Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences

Abdulrahman Abdullah Arishi[1], Nazhatul Hafizah Kamarudin[2], Khairul Azmi Abu Bakar[3], Zarina Binti Shukur[4], Mohammad Kamrul Hasan[5]

Master's Degree in Cybersecurity, Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi, Selangor[1]
Research Coordinator, CYBER, Universiti Kebangsaan Malaysia (UKM)[2]
Assistant Dean (Teaching and CITRA), Universiti Kebangsaan Malaysia (UKM)[3]
APEL Q Coordinator, Universiti Kebangsaan Malaysia (UKM)[4]
Head of Network & Communication Technology (NCT) Lab CYBER, Universiti Kebangsaan Malaysia (UKM)[5]

***Abstract*—This systematic literature review examines cybersecurity awareness in schools, focusing on effective practices, challenges, and future directions. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, peer-reviewed publications in English were sourced from ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink, and Emerald, covering the period from 2019 to 2024. Studies were included if they focused on cybersecurity awareness in primary and secondary educational settings, excluding those unrelated to educational contexts or published before 2019. A total of 816 records were identified, of which 220 were duplicates and removed. After screening and eligibility assessments, 14 studies met the inclusion criteria. Risk of bias was minimized by adhering to strict inclusion criteria, such as limiting the review to high-quality, peer-reviewed studies, and ensuring consistency in the data extraction process. The review highlights effective practices such as using serious games, mobile apps, and tailored programs to enhance cybersecurity awareness. Challenges include inconsistent curricula, insufficient parental involvement, and resource limitations. These results emphasize integrating cybersecurity education across school curricula and regularly updating content to reflect evolving threats. Limitations include the exclusion of non-English and non-peer-reviewed studies. Future research should consider broader contexts and additional sources.**

Keywords*—*Cybersecurity awareness; threats; awareness programs; education; school security

I. Introduction

In the digital age, educational institutions have progressively embraced technology, integrating it extensively into classroom instruction and administrative management. While this integration offers numerous advantages, it also significantly increases schools' exposure to cybersecurity risks, threatening the integrity of educational delivery and the privacy of student and teacher data [1,2]. The vulnerability of schools to cyber threats is particularly exacerbated by limited resources, which leave educational networks open to unauthorized access and data theft [3]. Additionally, the swift transition to e-learning platforms, particularly during the COVID-19 pandemic, has expanded the attack surface, providing cybercriminals with more opportunities to exploit outdated or unpatched systems [1,4].

Historically, responses to cybersecurity threats within educational settings have tended to be reactive rather than proactive. There is now a critical and urgent need to enhance cybersecurity awareness and improve practices across all stakeholders, particularly as the Internet becomes an indispensable part of educational infrastructure [5,6]. Effective cybersecurity awareness programs must encompass a wide audience, including students, who require adequate guidance and supervision to navigate online risks safely [7]. The current systematic literature review aims to meticulously examine the state of cybersecurity awareness in schools, delineating effective practices and identifying ongoing challenges. The review addresses the growing complexity and scale of cyber threats and underscores the necessity for comprehensive strategies that integrate public education, technology updates, and community involvement [8,9]. The outcomes of this review are designed to inform educational policymakers, school IT administrators, and educators, providing them with strategic insights to develop and implement robust, effective cybersecurity education and awareness programs.

Research Questions:

1) What are effective practices for improving cybersecurity awareness in schools?

2) What are schools' current problems and challenges in implementing cybersecurity awareness programs?

3) Who is the target audience for the current cybersecurity awareness assessment?

By addressing these questions, the research aims to contribute significantly to the body of knowledge on cybersecurity in education, facilitating the development of secure learning environments that effectively leverage digital technologies.

II. Literature Review

Cybersecurity awareness has become an essential aspect of contemporary education systems, driven by the widespread

integration of digital technologies in schools. As students, educators, and administrators increasingly depend on digital platforms, educational institutions face heightened exposure to cyber threats. This literature review examines the practices, challenges, and target audiences in fostering cybersecurity awareness in school environments.

Yuliana (2022) underscores the importance of raising cybersecurity awareness among children, particularly in the context of online schooling, which increases their vulnerability to cyberattacks and malware. The study demonstrates that digital literacy training can significantly enhance children's awareness of cybersecurity. It advocates teaching children how to avoid risky online behaviour, such as falling victim to phishing scams, pornography, cyberbullying, identity theft, and privacy breaches. Additionally, it stresses the importance of educating children on password security and fostering caution when engaging in online gaming [10].

Ondrušková and Pospíšil (2023) argue that the increasing use of the Internet necessitates adequate cybersecurity awareness to mitigate the risks and dangers associated with the online environment. Their findings reveal only a moderate level of cybersecurity awareness during initial testing and show that one-off training sessions have an insignificant impact on improving online behavior. The study concludes that one-time interventions are insufficient and recommends integrating cybersecurity awareness education throughout the entire educational process to effectively enhance online safety skills [11].

Nehrar and Deepanshi (2023) highlight the critical role of cybersecurity awareness and education programs in an era characterized by pervasive digital connectivity and cyber threats. They emphasize that such programs are effective in enhancing knowledge, fostering behavioral changes, and ensuring long-term impact on cybersecurity practices [12].

Prümmer et al. (2024) emphasize the growing significance of cybersecurity in mitigating financial losses, productivity disruptions, and reputational damage caused by cyberattacks. Their research highlights the pivotal role of end-user behavior in achieving robust cybersecurity within organizational settings. Comprehensive training programs are identified as an effective means of improving cybersecurity behavior, with most studies reporting positive outcomes regardless of the training method or topic. Notably, game-based training methods are frequently employed, demonstrating their effectiveness in engaging participants and enhancing cybersecurity practices [13].

The integration of technology into education has brought both opportunities and challenges, particularly in the realm of cybersecurity. Buyu & Ogange (2021) notes that the rapid adoption of digital tools in schools has introduced significant cybersecurity risks, including malware, ransomware, phishing, and denial-of-service attacks, which disrupt teaching, compromise data security, delay assessments, and erode trust between teachers and students. These challenges are exacerbated in developing countries, where schools often lack the funding, infrastructure, and expertise to effectively address these threats. Moreover, teachers frequently lack the necessary cybersecurity knowledge to protect themselves and their students, while young learners remain particularly vulnerable due to limited awareness of online risks and poor adherence to safe practices [14].

The transition to online education, particularly during the COVID-19 pandemic, has further amplified these challenges. Al-Fatlawi (2024) highlights how the rapid shift to digital learning exposed vulnerabilities, as many educators lacked the skills and resources to secure online environments. Students with low cybersecurity awareness became frequent targets of phishing, malware, and data breaches. The lack of structured training for teachers has compounded these issues, preventing them from adequately guiding students in safe online behaviours. Additionally, disparities in motivations and levels of understanding between different demographics, including educators and students, complicate the development of comprehensive and effective cybersecurity strategies [15].

Efforts to incorporate cybersecurity awareness into school curriculums face significant hurdles. According to Triplett (2023), while methods such as game-based learning show promise in engaging students and raising awareness, they often fall short of addressing the full range of skills and knowledge required to tackle real-world cybersecurity threats. A shortage of trained mentors and educators specializing in cybersecurity further diminishes the effectiveness of these initiatives. This gap underscores the need for sustained investment in teacher training and the integration of cybersecurity education across all levels of schooling [16].

The growing reliance on the Internet in education has also led to an increase in cyber-related issues such as cyberbullying, online fraud, racial abuse, pornography, and gambling, as noted by Sareen and Jasaiwal (2021). These problems arise from a lack of awareness among internet users and disproportionately affect children, especially in the context of online education. Limited teacher expertise, inadequate funding, and insufficient resources hinder schools' ability to implement robust cybersecurity education programs. Addressing these challenges requires a collaborative effort among educators, parents, policymakers, and media platforms to cultivate a culture of cybersecurity awareness from an early age [17].

The literature review underscores the critical need for robust cybersecurity awareness initiatives in contemporary education systems. As digital technologies become integral to learning, schools face escalating cyber threats that compromise safety, disrupt teaching, and erode trust. Studies highlight the importance of integrating comprehensive and sustained cybersecurity education across all levels of schooling to address vulnerabilities among students and educators. Effective approaches, such as digital literacy training and game-based learning, show promise but require adequate resources, skilled mentors, and long-term strategies to ensure meaningful impact. Addressing these challenges necessitates collaboration among educators, parents, policymakers, and media, fostering a culture of cyber safety that empowers learners and mitigates the risks of an increasingly connected educational landscape.

III. METHODOLOGY

To deliver an exhaustive review of cybersecurity awareness within school and educational settings and to bridge identified research gaps, this study is grounded in the PRISMA ("Preferred

Reporting Items for Systematic Reviews and Meta-Analyses") framework [18].

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement is an authoritative and updated guideline that enhances transparency in the reporting of systematic reviews. It addresses the rationale, methods, and outcomes of reviews [19]. The choice of the PRISMA framework was driven by its standardization, which ensures consistency and reliability in the systematic review process; and its comprehensiveness [20], which is crucial to addressing the multi-faceted issues of cybersecurity comprehensively and practically in the education sector [21]. The review process was initiated using the PRISMA framework, which consists of four phases: identification, screening, eligibility, and inclusion. The flow diagram, providing detailed information and statistics, is shown in Fig. 1. The four phases are explained in detail below. Data collection was conducted by a single reviewer to maintain consistency in the extraction process. Four instructors provided guidance and oversight, ensuring the integrity and accuracy of the data collection.

A. Identification Phase

1) Selecting database: In the initial phase of the literature review for a systematic review of cybersecurity awareness in schools, a range of scholarly and normative databases were carefully selected to ensure comprehensive coverage of the relevant literature. Selected databases include ACM Digital Library, IEEE Xplore, ScienceDirect; SpringerLink, and Emerald .These platforms were strategically selected to access diverse, high-quality academic resources essential for the comprehensive exploration of current studies.

2) Selecting keywords: In the keyword selection phase of the Systematic Literature Review (SLR) on cybersecurity awareness in schools, specific research questions were identified to guide the research process.

- To explore practices for improving cybersecurity awareness in schools, (“cybersecurity” OR “security” OR “cybersecurity”) AND (“awareness” OR “learning”) AND (“framework” OR “model”), and Added Educational Context More detailed (“Education Sector”, “Academy”, “School” or “Educational Institution”) were used.
- Regarding the current problems and challenges that schools face in implementing cybersecurity awareness programs, the keywords (“challenges of cybersecurity education” OR “barriers to cybersecurity training” OR “cyber threats”) and (“education sector”) were used.
- For the target audience in cybersecurity awareness assessments, the keywords (“cybersecurity” OR “security” OR “cybersecurity”) AND (“awareness” OR “learning”) AND (“assessment” OR “evaluation”) were used.

These keywords were carefully selected to ensure comprehensive coverage and relevance to the study's specific areas of investigation.

3) Initial search :In the initial search stage of the systematic literature review (SLR) following the PRISMA framework, a comprehensive search was conducted across the selected databases. This search, based on the keywords identified in the previous stage, aimed to retrieve relevant scientific papers and yielded a total of 816 records.

4) Inclusion/exclusion criteria: To maintain the integrity and relevance of the systematic review, rigorous inclusion and exclusion criteria have been applied focused on impurity removal. The review is confined to studies published within the past five years (from 2019 to 2024), ensuring the data's freshness and pertinence to current contexts. Sources have been restricted to peer-reviewed articles which are critical for upholding high research standards and credibility. Additionally, all studies included in the review are published in English, setting a necessary linguistic criterion that aids in uniform comprehension and analysis. Furthermore, only studies classified as Q1 or Q2 are included to ensure the inclusion of high-quality research. On the exclusion front, any studies published before 2019 are omitted to reinforce the recency of the included research. Non-peer-reviewed materials are also excluded to preserve the scientific integrity and quality of the review. Studies not available in English or not meeting the quality classification are systematically excluded.

5) Duplicate removal: All the duplicate records were eliminated, which summed up to 220. It resulted in many duplicate records. Finally, the total remaining articles after the identification phase was .596

B. Screening Phase

Following the identification phase, the screening phase involved a detailed review of the title and abstract of each selected article 5 96articles met the criteria during this phase and were advanced to the subsequent eligibility phase. The screening was conducted using new inclusion and exclusion criteria specifically tailored for this stage, as outlined below.

Inclusion and Exclusion Criteria: During this phase of the PRISMA systematic review, criteria to refine the selection of articles were applied. Only studies that specifically focused on cybersecurity awareness within educational settings were included, as articles that did not directly focus on cybersecurity awareness within educational settings were excluded. For example, the study by Renaud & Ophoff, which explored cybersecurity implementation in SMEs rather than educational institutions, was excluded [22]. Additional exclusions included works such as those reported in Reference, Although it presents a cybersecurity awareness framework based on the behaviour change wheel, did not specifically target educational settings [23]. When information was missing or unclear, assumptions were made based on the available data. For instance, if a study did not specify the age range of students but was conducted in primary schools, it was assumed that the participants were aged 5–12 years, based on common educational structures. Similarly, for studies with incomplete intervention details, those elements were excluded from the analysis unless sufficient information justified their inclusion. This criterion led to the exclusion of 252 records that solely addressed information security awareness,

cybersecurity awareness, or other general security issues without a direct educational context.

C. Eligibility Phase

A total of 344 articles that successfully passed the second screening stage were chosen for in-depth full-text review during the eligibility stage. All articles were accessed, and the established filtering criteria were applied to evaluate each article at this stage.

Inclusion and Exclusion Criteria: During the eligibility phase of the PRISMA systematic review, stringent criteria were applied to refine the selection of articles, focusing on studies specifically within the context of schools to ensure alignment with the research aim. For example, the framework proposed in [24] for assessing cybersecurity maturity in higher education institutes (HEIs) in the UK, despite its comprehensive approach and use of recognized Capability Maturity Model (CMM) methodology, was excluded due to its specific focus on higher education. Rather than the specific educational context (schools), this careful selection process resulted in a significant reduction in eligible articles. This drastic decline stems from the overwhelming number of studies focusing on cybersecurity in educational settings, particularly schools, highlighting the challenge of finding research that focuses exclusively on the educational context, especially in schools. A careful selection and exclusion process ensures that the final set of articles strongly represents the most relevant and up-to-date research regarding cybersecurity awareness in schools, thus providing a solid foundation for identifying effective strategies and challenges specific to this educational context. In addition, a group of articles was excluded due to a lack of access to the full text, which will be illustrated in Fig. 1. Given that the studies evaluated during the Q1-2 phases are peer-reviewed, validated articles that have been thoroughly evaluated and reviewed by referees, issues of bias due to missing data were not encountered. This rigorous selection process ensures the reliability and integrity of the systematic review findings, providing a solid foundation for identifying effective strategies and challenges specific to cybersecurity awareness in schools.

D. Included Phase

All articles that successfully passed the third eligibility stage were carried forward into the final in-depth analysis of this study. Consequently, 14 articles that met all the criteria of this search were included for detailed examination.

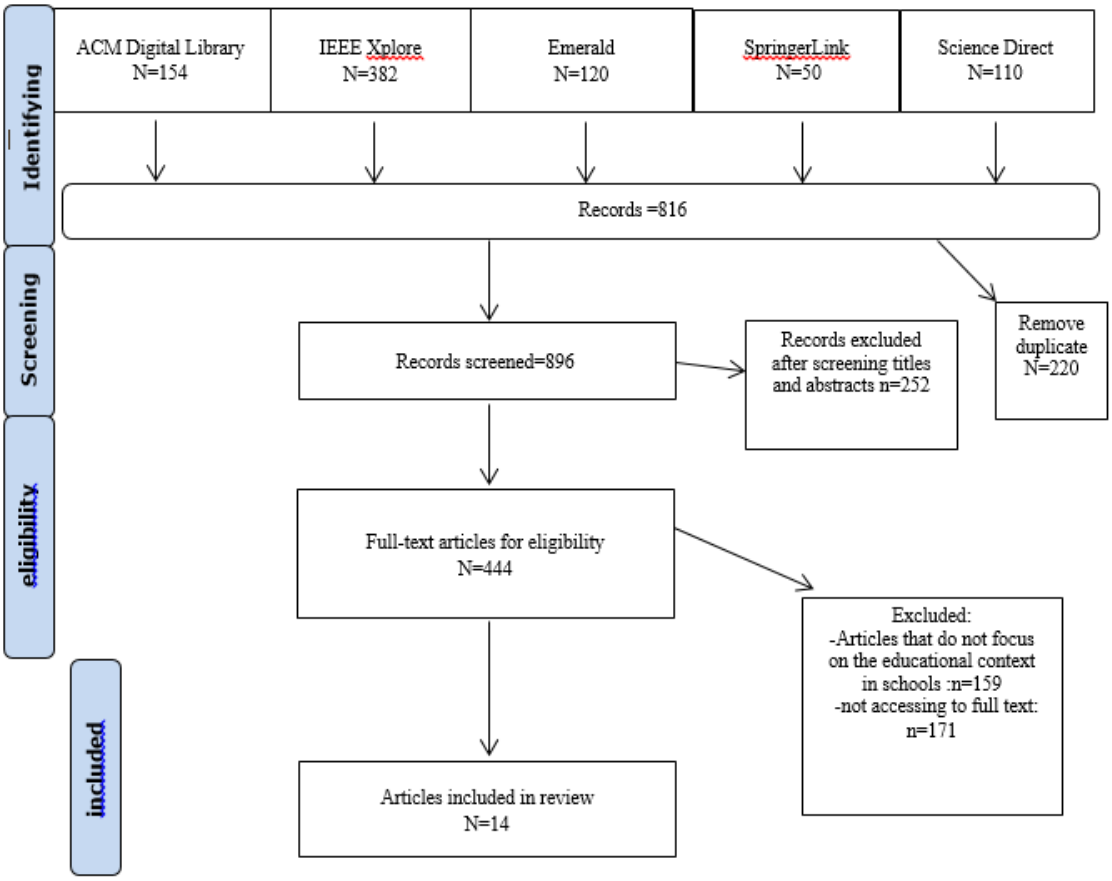

Fig. 1. Prisma flow chart.

IV. Results and Analysis

The results of this systematic review are presented based on the research questions through the analysis of the included studies (n = 14). Fig. 2 shows the distribution of the studied articles over the years in which they were published, these studies span from 2020 to 2024.

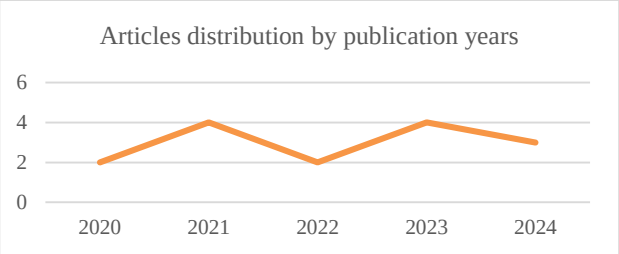

Fig. 2. Articles distribution by publication years.

While Fig. 3 shows the classification of the types of studied articles:

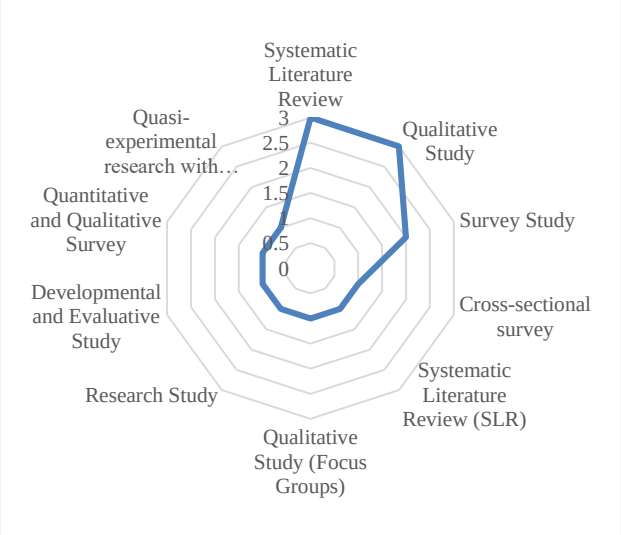

Fig. 3. The classification of the types of studied articles.

Addressing bias in systematic reviews

- Consultation with Experts: Collaboration with experts in the field of cybersecurity education was done to uncover any overlooked or insufficiently reported elements of cybersecurity awareness initiatives.
- The comprehensiveness of Reporting: Each study's reporting thoroughness was meticulously evaluated. Any discrepancies were looked for where expected results or data were absent and unaccounted for in the reports.

RQ1: what are effective practices to improve Cybersecurity awareness in schools?

Digital comics, serious games, and mobile applications are extensively used to foster engaging and interactive cybersecurity education, enhancing learning experiences by employing real-world scenarios and relevant challenges. This approach is particularly effective in engaging children and enhancing their understanding of cybersecurity concepts [25].Techniques such as the use of a web-based Learning Content Management System (LCMS) and mobile apps provide game-based cybersecurity education that captivates students' interest through interactive gameplay, which is crucial in maintaining student engagement and reinforcing cybersecurity [26]. Additionally, the gamified framework "Cyber-Hero" incorporates narrative techniques with serious games to offer an immersive learning experience that emphasizes critical cybersecurity skills, such as creating robust passwords and understanding online threats [27].

Tailored educational programs and comprehensive integration of cybersecurity into curricula are fundamental to creating a robust educational foundation. Segmented educational programs cater to specific demographic groups such as students, teachers, and parents, ensuring that each group receives relevant and effective cybersecurity knowledge [28]. Furthermore, the integration of cybersecurity topics throughout all K-12 levels ensures that students develop a comprehensive understanding from an early age, which is crucial for building a solid cybersecurity foundation [29].

Comprehensive cybersecurity education also involves the integration of national cybersecurity strategies into school curricula to align educational efforts with broader national security objectives [30]. Narrative-based learning techniques, which use storytelling and problem-solving to enhance engagement and understanding, are also highlighted as effective methods in making cybersecurity education more relatable and effective [11] [31].

Enhanced training programs for teachers and parents are critical to equipping them with the necessary skills to effectively impart cybersecurity knowledge and oversee children's online activities. These training programs not only enhance teachers' ability to teach cybersecurity effectively but also empower parents to supervise their children's online interactions more effectively [29]. Regular training sessions for both educators and parents help to ensure that children are adequately supervised and educated about the risks and safety measures associated with cyber activities [31] [32]. Additionally, the development of E-Safety frameworks that address ICT risks and the incorporation of feedback mechanisms into cyber wellness programs help monitor and control the effectiveness of cybersecurity education, adapting to new challenges and ensuring the safety of learners [33] [28]. Curriculum content that is framed around broad categories and uses innovative teaching methods like gamification not only enhances learning but also encourages active participation from students, making the learning process both enjoyable and educational [34]. Finally, the recommendations for interactive and practical teaching methods aim to engage students effectively and ensure that cybersecurity education evolves in response to new cybersecurity challenges, thus maintaining its relevance and effectiveness in educating young learners [11]

TABLE I. ANALYSIS OF PRACTICES OF CYBERSECURITY AWARENESS IN SCHOOL

Ref	Authors & year	study appraisal	Study type	Practices
[25]	Farzana Quayyum , Daniela S. Cruzes, Letizia Jaccheri (2021)	Q1	Systematic Literature Review	The review highlights multiple approaches to raising cybersecurity awareness among children. These include digital comics, serious games, and mobile apps focused on cybersecurity education. It emphasizes engaging children through interactive learning that covers internet fundamentals, privacy awareness, and risk management strategies.
[28]	T€urkera, Mıhcı and C¸akmakb, Ebru Kılıc¸ (2020)	Q2	Cross-sectional survey	The research utilizes detailed surveys to identify specific gaps in cyber wellness knowledge among students, teachers, and parents. Based on survey results, it recommends tailored educational interventions that address these specific knowledge gaps. Key practices include 1. Segmented Educational Programs: Developing age and role-specific educational materials that cater specifically to students, teachers, or parents. 2. Interactive Learning Modules: Implementing interactive and engaging learning modules that cover key topics like netiquette, cyberbullying, and online privacy practices. 3. Awareness Campaigns: Running targeted awareness campaigns that encourage safe and responsible internet use, focusing on the risks of internet addiction and the importance of copyright laws. 4. Feedback Mechanisms: Incorporating feedback mechanisms to continuously assess and improve the effectiveness of cyber wellness programs.
[29]	Ahmed Ibrahim, Marnie McKee, Leslie F. Sikos, Nicola F. Johnson (2022)	Q1	Systematic Literature Review (SLR)	The review suggests several targeted practices to enhance cybersecurity awareness: 1. Development of clear and consistent terminology across cybersecurity education to standardize teaching materials. 2. Incorporation of cybersecurity topics into curricula at all K-12 levels, ensuring a comprehensive understanding from a young age. 3. Enhanced teacher training programs to provide educators with the necessary skills and knowledge to effectively teach cybersecurity. 4. Use of interactive and practical learning modules to engage students and reinforce cybersecurity concepts
[32]	Stephanie Bannon, Tracy McGlynn, Karen McKenzie, Ethel Quayle (2024)	Q1	Qualitative Study (Focus Groups)	Inclusive Education Programs: Implement specialized cybersecurity education programs that account for the diverse needs of ASN students, emphasizing practical strategies to manage online risks. Parent and Teacher Training: Provide training for parents and teachers on how to support ASN students in navigating online spaces safely. Development of Tailored Online Safety Rules: Create school policies that address the specific online safety needs of ASN students, ensuring that they are comprehensible and enforceable.
[31]	Mohamed Ayyash, Tariq Alsboi, Omar Alshaikh, Isa Inuwa-Dutse, Saad Khan, and Simon Parkinson (2024)	Q1	Survey Study	Integration of Cybersecurity in Curriculum: Implement comprehensive cybersecurity education in schools. Narrative-based Learning: Emphasize storytelling, problem-solving, and video-based teaching methods to enhance engagement and understanding. Parent and Teacher Workshops: Organize regular training for parents and teachers to equip them with effective strategies to supervise and educate children on cybersecurity.
[35]	Ana Kovačević, Nenad Putnik, Oliver Tošković (2020)	Q1	Survey Study	Curriculum Improvement: Based on the study's findings, schools can enhance their curriculum to include more comprehensive cybersecurity education, focusing on practical knowledge and secure behaviors. Educational Programs: Development of targeted educational programs that address identified gaps in student knowledge and behaviors.
[34]	Rahime Belen Sağlam, Vincent Miller, Virginia N. L. Franqueira (2023)	Q1	Systematic Literature Review	- Curriculum content framed around six broad categories -Innovative teaching methods like gamification for a 'hands-on' experience. - Engaging students in curriculum design - Incorporating a 'bottom-up' approach listening to children's views.
[36]	Abel Moyo, Theo Tsokota, Caroline Ruvinga, Colletor T. Chipfumbu Kangara(2021)	Q1	Qualitative Research	- Development of an E-Safety framework to teach and safeguard learners from ICT-related risks. - Integration of cybersecurity knowledge into school curricula. - Continuous education, monitoring, and control of ICT use.
[37]	Farzana Quayyum, Jonas Bueie, Daniela S. Cruzes, Letizia Jaccheri, Juan Carlos Torrado Vida (2021)	Q1	Qualitative Study	- The study found that parents often discuss online security with their children at home, using real-world incidents reported in the media as teachable moments. - Schools in Norway enhance cybersecurity awareness by collaborating with organizations like Barnevakten, Bruk Hue, and Medietilsynet. These organizations assist in providing targeted cybersecurity training and lectures, not just for students but also for teachers and parents, fostering a comprehensive educational environment.
[27]	Hani Qusa, Jumana Tarazi (2021)	Q1	Research Study	- A new educational method is presented, the Gamification Framework (Cyber-Hero), which utilizes a specially designed gamified framework to boost early cybersecurity training in high schools. - This framework incorporates narrative instruction into serious games, which are strategically used to teach critical cybersecurity concepts, such as creating strong passwords. This method aims to make learning both engaging and effective.

				- The framework emphasizes two main dimensions—motivation and deployment. Motivational strategies include invoking emotions like fear to encourage proactive learning behaviors, while deployment strategies involve periodic gameplay and iterative learning, ensuring students can see their progress and are motivated to improve.
[30]	Saleh AlDaajeha , Heba Saleousa , Saed Alrabaeea, , Ezedin Barkaa , Frank Breitingerb , Kim-Kwang Raymond Chooc (2022)	Q1	Qualitative Analysis	- The study emphasizes the importance of integrating national cybersecurity strategies (NCSP) into educational curricula. - It suggests developing and aligning cybersecurity educational practices to meet the strategic objectives laid out by national policies.
[26]	Filippos Giannakas, Andreas Papasalouros, Georgios Kambourakis, Stefanos Gritzalis, 2023	Q2	developmental and evaluative study	- Utilization of a web-based Learning Content Management System (LCMS) and mobile application to deliver engaging, game-based cybersecurity education. - Application of the ARCS model of motivation to ensure the educational content is engaging and effective. - Flexible learning modes (standalone or client/server) to accommodate different learning environments and scenarios.
[13]	Julia Prümmer, Tommy van Steen, Bibi van den Berg (2024)	Q1	Systematic Literature Review	- Incorporate game-based training methods which were most frequently used and shown to be effective. - Employ a variety of training approaches, including simulation and presentation-based, to cater to different learning preferences and enhance effectiveness. - Use multi-method training campaigns to cover a broader range of cybersecurity topics effectively. - Ensure training includes interactive and engaging content to maintain participant interest and improve learning outcomes.
[11]	Dana Ondrušková, Richard Pospíšil, (2023)	Q2	Quasi-experimental research using time-series data to evaluate the impact of cyber security training on the online behavior of school children.	- Recommends integrating cybersecurity education into the ongoing educational curriculum rather than relying on one-off interventions. - Suggests using interactive and practical teaching methods to engage students effectively. - Recommends ongoing assessments and adaptations of educational content to ensure it meets the evolving challenges of cybersecurity.

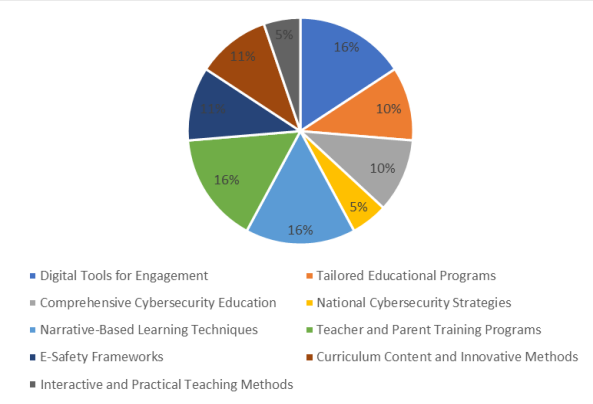

Fig. 4. Effective cybersecurity awareness practices in schools.

RQ2: What are the current issues and challenges that schools face in implementing cybersecurity awareness programs?

- Comprehensive Curriculum and Effective Educational Approaches*:*

The development of a comprehensive, consistent curriculum is critical yet challenging, necessitating curricula that not only cover a broad range of cybersecurity topics but are also adaptable to various learning needs, including those of students with Additional Support Needs (ASN). The challenge is compounded by often inconsistent educational content across different programs, which can lead to gaps in student knowledge and preparedness. Furthermore, traditional training methods have shown limitations in effectively engaging and educating students, highlighting the need for innovative approaches that cater effectively to today's diverse student bodies [25] [34] [26]. Fig. 4 shows effective cybersecurity awareness practices in schools.

- Parental Involvement and Supervision:

The role of parents in reinforcing cybersecurity education at home is crucial, yet many parents lack adequate cybersecurity awareness, which undermines their ability to support their children's learning and enforce safe online practices. Schools face the challenge of empowering parents with the necessary tools and knowledge to better manage and monitor their children's online activities. This includes providing parents with training and regular updates on cybersecurity practices and potential threats, thereby extending the learning environment beyond the classroom and fostering a holistic approach to cybersecurity education [31] [37]

- Knowledge and Awareness Gaps:

A major barrier to effective cybersecurity education is the lack of clarity in cybersecurity terminology and the absence of systematic teaching methods, particularly at the K-12 level. These gaps not only affect students but also impact educators and parents, complicating the task of achieving a comprehensive

understanding of cybersecurity across all stakeholders. The disparities in awareness based on demographic factors such as gender, class, and daily internet usage necessitate tailored educational efforts to ensure that all students, regardless of background, receive adequate and effective cybersecurity training [28] [29] [35].

- Human and Resource Limitations:

Human error is identified as a significant vulnerability in cybersecurity, exacerbated by a shortage of trained specialists within the educational sector. This shortage hampers the ability of schools to develop and deliver effective cybersecurity education, further strained by inadequate resources. Addressing these limitations requires not only more specialized training for educators but also sufficient funding to ensure that schools can afford to implement robust cybersecurity programs [27] [30].

- Engagement and Methodology Effectiveness:

Keeping students engaged in cybersecurity learning is a major challenge, particularly for younger audiences who may find traditional methods unappealing. The effectiveness of various training methodologies varies widely, and contradictory findings in research on optimal training methods create confusion about the best approaches to take. This situation calls for continuous experimentation and adaptation of teaching strategies to find what works best in different educational contexts [26] [13]

- Monitoring and Control Difficulties:

Implementing effective digital monitoring in schools involves navigating complex privacy issues and technical challenges. Schools must balance the need to monitor students' online activities to ensure their safety with the need to respect privacy rights. Effective policies and tools are needed to navigate these waters successfully, which requires ongoing dialogue among educators, parents, and policymakers [33]

- Intervention and Training Impact:

The impact of cybersecurity interventions and training programs varies widely, with some interventions showing limited effects on long-term behavioural changes and awareness among children. The success of these interventions often hinges on their duration and intensity. Well-designed, sustained programs that are integrated into the regular curriculum are more likely to have a lasting impact, highlighting the need for continuous evaluation and adaptation of these programs to meet evolving educational needs [11].

TABLE II. ANALYSIS OF CHALLENGES OF CYBERSECURITY AWARENESS IN SCHOOL

challenges	No. references
Comprehensive Curriculum and Effective Educational Approaches	[25] [34] [26]
Parental Involvement and Supervision	[31] [37]
Knowledge and Awareness Gaps	[28] [29] [35]
Human and Resource Limitations	[27] [30]
Engagement and Methodology Effectiveness	[26] [13]
Monitoring and Control Difficulties	[36]
Intervention and Training Impact	[11]

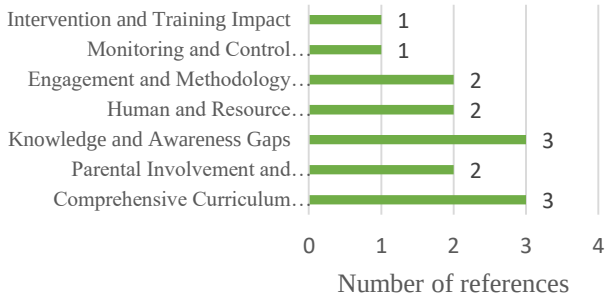

Fig. 5. Challenges of cybersecurity awareness.

RQ3: Who is the target audience in the current assessment of cybersecurity awareness?

The current assessment of cybersecurity awareness (Fig. 5) comprehensively addresses a diverse array of target audiences, each identified as critical in the ongoing efforts to enhance cybersecurity education. Primary school students are among the youngest learners, and their engagement is facilitated through digital tools such as comics, serious games, and mobile applications. These tools are essential in introducing foundational cybersecurity concepts in an age-appropriate and engaging manner, fostering early awareness and safe online behaviours [26] [25]. Secondary and high school students represent a slightly older demographic that faces more complex online risks, including cyberbullying, online privacy issues, and password security. For these students, educational programs often incorporate interactive and gamified learning experiences designed to maintain their engagement while reinforcing critical cybersecurity skills. These approaches are tailored to address the developmental and cognitive abilities of this age group, ensuring that the learning is both relevant and effective [28][33][27][30]. Teachers are a pivotal audience in this context, as they are the primary facilitators of cybersecurity education within schools. Training programs for teachers are therefore crucial, providing them with the necessary knowledge and pedagogical tools to effectively deliver cybersecurity education. Such programs also emphasize the importance of continuous professional development, enabling teachers to stay updated with the latest cybersecurity trends and threats [28][31][33]. Meanwhile, parents are recognized as the first line of defense in a child's online life. However, many parents lack the requisite knowledge and tools to effectively monitor and guide their children's online activities. Studies recommend targeted training for parents to improve their understanding of cybersecurity risks and how to communicate these risks effectively to their children, thereby extending cybersecurity education from the classroom to the home environment [31][37]

Curriculum designers and policymakers play a strategic role in shaping the educational landscape to include comprehensive cybersecurity education. Their responsibility involves integrating cybersecurity topics into the broader educational curriculum, ensuring that these efforts are aligned with national security objectives and are adaptable to the rapidly evolving digital threats [29] [11]. Additionally, in the corporate sector, corporate trainers and HR professionals are identified as key

audiences for cybersecurity training. These professionals are tasked with implementing training programs that not only educate employees about cybersecurity risks but also engage them through innovative methods such as game-based learning, which has been shown to enhance the effectiveness of these programs[13]. Finally, cybersecurity professionals are a crucial audience, as they are directly involved in protecting organizations from cyber threats.

The studies underscore the need for advanced educational frameworks tailored to these professionals, focusing on developing their skills to address the dynamic and complex nature of cyber threats. These frameworks are designed to enhance the preparedness of cybersecurity teams, ensuring they are equipped to handle real-world challenges effectively [30][13].

This comprehensive, multi-audience approach to cybersecurity awareness is critical in creating a resilient educational ecosystem that prepares all relevant stakeholders to navigate the digital world safely and responsibly.

TABLE III. ANALYSIS OF TARGET AUDIENCES

Category	Reference Numbers
Primary School Students	[26][25]
Secondary School Students	[28] [34] [36] [27]
K-12 Students	[29]
Children Aged 13-15	[11]
Special Needs Students	[32]
Teachers	[28] [36] [31]
Parents	[31] [37]
Curriculum Designers and Policymakers	[26] [29] [11]
Cybersecurity Professionals	[30] [13]

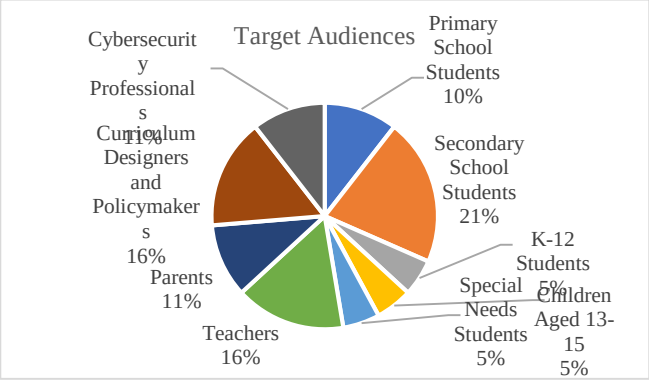

Fig. 6. Target audiences for cybersecurity awareness.

This systematic review systematically explores key practices, challenges, and target audiences (Fig. 6) in advancing cybersecurity awareness within educational institutions. The findings demonstrate that strategies such as the integration of digital tools, embedding cybersecurity within K-12 curricula, and targeted training for educators and parents significantly enhance student engagement and comprehension. However, challenges such as inconsistencies in curricular content, insufficient parental involvement, and resource constraints persist as significant barriers. The review underscores the necessity of tailoring cybersecurity practices to diverse target groups, including students, teachers, parents, and policymakers, to develop a comprehensive and resilient cybersecurity education framework. Crucially, the practices identified in the literature varied substantially depending on the target audience, leading to a wide range of specific outcomes for each group. The certainty of the evidence was evaluated, with particular attention to directness, ensuring that the findings closely aligned with the research questions and provided a robust foundation for the recommendations, despite some variations in study design and reporting rigor.

V. DISCUSSION

The findings from this systematic literature review reveal several dimensions of cybersecurity awareness in schools, emphasizing both effective practices and persistent challenges. The necessity for comprehensive and adaptable cybersecurity curricula is underscored, reflecting a critical need to bridge the gap between the evolving demands of the digital world and current educational offerings. This aligns with Blažič & Blažič, 2022 [38], who highlight the disconnect between educational content and the realities of digital threats, suggesting a pressing need for curriculum updates that mirror current technological landscapes. Innovative teaching methods, particularly those incorporating interactive tools like serious games and mobile apps, have proven effective. These methods resonate with findings from Jin et al., 2018, who confirm the efficacy of game-based learning in engaging students and enhancing their understanding of complex cybersecurity concepts [39]. However, the review also points to significant barriers in the development and implementation of such curricula, notably the inconsistency across educational programs which leads to gaps in cybersecurity knowledge and preparedness, as discussed by Lehto, 2022, this inconsistency can leave students underprepared for the cybersecurity challenges they face [40]. Furthermore, the review brings attention to the necessity of inclusive education strategies, particularly for students with Additional Support Needs (ASN). Ensuring that cybersecurity education is accessible to all students is crucial, a sentiment echoed by Ondrušková & Pospíšil, 2023 , who stress the importance of tailored approaches for students with special needs to safely navigate the digital world [11]. Parental engagement emerges as another vital component. The effectiveness of cybersecurity education often hinges on the support and knowledge of parents, yet many lack the necessary skills to guide their children in safe online behaviors, a gap highlighted by Al-Naser et al., 2019 emphasizes the need for programs that not only educate students but also empower parents with the necessary cybersecurity knowledge[41].

Additionally, the review identifies widespread gaps in knowledge among students, teachers, and parents, exacerbated by unclear cybersecurity terminology and a lack of systematic teaching approaches. This challenge is supported by O'Brien, 2019, who notes that the absence of standardized cybersecurity curricula in public schools underscores a widespread educational deficiency [42].

Demographic factors such as age, gender, and internet usage habits also influence cybersecurity awareness, necessitating more personalized educational interventions to address these disparities, as noted by Fatokun et al., 2019, this approach ensures that cybersecurity education is effective and inclusive, catering to the diverse needs of all students [43].

Moreover, the scarcity of trained cybersecurity specialists and adequate funding further constrains the ability of schools to offer effective cybersecurity education, a situation highlighted by Catota et al., 2019 argue for increased investment in both human resources and financial support to enable the development of comprehensive cybersecurity programs [44]. Issues of privacy and the need for effective digital monitoring are also discussed, pointing out the increasing complexity of maintaining privacy in an age of widespread digital surveillance[45]. This complexity necessitates clear policies and careful decision-making to balance safety and privacy rights effectively. Lastly, the variable impact of cybersecurity interventions is noted, with some programs significantly enhancing awareness and behavior, while others show limited long-term effects. Nasir, 2023 supports this observation, suggesting that the effectiveness of cybersecurity education programs can vary greatly depending on their design and implementation, highlighting the need for well-structured, sustainable initiatives[46].

Based on the discussion, this systematic literature review outlines strategies to boost cybersecurity awareness across educational levels through adaptable curricula incorporating key cybersecurity concepts and evolving through expert collaboration. It emphasizes creating targeted programs to enhance parental awareness, designing inclusive curricula with interactive tools like comics and games, and engaging the community through regular outreach. Recommendations include ongoing professional development for teachers, regular curriculum assessments, and partnerships with cybersecurity organizations to keep educational content current. Additionally, establishing clear online safety policies is advocated to ensure a secure learning environment. These measures aim to prepare students, teachers, and parents to confidently navigate digital challenges, underscoring the need for continuous research to keep educational practices up-to-date with the digital landscape.

VI. Conclusion

The systematic literature review on cybersecurity awareness in schools reveals critical issues and effective practices necessary for improving cybersecurity education. Key challenges include the lack of a consistent and comprehensive curriculum, inadequate parental supervision and knowledge, and the diverse needs of students, especially those with additional support needs (ASN). Effective practices identified include using interactive educational tools, tailored interventions, gamification, and narrative-based learning. Additionally, community involvement and continuous improvement of cybersecurity programs are essential. Recommendations include developing standardized curricula, enhancing parental education, tailoring programs for diverse needs, using interactive tools, implementing innovative teaching methods, fostering community involvement, providing ongoing professional development for educators, conducting regular assessments, establishing partnerships with cybersecurity organizations, and promoting safe online practices. Implementing these recommendations can significantly enhance cybersecurity awareness among students, educators, and parents, creating a safer online environment.

VII. Study Limitations

Despite the comprehensive approach taken in this systematic literature review, several limitations must be acknowledged. The scope was confined to studies published in the past five years and limited to peer-reviewed articles in English, potentially excluding valuable insights from earlier research, non-English publications, and grey literature. The selected databases, although extensive, may not encompass all relevant studies, especially those in lesser-known journals or emerging sources, leading to an incomplete representation of the current state of cybersecurity awareness in schools. The PRISMA framework relies heavily on the quality and reporting standards of included studies, so any deficiencies directly impact the reliability and generalizability of the findings. Additionally, the exclusion of articles due to lack of full-text access or lower quality thresholds might have omitted pertinent studies. Potential bias introduced by the subjective nature of the inclusion and exclusion criteria, despite consistent application efforts, could influence the final selection of articles. Furthermore, the review did not deeply analyze the diverse educational contexts and varying levels of technological infrastructure across different regions and countries, which means the applicability of certain findings and recommendations may be limited or require adaptation to fit specific local contexts. Addressing these limitations in future research will be essential to developing a more comprehensive and nuanced understanding of cybersecurity awareness in schools, enhancing the effectiveness of educational strategies and interventions across diverse settings.

- Funding statement:

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. All resources utilized were provided by the authors' own efforts.

- Registration Information:

The review was not registered in any systematic review protocol registry.

- Review Protocol Access:

No protocol was prepared for this systematic review.

- Amendments to Protocol or Registration:

As no protocol was prepared or registered, there were no amendments related to registration or protocol.

- Competing Interests

There are no competing interests to declare. No financial, personal, or professional conflicts influenced the conduct, results, or reporting of this systematic review.

- Availability of Data, Code, and Other Materials:

This systematic review exclusively involves the inclusion and analysis of previously published studies. No new data,

analytic code, or other materials were generated for this review. Therefore, there are no additional materials available for public access. All relevant data have been extracted from the included studies and are presented within the manuscript.

REFERENCES

[1] M. Bada and J. R. C. Nurse, "Chapter 4 - The social and psychological impact of cyberattacks," V. Benson and J. B. T.-E. C. T. and C. V. Mcalaney, Eds. Academic Press, 2020, pp. 73–92. doi: https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

[2] B. Pranggono and A. Arabo, "COVID-19 pande.. cybersecurity issues," Internet Technol. Lett., vol. 4, no. 2, p. e247, Mar. 2021, doi: https://doi.org/10.1002/itl2.247.

[3] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," Int. J. Qual. Heal. Care, vol. 33, no. 1, pp. 1–12, 2021, doi: 10.1093/intqhc/mzaa117.

[4] S. A. Jawaid, "Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity," Int. J. Data Sci. Big Data Anal., vol. 2, no. 2, 2022, doi: 10.51483/ijdsbda.2.2.2022.11-17.

[5] S. M. Zurkarnain and A. A. Abdulsahib, "Investigating The Correlation between The Five Major Personality Traits and a Student's Online Habits," Asia-Pacific J. Inf. Technol. Multimed., vol. 12, no. 01, pp. 57–69, 2023, doi: 10.17576/apjitm-2023-1201-04.

[6] A. Arifin, U. Mokhtar, Z. Hood, S. Tiun, and D. Jambari, "Parental Awareness on Cyber Threats Using Social Media," J. Komun. Malaysian J. Commun., vol. 35, pp. 485–498, Jun. 2019, doi: 10.17576/JKMJC-2019-3502-29.

[7] M. J. A. Rahman, M. I. Hamzah, M. H. M. Yasin, M. M. Tahar, Z. Haron, and N. K. E. Ensimau, "The UKM Students Perception towards Cyber Security," Creat. Educ., vol. 10, no. 12, pp. 2850–2858, 2019, doi: 10.4236/ce.2019.1012211.

[8] B. M. Dioubate, W. D. W. Norhayate, Z. F. Anwar, S. Fauzilah, H. M. Faiz, and L. O. Hai, "The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions," J. Pengur., vol. 67, pp. 31–41, 2023, doi: 10.17576/pengurusan-2022-67-03.

[9] S. S. I. Rahim, M. I. M. Huda, S. Sa'ad, and R. Moorthy, "Cyber Security Crisis/Threat: Analysis of Malaysia National Security Council (NSC) Involvement Through the Perceptions of Government, Private and People Based on the 3P Model," vol. 1, no. 2, pp. 4–6, 2024.

[10] Y. Yuliana, "THE IMPORTANCE OF CYBERSECURITY AWARENESS FOR CHILDREN," Lampung J. Int. Law, vol. 4, pp. 41–48, Jun. 2022, doi: 10.25041/lajil.v4i1.2526.

[11] D. Ondrušková and R. Pospíšil, "The good practices for implementation of cyber security education for school children," Contemp. Educ. Technol., vol. 15, no. 3, 2023.

[12] S. Nehra and M. Deepanshi, "Cybersecurity Awareness and Education Programs : A Review of Effectiveness," Int. J. Creat. Res. Thoughts, vol. 11, no. 7, pp. 504–508, 2023.

[13] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," Comput. Secur., vol. 136, no. July 2023, p. 103585, 2024, doi: 10.1016/j.cose.2023.103585.

[14] W. Buyu and B. Ogange, "Cybersecurity in Online Learning: Innovations for Teacher Training and Empowerment," p. 6, 2021.

[15] H. H. M. A. Al-Fatlawi, "Awareness of cyber security aspects in distance education," J. Pedagog. Sociol. Psychol., vol. 6, no. 1, 2024, doi: 10.33902/jpsp.202424403.

[16] W. Triplett, "Addressing Cybersecurity Challenges in Education," Int. J. STEM Educ. Sustain., vol. 3, pp. 47–67, Jan. 2023, doi: 10.53889/ijses.v3i1.132.

[17] D. A. Sareen and S. Jasaiwal, "Need of cyber security education in modern times," Int. J. Multidiscip. Trends, vol. 3, no. 2, pp. 188–191, 2021, doi: 10.22271/multi.2021.v3.i2c.179.

[18] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," Inf. Softw. Technol., vol. 51, no. 1, pp. 7–15, 2009, doi: https://doi.org/10.1016/j.infsof.2008.09.009.

[19] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews.," BMJ, vol. 372, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[20] Li T, Higgins JPT, and Deeks JJ (editors)., "Chapter 5: Collecting data | Cochrane Training," in Cochrane Handbook for Systematic Reviews of Interventions version 6.2 (updated February 2021)., 2021.

[21] R. Hamdi, "CYBERSECURITY AWARENESS IN SAUDI ARABIA: A SYSTEMATIC LITERATURE REVIEW," 14th International Conference on Education and New Learning Technologies. pp. 4805–4815, 2022.

[22] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," Organ. Cybersecurity J. Pract. Process People, vol. 1, no. 1, pp. 24–46, 2021.

[23] M. Alshaikh, H. Naseer, A. Ahmad, and S. B. Maynard, "Toward sustainable behaviour change: an approach for cyber security education training and awareness," 2019.

[24] A. Aliyu et al., "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," Appl. Sci., vol. 10, no. 10, p. 3660, 2020.

[25] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," Int. J. Child-Computer Interact., vol. 30, p. 100343, 2021, doi: 10.1016/j.ijcci.2021.100343.

[26] F. Giannakas, A. Papasalouros, G. Kambourakis, and S. Gritzalis, "A comprehensive cybersecurity learning platform for elementary education," Inf. Secur. J., vol. 28, no. 3, pp. 81–106, 2019, doi: 10.1080/19393555.2019.1657527.

[27] H. Qusa, "Cyber-Hero : A Gamification framework for Cyber Security Awareness for High Schools Students," pp. 677–682, 2021.

[28] P. Mıhcı Türker and E. Kılıç Çakmak, "An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents," Comput. Sch., vol. 36, no. 4, pp. 293–318, 2019, doi: 10.1080/07380569.2019.1677433.

[29] A. Ibrahim, M. McKee, L. F. Sikos, and N. F. Johnson, "A Systematic Review of K-12 Cybersecurity Education Around the World," IEEE Access, vol. 12, pp. 59726–59738, 2024, doi: 10.1109/ACCESS.2024.3393425.

[30] S. Aldaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K. R. Choo, "The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education," 2022.

[31] M. Ayyash, T. Alsboui, O. Alshaikh, I. Inuwa-Dute, S. Khan, and S. Parkinson, "Cybersecurity Education and Awareness among Parents and Teachers: A Survey of Bahrain," IEEE Access, vol. 12, no. May, pp. 86596–86617, 2024, doi: 10.1109/ACCESS.2024.3416045.

[32] S. Bannon, T. McGlynn, K. McKenzie, and E. Quayle, "The internet and young people with Additional Support Needs (ASN): Risk and safety," Comput. Human Behav., vol. 53, pp. 495–503, 2014, doi: 10.1016/j.chb.2014.12.057.

[33] A. Moyo, T. Tsokota, C. Ruvinga, and C. T. Chipfumbu, "An E _ safety Framework for Secondary Schools in Zimbabwe," Technol. Knowl. Learn., no. 0123456789, 2021, doi: 10.1007/s10758-021-09545-y.

[34] R. Belen and N. L. Virginia, "Kent Academic Repository A Systematic Literature Review on Cyber Security Education for Children," vol. 66, 2023, doi: 10.1109/TE.2022.3231019.

[35] A. N. A. Kovačević, N. Putnik, and O. Tošković, "Factors Related to Cyber Security Behavior," vol. 8, 2020, doi: 10.1109/ACCESS.2020.3007867.

[36] A. Moyo, T. Tsokota, C. Ruvinga, and C. T. Chipfumbu, "An E - safety Framework for Secondary Schools in Zimbabwe," Technol. Knowl. Learn., no. 0123456789, 2021, doi: 10.1007/s10758-021-09545-y.

[37] F. Quayyum, J. Bueie, D. S. Cruzes, L. Jaccheri, and J. Carlos, "Understanding parents ' perceptions of children ' s cybersecurity awareness in Norway," vol. 1, no. 1, pp. 1–6, 2021.

[38] B. J. Blažič and A. J. Blažič, "Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity," Sustain., vol. 14, no. 8, 2022, doi: 10.3390/su14084763.

[39] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Evaluation of Game-Based Learning in Cybersecurity Education for High School Students," J.

Educ. Learn., vol. 12, no. 1, pp. 150–158, 2018, doi: 10.11591/edulearn.v12i1.7736.

[40] M. Lehto, Development Needs in Cybersecurity Education : Final report of the project, no. 96. 2022.

[41] A. E. Al-Naser, A. Bushager, and H. Al-Junaid, "Parents' awareness and readiness for smart devices' cybersecurity," IET Conf. Publ., vol. 2019, no. CP758, pp. 0–6, 2019, doi: 10.1049/cp.2019.0226.

[42] C. O'Brien, "TEACHERS' PERCEPTIONS ABOUT USE OF DIGITAL GAMES AND ONLINE RESOURCES FOR CYBERSECURITY BASICS EDUCATION: A CASE STUDY," no. January, pp. 1–19, 2019.

[43] F. B. Fatokun, S. Hamid, A. Norman, and J. O. Fatokun, "The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities," J. Phys. Conf. Ser., vol. 1339, no. 1, 2019, doi: 10.1088/1742-6596/1339/1/012098.

[44] F. E. Catota, M. Granger Morgan, and D. C. Sicker, "Cybersecurity education in a developing nation: The Ecuadorian environment," J. Cybersecurity, vol. 5, no. 1, pp. 1–19, 2019, doi: 10.1093/cybsec/tyz001.

[45] D. J. Power, C. Heavin, and Y. O'Connor, "Balancing privacy rights and surveillance analytics: a decision process guide," J. Bus. Anal., vol. 4, no. 2, pp. 155–170, Jul. 2021, doi: 10.1080/2573234X.2021.1920856.

[46] S. Nasir, "Exploring the Effectiveness of Cybersecurity Training Programs : Factors , Best Exploring the Effectiveness of Cybersecurity Training Programs : Factors , Best Practices , and Future Directions," no. August, 2023, doi: 10.22624/AIMS/CSEAN-SMART2023P18.