-test-post-test design with a single group was employed. The study population includes higher secondary school students in Kerala. The investigator selected 90 secondary school students for experimental purposes, giving weightage to the selected subsamples of the study.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 6: 2583-2590, 2025
DOI: 10.55214/25768484.v9i6.8450

2.1. Tools and Materials Used for the Study

1. Instructional Package for enhancing e-safety awareness
2. e-safety Awareness Test

In the present study, the Instructional package is the independent variable, whereas the secondary school students' awareness of e-safety is the dependent variable. All pertinent research on cyber dangers was considered when creating the e-safety awareness test. Additionally, the researcher gathered qualitative information from educators, administrators, counselors, and cyber cell officers to identify several security threat categories among high school pupils and develop the e-safety awareness test. The indices of validity (0.80) and reliability co-efficient (0.71) show that the cyber threat awareness test is a reasonably valid and reliable tool for finding e-safety awareness among higher secondary school students. The instructional package named ' e-SHIELD'-Safe Handling of Internet and Electronic Devices' covered the various dimensions of e-safety measures regarding devices, operational security, and personal security. The plan of action includes five phases, namely the introductory Phase, the learning phase, the interaction phase, the interim assessment phase, and the conclusion. The package encompasses a range of instructional activities in the classroom, including a questionnaire to assess the student's awareness about e-safety and comprehension of online safety concerns, exposure to educational materials, interactive quizzes, campaigns, an e-safety workshop, open discussions, and evaluation. The main goal of the package is to provide e-safety awareness to students at higher secondary level in Kerala. Here the considered audiences are Students, Teachers, Parents, and Trainers.

2.2. Statistical Techniques used

Statistical techniques are tools used to analyze and interpret data in order to uncover patterns, relationships, and insights within the information collected. These techniques provide a structured way to make sense of complex data sets and draw meaningful conclusions. The statistical techniques used in this study are: Arithmetic mean, Standard deviation, and T-test to compare the means of two groups (Experimental and Control) and determine if their differences are statistically significant.

3. Research Result

The paired "t" test was used to calculate the sample's mean pre-and post-test scores on e-safety awareness. This was done to determine if there was a significant difference between the experimental group's mean pre-and post-test scores in this area. Table 1 displays the data and outcome of the significance test of the difference between means of pre-and post-test scores of the experimental group on cyber threat awareness.

Table 1.
Results of the statistical analysis examining the difference between the experimental group's pre- and post-test averages for e-safety awareness.

Whole Sample	Statistical Indices	Pre test	Post test	MD	t value	Level of Significance
90	Mean	122.4	157.57	35.17	28.14	0.01
	SD	28.61	21.19			

Table 1 yielded a t value of 28.14 ($p<0.01$), indicating statistical significance across all levels. This demonstrates a statistically significant difference between the means of the secondary school pupils in the experimental group's pretest and posttest scores on e-safety awareness. The mean score from the post-test is noticeably higher than the mean score from the pretest. This demonstrates unequivocally how beneficial the teaching package is in raising secondary school pupils' understanding of e-safety.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 6: 2583-2590, 2025
DOI: 10.55214/25768484.v9i6.8450

Table 2.
Comparison of pretest and post-test scores on e-safety awareness of the subsamples.

Groups	N	M(post)	M(pre)	SD1	SD2	t
Boys	39	156.44	119.18	28.88	20.53	21.17
Girls	51	158.9	126.23	28.42	21.46	18.35
Rural	45	156.28	120.83	27.63	21.12	20.37
Urban	45	158.95	123.98	29.68	21.27	18.95

The combined findings from the significance test for the variation in the average pre-and post-test scores on e-safety awareness among the experimental group's subsamples.

The calculated "t" value for the boys in the subsample is significantly higher than the values in the table at every stage. The means of the pretest and post-test scores on the boys' e-safety awareness in the experimental group differ significantly. The resulting "t" values for every other sub-sample are, at every level, significantly higher than the table values. As a result, it is evident that there is a substantial difference between the study's pretest and posttest means for girls' e-safety knowledge in the urban and rural subsamples. All the post-test mean scores are significantly more significant than the corresponding pretest mean scores. This proves the effectiveness of the instructional package in enhancing e-safety awareness among secondary school students based on subsamples.

4. Discussion on Results

The pretest results demonstrated that secondary school students did not have high e-safety awareness. Given that most students spend most of their time on non-educational content, an e-Safety intervention was necessary. The results [14] *which* contend that many citizens are ignorant of and unprepared for the problems of e-Safety, are consistent with this. Also, the findings are in tune with Öğütçü, et al. [15] that the level of awareness is inconsistent and unsatisfactory. The general public is not aware of accepted cybersecurity procedures. Concerning cybercrime-related issues, the government and relevant organizations are not very active. A suitable set of guidelines is necessary. Regarding the effectiveness of the prepared instructional Package, the post-test mean scores were greater than the pretest scores, which shows the enhancement of the e-safety awareness . This is consistent with findings by Bernd, et al. [14] *who found that when students' pre-and* post-test results were compared, there was a statistically significant difference in the experimental group's e-safety performance. The study [14] also offers proof of the web-based learning environment's efficacy and motivational potential for enhancing kids' e-safety knowledge. This environment can be utilised in both formal and informal learning contexts. Regarding the findings with respect to the subsamples all the post test mean scores are significantly greater than the corresponding pretest mean scores. The results of the study by Vishwanath, et al. [16] showed that 16 (24.2%) children attending schools in the city and 6 (11.3%) kids attending schools in the rural lacked enough knowledge of the Internet's functions. In comparison to their rural counterparts, students from urban areas demonstrated a greater understanding of the notion of personal data. Results from the study Vishwanath, et al. [16] also highlights the need for an appropriate educational intervention. Encouraging educators and students to become more knowledgeable about cyber issues is one action that relevant parties could take to shield these groups from emerging cyber security dangers. To safeguard internet users from both prospective cybercrimes and emerging cyber threats, cyber security awareness education is essential. Many researchers think that cyber security education and training are crucial for shielding internet users from cyber security dangers, despite the opinions of some security specialists to the contrary. Since these protective elements are crucial in containing growing cyber security risks, education is the key in addressing them. It is imperative that teacher education programs equip their future educators with the necessary skills to not only teach cyber security principles and safe computing practices, but also to model ethical behaviour and help future generations be safe and secure online. Implementing cyber security instruction in schools is fraught with difficulties due to a lack of resources, financing, and experience. Instructors are neither knowledgeable or skilled in internet. Facilities and resources for implementing

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 6: 2583-2590, 2025
DOI: 10.55214/25768484.v9i6.8450

cyber security education may be lacking in government ministries and schools. The rate at which technology is developing creates new risks that call for new solutions. Instructors may encounter difficulties keeping up with the latest technological advancements and guaranteeing the safety of their students. Teachers face a significant challenge since they must adapt to technological change and lack access to learning resources. Cyber security symposiums should be used to encourage early exposure and training for students in schools. It is thus anticipated that those who receive cyber security training and exposure will be the nation's future supply of cyber defense.

5. Conclusion

Developing instructional initiatives that encourage the responsible use of new technology is crucial. Young people are unaware of the psychological and legal repercussions that their online abuse may have on them, the victims, their families, and their social circles. Creating instructional plans that encourage the responsible use of the new technology is vital. Young people are unaware of the negative effects that their cyber-attacks can have on themselves, the victims, their families, and their social surroundings, as well as the psychological and legal repercussions. Since some of the perpetrators and victims were unaware of the issues with e-Safety, education is therefore a crucial component of e-Safety. Therefore, the primary source of e-Safety concerns was a lack of awareness. All the stakeholders must work together to ensure e-safety. As such, increasing awareness and implementing educational initiatives can greatly help to improve e-Safety. The e-SHIELD Instructional Package helps to make sense of a few important points regarding the growing issue of cyber risks that many districts in Kerala face with regard to teenagers. The Instructional Package helped to shed light on a few important points regarding the cybercrime epidemic that is affecting pupils in several districts of Kerala. It is not acceptable for society to wait for internet safety to be taught in schools or to rely just on parents, who might not be qualified to do so. Teaching kids how to use technology securely is a duty that educators must share with pupils. Both teachers and children can benefit from the package's understanding of proactive online safety. In addition to implementing policies to prevent harassment via digital media, schools should concentrate on teaching children and their families how to use social networking sites responsibly. The awareness on social networking threats on this package can contribute to this problem. Teachers must teach pupils about internet ethics in addition to these crucial topics. Many of the moral conundrums related to cyber safety are resolved by the e-safety dimensions chosen for the Instructional Package. Since prevention is the best form of intervention, this instructional package might serve as a model. Teachers need to become more aware of how schools may help kids build their cyber ethics, cyber citizenship, and cyber safety, which has become one of education's most important but understudied areas. The schools in our country ought to be violent and crime-free havens for instruction and learning. Every incident of any criminal activity or violence in schools impacts the people involved as well as on bystanders, the school, the community at large, and the educational process.

Funding:

The authors offer special gratitude to INTI International University for the opportunity to conduct research and publish the research work. In particular, the authors would like to thank INTI International University for funding the publication of this research work. Also, we extend our heartfelt gratitude to all research participants for their valuable contributions, which have been integral to the success of this study.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Acknowledgments:
The authors thank all the respondents who provided valuable responses and support for the survey. They offer special gratitude to INTI International for publishing the research work, particularly to INTI International University for funding its publication.

References
[1] P. Duggal, *Cyber law books*. Cyberlawbooks.com 2022.
[2] National Crime Records Bureau, *Crime in India ministry of home affairs*. New Delhi: Government of India, East Block-7, R.K. Puram, 2014.
[3] A. A. Al Shamsi, "Effectiveness of cyber security awareness program for young children: A case study in UAE," *International Journal of Information Technology and Language Studies*, vol. 3, no. 2, pp. 8-29, 2019.
[4] E. Vanderhoven, T. Schellens, and M. Valcke, "Exploring the usefulness of school education about risks on social network sites: A survey study," *Journal of Media Literacy Education*, vol. 5, no. 1, p. 2, 2013.
[5] N. Siyam and M. Hussain, "Cyber-safety policy elements in the era of online learning: A content analysis of policies in the UAE," *TechTrends*, vol. 65, no. 4, pp. 535-547, 2021.
[6] L. Cilliers and W. Chinyamurindi, "Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa," *The Electronic Journal of Information Systems in Developing Countries*, vol. 86, no. 4, p. e12131, 2020.
[7] E. M. Jacob, "The extent of cyber exploitation and safety of children in kerala: Report of study on the extent of cyber exploitation and safety of children in kerala," 2022.
[8] S. R. Sebastian, B. P. Babu, and S. Sebastian, "Are we cyber aware? A cross sectional study on the prevailing cyber practices among adults from Thiruvalla, Kerala," *International Journal of Community Medicine and Public Health*, vol. 10, no. 1, pp. 235-239, 2022.
[9] M. Weinberger, M. Zhitomirsky-Geffet, and D. Bouhnik, "Factors affecting users' online privacy literacy among students in Israel," *Online Information Review*, vol. 41, no. 5, pp. 655-671, 2017.
[10] F. Annansingh and T. Veli, "An investigation into risks awareness and e-safety needs of children on the internet: A study of Devon, UK," *Interactive Technology and Smart Education*, vol. 13, no. 2, pp. 147-165, 2016.
[11] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304-312, 2014.
[12] G. M. Abaido, "Cyberbullying on social media platforms among university students in the United Arab Emirates," *International Journal of Adolescence and Youth*, vol. 25, no. 1, pp. 407-420, 2020. https://doi.org/10.1080/02673843.2019.1669059
[13] S. Baller, S. Dutta, and B. Lanvin, *Global information technology report 2016*. Switzerland: Ouranos Geneva, 2016.
[14] J. Bernd, D. Garcia, B. Holley, and M. Johnson, "Teaching cybersecurity: Introducing the security mindset," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2*, 2022, pp. 1195-1195.
[15] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Computers & Security*, vol. 56, pp. 83-93, 2016. https://doi.org/10.1016/j.cose.2015.10.002
[16] A. Vishwanath *et al.*, "Cyber hygiene: The concept, its measure, and its initial tests," *Decision Support Systems*, vol. 128, p. 113160, 2020. https://doi.org/10.1016/j.dss.2019.113160