Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P. 18282-182303

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Critical Analysis of Cybersecurity Awareness Programs in School Education

[1]Atul Kumar Srivastava*, [2]Prof. (Dr) Ajay Vikram Singh and [3]Prof. (Dr) Subhranil Som

[1] Research Scholar at Amity Institute of Information Technology , AMITY University, Noida, U.P, India
[2] Faculty at Amity Institute of Information Technology, Amity University Uttar Pradesh Noida India
[3] Prof (Dr) Subhranil Som, Principal, Bhairab Ganguly College, Kolkata, India

[1,2,3] College of Innovation and Management, Suan Sunandha Rajabhat University, Dusit, Bangkok, Thailand
741201542@qq.com; sudawan.so@ssru.ac.th; Akramanee.so@ssru.ac.th
.

How to cite this article: Atul Kumar Srivastava,Ajay Vikram Singh, Subhranil Som (2024) Critical Analysis of Cybersecurity Awareness Programs in School Education. *Library Progress International,* 44(3), 18282-182303.

ABSTRACT

Cybersecurity threats have emerged as a critical concern affecting educational institutions, with schools becoming prime targets for cyberattacks. In response to this growing threat landscape, this paper critically analyses and assesses various cybersecurity awareness programs designed for the school education system. The introduction sets the stage by highlighting the increasing importance of cybersecurity in schools and outlining the objectives of the analysis. Firstly, it examines the array of cybersecurity threats that schools face, underscoring the potentially severe consequences of these threats. The analysis then elaborates on the imperative need for cybersecurity awareness in schools, emphasizing the vulnerabilities inherent in educational institutions and the vital role of education in mitigating these risks. A thorough examination of existing cybersecurity awareness programs in schools follows, offering insights into their objectives, methodologies, and target audiences. Despite their merits, existing programs confront various challenges and limitations, including financial constraints, scalability issues, and adaptability concerns, which are scrutinized in detail. Moreover, the paper addresses the pivotal roles played by teachers and school administrators in promoting cybersecurity awareness, emphasizing their training requirements and responsibilities. The paper also considers the legal and ethical dimensions of cybersecurity education in schools, with a focus on safeguarding student privacy and obtaining consent. Anticipating the evolving landscape of cybersecurity, the paper concludes with a forward-looking perspective, offering predictions about future trends in cybersecurity and providing actionable recommendations for enhancing cybersecurity awareness programs in schools. In summary, this critical analysis offers valuable insights into the complex world of cybersecurity education in schools, emphasizing the need for proactive measures to safeguard educational institutions and their stakeholders in an increasingly digital world.

KEYWORDS

Cybersecurity, Awareness, School education, Cyber-safety, Cyber threats and Cybersecurity Awareness Programs.

1. Introduction

Cybersecurity awareness is crucial in a world going more digital, especially for K–12 students [1]. Schools are at serious risk from cyber threats, so evaluating the success of cybersecurity awareness initiatives is crucial. Promoting and teaching students about online safety is a critical duty of schools [2]. Educators are now unintentionally acting as online safety tutors, with the difficult responsibility of tackling problems like dispelling misinformation and encouraging youth to recognize the wider effects and dangers of media. The essential elements of evaluating such programs in K–12 classrooms are examined including cultivating a healthy skepticism, gauging knowledge and comprehension, evaluating attitudes, and establishing success criteria. [3]. Schools can improve cybersecurity education, safeguard their systems, and give staff, faculty, and students the skills they need to safely traverse the digital world by taking into account these factors. A lot of us use social media as a forum to communicate, spark debates, or establish our identities [4]. Because so many people like to be the first to voice a problem, they occasionally disregard whether the material being offered is reliable or not. Adults are not the only ones who use the internet, but in this day and age of technology and multimedia, children should also understand cybersecurity. Excessive use of the Internet can be harmful as it can lead to cyber risks such as cyber addiction, gaming and gambling addiction, cybersex, pornography, and exposure to personal information, even though the Internet has a lot to offer everyone [5].

Parents should be concerned about cybercrime against children and teenagers because, in certain cases, they may be unaware that their child is a victim of this type of crime [6]. A large number of parents are ignorant of the things their kids do online. Children can be intimidated, harassed, abused, or sexually exploited in addition to being bullied verbally and through insults. [7] Since children now have access to the internet at a younger age, it is crucial for everyone to take safety precautions and be aware of potential risks like cyberbullying when taking advantage of the benefits of the internet. Teachers must spread cybersecurity education to encourage responsible online conduct. Schools play a crucial role in educating students in critical digital literacy and in advising and educating parents about their children's use of the internet at home [8]. The goal of cybersecurity education is to inform technology users about the risks they may encounter when utilizing online communication platforms like social media, chat, online gaming, email, and instant messaging. Many studies have been done on cyber security in the past, but most of them have been in different domains. For instance, there aren't many articles that specifically address the actions that schools should take to foster cyber security awareness [9].

The contributions for the current Systematic Literature Review are outlined are as follows.

- The analysis delves deeply into the growing cybersecurity threats faced by educational institutions, especially schools.
- The Kitchenham and Charters framework, along with PRISMA guidelines, guarantee a thorough and methodical approach to the review process.
- The analysis determines the contributions of different nations to cybersecurity education by examining each one separately.

The current analysis follows a methodical approach, breaking down its material into six discrete sections to guarantee readability and in-depth examination. The research questions relevant to the subjects are formulated in Section II, which lays the groundwork for the investigation of the topics. A well-defined protocol that outlines the methodology to be used in Section III, directs the systematic analysis that is conducted throughout the review. A thorough summary of the research is presented in Section IV, which also includes an analysis of the literature and its applicability to the topic. Section V, which follows, is an analytical discussion that clarifies the implications that can be drawn from the results that were obtained. It provides an understanding of the importance and implications of the findings. Section VI, the analysis final section, provides a concise summary of the major discoveries and their wider implications, offering a final perspective based on the thorough analysis this study undertook.

1.1.Motivation

The urgent need to address changing threats is the driving force behind the critical examination of cybersecurity awareness programs in school education. Early mental development and preparing children for the intricacies of the digital world are major tasks performed by educational institutions. Educating people about the dangers of the internet is crucial, and many countries have started their own campaigns to achieve this. Educating young people about proper online behavior is of utmost importance, as the falsehoods they encounter on the internet are often accepted without question. In today's digital world, where personal data needs to be protected at all times, children typically don't know enough about protecting their personal information. The importance of data security and cyber threats are key topics that cybersecurity awareness campaigns help users understand. The degree to which users can defend themselves against cyberattacks is directly correlated with their understanding of information security. Cybersecurity vulnerabilities can impact both individuals and organizations, underscoring the importance of having a broad understanding of this field. Teaching young people about cybersecurity lays the groundwork for future security while also providing immediate protection. Effective programs can help develop a generation of people who can safely navigate the digital world, which will lessen the threat posed by cyberattacks. Through the creation of a more resilient and secure digital environment, this coordinated effort seeks to empower people, especially the younger generation.

1.2.Challenges of this analysis

Analyzing cybersecurity awareness programs in school education poses challenges due to the diverse landscape of these initiatives. Governments implement programs of varying quality, leading to unequal educational experiences for students across different regions. Disparities in resources, curricular integration, and teaching methods contribute to this challenge. Additionally, the rapid evolution of technology and cyber threats makes it challenging to maintain current and relevant educational content. Outdated curriculum content might leave students ill-prepared to handle emerging cybersecurity challenges. Another obstacle is the scarcity of certified educators proficient in cybersecurity. Limited access to specialized training programs for teachers further hinders effective cybersecurity education in many educational institutions.

1.3.Need for this analysis

The necessity for a comprehensive analysis of cybersecurity awareness programs in school education arises from the increasing importance of digital literacy and safety in today's interconnected world. As technology becomes integral to education, assessing and strengthening cybersecurity education in K–12 systems become imperative. This paper systematically evaluates various nations' initiatives in implementing cybersecurity awareness programs within their educational systems. Governments worldwide have launched campaigns to promote cybersecurity in schools, and assessing the impact and efficacy of these programs is crucial for informing policymakers and education authorities about areas needing improvement or refinement. Empowering young students with cybersecurity knowledge enables them to navigate the digital world safely and make informed decisions. This analysis aims to consolidate information on diverse cybersecurity awareness initiatives across K–12 educational systems globally, emphasizing the importance of equipping students with essential skills for online safety.

2. Research questions and methodology

The research attempts to comprehend the efficacy concerns in a variety of circumstances and thoroughly investigate the difficulties faced by cyber safety stakeholders. This research is essential for creating strategies that will improve cyber safety measures and require a thorough comprehension of the complex issues at hand. Furthermore, the study aims to assess current cyber security awareness programs in school education systems, with the goal of aligning them with established models and suggesting modifications to improve students' cyber resilience. RQ1 and RQ2 are research questions that aim to address the urgent need for improved cyber threat awareness in both general and educational environments.

Research Question 1 (RQ1):

What are the multifaceted challenges and efficacy concerns encountered by stakeholders in addressing cyber safety, hygiene, and security within various contexts?

RQ1 is driven by the need to gain a thorough understanding of the complex issues and concerns those stakeholders in cyber safety, hygiene, and security face in a variety of situations. The dynamic cyber environment poses complex challenges that require investigation, involving a range of stakeholders and contexts, such as the social, technological, and educational places. To effectively develop strategies for improving cyber safety measures, it is essential to comprehend these challenges.

Research Question 2 (RQ2):

How do cyber security awareness programs within school education systems align with established models, and what improvements can be made for better cyber resilience?

RQ2's objectives are to evaluate how well school education systems' cyber security awareness programs adhere to established models and to suggest possible enhancements for boosting cyber resilience. The need to assess the effectiveness of current cyber security programs in educational settings is the driving force behind this question. Refinement of educational initiatives to effectively prepare students to deal with cyber threats is supported by an understanding of the alignment with established models and suggestions for improvements.

3. Scope and Methodology

The research methodology utilized in this systematic literature evaluation is the framework proposed by Kitchenham and Charters [10]. It was done in phases, including creating a review protocol, determining inclusion and exclusion criteria, and searching bibliographic databases for pertinent studies using keywords. The technique employed in this review rigorously follows the recommendations outlined by PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). These guidelines are designed to establish a uniform framework that facilitates thorough and systematic review processes.

3.1.Protocol development

The protocol created a methodologically rigorous framework that is structured and essential. With regard to collecting, evaluating, and interpreting data, it sought to guarantee a thorough approach. The included establishing precise research goals with an emphasis on complex issues and efficacy concerns related to cyber safety, hygiene, and security, especially in a variety of settings. Determining the search parameters was essential. The research domains were the focus of the careful selection and fusion of keywords and controlled vocabulary terms. Furthermore, the boundaries of the inclusion/exclusion criteria were carefully drawn in order to include pertinent studies while excluding those that did not directly address the research questions.

3.2.Search strategy based on keywords

The search strategy collected a broad range of scholarly literature by thoroughly exploring several credible academic databases. A set of keywords was used to systematically search databases such as JSTOR, IEEE Xplore, Scopus, Web of Science. This methodical approach sought to optimize search results while guaranteeing an extensive compilation of relevant research concerning cyber safety, hygiene, security, stakeholders, obstacles, concerns about efficacy, and cyber security awareness programs in educational systems. Stage 1 involved two sets of keywords that we used to search the databases for article titles, abstracts, and keywords. The review is conducted in bibliographic databases for literature. The search was conducted using the following keyword and combination combinations:

The search strategy focuses on capturing the diverse challenges and efficacy concerns pertaining to cyber safety, hygiene, and security across different contexts by Boolean expressions (AND/OR) combination of terms : cyber safety, cyber hygiene, cybersecurity, stakeholders, participants, challenges, issues, difficulties, problems, effectiveness, efficacy, impact, cyber awareness programs, security education initiatives, evaluation, assessment, examination, contexts, environments, situations, scenarios, frameworks, standard practices, cyber resilience, analysis, evaluation, assessment .

To ensure a thorough and inclusive approach to gathering relevant literature that might not have been covered comprehensively by the initial electronic database search, a manual search using Google Scholar was conducted as an additional measure. Applying the same set of keywords used in the electronic database search, Google Scholar was accessed as a large collection of scholarly articles and publications. This manual search was essential to find any possible academic papers, studies, or articles that might not have been available or indexed in the previously used electronic databases. The objective of the literature review was to maximize its scope and profundity by incorporating a diverse array of sources, guaranteeing an all-encompassing comprehension of the intricate problems, concerns about efficacy, and assessments related to cyber safety, hygiene, and security.

Every study that was chosen in Stage 1 of the process had to be carefully examined in Stage 2. All of the studies were read in order to fully comprehend their methodology, content, and applicability to the research questions in the stage 2. In order to determine whether these studies met certain requirements that were essential for the research, the analysis process first screened the abstracts of these studies. These included alignment with stakeholder involvement, applicability to a variety of contexts, empirical support, and relevance to the research focus on cyber safety, hygiene, and security concerns. Studies failing to meet these criteria were eliminated from the selection process to maintain the quality and relevance of the literature being included.

3.3.Inclusion and Exclusion criteria

The purpose of these inclusion and exclusion criteria is to eliminate studies or materials that do not correspond to the particular research objectives and topic focus of critically examining cybersecurity awareness programs in K-12 education within the designated prime countries. The selection of articles that fulfilled the study's objectives was based primarily on inclusion criteria. Its highlighted peer-reviewed research on complex issues and efficacy concerns in a range of cyber safety, hygiene, and security contexts.

Inclusion criteria is focused on studies where articles concentrate on cyber safety, stakeholder challenges related to cyber hygiene, cyber security awareness programs in K–12 education systems, focused on children, cyber awareness program analytic models, and comparisons between suggested and current models offering valuable insightful analyses, thorough reviews, critical interpretations, or assessments of programs promoting cyber security awareness in the classroom or studies providing in-depth evaluations, analyses, or critical assessments of the advantages, disadvantages, or efficacy of cyber-awareness initiatives available in English language . The published time frame of articles has been considered from current year to last ten years to guarantee accuracy and relevance. Publication type include scholarly works undergoing a peer-review process, or peer-reviewed experience reports like conference papers. Search string key words are: cyber security awareness programs; K12 education; government initiatives; cyber hygiene challenges; analytical models; comparative analysis; and variations according to the goals.

The exclusion criteria were meticulously designed to eliminate sources that were not in line with the research questions or did not adhere to rigorous methodology. This included eliminating studies that did not address the stated research objectives, publications that were not written in English, non-peer reviewed sources, publications that were outside the timeframe specified, and publications that had nothing to do with the study's objectives. The exclusion criteria is by excluding irrelevant research papers that do not precisely investigate the cybersecurity education for students, outdated information which are older than the current year by ten years, materials that are solely available in languages other than English and lack accurate translations to facilitate comprehension and analysis. Any non-academic sources, non-peer-reviewed articles, blog posts, opinion pieces, non-academic websites, or sources lacking scholarly rigor or irrelevant publication type that are not specifically related to cybersecurity or education, such as marketing materials, press releases, promotional content, or press releases, incomplete or superficial articles are also excluded from this analysis.

Initially, a comprehensive search over several databases produced a pool of 290 articles for the purpose of research selection and screening. This thorough extraction included numerous academic journals, conference proceedings, scholarly repositories, and other reliable sources relevant to the study's focus on cybersecurity awareness initiatives. The articles came from well-known databases that are well-known for cybersecurity, and related topics. This first phase was designed to be broadly inclusive in order to include a variety of viewpoints, analyses, and assessments pertinent to the research goals outlined for the critical examination of cybersecurity initiatives in the K–12 educational systems of chosen nations.

After that, the chosen articles go through a more extensive review. In order to eliminate studies that do not specifically address the focus areas specified in the research objectives, inclusion and exclusion criteria are used. During this phase, articles that are out-of-date, didn't relate to the targeted countries, or lacked in-depth analysis are systematically removed. Finding academic articles, conference papers, and reports that provided significant insights, critical analyses, empirical support, or theoretical frameworks relevant to the thorough evaluation and critical analysis of cybersecurity awareness programs in K–12 education throughout the chosen nations is the ultimate goal of the selection process.

3.4.Quality Research selection

In research, quality selection involves a careful assessment of articles to make sure they satisfy specific requirements and standards. In this instance, a multi-stage approach was used in the quality selection process for the systematic literature evaluation in order to reduce the initial pool of articles and choose those that follow to strict methodological standards and closely match the study objectives. A total of 290 articles were found in the first search across several databases. Of these, 249 unique articles were left for additional screening after 41 cases

of duplication were found and eliminated. A preliminary assessment was conducted as part of the initial screening phase to eliminate out articles that didn't fit the criteria. A total of 120 articles were eliminated because they did not meet the search objectives, and another 50 were excluded because there was not enough information. A series of quality assessment questions was developed in order to evaluate the quality of the remaining articles. These queries most likely addressed issues with methodology, research objectives, sample size, contextual relevance, validity of results, and alignment with research questions. Articles that fell short of the requirements were not accepted. For example, a study was eliminated if its quality questions yielded fewer than four points.
The quality research questions considered in this analysis are

- Who comprises the intended audience for the research?
- What was the setting or environment where the research took place?
- What specific software products or materials were utilized in the research?
- How was the awareness raised or the risks addressed using the research findings?
- Has the researcher provided a rationale or explanation for their chosen research design?

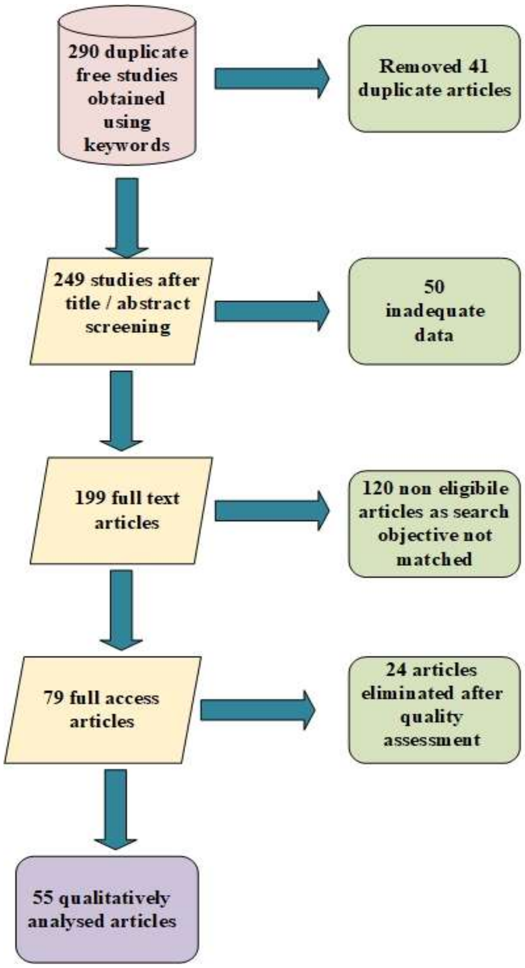
290 duplicate free studies obtained using keywords
Removed 41 duplicate articles
249 studies after title / abstract screening
50 inadequate data
199 full text articles
120 non eligibile articles as search objective not matched
79 full access articles
24 articles eliminated after quality assessment
55 qualitatively analysed articles

Figure 1. Screening process of the selected papers

Following the first screening and application of the quality assessment questions, a more thorough and exacting quality assessment was conducted manually on the remaining articles. This involved carefully examining a number of factors related to each study, including the robustness of the methodology, the significance of the context and research aims, the validity of the findings, and the dependability of the data collection. 55 studies were found to meet the quality requirements for inclusion after 24 additional papers were eliminated based on this thorough quality assessment. Figure 1 shows the screening process of the research papers

4. Overview of this research

The RQ1 emphasized the growing significance of cybersecurity education for educators as well as students. The importance of increasing teachers' proficiency in teaching cybersecurity was underlined. The study investigated cyberthreats that aim to compromise educational establishments, such as K–12 schools and universities, resulting in security breaches and monetary damages. It made clear that comprehensive plans were required to lessen these risks.

In 2023, Childers, G., et al [11] have discussed the value of professional development and cybersecurity education for K–12 educators. Even though cybersecurity education for students had received a lot of attention, more needed to be done to help teachers become knowledgeable and use good teaching techniques. The study investigated the potential benefits of boosting educators' self-esteem on their ability to create and carry out cybersecurity training. According to Liluashvili, G.B. (2021) [12], there has been an increase in cyberattacks targeting higher education institutions, with over 1,300 breaches documented in the US between 2005 and 2020. Some 24.5 million records had been compromised or stolen as a result of these attacks. These hacks may cost anywhere between $140 and $260 for each stolen record, with total costs potentially reaching the billions of dollars. Finding the weaknesses that made universities targets for these attacks required researching cyberattacks and putting effective threat mitigation techniques in place. At a private postsecondary educational institution in South Africa in 2017, Chandarman, R., and Van Niekerk, B., [13] spoke about the significance of cybersecurity awareness among students. The importance of cybersecurity in defending people and systems was emphasized as internet-based attacks increased in frequency. The purpose of the study was to evaluate students' awareness of cybersecurity. Their perception of their own cybersecurity skills and their level of cybersecurity knowledge were assessed using a questionnaire. Table 1. reviews the need of Cybersecurity education

Table 1. Cybersecurity education need

Citation	Author/ Year	Research Focus	Country
[11]	Childers, G., et al./2023	Emphasizing for K–12 teachers the importance of professional development and cybersecurity education.	USA, North Georgia
[12]	Liluashvili, G.B./2021	Analysis of cyberattacks directed at US higher education institutions, recording security lapses and compromised/stolen data between 2005 and 2020.	USA
[13]	Chandarman, R., and Van Niekerk, B. /2017	Emphasizing the importance of cybersecurity awareness among South African students attending a private postsecondary institution.	South Africa

4.1.Significance of cybersecurity education

The significance of cyber security education in developing nations was examined in 2013 by Kortjan, N. and von Solms, R., [14] using South Africa as a case study. Security of cyberspace was deemed essential since it was highlighted that cyberspace was vital to the health of people, businesses, and national economies. In order to compare South Africa's level of cyber security awareness and education to that of more developed nations, the article tried to analyze it at the time. Based on effective policies and implementations in other nations, it was suggested that developing nations should have taken into account a few crucial points in their plans for cyber security education. Online safety is becoming a bigger concern in South Africa, especially for high school students, as noted by Kritzinger, E. in 2014 [15]. Students were exposed to possible risks and threats if they did not protect themselves and their personal information due to the growing availability and accessibility of information communication technology (ICT) devices. Regarding internet safety, South Africa was lagging behind other nations. The article offered both short- and long-term solutions to increase South African students' online safety and integrate online safety into the classroom. S. Parimalam et al. 2020 [16] looked at the benefits and drawbacks of the systems in place and made suggestions for raising cybersecurity awareness. To gather data using survey forms, a stratified sampling probability sampling technique was suggested. The findings were supposed to be utilized in the creation of a self-learning cybersecurity education program for kids and teens, encouraging Gen Z users to use the internet responsibly. Rahman, N.A.A., et al. 2020 [17] drew attention to the detrimental effects of internet use, including gambling, pornography, racial abuse, cyberbullying, and online fraud. It highlighted how internet users' ignorance of security protocols and lack of awareness contributed to the rise in these risky behaviors. The article aimed to investigate the significance of teaching contemporary students about the dangers of being active on the internet and to suggest methods for encouraging cybersecurity education in educational institutions. Using data from nearly 200,000 public tweets from over 15,000 schools, Knott, J., et al. (2023) [18] investigated the level of cyber security and online safety education in UK schools. By using methods like topic modeling, sentiment analysis, visualization, and descriptive statistics, the study offered fresh perspectives on how UK schools were utilizing Twitter to teach students about online safety and cyber security. Table 2 shows the significance of cybersecurity education.

Table 2. Significance of cybersecurity education

Citation	Author/Year	Research Focus	Country
[14]	Kortjan, N. and von Solms, R. /2013	An analysis of cyber security education in developing countries with a focus on South Africa is presented.	South Africa
[15]	Kritzinger, E./2014	Highlight the issues raised by South African high school students about online safety and the suggested immediate and long-term fixes.	South Africa
[16]	S. Parimalam	A self-learning program is	Australia

	et al./2020	suggested, along with an assessment of current systems and recommendations for raising cybersecurity awareness.	
[17]	Rahman, N.A.A., et al./2020	Examination of the harmful consequences of internet usage and the significance of educating students about cybersecurity in the modern world.	USA
[18]	Knott, J., et al. /2023	Twitter data and analytical techniques are being used to investigate cyber security and online safety education in UK schools.	UK

4.2.Cybersecurity Education in Educational institutions

The awareness of school teachers about cybersecurity among their students was investigated by Ahmed, O.S in 2021 [19]. The study was carried out in Ajman, United Arab Emirates, in private schools. A total of 172 teachers from 29 different schools were included in the survey sample. The findings indicated that while teacher awareness of student safety and protection had grown in 13 of the areas examined, it had declined in eight of the other areas. A cyber safety model for Mozambique's primary and secondary schools has been suggested by De Barros et al. in 2018 [20]. It emphasized the significance of teaching kids and teenagers about online risks like identity theft, child pornography, and cyberbullying. The suggested model sought to close this gap and encourage young people in Mozambique to adopt a cybersafety mindset. A UK case study on cybersecurity certification and education was presented by Crick, T., et al in 2019 [21]. The study examined a number of cybersecurity education-related topics, such as the interaction between software and hardware, the application of theory to practice, and the impact of politics, policy, and human factors. Wisconsin's growing need for cybersecurity experts and the difficulties the state was facing in advancing cybersecurity were covered by Wang, J., et al in 2019 [22]. The demand for cybersecurity professionals still outstripped the supply despite initiatives to promote cybersecurity as a career path and to foster collaboration between the public and private sectors.

In 2023 Salem, M.A. and Sobaih, A.E.E. [23] created the quadruple "E" approach (QEA), an integrated cyber-hygiene model. The strategy was divided into four phases: inform, investigate, carry out, and assess. Before and after the QEA was implemented, the study compared the attitudes and behaviors of students regarding cyber hygiene. The findings demonstrated that following the adoption of the QEA, students displayed more positive behavior and attitudes toward online learning. The convergence of Saudi Arabia's Vision 2030 with the growing reliance on the Internet for education was examined by Mian, T.S., and Alatawi, E.M. in 2023 [24]. The researchers looked at the possible threats to cybersecurity and how parental attitudes affect kids' readiness to take precautions. The data was analyzed using structural equation modeling and a quantitative approach in this study. To safeguard students from these dangers, Amankwa, E. in 2021 [25] that cybersecurity education is essential. It was recommended that education be given to youth on how to use cyberspace safely and defend themselves against fraud. Teachers can use the strategies in the article to encourage cybersecurity education in the classroom. AlDaajeh, S., et al. in 2022 [26] emphasized the importance of cybersecurity education in bolstering national security and building a robust cybersecurity ecosystem. To shed light on industry best practices, a sample of international cybersecurity strategies was examined in this study.

Siyam, N., and Hussain, M., in 2021 [27] examined the cyber-safety policies of twenty private schools in Dubai, United Arab Emirates, with an emphasis on five primary areas: definitions, preventive measures, incident reporting and response, linkages to other policies, and reference to extant laws. The analysis showed that although cybersafety issues were covered by some policies, cyberbullying was the main focus. In 2023, Ondrušková, D. and Pospíšil, R. [28] tested the cyber security knowledge and risk identification of Czech primary school students. The children were pre-tested, trained, and then tested again to see how well they retained and applied their skills in the virtual setting. The research highlights the necessity of integrating cyber security education into the whole educational process and offers suggestions for creating an all-inclusive cyber security curriculum for educational institutions.

In 2023, Triplett, W.J. [29] concentrated on tactics educational institutions could employ to raise students' awareness of cybersecurity and inspire them to seek careers in the field. The study recommended that in addition to expanding students' understanding of cybersecurity, game designers should have produced more difficult games that evaluated players' cybersecurity prowess and capacity to fend off cyberattacks. Student interest in and awareness of cybersecurity have been found to rise in response to game-based strategies. Using free educational resources, Von Solms, R. and Von Solms, S. in 2015 [30] created a curriculum for cyber safety. This curriculum attempted to provide junior or primary school teachers with the tools they needed to teach their students about online safety. Primary schools in nations where governments or education departments did not supply such educational materials were supposed to have access to the curriculum after testing was finished. Walsh, K., et al. in 2022 [31] evaluated the work being done by the eSafety Commissioner (eSafety) to create Australia's national framework for online safety education. Researchers, eSafety, experts, and stakeholders collaborated on a two-stage sequential mixed-methods study that led to this development. In the first stage, a quick analysis of eight sources of evidence served as the foundation for a multi-component framework that included essential components and practical suggestions for teaching online safety. In Stage 2, stakeholders from school-sector organizations and children's advocacy groups participated in focus groups and one-on-one interviews with online safety experts to test and refine the framework. Table 3 illustrates the review table for cybersecurity education in institutions.

Table 3. Cybersecurity in educational institutions

Citation	Author/Year	Research Focus	Country
[19]	Ahmed, O.S. / 2021	Investigating teachers' awareness of student cyber safety in private schools in Ajman, UAE.	UAE
[20]	De Barros et al. /2018	To address the risks that young people face when using the internet,	Mozambique, South-eastern Africa

		a cyber safety model is being suggested for Mozambique's primary and secondary schools.	
[21]	Crick, T., et al. /2019	Investigating a range of cybersecurity education-related topics while conducting a case study in the UK on cybersecurity certification and education.	
[22]	Wang, J., et al. /2019	Discussing the need for cybersecurity specialists in Wisconsin, the obstacles to cybersecurity advancement, and the supply and demand imbalance in the industry.	Wisconsin, USA
[23]	Salem, M.A. and Sobaih, A.E.E. / 2023	To help students adopt better attitudes and practices regarding cyber hygiene, the	Saudi Arabia

		quadruple "E" approach (QEA) is being introduced.	
[24]	Mian, T.S., and Alatawi, E.M. / 2023	Examining the cybersecurity implications of Saudi Arabia's Vision 2030 and the attitudes of parents and how they affect their children's preparedness.	Saudi Arabia
[25]	Amankwa, E. / 2021	Stressing the value of educating young people about cybersecurity so they can protect themselves from fraud and use the internet safely, while offering advice to educators.	
[26]	AlDaajeh, S., et al./ 2022	Analyzing global cybersecurity tactics and highlighting the role that cybersecurity education plays in bolstering national security.	Australia

[27]	Siyam, N., and Hussain, M. /2021	Examining the cyber safety policies of the private schools in Dubai, paying particular attention to definitions, precautions, and incident reporting.	UAE
[28]	Ondrušková, D. and Pospíšil, R. / 2023	Assessing the awareness of cyber security and risk identification of Czech primary school students and suggesting the inclusion of cyber security education in the curriculum.	Czech Republic
[29]	Triplett, W.J. / 2023	Emphasizing game-based tactics and instructional techniques to raise students' awareness of cybersecurity and encourage careers in the field.	
[30]	Von Solms, R. and Von Solms, S. /	Developing a curriculum on cyber	African countries

	2015	safety for primary school teachers to instruct students about online safety, particularly in areas with limited educational resources.	
[31]	Walsh, K., et al. / 2022	Assessing Australia's national framework for e-safety education in cooperation with experts, stakeholders, and the eSafety Commissioner.	Australia

The RQ2 encompasses a wide range of studies pertaining to cybersecurity initiatives, programs, and education within educational systems. The compilation of research highlights how important cybersecurity awareness and education are in academic settings, especially in K–12 and higher education. The research, which is conducted across multiple nations and contexts, offers insights into the difficulties, approaches, and assessments associated with cybersecurity awareness campaigns.

A conceptual framework to improve cybersecurity knowledge in academic institutions was suggested by Khader, M., et al. in 2021 [32], along with a discussion of the significance of cybersecurity awareness. The discussions focused on raising user awareness and the difficulties in thwarting cyberattacks. In 2022, Da Veiga, A., et al. [33] discussed about the difficulties people have in controlling the risks they take online and the initiatives governments take to increase public awareness of privacy, security, and cyber safety. The discussion focused on how crucial it is to evaluate current awareness levels in order to make sure that awareness campaigns successfully addressed knowledge gaps. A cybersafety culture among educators and students was evaluated by Kritzinger, E. in 2020 [34]. The study assessed infrastructure, education, standards and inspection, leadership and policies, and education as the four main components required to improve cybersafety. Table 4 reviews the importance of cybersecurity programs.

Table 4. Cybersecurity programs importance

Citation	Author/Year	Research Focus	Country
[32]	Khader, M., et al. /2021	Intellectual framework for enhancing cybersecurit	USA

		y knowledge in educational settings; importance of cybersecurity awareness; difficulties in averting cyberattacks.	
[33]	Da Veiga, A., et al. /2022	Managing online risks can be challenging. Government initiatives to raise public awareness of privacy, security, and cyber safety are underway. Evaluating awareness levels can help create awareness campaigns that are effective.	South Africa
[34]	Kritzinger, E. /2020	Assessment of the culture surrounding cybersafety among educators and students; evaluation of the leadership, policies, infrastructure, education, standards, and inspection aspects of enhancing cybersafety.	South Africa

4.3.Cybersecurity Education programs for children

Javidi, G., and Sheybani, E. in 2018 [35] focused on K–12 education in an effort to alleviate the scarcity of cybersecurity expertise. The STEM community thought that the main reason for this shortage was students' disinterest in STEM subjects. The study evaluated a number of delivery strategies, timing, format, pacing, and outcomes alignment factors in order to establish a baseline for further investigation and integration with current cybersecurity programs. The difficulties Ecuador's higher education system faced in creating cybersecurity education were covered by Catota, F.E., et al. in 2019 [36]. Lack of structural capabilities, social integration, financial resources, and governance ability were among these difficulties. A national cybersecurity education strategy involving cooperation between the public, private, and academic sectors was recommended by the article. A survey of 318 preservice teachers was carried out in 2011 by Pusey, P., and Sadera, W.A. [37] to determine their confidence, knowledge, and comprehension of specific subjects. The bulk of preservice teachers were not sufficiently prepared, according to the findings, to instruct or serve as role models in these areas. In 2021, Ali, A. and Umar, Z.,[38] concentrated mainly on social media and the internet, but a thorough knowledge of how cybercrime specifically affected young people was lacking. The purpose of the study was to close this knowledge gap and offer insights into how young people view and interact with cybercrime.

In 2015, Kritzinger, E. [39] discussed about how important it is to teach schoolchildren in developing nations how to use information and communication technology (ICT) devices safely and appropriately. To teach kids about cyber safety in South Africa, the article suggested creating cyber safety games that could be translated into various languages and given to schools for free. Al-Janabi, S., and Al-Shourbaji, I. in 2016 [40] discussed about a study done in the Middle East to examine how knowledgeable academic staff, researchers, undergraduate students, and workers in educational institutions are about information security. The purpose of the study was to ascertain the participants' understanding of information security, the risks involved, and the effect on institutions. The growing frequency of cyberattacks and a shortage of cybersecurity professionals prompted Chen, W., et al. in 2021 [41] to examine the significance of cybersecurity education at the K–12 level. The article tackled the difficulties in cybersecurity education and offered recommendations for instructional strategies, curriculum development, and learning assessment. A list of well-liked educational resources in five categories career information, curriculum, competitions, cyber-camps, and labs and gaming is presented by Bowen, D., et al. in 2022 [42] when they address the significance of cybersecurity education at the K–12 level. Links, supported K–12 levels, price details, and topics covered are all included in the list of resources. For teachers and students interested in K–12 cybersecurity education, this is a useful place to start, even though it is not an exhaustive list.

Zhang-Kennedy, L., et al. in 2017 [43] addressed about the creation and assessment of Cyberheroes, an interactive e-book meant to teach kids about internet privacy. To determine whether the ebook was beneficial in improving kids' understanding and behavior around online privacy, they carried out a user study with 22 kids and their parents. In 2022, Wiechetek, Ł. and Mędrek, M.,[44] set out to investigate whether Generation Z members believed everything about cybersecurity concerns and whether they had a rudimentary understanding of threats and safety-improving techniques. The study examined how business students responded to a cyber incident and whether or not they were willing to learn more about and become more proficient with cyberspace. For the United States to remain competitive in the digital economy, Ivy, J., et al. 2019 [45] discussed about how cybersecurity and computer education need to be increased. In order to learn more about teachers' comprehension, application, and knowledge of cyber principles in the classroom, the authors carried out a study.

Corradini, I. and Nardelli, E. in 2020 [46] surveyed more than 2,000 teachers in Italy. Teachers understood the value of educating students about the risks associated with digital technologies, including cyberbullying, protecting personal information, and determining the veracity of news on social media, according to the survey results. Furthermore, the outcomes emphasized the educators' stated requirement for targeted instruction in digital literacy and assistance with their teaching endeavors in this field. Swain, N. in 2014 [47] emphasized the increasing dependence of people on information networks and services in their daily lives and the need for people to be aware of the dangers and vulnerabilities associated with cybersecurity breaches. The need for cybersecurity experts is growing faster than the talent pool, which emphasizes how important it is for universities to graduate students who understand cybersecurity principles and technologies. Cybersecurity education programs is reviewed in Table 5.

Table 5. Cybersecurity education programs for children

Citation	Author/Year	Research Focus	Country
[35]	Javidi, G., and Sheybani, E./2018	Techniques for teaching cybersecurity in grades K–12 that address student disinterest in STEM, delivery methods, and outcomes alignment.	United States
[36]	Catota, F.E., et al./2019	Issues with cybersecurity education that Ecuador's higher education system is facing and suggestions for a national education plan.	Ecuador
[37]	Pusey, P., and Sadera, W.A./2011	Survey on the assurance, expertise, and readiness of preservice teachers in particular areas linked to cyber safety.	United States
[38]	Ali, A. and Umar, Z./2021	Investigating the effects of cybercrime on the online and social interactions of youth.	Peshawar, Pakistan

[39]	Kritzinger, E./2015	ICT safety education is crucial for students in developing countries, and games about cyber safety should be developed.	South Africa
[40]	Al-Janabi, S., and Al-Shourbaji, I./2016	Assessment of Middle Eastern academic staff and students' knowledge of information security.	Middle East countries
[41]	Chen, W., et al./2021	Significance of cybersecurity education for grades K–12, including challenges, teaching methods, and curriculum creation.	
[42]	Bowen, D., et al./2022	Collection of learning materials covering a range of topics for K–12 cybersecurity education.	
[43]	Zhang-Kennedy, L., et al./2017	An interactive e-book called Cyberheroes was created and evaluated to	

		teach children about internet privacy.	
[44]	Wiechetek, Ł. and Mędrek, M./2022	Analysis of Generation Z's perceptions of cybersecurity issues and how they react to incidents.	Polish
[45]	Ivy, J., et al /2019	The need to improve computer education and cybersecurity in the US is discussed.	
[46]	Corradini, I. and Nardelli, E./2020	An investigation into the necessity of teaching students about digital risks and the requirements for teaching was conducted among Italian teachers.	Italy
[47]	Swain, N /2014	The need of cybersecurity education in universities and our growing reliance on information networks are	United States

		emphasized.	

4.4.Game based cybersecurity awareness

Gamification, especially in its early phases, has the power to significantly alter people's behavior and enhance cybersecurity abilities. In 2015, Giannakas, F., et al. [48] explained about developing the smartphone app Cyber-Aware with the goal of raising awareness and educating users about cybersecurity. Specifically created with elementary school students in mind, the app can be used for both formal and informal learning. It was flexible enough to be used in both indoor and outdoor environments. To address human error in cybersecurity, Qusa, H., and Tarazi, J., in 2021 [49] presented the "Cyber-Hero" framework. Students were involved in a serious game designed by the framework that taught them how to create strong passwords. Targeting the common cybersecurity vulnerability of human error, the Cyber-Hero framework offered a positive implementation of gamification to improve high school students' knowledge and training in information security. Jin, G., et al. in 2018 [50] explored about the GenCyber program, which aims to attract K–12 students' interest in cybersecurity. Four GenCyber summer camps were successfully launched by Purdue University Northwest, which teaches cybersecurity principles through game-based learning and interactive labs. The Cyber Defense Tower Game was one example of an instructive exercise where students had to defend servers against cyberattacks. Jin, G., et al. in 2018 [51] developed a game-based learning strategy for cybersecurity education in high schools. GenCyber high school summer camps were started by Purdue University Northwest for about 200 students in the Chicago metropolitan area. According to a post-camp survey, the game-based learning strategy for cybersecurity education was very successful in increasing participants' awareness of cybersecurity. Table 6 shows the review for cybersecurity game-based awareness programs

Table 6. Game based cybersecurity awareness

Citation	Author/Year	Research Focus	Country
[48]	Giannakas, F., et al./2015	The creation of the Cyber-Aware smartphone app, which offers flexible learning in a variety of settings and raises awareness of cybersecurity issues for elementary school students.	
[49]	Qusa, H., and Tarazi, J. /2021	A serious game aimed at addressing human error in cybersecurity and teaching students how to create strong	UAE

		passwords is used to introduce the "Cyber-Hero" framework.	
[50]	Jin, G., et al./2018	Examining the GenCyber initiative, which uses the Cyber Defense Tower Game as an example of game-based learning to introduce K–12 students to cybersecurity.	US
[51]	Jin, G., et al./2018	Creation and effective implementation of a game-based learning approach for high school cybersecurity education through GenCyber high school summer camps.	US

4.5.Cybersecurity Awareness Program

In 2019, Al Shamsi, A.A. [52] investigated the efficacy of a cybersecurity awareness program for children in the United Arab Emirates, aged 8 to 10. The Ministry of Education offered this program with the goal of educating people about internet safety precautions and best practices. The study made use of qualitative techniques, such as student and program trainer interviews. Children are exposed to a variety of online risks, according to the findings, which also show that the program's topics effectively addressed these risks. Three steps make up the integrated cybersecurity and cyberawareness strategy that Antunes, M., et al. presented in 2021 [53]: self-diagnosis, teaching/learning activities, and attitude and behavior assessment. A self-diagnosis tool to assess students' cybersecurity proficiency, questionnaires to assess risky attitudes and behaviors, and a lesson plan integrating cybersecurity awareness into ICT and citizenship education were all part of the strategy. The study found that, when compared to sixth-grade students, ninth-grade students generally exhibited lower levels of cybersecurity attitudes and behaviors. This emphasized the need for specialized interventions at different learning levels. A framework consisting of four stages was suggested by Al-Tajer, M. and Ikuesan, R.A in 2022 [54]. The phases are: Identification of Threats and Attacks, Existing Awareness Discovery, Creating Awareness Approach, and Examination of Awareness Approach. The framework was designed to provide K–12 students with efficient methods for cybersecurity education in Qatar. In order to engage and educate teenagers about cyber threats, the study's output was a cybersecurity awareness approach that makes use of cybersecurity emojis. The awareness of cybersecurity among parents, teachers, and secondary school students in Malaysia was examined by Zulkifli, Z., et al in 2020 [55]. Data from respondents in the Klang Valley region were gathered for the study using both offline and online surveys. The findings showed that while most respondents were aware of the dangers and hazards present in cyberspace, very few actually took precautions to stay safe when using the internet.

In 2023, Eltahir, M.E. and Ahmed, O.S. [56] discussed the undergraduate students in Sudan's higher education institutions exhibited a generally low level of cybersecurity awareness. This highlights the necessity for improved education and training in this area. Most of the 1,200 undergraduate students from six public universities in Sudan who participated in the survey had low awareness of cybersecurity. In addition, compared to female students, male students showed somewhat higher levels of cybersecurity awareness. Most participants indicated that they would like to learn more about cybersecurity and that they thought it should be covered in school curricula. A framework for cybersecurity awareness and education in South Africa was presented by Kortjan, N. and Von Solms, R. in 2014 [57]. This framework was developed by analyzing similar programs that have been put into place in other nations. The lack of state-sponsored and directed cybersecurity awareness and education programs in South Africa highlighted the need for a thorough framework in this area. Table 7 illustrates the cybersecurity awareness program.

Table 7. Cybersecurity awareness program

Citation	Author/Year	Research Focus	Country
[52]	Al Shamsi, A.A. /2019	Examining the effectiveness of a youth cybersecurity awareness program in UAE.	UAE
[53]	Antunes, M., et al. / 2021	Introducing an integrated approach to cybersecurity that includes attitude/behaviour assessment.	Portugal
[54]	Al-Tajer, M. and Ikuesan, R.A. /2022	Offering a step-by-step framework for cybersecurity education in Qatar.	Qatar
[55]	Zulkifli, Z., et al. / 2020	Analyzing the knowledge of cybersecurity among Malaysian parents, educators, and secondary school pupils	Malaysia
[56]	Eltahir, M.E. and Ahmed,	Addressing the lack of knowledge	Sudan

	O.S. /2023	about cybersecurity among undergraduate students from Sudan	
[57]	Kortjan, N. and Von Solms, R. /2014	Introducing a curriculum for cybersecurity education and awareness in South Africa,	South Africa

4.6.Initiatives and Evaluation of Cybersecurity awareness

The Four Learning Evaluation Model by Kirkpatrick served as the conceptual framework for the methodical assessment in Malaysia conducted by Rahim, N.H.A., et al in 2019 [58]. Phase 1 is reaction, Phase 2 is learning, Phase 3 is behaviour, and Phase 4 is result are the four sequential assessment phases covered by the model. For the purpose of assessment, the study used a mixed-method research methodology. Phases 1 through 4 employed the following instruments: a survey, web recording observation, focus group interviews, pre- and post-test surveys. Garba, A.A., et al. in 2020 [59] carried out a study with the goal of determining how much students knew about fundamental cybersecurity concepts. The study used a quantitative methodology, collecting data with the use of specially created questionnaires. This approach was selected in order to evaluate the students' understanding of cybersecurity and monitor their online activities. The survey for the study was completed by 201 computer science students from Yobe State University in Nigeria's Department of Computer Science. The study on cybersecurity awareness programs for students in South Africa and the UK was presented by Kritzinger, E., et al. in 2017 [60]. In order to create successful cybersecurity awareness programs, the article emphasized the value of cooperation between governmental bodies, academic institutions, and business stakeholders. In 2022, Torres, M., et al. [61] addressed about how the frequency of cyberattacks targeting schools is increasing the need for cybersecurity measures in the K–12 education sector. A new self-assessment tool designed specifically for Australian K–12 schools was introduced in the article. The National Institute of Standards and Technology's (NIST CSF) cybersecurity framework compliance was assessed using this tool. Alharbi, T., and Tassaddiq, A. in 2021 [62] emphasized the importance of cybersecurity awareness among Majmaah University students. This study focused on the importance of user education, training, and awareness by quantitatively evaluating students' knowledge of cybercrime and countermeasures. To assess and examine their hypotheses, they used a quantitative research approach and a variety of statistical tests, such as ANOVA, Kaiser–Meyer–Olkin (KMO), and Bartlett's tests.

According to an extended knowledge-attitude-behavior (KAB) model put forth by Hong, W.C.H., et al. in 2023 [63], the relationship between knowledge and attitude is moderated by societal education levels. Using the Human Aspects of Information Security Questionnaire (HAIS-Q), they carried out a comprehensive survey to test these hypotheses. Three different participant groups from China participated in the survey. Kaur, M., and Saini, M. in 2023 [64] discussed about the initiatives that the Indian government has taken to address the problem of cyberbullying in higher education. Cyberbullying has grown to be a serious issue, particularly for young people, as a result of increased internet use. Helplines, complaint boxes, and cyber cells are just a few of the measures the government has put in place to support victims of cyberbullying. Martin, F., et al. in 2023 [65] investigated the application of cybersecurity techniques and technologies in K–12 school districts. The study looked at the security technologies used in these situations, as well as good practices, problems, issues, and the goals of technology leaders. District websites and interviews with tech executives provided the data. The use of platforms like Clever or Class Link, cloud-based technologies, segregated networks, two-factor authentication, and access restrictions were among the best security practices found. Table 8 reviews the initiatives and evaluation of cybersecurity awareness.

Table 8. Initiatives and Evaluation of cybersecurity awareness

Citatio	Author/Yea	Research	Country

n	r	Focus	
[58]	Rahim, N.H.A., et al. / 2019	Assessed cybersecurity education in Malaysia using Kirkpatrick's Four Learning Evaluation Model	Malaysia
[59]	Garba, A.A., et al. / 2020	Utilized quantitative approaches and specially designed questionnaires to evaluate the foundational cybersecurity knowledge of Yobe State University, Nigerian students.	Nigeria, Africa
[60]	Kritzinger, E., et al./ 2017	Investigated student cybersecurity awareness initiatives with a focus on governmental bodies working together	South Africa and UK
[61]	Torres, M., et al. / 2022	Tackled the growing number of cyberattacks targeting K–12 educational institutions,	Australia
[62]	Alharbi, T., and Tassaddiq, A./ 2021	Centered on raising students' knowledge of cybersecurit	Saudi Arabia

		y at Majmaah University	
[63]	Hong, W.C.H., et al. / 2023	Established a broader version of the KAB model and used surveys to examine the relationship between knowledge and attitude	China
[64]	Kaur, M., and Saini, M. / 2023	Initiatives from the Indian government to combat cyberbullying in higher education were discussed.	India
[65]	Martin, F., et al / 2023	Examined security technologies and the use of cybersecurity techniques in K–12 school districts.	US

5. Results and Analysis

In this section the analysis for the year wise published articles from 2011 to 2023 have been collected and compared. Analysing the publication trends during this period of time probably offers important insights into the growing focus on children's cybersecurity education. It's critical to recognize the significance of this upward trend, as it highlights the increasing realization of how critical it is to equip younger generations with the skills, they need to safely navigate the digital world. A more thorough comprehension of the preferred research methodologies in the field can also be obtained by comparing different study types, such as case studies, mapping studies, and conference papers. Furthermore, different regions have contributed to cybersecurity education to differing degrees, according to an analysis of the countries involved.

5.1.Publication trend

Figure 2 illustrates the year-wise distribution of published articles from 2011 to 2023, expressed as a percentage.

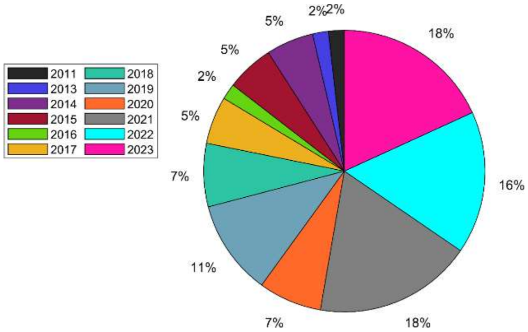

Figure 2. Year wise distribution of articles from 2011 to 2023 in percentage

From the figure 2 it is depicted that the articles published from 2011 to 2023 is increasing every year in percentage. The data shows a steady increase in the number of articles published annually, suggesting that cybersecurity education specifically designed for children is becoming increasingly important. This pattern coincides with an increasing number of reports of cybercrimes affecting children in school environments, which highlights the need to strengthen their online safety. The steady increase in articles from 2011 through 2023 underscores the heightened scholarly interest in comprehending and mitigating the risks posed by cyber threats to children. With the digital revolution influencing various facets of society, educational institutions have become prime targets for cybercriminals, necessitating a more focused approach to cybersecurity education for the younger demographic. Future research should aim to close the knowledge gap between theory and practice by providing useful advice and solutions to lessen the risks children face when using online resources.

Study type distribution

Figure 3 depicts the study types distribution of selected articles from the year 2011 to 2023.
A comparison of study types is shown in Figure 3, where case studies predominate over mapping studies, case studies, and conference papers in the field of cybersecurity education.

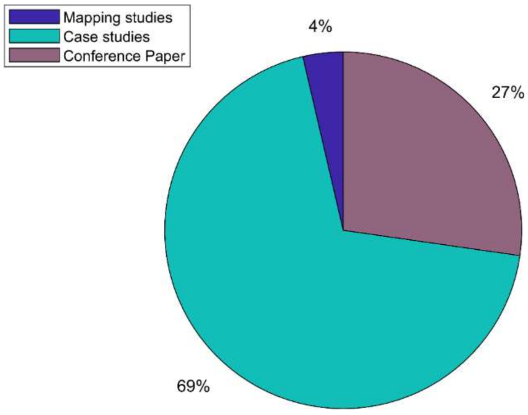

Figure 3. Distribution of study types for the taken articles

Compared to mapping studies and conference papers, case studies have a significantly higher publication percentage, according to the data. The prevalence of case studies indicates a general tendency among researchers to focus on particular cases and practical implementations of cybersecurity education. These studies most likely provide in-depth analyses, real-world examples, and workable solutions relevant to the difficulties encountered in teaching people about cybersecurity risks and recommended practices.

Conversely, the number of mapping studies seems to be relatively low, suggesting that less research has been done to systematically collect and synthesize the body of knowledge already known in the field of cybersecurity education. Conferring to case studies, conference papers make up a smaller portion of the total, suggesting that, in the context of cybersecurity education, conference settings are not as important for sharing research results and insights.

5.3.Geographical analysis for selected SLR

Figure 4 illustrates the country wise published articles involved in cybersecurity education from the year 2011 to 2023 in percentage.

From the figure 4, it is observed that the countries involved in cybersecurity education for children are compared and expressed in percentage.

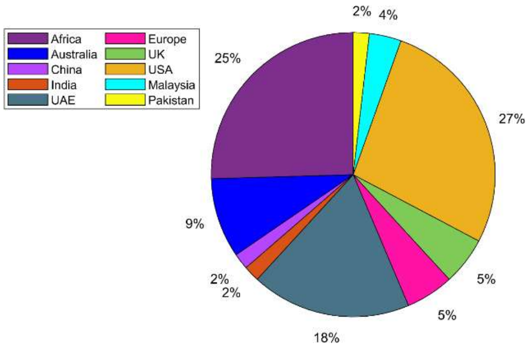

Figure 4. Country wise distribution of articles for cybersecurity education

percentage. According to the analysis, the United States is the leading country that contributes to research and initiatives related to children's cybersecurity education. This nation has demonstrated a strong commitment to researching and creating educational initiatives targeted at addressing student cyberthreats. Furthermore, developing nations, particularly African countries, have also recognized the significance of cybersecurity education in schools. Despite lower percentages compared to the United States, countries in Africa have shown notable efforts in initiating awareness campaigns and educational programs to tackle cybercrimes, acknowledging the need to educate their populace, which is often less informed about cyber threats. The UAE, India, Australia, China, Malaysia, European countries, and Pakistan are among the other participating nations that demonstrate a moderate level of involvement in children's cybersecurity education initiatives. Even though their contributions may not be as large as those of the US, they have shown a growing understanding of the value of cybersecurity education and have taken a few initiatives to address this issue.

6. Conclusion

The increasing cybersecurity threats that educational institutions, especially schools, are facing are thoroughly examined in this review, which also highlights the critical role that cybersecurity awareness programs play in reducing hazards. It offers feasible recommendations to improve cybersecurity education in educational settings by critically analysing current programs and envisioning future trends. In response to Research Questions 1 and 2, it examines international obstacles to promoting cyber safety and resilience, paying particular attention to the educational system. This systematic literature review, which makes use of the PRISMA guidelines and the

Kitchenham and Charters framework, carefully assesses an increasing number of yearly publications, highlighting the increasing significance of specialized cybersecurity education for children. As the digital revolution affects educational institutions, there is an increasing trend of cybercrimes affecting school-age children, which highlights the need to strengthen their online safety. The analysis is important for its comprehensive methodology, which carefully examines current problems, evaluates current initiatives, and offers progressive suggestions, providing a comprehensive view of cybersecurity education in schools. It provides a comprehensive analysis of the various study types, differentiating it from mapping studies and conference papers by emphasizing the prevalence of case studies and their usefulness in educating people about cybersecurity risks. Analysing countries separately shows that the United States has made a significant contribution to research on cybersecurity education for children. African nations have also made notable efforts, and other countries have contributed moderately. The review process is made more credible and reliable by utilizing well-established methodologies, such as the Kitchenham and Charters framework and PRISMA guidelines, to ensure robustness in data analysis and review procedures.

References

[1] Moletsane, T. and Tsibolane, P., 2020, March. Mobile information security awareness among students in higher education: An exploratory study. In 2020 conference on information communications technology and society (ICTAS) (pp. 1-6). IEEE.

[2] Taylor, R.D., Oberle, E., Durlak, J.A. and Weissberg, R.P., 2017. Promoting positive youth development through school-based social and emotional learning interventions: A meta-analysis of follow-up effects. Child development, 88(4), pp.1156-1171.

[3] Cheung, R.S., Cohen, J.P., Lo, H.Z. and Elia, F., 2011. Challenge based learning in cybersecurity education. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[4] Ahmad, N., Laplante, P.A., DeFranco, J.F. and Kassab, M., 2021. A cybersecurity educated community. IEEE Transactions on Emerging Topics in Computing, 10(3), pp.1456-1463.

[5] Paat, Y.F. and Markham, C., 2021. Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Social Work in Mental Health, 19(1), pp.18-40.

[6] Oyemndu, N.E. and Gilbert, N.O., 2020. The Effect of Parenting Style on Children's Involvement in Cyber Crime. J. Humanit. Soc. Sci, 20(6), pp.384-99.

[7] Djanggih, H., Thalib, H., Baharuddin, H., Qamar, N. and Ahmar, A.S., 2018, June. The effectiveness of law enforcement on child protection for cybercrime victims in Indonesia. In Journal of Physics: Conference Series (Vol. 1028, No. 1, p. 012192). IOP Publishing.

[8] Petrie-Wyman, J., Rodi, A. and McConnell, R., 2021, March. Why Should I Behave? Addressing Unethical Cyber Behavior through Education. In Developments in Business Simulation and Experiential Learning: Proceedings of the Annual ABSEL conference (Vol. 48).

[9] Rowe, D.C., Lunt, B.M. and Ekstrom, J.J., 2011, October. The role of cyber-security in information technology education. In Proceedings of the 2011 conference on Information technology education (pp. 113-122).

[10] Khoie, M., Mohammadi, M. and Ezadi Yeghaneh, M., 2023. Scientific Social Networks in the Mirror of Iranian Academic Research: A Systematic Review Using the Kitchenham & Charters Model. International Journal of Information Science and Management (IJISM), 21(3), pp.383-402.

[11] Childers, G., Linsky, C.L., Payne, B., Byers, J. and Baker, D., 2023. K-12 educators' self-confidence in designing and implementing cybersecurity lessons. Computers and Education Open, 4, p.100119.

[12] Liluashvili, G.B., 2021. Cyber Risk Mitigation in Higher Education. Law & World, 17, p.15.

[13] Chandarman, R. and Van Niekerk, B., 2017. Students' cybersecurity awareness at a private tertiary

educational institution. The African Journal of Information and Communication, 20, pp.133-155.

[14] Kortjan, N. and von Solms, R., 2013. Cyber security education in developing countries: A South African perspective. In e-Infrastructure and e-Services for Developing Countries: 4th International ICST Conference, AFRICOMM 2012, Yaounde, Cameroon, November 12-14, 2012, Revised Selected Papers 4 (pp. 289-297). Springer Berlin Heidelberg.

[15] Kritzinger, E., 2014, August. Online safety in South Africa-A cause for growing concern. In 2014 Information Security for South Africa (pp. 1-7). IEEE.

[16] Parimalam, S., Kasmin, I.F., Abidin, Z.M.Z. and Vasudavan, H., 2022. Cybersecurity Awareness Among Teenagers and Children Using Self-Learning System. International Journal of Data Science and Advanced Analytics, 4, pp.131-138.

[17] Rahman, N.A.A., Sairi, I.H., Zizi, N.A.M. and Khalid, F., 2020. The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), pp.378-382.

[18] Knott, J., Yuan, H., Boakes, M. and Li, S., 2023, March. Cyber Security and Online Safety Education for Schools in the UK: Looking through the Lens of Twitter Data. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 1603-1606).

[19] Ahmed, O.S., 2021. Teacher's awareness to develop student cyber security: A Case Study. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), pp.5148-5156.

[20] De Barros, M.J.Z. and Lazarek, H., 2018, January. A cyber safety model for schools in Mozambique. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal (pp. 22-24).

[21] Crick, T., Davenport, J.H., Irons, A. and Prickett, T., 2019, October. A UK case study on cybersecurity education and accreditation. In 2019 IEEE Frontiers in Education Conference (FIE) (pp. 1-9). IEEE.

[22] Wang, J., Brylow, D. and Perouli, D., 2019, July. Implementing cybersecurity into the Wisconsin K-12 classroom. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 312-317). IEEE.

[23] Salem, M.A. and Sobaih, A.E.E., 2023. A Quadruple "E" Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic. Electronics, 12(10), p.2268.

[24] Mian, T.S. and Alatawi, E.M., 2023. Investigating How Parental Perceptions of Cybersecurity Influence Children's Safety in the Cyber World: A Case Study of Saudi Arabia. Intelligent Information Management, 15(5), pp.350-372.

[25] Amankwa, E., 2021. Relevance of cybersecurity education at pedagogy levels in schools. Journal of Information Security, 12(4), pp.233-249.

[26] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F. and Choo, K.K.R., 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, p.102754.

[27] Siyam, N. and Hussain, M., 2021. Cyber-safety policy elements in the era of online learning: a content analysis of policies in the UAE. TechTrends, 65(4), pp.535-547.

[28] Ondrušková, D. and Pospíšil, R., 2023. The good practices for implementation of cyber security education for school children. Contemporary Educational Technology, 15(3), p.ep435.

[29] Triplett, W.J., 2023. Addressing Cybersecurity Challenges in Education. International Journal of STEM Education for Sustainability, 3(1), pp.47-67.

[30] Von Solms, R. and Von Solms, S., 2015. Cyber safety education in developing countries.

[31] Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T.

and Rogic, N., 2022. Best practice framework for online safety education: results from a rapid review of the international literature, expert review, and stakeholder consultation. International journal of child-computer interaction, 33, p.100474.

[32] Khader, M., Karam, M. and Fares, H., 2021. Cybersecurity awareness framework for academia. Information, 12(10), p.417.

[33] Da Veiga, A., Loock, M. and Renaud, K., 2022. Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. The Electronic Journal of Information Systems in Developing Countries, 88(1), p.e12198.

[34] Kritzinger, E., 2020. Improving cybersafety maturity of South African schools. Information, 11(10), p.471.

[35] Javidi, G. and Sheybani, E., 2018, October. K-12 cybersecurity education, research, and outreach. In 2018 IEEE Frontiers in Education Conference (FIE) (pp. 1-5). IEEE.

[36] Catota, F.E., Morgan, M.G. and Sicker, D.C., 2019. Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), p.tyz001.

[37] Pusey, P. and Sadera, W.A., 2011. Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. Journal of Digital Learning in Teacher Education, 28(2), pp.82-85.

[38] Ali, A. and Umar, Z., 2021. Understanding Cybercrime and Youth: A Perception Based Approach. Pakistan Journal of Social Research, 3(3), pp.130-136.

[39] Kritzinger, E., 2015, July. Enhancing cyber safety awareness among school children in South Africa through gaming. In 2015 science and information conference (SAI) (pp. 1243-1248). IEEE.

[40] Al-Janabi, S. and Al-Shourbaji, I., 2016. A study of cyber security awareness in educational environment in the middle east. Journal of Information & Knowledge Management, 15(01), p.1650007.

[41] Chen, W., He, Y., Tian, X. and He, W., 2021, October. Exploring cybersecurity education at the k-12 level. In SITE Interactive Conference (pp. 108-114). Association for the Advancement of Computing in Education (AACE).

[42] Bowen, D., Jaurez, J., Jones, N., Reid, W. and Simpson, C., 2022. Cybersecurity Educational Resources for K-12. Journal of Cybersecurity Education, Research and Practice, 2022(1), p.6.

[43] Zhang-Kennedy, L., Abdelaziz, Y. and Chiasson, S., 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. International Journal of Child-Computer Interaction, 13, pp.10-18.

[44] Wiechetek, Ł. and Mędrek, M., 2022. Human Factors in Security–Cybersecurity Education and Awareness of Business Students. Annales Universitatis Mariae Curie-Skłodowska, sectio H–Oeconomia, 56(1), pp.119-142.

[45] Ivy, J., Lee, S.B., Franz, D. and Crumpton, J., 2019. Seeding cybersecurity workforce pathways with secondary education. Computer, 52(3), pp.67-75.

[46] Corradini, I. and Nardelli, E., 2020. Developing digital awareness at school: a fundamental step for cybersecurity education. In Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, July 16–20, 2020, USA (pp. 102-110). Springer International Publishing.

[47] Swain, N., 2014, June. A multi-tier approach to cyber security education, training, and awareness in the undergraduate curriculum (CSETA). In 2014 ASEE Annual Conference & Exposition (pp. 24-72).

[48] Giannakas, F., Kambourakis, G. and Gritzalis, S., 2015, November. CyberAware: A mobile game-based app for cybersecurity education and awareness. In 2015 International conference on interactive mobile communication technologies and learning (IMCL) (pp. 54-58). IEEE.

[49] Qusa, H. and Tarazi, J., 2021, January. Cyber-hero: A gamification framework for cyber security awareness for high schools students. In 2021 IEEE 11th Annual Computing and Communication Workshop and

Conference (CCWC) (pp. 0677-0682). IEEE.

[50] Jin, G., Tu, M., Kim, T.H., Heffron, J. and White, J., 2018, February. Game based cybersecurity training for high school students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (pp. 68-73).

[51] Jin, G., Tu, M., Kim, T.H., Heffron, J. and White, J., 2018. Evaluation of game-based learning in cybersecurity education for high school students. Journal of Education and Learning (EduLearn), 12(1), pp.150-158.

[52] Al Shamsi, A.A., 2019. Effectiveness of cyber security awareness program for young children: A case study in UAE. Int. J. Inf. Technol. Lang. Stud, 3(2), pp.8-29.

[53] Antunes, M., Silva, C. and Marques, F., 2021. An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. Applied Sciences, 11(23), p.11269.

[54] Al-Tajer, M. and Ikuesan, R.A., 2022. Cyber security threat awareness framework for high school students in Qatar. arXiv preprint arXiv:2207.00820.

[55] Zulkifli, Z., Molok, N.N.A., Abd Rahim, N.H. and Talib, S., 2020. Cyber Security Awareness Among Secondary School Students in Malaysia. Journal of Information Systems and Digital Technologies, 2(2), pp.28-41.

[56] Eltahir, M.E. and Ahmed, O.S., 2023. Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. Inf. Sci. Lett, 12.

[57] Kortjan, N. and Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal, 52(1), pp.29-41.

[58] Rahim, N.H.A., Hamid, S. and Kiah, L.M., 2019. Enhancement of Cybersecurity Awareness Program on Personal Data Protection Among Youngsters in Malaysia: An Assessment. Malaysian Journal of Computer Science, 32(3).

[59] Garba, A.A., Siraj, M.M., Othman, S.H. and Musa, M.A., 2020. A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. Int. J. Emerg. Technol, 11(5), pp.41-49.

[60] Kritzinger, E., Bada, M. and Nurse, J.R., 2017. A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10 (pp. 110-120). Springer International Publishing.

[61] Torres, M., Mullins, A. and Thompson, N., 2022. Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector.

[62] Alharbi, T. and Tassaddiq, A., 2021. Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), p.23.

[63] Hong, W.C.H., Chi, C., Liu, J., Zhang, Y., Lei, V.N.L. and Xu, X., 2023. The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. Education and Information Technologies, 28(1), pp.439-470.

[64] Kaur, M. and Saini, M., 2023. Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. Education and Information Technologies, 28(1), pp.581-615.

[65] Martin, F., Bacak, J., Byker, E.J., Wang, W., Wagner, J. and Ahlgrim-Delzell, L., 2023. Examination of Cybersecurity Technologies, Practices, Challenges, and Wish List in K-12 School Districts. Journal of Cybersecurity Education, Research and Practice, 2023(1).

Author Details

1. Atul Kumar Srivastava : Atul Kumar Srivastava is a Ph.D candidate in Amity Institute of Information Technology , AMITY University, Noida, U.P, India. He has a B.Sc. degree in Science from CSJM University , Kanpur and received a Master degree in Computer Application from Maharishi Dayanand University, Rohtak , India. His research interest is cyber security, computer network technology, IoT, education technology and soft computing techniques. https://orcid.org/0000-0003-1183-680X.
2. Prof (Dr) Ajay Vikram Singh, Faculty at Amity Institute of Information Technology, Amity University Uttar Pradesh Noida India
3. Prof (Dr) Subhranil Som, Principal, Bhairab Ganguly College, Kolkata, India

Author mail id :

1. atul.srivastava@s.amity.edu
2. avsingh1@amity.edu
3. subhranil.som@gmail.com