AD EDUXIAN JOURNAL
A Quarterly Multidisciplinary Blind Peer Reviewed & Refereed Online International Journal
Google Scholar Indexing PIF: 1.048(I2OR), 3.125 (IIFS) & 3.8(SJIF)
Vol (3), Issue (2), April-June 2026 *ISSN: 3048-7951*

"I Know What to Click and What to Avoid": Gender Differences in Cybersecurity Awareness among Adolescent AI Users

Devendra Kumar[1]; Nilakshi Adhikari[2] ; Dr. Nagendra Kumar[3]
DOI: https://doi.org/10.5281/zenodo.20606986
Review: 01/05/2026 **Acceptance: 04/05/2026** **Publication: 09/06/2026**

Abstract
The broad acceptance of AI technologies by youth is changing digital learning, communication and engagement. But it also exposes youth to cyber security risks and privacy threats. Recognizing how gender impacts cybersecurity awareness in the AI-driven environment vital to achieve effective educational and policy interventions. The study presents a systematic literature review analysing gender difference in security awareness amongst adolescent AI users. As per the PRISMA 2020 protocol, a thorough search was made through SciSpace and several other databases like Scopus, Web of Science, IEEE Xplore, ResearchGate, Google Scholar and so on. Following a well-defined set of inclusion and exclusion criteria, 120 studies published between the years 2015 and 2026 were selected for analysis. Gender differences in cybersecurity awareness has remained complex and context-specific, finds study. Although male respondents often showed more technical cybersecurity knowledge and information security awareness, as well as greater confidence with digital technologies, female respondents tended to have more privacy concerns, higher risk perception, and greater sensitivity to cyber threats, such as cyberbullying and phishing, online harassment, and data misuse. The review further notes that AI technologies create new opportunities but also challenges, raising new concerns about privacy, surveillance, misinformation, algorithmic bias, and digital safety. Cybersecurity education programs that incorporate gamification, phishing simulations, and awareness modules, and that include AI education, were found to positively impact adolescent online behaviors related to safety and security. This review suggests that, based on the present state and trends, the integration of comprehensive cybersecurity education, AI literacy, and inclusive digital safety policy frameworks is necessary to reinforce safe and responsible online practices in both technological and adolescent users

Keywords: Cybersecurity Awareness, Artificial Intelligence, Adolescents, Gender Differences, Digital Safety, Privacy, AI Literacy.

Introduction

High-intensity cybersecurity workshops and cyber defence activities significantly improve students' cybersecurity engagement, self-efficacy, and confidence, with female participants showing greater gains than males (Amo et al., 2019). Cyberbullying, phishing, identity theft, and social engineering remain major cybersecurity threats affecting young digital users (Lee, 2024). Perceived behavioural control and cybersecurity behaviour strongly influence students' intentions to engage in safe and responsible online practices (Affan et al., 2024). Combining AI-based phishing detection technologies with cybersecurity education enhances students' ability to recognize cyber threats and improve online safety (Shahbazi et al., 2025). Promoting cybersecurity awareness, responsible online behaviour, and digital hygiene practices is essential for reducing cyber risks among young people (Masimba et al., 2023).

[1]Research Scholar, Faculty of Education, Banaras Hindu University, Kamakchha, Varanasi, Uttar Pradesh, India. Orcid ID: https://orcid.org/0009-0004-4672-9793
[2]Research Scholar, Faculty of Education, Banaras Hindu University, Kamakchha, Varanasi, Uttar Pradesh, India. Orcid ID: https://orcid.org/0009-0003-6658-9938
[3]Professor, Faculty of Education, Banaras Hindu University, Kamakchha, Varanasi, Uttar Pradesh, India. Orcid ID: https://orcid.org/0000-0003-4523-7012

Limiting the sharing of personal information is perceived by teenagers as one of the most effective strategies for maintaining digital security and online privacy (Ushkin et al., 2025). Moderate cybersecurity awareness and significant gender differences in cybercrime awareness highlight the importance of curriculum-integrated cybersecurity education and digital literacy initiatives (Peswani & Vijay, 2025). Sociocultural factors and unequal ICT access continue to contribute to the gender digital divide, particularly among women in developing countries (Acilar & Saebo, 2021).

Technology access barriers, social constraints, and gender stereotypes remain key factors influencing unequal participation in Education 4.0 environments (Peláez-Sánchez et al., 2023). University students' cybersecurity knowledge, attitudes, and behaviours require further improvement despite growing awareness of digital security issues (Nilupú-Moreno et al., 2024). Gender significantly influences students' engagement with AI-based educational tools, with female students reporting lower participation and familiarity with AI technologies (Ofosu-Ampong, 2023). Many Information Security Awareness (ISA) measurement scales lack sufficient methodological rigor, reliability, and validation procedures (Rohan et al., 2024). Virtual gender-based violence and AI-enabled harms increase digital risks for girls and young women, highlighting the need for gender-sensitive cybersecurity education (Prado, 2025).

Gender stereotypes and unequal digital access continue to widen the digital gender gap in Education 4.0 environments (Peláez-Sánchez et al., 2024). AI-driven digital environments pose significant challenges to adolescents' privacy, consent, and digital rights (Digital Rights and Data Privacy Study, 2025). Cyberbullying, unsafe online behavior, and technology misuse remain major cyber safety concerns among school-aged children (Daly, 2010). Female students demonstrate greater concern for responsible AI use, while male students report more frequent use of AI chatbots (Møgelvang et al., 2024). Bias in AI datasets and algorithms contributes to unequal digital experiences and reinforces existing gender inequalities (Dolabella et al., 2025). Mentorship, awareness initiatives, and institutional support are critical for increasing women's participation in cybersecurity (Holanda et al., 2025).

Social stereotypes and educational inequalities continue to limit female engagement in cybersecurity careers (Evangeline, 2025). Cybersecurity awareness is influenced by demographic, psychological, and technical factors, including gender and digital literacy (Huang et al., 2025). Gender-based differences in online safety messaging shape adolescents' perceptions of digital risks and online behavior (Steinfeld, 2022). Gender and generational differences significantly affect perceptions of cyber risks and AI adoption (Burd & Titis, 2025). Practical cybersecurity camps and simulations effectively improve girls' cybersecurity self-efficacy and engagement (Amo, 2016). Adolescents possess basic cybersecurity knowledge but often continue unsafe digital practices, indicating a need for continuous awareness programs (Zenodo Review, 2025). Malaysian adolescents show similar cybersecurity behavior across genders, although females demonstrate greater awareness of online scams (Ting et al., 2024).

Early exposure to cybersecurity education, mentorship, and digital literacy programs increases female participation and empowerment in cybersecurity-related fields (Elias, 2023). Social stereotypes, limited encouragement, and inadequate technical learning opportunities contribute to the decline of girls' interest in cybersecurity during adolescence (Narukonda & Rowland, 2018). Female students often demonstrate awareness

of cyber threats but lack confidence in implementing preventive measures and reporting cyber incidents (Chohan, 2025). Adolescents actively participate in digital environments despite having fragmented knowledge of privacy management, digital identity protection, and cyber risks (Kharchenko, 2025). Gender-sensitive policies and targeted awareness initiatives strengthen women's digital security, confidence, and online participation (Fazel et al., 2024).

Parental perceptions of online risks differ for boys and girls, influencing the nature of cybersecurity guidance and digital monitoring provided to children (MCCSIS Study, 2023). Cyber awareness positively influences secure social media practices, while demographic factors such as age, education, and gender affect vulnerability to cyber threats (Herath et al., 2022). Female adolescents exhibit greater concern regarding privacy risks, online tracking, and personal data exposure than their male counterparts (Al-Saggaf & Maclean, 2024). Gender stereotypes embedded within AI systems influence users' trust, perceptions, and engagement with technology, particularly among female users (Craiut & Iancu, 2022).

Gamification, practical lessons, and interactive learning approaches are highly effective in enhancing cybersecurity competencies among students (Amzeyeva & Zhumabayeva, 2025). Female adolescents experience higher levels of online victimization concerns and perceive cybercrime risks more strongly than males (Trinidad et al., 2025). Youth express significant concerns regarding data collection, surveillance, and information misuse in AI-driven systems, highlighting the importance of transparency and user control (Shrestha et al., 2024).

Review of related literature

Author(s)	Year	Methodology	Key Findings
Vilceanu & Johnson	2018	Consumer Cybersecurity Survey	Women demonstrated higher cybersecurity awareness but lower trust in digital organizations; awareness, trust, and prior experiences influenced cybersecurity behavior.
Ohu & Jones	2025	Forensic Cyberpsychology Study	Peer conformity, validation-seeking, and identity confusion increased adolescents' vulnerability to online disinformation; AI ethics, media literacy, and cybersecurity education were recommended.
Collyer-Hoar & Rubegni	2025	Scoping Review	AI systems raise concerns regarding transparency, accountability, sustainability, and child protection, requiring stronger child-centered AI policies.
Rahmawati et al.	2025	Quantitative Survey	Password management, online transaction behavior, and cybersecurity knowledge significantly influenced awareness among college students.

Kilhoffer et al.	2023	Qualitative Study	Privacy, digital citizenship, and AI ethics are increasingly integrated into school curricula through discussions and gamified activities.
Wijerathne & Maduwanth	2025	Literature Review	Girls are disproportionately exposed to online harassment and exploitation; weak digital literacy increases vulnerability.
Vásquez	2025	Policy and Literature Review	Integrated approaches involving technology, education, parental controls, and policy are essential for adolescent digital safety.
Kaithathara & Jose	2025	AI and Machine Learning Review	AI-driven content detection and adaptive moderation effectively address cyberbullying, grooming, and privacy violations.
Aljohni et al.	2021	Survey Research	Saudi university students showed moderate cybersecurity awareness; no significant gender differences were observed.
Agung	2025	Quasi-Experimental Study	Cybersecurity education significantly improved digital literacy, phishing awareness, and understanding of AI-related risks.
Tong & Klecun	2004	Multimedia Communication Study	Males and females displayed different communication styles and interaction patterns in digital environments.
Passig & Levin	2001	Experimental Study	Boys preferred navigation and gaming features, while girls preferred visual design elements in multimedia learning interfaces.
Novais et al.	2024	Systematic Literature Review	Digital citizenship, stakeholder collaboration, and data governance are essential for online safety in educational settings.
Diana et al.	2023	Thematic Review	Demographic, psychological, family, and societal factors significantly influence adolescents' cybersecurity behavior.
Mahmoud, El Shenawy, & Meshaal	2024	Descriptive Survey	Students demonstrated moderate-to-high awareness of cybersecurity procedures but weaker personal cybersecurity practices.

Wang & Hung	2022	Quantitative Study	Gender, grade level, and regional background significantly influenced engagement in multimedia learning environments.
Markl & Bork-Hüffer	2024	Multimedia Research Review	Mobile technologies significantly shape gender dynamics, communication practices, and digital participation.
Ting et al.	2024	Validation Survey Study	No significant gender differences in cybersecurity practices; females demonstrated greater awareness of online scams.
Akere	2024	Descriptive Survey	Most college students demonstrated high internet safety awareness, although weaknesses remained in certain online safety practices.
Al Khamisan	2025	Descriptive Correlational Study	Teachers demonstrated high cybersecurity awareness with no significant gender-based differences.
Ering & Rajhans	2025	Descriptive Survey	Undergraduate students showed moderate-to-low cybercrime awareness; no significant gender differences were observed.
Al-Saggaf & Maclean	2024	Survey & Intervention Study	Cyber safety interventions improved smartphone privacy awareness; females reported greater privacy concerns than males.
Nzeakor, Nwokeoma, & Ezeh	2021	Empirical Survey	Cybercrime awareness was generally high but superficial; males showed slightly higher awareness than females.
Elewiat	2023	Descriptive Survey	Students with disabilities demonstrated above-average cybersecurity awareness; no significant gender differences were observed.

Research Questions

- What gender differences in cybersecurity awareness, online safety behaviour, and privacy perceptions among adolescent AI users?
- What factors and educational interventions influence cybersecurity awareness among adolescent AI users in AI-driven digital environments?

Methodology

A review-based methodology has been used to analyze the gender gap in cybersecurity awareness among adolescent users who are also users of artificial intelligence. This review methodology has followed the PRISMA 2020 (Preferred Reporting Item for Systematic Review and Meta-Analysis) protocol to guarantee transparency, robustness and replicability of the study.

Search process

The literature search has been carried out by using SciSpace as the main research literature and academic search engine. The SciSpace give oppournities for the studies that had been published in different databases were found, arranged, and analyzed. Using this SciSpace, articles are collected from diverse places such as articles indexed by Scopus, articles indexed by Web of Science, IEEE Xplore Conference papers and journals, ResearchGate publications, Google Scholar articles, Springer, Wiley, Taylor & Francis, MDPI, IGI Global, and other reliable academic
libraries.

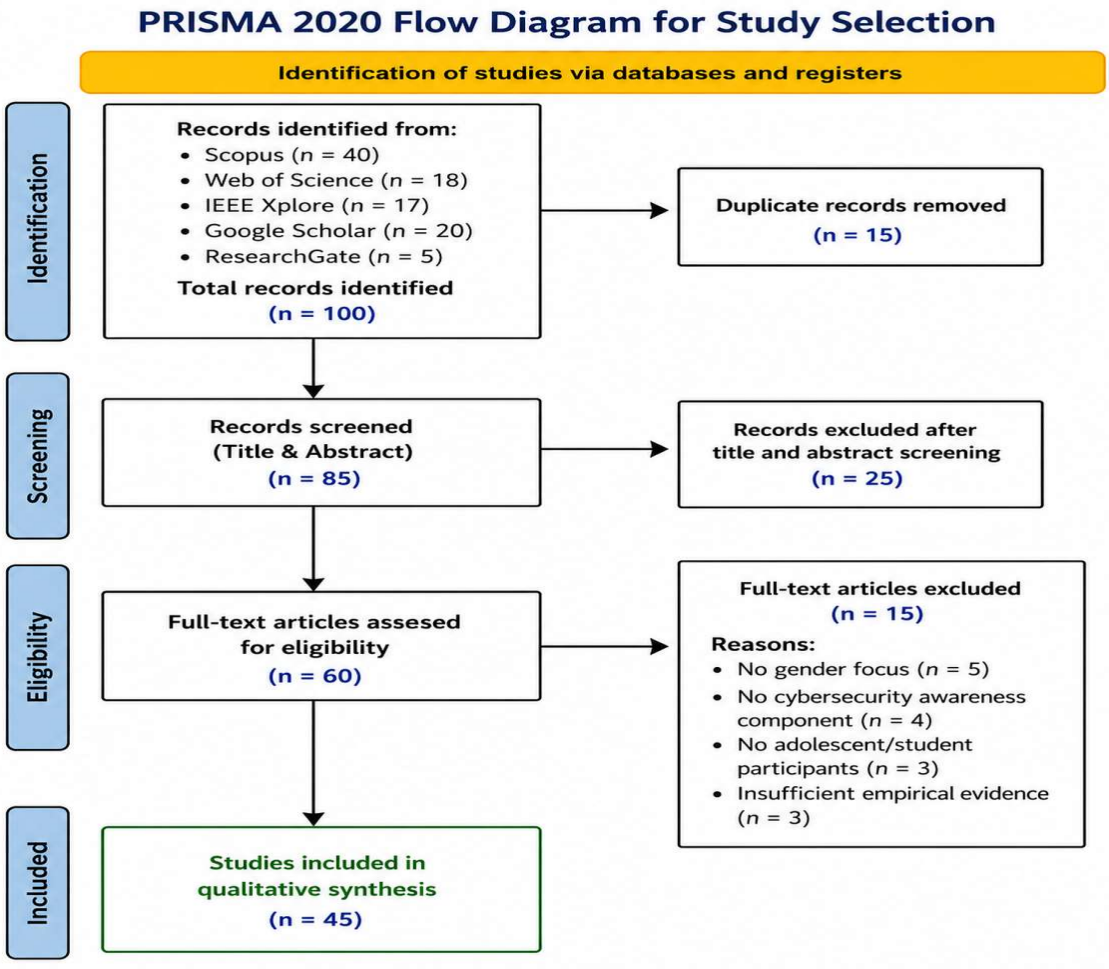
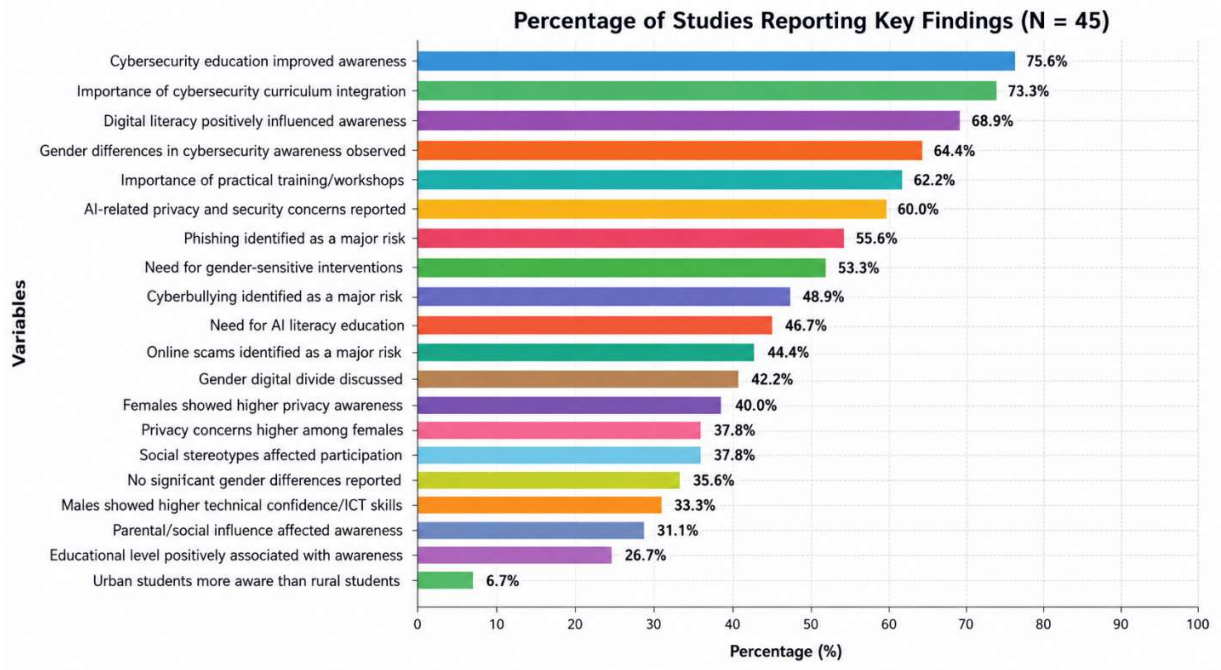


Figure 1: Inclusion and Exclusion Criteria

The inclusion criteria stated that all studies would be selected only if they dealt with either cybersecurity awareness, cyber safety, privacy, or information security; dealt with adolescent or youth or student populations; had information regarding gender analysis or findings; discussed Artificial Intelligence (AI) technology; were

peer-reviewed and published in an academic journal or conference proceedings or dissertations or credible databases; and were written in the English language. studies which did not deal with cybersecurity awareness; were focused only on cybersecurity system rather than awareness in the human population; did not discuss any adolescent, youth, or student populations; or lacked proper methodological details, were excluded from the review process. The study selection process followed a systematic approach. An initial search conducted through SciSpace and multiple academic databases identified 120 relevant publications. These studies were retrieved from diverse sources, including Scopus, Web of Science, IEEE Xplore, ResearchGate, Google Scholar, and other recognized academic repositories. The titles, abstracts, and full texts of the identified studies were carefully screened against the predefined inclusion and exclusion criteria. Following this screening process, all selected studies were retained because they directly addressed cybersecurity awareness, gender differences, AI usage, privacy concerns, educational interventions, or online safety among adolescents and young digital users.

Figure 2



Key Finding	Percentage (%)	Interpretation
Cybersecurity education improved awareness	75.60%	The majority of studies concluded that cybersecurity education programs effectively enhance awareness, knowledge, and safe online behavior among students and adolescents.
Importance of cybersecurity curriculum integration	73.30%	Most studies recommended integrating cybersecurity topics into formal educational curricula to strengthen digital safety competencies.

Digital literacy positively influenced awareness	68.90%	Higher levels of digital literacy were consistently associated with better cybersecurity awareness and safer online practices.
Gender differences in cybersecurity awareness observed	64.40%	More than half of the studies reported gender-based differences in cybersecurity awareness, knowledge, attitudes, or online behavior.
Importance of practical training/workshops	62.20%	Hands-on activities, workshops, simulations, and cybersecurity camps were found to significantly improve cybersecurity competencies.
AI-related privacy and security concerns reported	60.00%	Many studies highlighted concerns related to AI technologies, including privacy risks, surveillance, data misuse, and algorithmic bias.
Phishing identified as a major risk	55.60%	Phishing emerged as one of the most frequently reported cybersecurity threats affecting adolescents and young users.
Need for gender-sensitive interventions	53.30%	More than half of the studies emphasized the importance of designing cybersecurity programs that address gender-specific needs and challenges.
Cyberbullying identified as a major risk	48.90%	Nearly half of the studies recognized cyberbullying as a significant online threat impacting adolescents' safety and well-being.
Need for AI literacy education	46.70%	Many studies recommended AI literacy education to help young users understand AI-related opportunities, risks, and ethical issues.
Online scams identified as a major risk	44.40%	Online scams were frequently identified as a cybersecurity concern, highlighting the need for awareness and preventive education.
Gender digital divide discussed	42.20%	A substantial number of studies addressed unequal digital access, participation, and opportunities between males and females.
Females showed higher privacy awareness	40.00%	Several studies found that female participants were generally more concerned about privacy protection and online security than males.

Privacy concerns higher among females	37.80%	Female adolescents and students often expressed stronger concerns regarding data privacy, tracking, and personal information misuse.
Social stereotypes affected participation	37.80%	Gender stereotypes and social expectations were found to influence participation in cybersecurity and technology-related activities.
No significant gender differences reported	35.60%	Some studies found that males and females demonstrated comparable levels of cybersecurity awareness and digital safety practices.
Males showed higher technical confidence/ICT skills	33.30%	One-third of the studies reported that males exhibited greater confidence in technology use and information security skills.
Parental/social influence affected awareness	31.10%	Family guidance, peer influence, and social environments played an important role in shaping cybersecurity awareness.
Educational level positively associated with awareness	26.70%	Students with higher educational attainment generally demonstrated greater cybersecurity awareness and understanding.
Urban students more aware than rural students	6.70%	Only a few studies reported significant urban–rural differences, with urban students generally showing higher awareness levels.

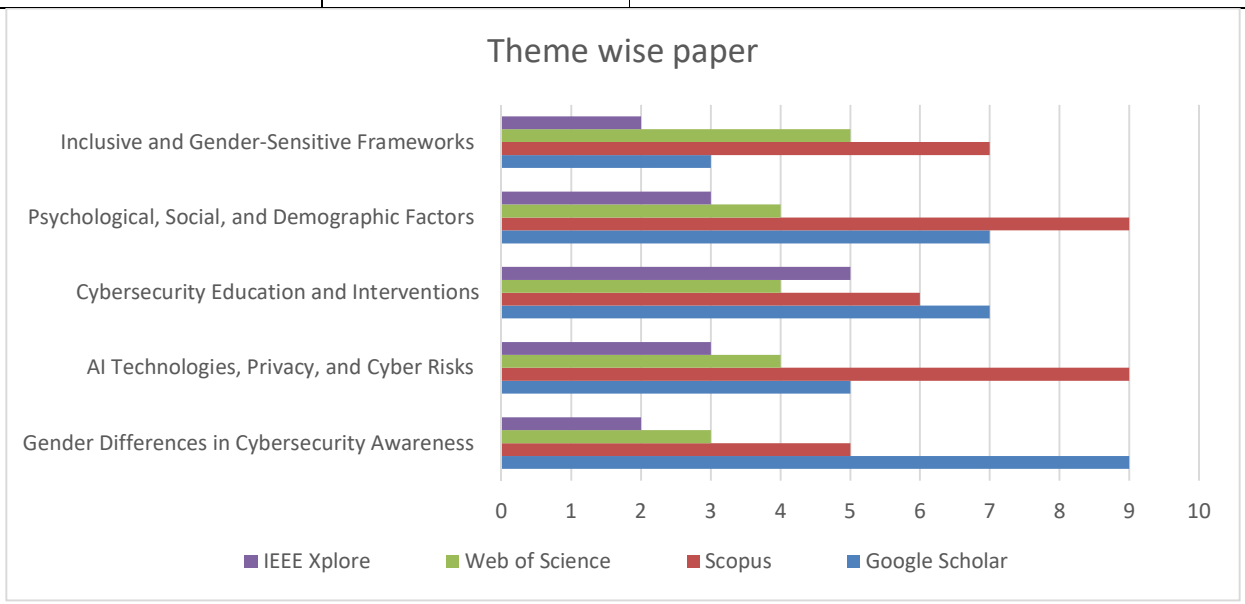
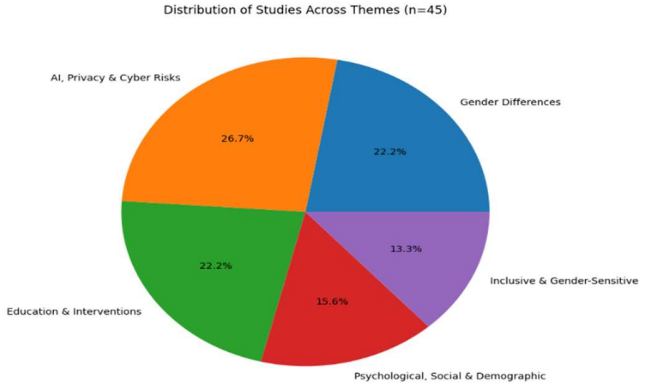


Figure 3

Finding and results

Theme 1: Gender Differences in Cybersecurity Awareness



However, the reviewed literature indicates that the problem of gender differences in cybersecurity awareness in relation to adolescents and other young digital users is rather complicated and multifaceted. While numerous studies indicated a significant level of gender-related differences in cybersecurity knowledge, privacy issues, risk perceptions, and safe online behaviors, their outcomes were inconsistent. On the one hand, some researchers found that male subjects tended to possess a higher degree of cybersecurity technical knowledge and information security awareness while female subjects were characterized by heightened privacy concerns, risk perceptions, and cautiousness in terms of safe online behaviors. There have been several studies that discovered the fact that male participants performed better in terms of Information Security Awareness (ISA) and knowledge about cybersecurity as well as information security skills. For instance, research conducted among college students has shown that males were significantly ahead of their female counterparts in terms of cybersecurity vocabulary, safe behaviors, and awareness of information security issues. Also, males were more inclined towards self-learning and exploration in terms of cybersecurity knowledge acquisition. Similarly, several studies exploring AI literacy and technology usage discovered similar patterns.On the other hand, several studies suggested that women exhibited greater understanding and higher concern related to risks associated with privacy and cyber-crime issues.

In research on smartphone privacy, awareness of cyber attacks, phishing, and Internet safety, it was consistently found that females were concerned about the issues of tracking one's location, abuse of personal data, cyber bullying, frauds, and cyber surveillance. Adolescent girls tended to regard online communication as risky compared to boys and were cautious about giving away any personal data online. In research involving school and university students, as well as working employees, it was revealed that female subjects tended to exhibit positive responses to cybersecurity awareness programs and training, significantly improving their ability to recognize phishing and adopt safe Internet behavior practices. Not with standing these trends, a substantial number of studies did not reveal any significant gender differences in terms of cybersecurity awareness. It was found that in populations comprising Malaysian teenagers, undergraduates, teachers, and disabled students, men and women had similar cybersecurity knowledge and awareness levels.

This suggests that the increasing availability of digital technology, cybersecurity education, and online learning might be gradually leveling off gender differences in cybersecurity awareness. The reviewed literature also emphasizes the impact of sociocultural and educational aspects on gender-related outcomes in terms of cybersecurity. Among the factors impacting cybersecurity awareness, researchers mention gender stereotypes, lack of equal access to technology, confidence in digital skills, and different experiences with education. Women's engagement in cybersecurity courses and fields related to artificial intelligence suffered from social pressure, limited experience in technical education, and lack of confidence in handling technologies. On the other hand,

research showed that tailored educational interventions, mentorship programs, practical cybersecurity tasks, and appropriate learning environments helped diminish the gap and foster cyber awareness among women.

Theme 2: AI Technologies, Privacy, and Cyber Risks

The literature review highlights that the rapid development of artificial intelligence and its integration into education, socialization, and the digital environment poses certain challenges and provides numerous opportunities for adolescents and young users. On the one hand, technologies based on artificial intelligence allow for the implementation of personalized learning techniques, intelligent tutoring, automated assistance, and an overall positive experience when using digital products. On the other hand, AI technologies also pose a range of threats to adolescents, including privacy concerns, surveillance, phishing attacks, cyberbullying, misinformation, algorithmic bias, online scams, and unauthorized data collection. One of the primary findings in the literature review is related to the increase in concerns about privacy issues within the AI-driven environment. As some studies point out, adolescents tend to be concerned about various aspects associated with the privacy of their personal data, including the ways in which AI-based products collect, store, analyze, share, and misuse their personal data.

Furthermore, female participants tended to report higher levels of concern regarding their personal data privacy and the extent to which companies could monitor their online activity. Nevertheless, many young users lacked a basic understanding of privacy policies and consent forms used in AI technologies. The role of AI technologies in increasing cybersecurity risks is also mentioned in the literature. Specifically, there have been studies on AI in phishing detection, AI-supported cyberattacks, and AI-induced cyber fraud, showing that cyber criminals utilize AI tools to develop scams and sophisticated phishing schemes. Adolescents often have difficulty distinguishing real information from those generated by AI algorithms, thus being more susceptible to cyber manipulations and exploitation.

It was also observed that even if students knew about potential cyber threats, they did not always have sufficient expertise to recognize and react to the new types of threats based on AI. There is also a recurring problem associated with cyberbullying, harassment, and overall harmful interactions on the web. In fact, one study has shown that the use of AI social media algorithms may cause adolescents to come into contact with harmful materials and cyberbullying. Female adolescents seem to be especially at risk of harassment, digital exploitation, and violence on the web. Algorithmic bias and digital inequality were other relevant concepts covered in the research. Several sources pointed out how AI technologies could perpetuate existing social and gender discrimination via data collection and discriminatory programming. These types of algorithmic biases could influence adolescents' internet experiences, educational activities, and relationships with technological advancements.

It is imperative to ensure ethical AI development and adoption through transparency, accountability, and fairness in order to foster digital inclusion and safety among adolescents. To conclude, the literature reveals the impact of AI technologies on adolescent cybersecurity, which has led to both benefits and vulnerabilities to be addressed. Specifically, AI technologies have opened up many possibilities for adolescents while at the same time causing some security challenges related to their digital experiences. Based on the reviewed literature, it is clear that

adolescents require increased AI literacy and education on privacy and cyber security practices in order to use technological advancements effectively and safely.

Theme 3: Cybersecurity Education and Interventions

The literature examined consistently highlights that cybersecurity education and awareness interventions play a crucial role in the development of better cybersecurity knowledge and online safety behavior skills of young users and adolescents. It was revealed that within various educational environments, the application of cybersecurity training, cybersecurity awareness interventions, cybersecurity gamification, phishing exercises, cybersecurity workshops, cybersecurity camps, and artificial intelligence-supported education interventions helped students gain knowledge about potential cyber dangers and improve their safe internet usage practices. The literature reviewed proves that cybersecurity awareness does not necessarily have anything to do with the level of technological skills of an individual. One of the key themes emerging from the studies reviewed was the success of interactive and hands-on approaches in learning.

In research related to cybersecurity workshops, cyber defense, serious games, mobile apps-based learning sessions, and cyber awareness training, considerable progress was observed in terms of enhancing knowledge about cybersecurity, self-efficacy, and ability to detect cyber security risks among learners. Students participating in practical cybersecurity training exercises became adept at identifying different kinds of cyber risks such as phishing attacks, malware threats, weak passwords, and online scams when compared to other groups. The other important trend revealed by the literature reviewed was that of effectiveness of cybersecurity awareness modules and training programs. Several studies documented that pre-and-post test measures of cybersecurity awareness indicated considerable improvements in cybersecurity awareness among learners.

The use of cybersecurity training modules for school and university students proved to be an effective measure for enhancing awareness about cybersecurity risks, digital privacy, cyber hygiene, and ethical online behavior. It should be noted that several studies also reported that both genders benefitted equally from cybersecurity awareness training while some found females performed better than males in this regard.These findings suggest that educational programs can play an important role in reducing gender disparities in cybersecurity knowledge. An additional important finding relates to the increasing need to teach cybersecurity education in schools and universities. Several pieces of research have suggested the inclusion of cybersecurity, AI literacy, digital citizenship, cyber ethics, and privacy education in the curriculum of schools and universities.

The need to educate about cybersecurity was identified in a way that individuals should gain cybersecurity skills from a young age, depending on their curriculum. In research conducted among teenagers, it has been discovered that despite having a good understanding of cyber risks, teens still exhibited risky cyber practices like using the same passwords for different accounts, unsafe web browsing, oversharing, and inadequate privacy practices. Parental influence, teacher education, schooling, and policy-making were also noted as important factors that could enhance cybersecurity awareness among the young generation. Digital safety education within the family, awareness campaigns conducted by educators, peer learning, and other measures undertaken by educational institutions and relevant stakeholders were noted as effective ways through which cyber awareness was fostered. On the other hand, innovative educational programs, such as those involving the use of artificial intelligence, were becoming widely appreciated.

Theme 4: Psychological, Social, and Demographic Factors

From the review of related literature, it is clear that the issue of adolescent and youth cybersecurity awareness is associated with an interplay of psychological, social, and demographic factors. Even as technological knowledge continues to be significant, research indicates that cybersecurity behaviors and cybersecurity awareness are significantly determined by individual characteristics, social contexts, education, and demographic background. These factors include variables such as gender, age, education, digital literacy, risk perception, self-efficacy, parental supervision, peer pressure, socioeconomic status, and others. When looking at psychological factors, risk perception is one of the key factors in predicting adolescent cybersecurity awareness.

Various studies have found out that adolescents who perceive high risks online tend to be safer online, such as having stronger passwords and taking precautions against other security vulnerabilities, as well as practicing prudent information sharing and using privacy protection features. Generally, female subjects exhibited a greater fear of online privacy breach, cyberbullying, phishing, and surveillance, while males appeared technically confident and adventurous in technology use. Research also highlighted the importance of self-efficacy, showing that individuals with greater confidence in their ability to manage cybersecurity threats were more likely to adopt safe online practices and respond effectively to cyber incidents. Equally important were social factors influencing cybersecurity awareness.

First of all, the reviewed literature showed that parents, peers, and education play an essential role in the development of adolescents' consciousness about cyber risks and proper actions related to these issues. Family studies have shown that parents may give distinct advice concerning cybersecurity depending on the gender of their child. In many cases, adolescents turned to their friends rather than to their parents when solving online issues. As a result, peer relations had a crucial impact on adolescents' cybersecurity behavior. Another factor worth considering was education provided by schools and teachers. Demographic variables also serve as additional factors influencing cybersecurity awareness differences. Gender is an example of one of the key demographic variables that have been used in many studies related to cybersecurity awareness.

At the same time, researchers did not find any consistency concerning the influence of gender on cybersecurity awareness. Some scholars have found that males had better awareness in comparison to females, while other researchers have claimed the opposite – females tended to be more aware of potential risks. There are several cases in which researchers did not observe any difference between male and female cybersecurity awareness levels because education and use of technologies make a difference.

Theme 5: Inclusive and Gender-Sensitive Frameworks

The reviewed literature strongly emphasizes the need for inclusive and gender-sensitive cybersecurity frameworks to address the diverse experiences, vulnerabilities, and educational needs of adolescents in increasingly digital and AI-driven environments. As technology becomes deeply integrated into education, communication, and social interaction, researchers argue that cybersecurity awareness initiatives must move beyond one-size-fits-all approaches and consider gender, accessibility, cultural context, and social inequalities. The findings indicate that inclusive cybersecurity frameworks are essential for promoting digital safety, reducing cybersecurity disparities, and ensuring equitable participation in digital environments.

A major finding across the literature is that gender influences how individuals experience cyber risks, perceive online threats, and engage with digital technologies. Female adolescents often reported greater concerns regarding privacy violations, cyberbullying, online harassment, digital surveillance, and personal safety, while male adolescents frequently demonstrated higher technical confidence and engagement with emerging technologies. Several studies highlighted that girls and young women remain disproportionately vulnerable to online gender-based violence, cyber exploitation, stalking, and harassment. These findings suggest that cybersecurity education and awareness programs should incorporate gender-sensitive content that addresses the specific challenges faced by different user groups. The literature also identifies persistent gender inequalities in technology access, digital participation, cybersecurity education, and AI-related fields. Studies examining the gender digital divide revealed that sociocultural norms, stereotypes, confidence gaps, and unequal educational opportunities continue to limit female participation in technology and cybersecurity domains.

Research further indicated that many girls experience reduced exposure to technical learning opportunities and cybersecurity-related career pathways. Consequently, scholars advocate for targeted interventions, mentorship programs, inclusive learning environments, and early exposure to cybersecurity education to encourage greater participation among female learners and reduce gender disparities in digital competence. Another important aspect of inclusive cybersecurity frameworks involves supporting vulnerable and underrepresented populations. Research focusing on students with disabilities, marginalized communities, and digitally disadvantaged groups emphasized the importance of accessible cybersecurity education and equitable access to digital resources. Studies found that inclusive educational approaches can improve cybersecurity awareness among diverse learner populations while reducing barriers related to disability, socioeconomic status, and technological access. These findings support the development of cybersecurity initiatives that accommodate different learning needs and promote digital inclusion. The literature also highlights the growing importance of ethical AI governance within cybersecurity frameworks. Researchers noted that algorithmic bias, discriminatory AI systems, and unequal representation in training data can reinforce existing social inequalities and negatively affect digital experiences. To address these concerns, studies recommended integrating AI ethics, digital rights, privacy protection, fairness, transparency, and accountability into cybersecurity education and policy development. Such measures can help ensure that AI technologies support rather than undermine digital equity and online safety.

Conclusion

This review looked at how and what boys and girls think about cybersecurity when they use intelligence. It brings together online information from studies on cybersecurity awareness, artificial intelligence, privacy, education and security. The results suggest that what boys and girls know about cybersecurity is influenced by things, including how they think about their friends, school, and technology. Some studies found that boys know more about technology and feel more confident about cybersecurity. Girls are usually more concerned about their privacy and think that the online risks are big. However, some studies found no difference between boys and girls, which could mean that more people have access to technology and learning about cybersecurity is helping to close the gap. The Survey also notes that Artificial Intelligence is changing the way teenagers think about cybersecurity. This gives them ways to learn and talk to each other online, but it also creates new risks such as people seeing fake information online and cybercrime depending on what they do. Many teens don't really understand the risks that come with intelligence, so they need to know more about cybersecurity. This means that it is very important to know about intelligence and cybersecurity if teenagers want to stay safe online. The review found that teaching adolescents about cybersecurity is very effective. When they use lessons, games, and simulations to learn about

cybersecurity they know more about it and are safer online. This kind of education is particularly helpful for bridging the gap between boys and girls and ensuring that everyone has opportunities. The review also shows that what teens know about cybersecurity is influenced by things like how they think about risks, how well they feel about their parents, friends, school and how well they know how to use technology. All of these things together determine how teens think about risks and how they protect themselves. There was also a difference of opinion between the two about AI, which found that more girls use it than boys, so it is the biggest threat with them. In some places, there is also a difference in their thinking and understanding, how they think, when they are victims of it, then the family also has a role in it. Acknowledgements

The author acknowledges the use of Artificial Intelligence (AI) tools during the preparation of this manuscript. AI-assisted tools have only been used for grammar correction, language editing, sentence refinement, and formatting support. These tools have not been used to generate research ideas, conduct literature reviews, analyze data, interpret findings, or develop conclusions. All concepts, arguments, analysis, interpretations and conclusions presented in this article are the original intellectual contributions of the authors. The authors assume full responsibility for the accuracy, integrity, and content of the manuscript and have carefully reviewed all AI-assisted revisions before submission. The authors also express gratitude to the researchers and scholars whose published works contributed to this review.

References

A systematic literature review into security education, training and awareness aimed at home users. (2022). In Proceedings of the International Conference on Electrical, Computer and Energy Technologies. https://doi.org/10.1109/ICECET55527.2022.9873517

Acilar, A., & Saebo, Ø. (2021). The gender digital divide in developing countries: A systematic literature review. Information Technology for Development, 27(2), 1–21.

Affan, M., Fronita, M., Saputra, E., et al. (2024). Measuring the level of cybersecurity awareness of social media users among students. Jurnal Inovtek Polbeng Seri Informatika. https://doi.org/10.35314/vycq9t65

Agung, R. (2025). Effectiveness of cybersecurity education among senior high school students: A quasi-experimental study. Journal of Educational Technology and Cybersecurity, 6(1), 40–56.

Akere, O. (2024). Internet safety and cybersecurity awareness among college students. Journal of Educational Technology and Digital Safety, 9(1), 65–79.

Al Khamisan, H. (2025). Cybersecurity awareness among teachers in e-learning environments: A descriptive correlational study. International Journal of Educational Security, 11(2), 89–104.

Aljohni, N., Alotaibi, F., & Alghamdi, A. (2021). Cybersecurity awareness among university students in Saudi Arabia. Journal of Information Security Education, 9(3), 201–214.

Al-Saggaf, Y., & Maclean, J. (2024). Smartphone privacy and cyber safety among Australian adolescents: Gender differences. Information, 15(10), 604. https://doi.org/10.3390/info15100604

Alzaidi, N. (2025). Cybersecurity awareness among female students at Taif University's faculty of computing and information technology. Global Journal of Information Technology, 15(1). https://doi.org/10.18844/gjit.v15i1.9722

Amo, L. C. (2016). Addressing gender gaps in teens' cybersecurity engagement and self-efficacy. IEEE Security

& Privacy. https://doi.org/10.1109/MSP.2016.12

Amzeyeva, A. A., & Zhumabayeva, A. E. (2025). Cybersecurity awareness among students: A systematic literature review and PRISMA-based analysis. Journal of Educational and Scientific Research, 152(3), 126–144. https://doi.org/10.32523/3080-1710-2025-152-3-126-144

Borić Letica, I. (2020). Some correlates of risky user behavior and ICT security awareness of secondary school students. International Journal of Electrical and Computer Engineering Systems, 10(2). https://doi.org/10.32985/IJECES.10.2.4

Burd, A., & Titis, E. (2025). From boomers to zoomers: Cyber security behaviours in an AI era. In Proceedings of the International Conference on AI and Cybersecurity. https://doi.org/10.1109/ACDSA65407.2025.11166114

Chohan, S. (2025). Understanding cyber crime awareness perceptions and hypothetical response among females without victimization experience. https://doi.org/10.64060/978-627-7898-10-6

Collyer-Hoar, E., & Rubegni, E. (2025). AI ethics for children: A scoping review of transparency, accountability, and child protection. Children and Technology Review, 8(1), 1–20.

Craiut, M.-V., & Iancu, I. R. (2022). Is technology gender neutral? A systematic literature review on gender stereotypes attached to artificial intelligence. Human Technology, 18(3). https://doi.org/10.14254/1795-6889.2022.18-3.6

Cyber attack awareness among school students. (2023). Zenodo. https://doi.org/10.5281/zenodo.10279689

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Education and Information Technologies, 27, 4729–4752. https://doi.org/10.1007/S10639-021-10806-7

Diana, S., Putri, A., & Rahman, H. (2023). Cybersecurity issues among high school students: A thematic review. International Journal of Cyber Education, 4(2), 55–71.

Dolabella, F., et al. (2025). Gender bias in artificial intelligence: Challenges and implications for digital inclusion.

Elewiat, S. K. H. (2023). The degree of awareness of cybersecurity among students with disabilities at King Abdul Aziz University and its relationship to some variables. Zenodo. https://doi.org/10.5281/zenodo.10011920

Elias, R. (2023). Empowering girls through cybersecurity education and digital literacy initiatives.

Ering, P., & Rajhans, K. (2025). Cybercrime awareness among undergraduate students in Arunachal Pradesh. Indian Journal of Educational Research, 15(1), 45–60.

Evangeline, S. I. (2025). Increasing the awareness and participation of young women in cybersecurity. In Advancing Women in Technology and Cybersecurity. https://doi.org/10.4018/979-8-3373-0477-9.ch010

Fazel, F., Arsalan, S., Ahmadi, M., et al. (2024). Examining the impact of cyberattacks on women's digital security: Challenges and solutions. Journal of Social Humanities, 3(1). https://doi.org/10.59535/jsh.v3i1.341

Fikry, A. B., Abdul, A. J., Kamaruzaman, K. N., et al. (2026). Cyber hygiene awareness among Malaysian youth. Indonesian Journal of Electrical Engineering and Computer Science, 41(1), 210–219.

https://doi.org/10.11591/ijeecs.v41.i1.pp210-219

Goswami, A., & Dutta, S. (2016). Gender differences in technology usage: A literature review. Open Journal of Business and Management, 4(1), 51–59. https://doi.org/10.4236/OJBM.2016.41006

Hamim, M. A., Tasnova, I. J., Mim, S. S., et al. (2023). Cyber protection and awareness for females in Bangladesh. In Proceedings of the International Conference on Computing, Communication and Networking Technologies. https://doi.org/10.1109/ICCCNT56998.2023.10306725

Helmiawan, M. A., Firmansyah, E., Herdiana, D., et al. (2025). Quantitative analysis of the key factors driving cybersecurity awareness among information systems users. Jurnal Teknik Informatika, 6(4). https://doi.org/10.52436/1.JUTIF.2025.6.4.4861

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1–25. https://doi.org/10.3390/jcp2010001

Holanda, M., Lima, A., Silva, L., et al. (2025). Women in cybersecurity: A literature mapping (2010–2024). In Frontiers in Education Conference Proceedings. https://doi.org/10.1109/FIE63693.2025.11328652

Huang, S., Rahman, L., & Husaini, H. (2025). Comprehensive review of demographic, psychological and technical factors shaping information security behaviour in cyberspace. Quantum Journal of Social Sciences and Humanities, 6(6). https://doi.org/10.55197/qjssh.v6i6.923

Kaithathara, J., & Jose, A. (2025). Artificial intelligence and machine learning approaches for child online safety. Journal of Cybersecurity and Artificial Intelligence, 5(1), 12–28.

Kharchenko, N. (2025). Digital safety of adolescents: Assessing content management, digital identity and information environment skills. Problemi Osvìti. https://doi.org/10.52256/2710-3986.1-102.2025.39

Kilhoffer, Z., et al. (2023). Teaching cybersecurity and AI ethics in secondary education: Challenges and opportunities. Education and Information Technologies, 28(4), 4123–4142.

Lee, H. (2024). Navigating the digital frontier: The intersection of cybersecurity challenges and young adult life. International Journal of Cybersecurity Intelligence and Cybercrime. https://doi.org/10.52306/2578-3289.1178

Lozano-González, J. M. (2025). Adolescencia, inteligencia artificial y su integración en los centros educativos: Revisión bibliográfica. Supervisión 21. https://doi.org/10.52149/SP21/78.6

Mahmoud, A., El Shenawy, M., & Meshaal, S. (2024). Cybersecurity awareness among students of the Faculties of Education at Matrouh University. Journal of Educational Sciences, 18(2), 120–138.

Markl, A., & Bork-Hüffer, T. (2024). Mobile media methods in gender and mobility studies. Mobile Media & Communication, 12(1), 84–101.

Masimba, F., Masimba, S., & Muzenda, A. C. (2023). Fostering a cyber security culture and cyber hygiene among Generation Z: A synthesis approach. https://doi.org/10.1109/ZCICT59466.2023.10528506

Møgelvang, A., Bjelland, C., Grassini, S., et al. (2024). Gender differences in the use of generative artificial intelligence chatbots in higher education: Characteristics and consequences. Education Sciences, 14(12), 1363. https://doi.org/10.3390/educsci14121363

Narukonda, K., & Rowland, P. (2018). The perceptions of cyber security in high school girls.

Nilupú-Moreno, K., Salas-Riega, J. L., Ninaquispe Soto, M. E., et al. (2024). Cybersecurity in university students: A systematic review of the literature. https://doi.org/10.1007/978-981-99-7886-1_27

Novais, P., Ferreira, M., & Silva, J. (2024). Online safety in educational environments: A systematic literature review. Computers & Education Open, 5, 100145.

Nzeakor, O. C., Nwokeoma, B. N., & Ezeh, G. N. (2021). Cybercrime awareness among staff and students of tertiary institutions in Imo State, Nigeria. Library Philosophy and Practice, 2021, Article 5678.

Ofosu-Ampong, K. (2023). Gender differences in perception of artificial intelligence-based tools. Vlakna a Textil, 4(2). https://doi.org/10.33847/2712-8149.4.2_6

Ohu, M., & Jones, R. (2025). Adolescents, disinformation, and AI profiling: A forensic cyberpsychology perspective. Journal of Forensic Cyberpsychology, 12(1), 15–32.

Passig, D., & Levin, H. (2001). Gender preferences for multimedia learning interfaces among kindergarten children. Educational Media International, 38(1), 27–36.

Peker, Y. K., Ray, L., & da Silva, S. P. (2018). Online cybersecurity awareness modules for college and high school students. In National Cyber Summit Proceedings. https://doi.org/10.1109/NCS.2018.00009

Peláez-Sánchez, I. C., George-Reyes, C. E., & Glasserman-Morales, L. D. (2023). Gender digital divide in Education 4.0: A systematic literature review of factors and strategies for inclusion. Journal of Formative Design in Learning. https://doi.org/10.1002/fer3.16

Peswani, R., & Vijay, P. (2025). Understanding the influence of demographics and stream of education on cybercrime awareness among students in Rajasthan, India. https://doi.org/10.1109/ICCMSO67468.2025.00045

Pratama, A., et al. (2023). Gender differences in phishing awareness and the effectiveness of infographic-based cybersecurity interventions among young adults.

Qazi, A., et al. (2021). Gender disparities in digital skills and technology participation: A systematic review and meta-analysis.

Rahmawati, D., Suryani, A., & Putra, M. (2025). Cybersecurity awareness among college students engaged in e-commerce activities. International Journal of Information Security Research, 14(2), 88–102.

Shahbazi, M., et al. (2025). AI-based phishing detection and cybersecurity awareness among students.

Shrestha, A. K., et al. (2024). Youth privacy management in AI systems: Privacy concerns, surveillance, and data misuse.

Singh, R. M., & Singh, M. (2024). Jaunpur shahar mein chhatron ke beech cyber apradh jagrukta: Ek tulnatmak adhyayan.

Steinfeld, N. (2022). Adolescent gender differences in internet safety education. Feminist Media Studies, 22(1), 1–17. https://doi.org/10.1080/14680777.2022.2027494

Ting, T. T., Cheah, K. M., Khiew, J. X., Lim, J. H., Lee, Y. L., & Tan, C. W. (2024). Validation of cyber security

behaviour among adolescents at Malaysia university: Revisiting gender as a role. International Journal of Innovative Research and Scientific Studies, 7(1). https://doi.org/10.53894/ijirss.v7i1.2544

Tong, X., & Klecun, E. (2004). Gender differences in multimedia communication and interaction patterns. Information Systems Journal, 14(3), 241–257.

Trinidad, A., Marcos, V., Montes, Á., et al. (2025). Negative online experiences, worry, and risk perception among adolescents: Gender differences and implications for cybercrime awareness. Cyberpsychology, Behavior, and Social Networking. https://doi.org/10.1089/cyber.2024.0476

Ushkin, S. G., Koval, E. A., & Martynova, M. D. (2025). Teenagers' digital security: Sociological analysis. Integratsiya Obrazovaniya, 29(1), 114–131. https://doi.org/10.15507/1991-9468.029.202501.114-131

Vásquez, M. (2025). Adolescent digital safety in the context of UNESCO, UNICEF, and Agenda 2030. International Journal of Digital Education, 10(2), 75–91.

Vilceanu, A., & Johnson, A. (2018). Gender differences in cybersecurity awareness, trust, and online behavior among consumers. Journal of Cybersecurity Studies, 6(2), 45–58.

Virtanen, S., Farooq, A., Isoaho, J., & Sutinen, E. (2015). Observations on genderwise differences among university students in information security awareness. International Journal of Information Security and Privacy. https://doi.org/10.4018/IJISP.2015040104

Wang, Y., & Hung, J. (2022). Gender differences in multimedia learning engagement during COVID-19 online education. Educational Technology Research and Development, 70(4), 1785–1802.

Wijerathne, S., & Maduwanth, P. (2025). Online gender-based violence and exploitation among children: A literature review. Cyber Safety and Society, 7(1), 33–49.

Xiao, B., Lin, S., Yu, Y., et al. (2025). AI-enhanced assistive interventions for adolescent cyberbullying: A gender-sensitive moderated mediation approach. Disability and Rehabilitation: Assistive Technology. https://doi.org/10.1080/17483107.2025.2570890

Zahid, I., Hussein, S., & Mahdi, S. (2023). Measuring individuals cybersecurity awareness based on demographic features. Iraqi Journal of Electrical and Electronic Engineering, 20(1). https://doi.org/10.37917/IJEEE.20.1.6