ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

CYBERSECURITY EDUCATION AND AWARENESS: A FRAMEWORK-BASED APPROACH FOR DIGITAL LITERACY

Emon Ojha[1], Dr. K. N. Chattopadhyay[2]
[1]*Research Scholar, Department of Education, The University of Burdwan, West Bengal, India.*
[2]*Professor, Department of Education, The University of Burdwan, West Bengal, India.*
Article DOI: https://doi.org/10.36713/epra22511
DOI No: 10.36713/epra22511

ABSTRACT
In the present digital society, an educative component around cybersecurity seems essential, if not vital, for ensuring a component of digital citizenship. This research study leads the way to a landscape around cybersecurity awareness that sheds the light of day onto the key challenges we face in this realm, offering an insightful evaluation of the awareness initiatives with which we hope to bridge the gap between digital natives who move through life as students and educators and the knowledge necessary for digital safe conduct. The CAPE Framework – Cognition, Application, Participation, and Empowerment – provides a structured lens for examining initiatives. It is a model for assessing non-stupid initiatives. Findings look at where initiative participants are. Who is aware of what? Why are initiative participants not applying, and why? Why is it so difficult to apply, with sustained effort, what is known not to be easily applied? Who is not being empowered to use the necessary tools wisely if we want to improve the Internet? The study emphasises the urgent need to undertake integrative, cross-sector efforts to ensure that cybersecurity is embedded throughout the curricula. It advocates for a system that seamlessly integrates curriculum and assessment. It promotes an integrative, cross-curricular model that includes not just computer science but also mathematics, social studies, and the humanities. It advocates for middle school as a key juncture for introducing a cybersecurity curriculum. It also emphasises the value of student assessment that aligns with cybersecurity learning objectives.

Keywords: *Cybersecurity Awareness and Education, Digital Citizens, Online Safety, Cyber Threats, Digital Literacy, Cybersecurity Behavior.*

1. INTRODUCTION
Cybersecurity Literacy is a critical asset in a modern digital scenario as it is the foundation of an individual's strategy in defending themselves from a plethora of threats [14]. Developing a strong security culture in any organization involves minimizing vulnerabilities caused by humans making mistakes; this can be achieved through the need for complete cybersecurity awareness programs [11]. Rollout of digital technologies into every sector is on the rise with making people aware of cybersecurity education and its importance. Cybersecurity literacy refers to the ability to understand, evaluate, and implement safe practices in digital environments, emphasizing technical skills and the critical mindset required to navigate an evolving threat landscape [15].

Awareness and education of cybersecurity are key to alleviating these threats because, as many of the literature posit, people and organizations are the most vulnerable part of the security system [4]. This research explores the impact of cybersecurity education on awareness and safe behaviour while online. Cybersecurity is an interdisciplinary domain, comprising the need for academia and industry to acknowledge the constantly growing threat of cybersecurity [6]. Cybersecurity educational programs are fundamental for mitigating the risk of cybercrimes because these programs provide individuals the necessary knowledge and skills to secure themselves and their businesses from cyber threats [10]. Yet existing cybersecurity educational programs may not always mesh with the real world [1]. Empirical evidence attests to the importance of cybersecurity awareness and education to prevent digital risks, as educated individuals have a better capability to protect themselves and their organizations from cyberattacks. This research aims to explore the influence of cybersecurity education on preventing digital citizenship growing from informed leads to informed prevention, and especially safe and secure online navigation.

1.1. Theoretical Framework
This study employs the CAPE Framework to direct the investigation into cybersecurity literacy; a conceptual model designed to comprehend and improve the essential elements of effective cybersecurity education and behaviour. CAPE is an acronym for Cognition, Application, Participation, and Empowerment. This concept is founded on known ideas of digital literacy, behavioural modification, and socio-technical systems within cybersecurity education.

1. Cognition: Cognition refers to an individual's awareness and knowledge of cybersecurity threats, terminology, and safe practices. This element is grounded in Bloom's Taxonomy, which emphasizes foundational knowledge as a prerequisite for higher-

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

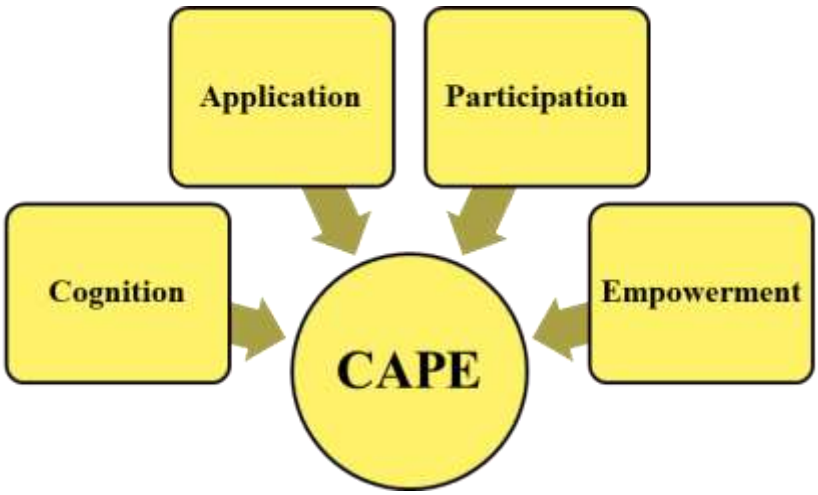
order thinking and application. In cybersecurity education, cognition involves recognizing risks like phishing, malware, and weak authentication [18].

2. Application: This dimension emphasizes the practical implementation of cybersecurity knowledge. Rooted in Experiential Learning Theory [19], this component highlights that learning is deepened when individuals actively engage in behavior, such as configuring secure passwords, recognizing suspicious links, or applying privacy settings on digital platforms.

3. Participation: Participation refers to an individual's engagement in structured educational initiatives, awareness programs, or collaborative learning environments. This aligns with Social Learning Theory [20, 21], which underscores that individuals learn through instruction and observation, interaction, and community involvement.

4. Empowerment: Empowerment reflects self-efficacy and confidence to make secure decisions and promote safe behaviors in broader social or organizational contexts. Drawing on Empowerment Theory and Self-Efficacy Theory [20, 21], this component recognizes that individuals must not only possess skills but also feel capable of acting and influencing others.

Figure 1.1: Theoretical Framework of CAPE



1.2. Relevance to the Study

The CAPE Framework functions as a diagnostic and analytical instrument in this study, directing the literature review, assessment of educational initiatives, and integration of best practices. It elucidates the efficacy of cybersecurity literacy initiatives by examining not only individuals' knowledge but also their application of that information, participation in programs, and internalization of digital responsibility.

The CAPE Framework fosters a comprehensive approach to cybersecurity education by incorporating cognitive, behavioral, and participative elements, which are vital for developing knowledgeable, skilled, and proactive digital citizens.

3. KEY PURPOSES OF THE INVESTIGATION

The purposes of this investigation comprise the following endeavours:

1. To assess the current level of cybersecurity awareness among students, educators, and other key stakeholders in educational settings.
2. To examine the effectiveness of existing cybersecurity education programs, curricula, and awareness initiatives across different educational levels and contexts.
3. Identify and synthesize best practices in cybersecurity literacy education, including instructional methods, curriculum integration, and stakeholder collaboration.
4. To analyze gaps and challenges in current cybersecurity literacy efforts, including implementation barriers, educator preparedness limitations, and evolving threat landscapes.
5. To recommend strategies for improving cybersecurity literacy through targeted interventions, policy changes, and future research directions.

4. REVIEW OF THE RELATED LITERATURE

4.1. Awareness of Cybersecurity Threats

The realm of cybersecurity is a constantly evolving landscape, necessitating continuous research and adaptation to address emerging threats and vulnerabilities [17]. Studies show that awareness of cyber threats varies widely by demographic, region, and educational context. For instance, research examining Czech schoolchildren found that their cybersecurity awareness remains at a medium level, suggesting significant room for improvement and the need for structured educational interventions [7]. In the education sector, teachers often report minimal training, with a majority receiving less than six hours of instruction on cybersecurity, and less than a quarter feeling adequately prepared [12]. These findings highlight a general lack of preparedness among both students and educators.

4.2. Education and Training Initiatives

Efforts to integrate cybersecurity education span from K-12 to higher education and even workplace training. National-level studies emphasize the importance of embedding cybersecurity education across all levels of schooling, with curricula regularly

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

updated to reflect evolving threats [9]. Effective programs often combine theoretical concepts with practical applications, using simulations, games, and real-world scenarios to reinforce learning [3]. Multimedia tools, including interactive videos and gamified learning platforms, have shown promise in increasing engagement and retention, though their long-term effectiveness requires further study [13]. In higher education, frameworks have been proposed to help institutions establish comprehensive cybersecurity awareness and training programs, focusing on both technical skills and ethical considerations [5]. However, challenges remain in keeping curricula current and relevant to the rapidly evolving threat landscape. Within organizations, cybersecurity education is seen as a cornerstone of risk management. Reviews indicate that traditional, one-off training sessions are less effective than ongoing, interactive programs that encourage employee engagement and accountability [16]. Effective approaches often involve customized content, frequent refresher courses, and the cultivation of a security-aware culture.

4.3. Best Practices in Cybersecurity Education

Best practices identified within the literature include -

- **Integration Across the Curriculum:** Cybersecurity topics should not be siloed; instead, they should be infused throughout various subjects to foster a more holistic understanding [8].
- **Continuous Professional Development:** Ongoing training for educators is essential to maintain up-to-date knowledge and teaching practices [12].
- **Use of Real-World Scenarios:** Simulated attacks, case studies, and role-playing exercises help learners understand consequences and apply best practices in realistic contexts [1].
- **Stakeholder Collaboration:** Partnerships between educational institutions, government, and industry improve resource development and ensure alignment with real-world needs [10].
- **Evaluation and Feedback:** Regular assessment of program effectiveness ensures continuous improvement [3].

5. METHODOLOGY

A systematic literature review was undertaken to synthesize existing knowledge on the topic of cybersecurity awareness and education, incorporating a myriad of sources, including academic literature, industry research reports, and government documents. Most studies employ a mix of quantitative surveys and qualitative case studies. Scoping reviews and systematic literature reviews are common, aiming to synthesize best practices and extract actionable recommendations from a broad array of interventions [1]. There is also a growing use of experimental designs, particularly in evaluating the effectiveness of multimedia and gamified educational tools [13].

5.1. Gaps in the Literature

Key gaps identified include

1. **Longitudinal Studies:** There is a lack of long-term data assessing whether increased awareness and education lead to sustained behavioral change.
2. **Standardized Metrics:** Few studies employ standardized measures for cybersecurity literacy, making cross-study comparisons difficult.
3. **Cultural and Regional Variations:** Most research is concentrated in North America and Europe; less is known about cybersecurity literacy in other regions.
4. **Impact of Emerging Technologies:** The literature is still catching up with new threats posed by AI, IoT, and other rapidly advancing technologies.

6. OBJECTIVE-WISE ANALYSIS

Objective-wise analysis is given below -

Objective 1. To assess the current level of cybersecurity awareness among students, educators, and other key stakeholders in educational settings

Analysis: Multiple studies reveal that cybersecurity awareness among both students and educators is generally moderate, with considerable variation across regions and age groups. For example, research on Czech schoolchildren found their awareness at a medium level, indicating an understanding of basic concepts but gaps in practical application and consistent safe behavior [7]. Among teachers, surveys show that most receive minimal formal training, often less than six hours, with only a minority feeling confident in their knowledge and ability to model best practices [12]. This points to a systemic need for increased investment in both awareness and ongoing professional development.

Objective 2. To examine the effectiveness of existing cybersecurity education programs, curricula, and awareness initiatives across different educational levels and contexts

Analysis: The effectiveness of cybersecurity education programs is closely tied to how well they are integrated into the broader curriculum and to the use of interactive, real-world learning tools. Programs that blend theoretical knowledge with practical exercises, such as gamification, simulations, and case studies, tend to achieve better engagement and retention [13]. However, the literature also notes a lack of standardized assessment methods and limited longitudinal evidence regarding whether short-term gains are sustained over time [3]. Programs with ongoing evaluation and feedback loops are more likely to adapt to evolving threats and remain effective.

Objective 3.Identify and synthesize best practices in cybersecurity literacy education, including instructional methods, curriculum integration, and stakeholder collaboration.

Analysis: Best practices highlighted in the literature include integrating cybersecurity content across different subjects (not only in standalone courses), utilizing active learning methods (e.g., simulations, real-world problem-solving), and fostering collaborations among educators, IT professionals, and external

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

stakeholders [1]. Continuous professional development for teachers, supported by up-to-date resources and training, is particularly emphasized [5]. Stakeholder collaboration—such as partnerships between schools, government agencies, and private sector organizations—has enhanced resource availability and relevance [10].

Objective 4. To analyze gaps and challenges in current cybersecurity literacy efforts, including barriers to implementation, limitations in educator preparedness, and evolving threat landscapes

Analysis: Notable gaps include a lack of long-term studies assessing behavioral change and a shortage of standardized metrics for measuring cybersecurity literacy [1]. Many programs lack sufficient resources or institutional support, and educators often feel underprepared to teach rapidly evolving content [12]. There's also a regional imbalance in research, with most studies focused on North America and Europe, and limited insights into challenges faced in other parts of the world. The rapid emergence of new threats (e.g., AI, IoT) outpaces most curricula, underscoring the need for agility in educational design and delivery [3].

Objective 5. To recommend strategies for improving cybersecurity literacy through targeted interventions, policy changes, and future research directions

Analysis: The literature recommends several strategies:

- Longitudinal research to evaluate the sustained impact of educational interventions.
- Development and adoption of standardized assessment tools to enable comparison and benchmarking across contexts.
- Broader inclusion of diverse educational settings to ensure global relevance and applicability.
- Continuous professional development for educators and agile curriculum updates to address emerging threats.
- Active partnerships between education, government, and industry to pool expertise and resources [1, 10].

These recommendations, if implemented, could significantly enhance the effectiveness and reach of cybersecurity literacy initiatives.

7. FINDINGS

The study's findings emphasise the complex nature of cybersecurity literacy and its use in educational settings. Utilising the CAPE Framework (Cognition, Application, Participation, Empowerment) to synthesise insights from the literature offers a systematic comprehension of current strengths, weaknesses, and opportunities. The principal findings are delineated below:

1. Cybersecurity Awareness (Cognition) Remains Inconsistent and Often Insufficient: Students' and teachers' understanding of cybersecurity is generally moderate and varies greatly between locations, educational institutions, and age groups. While students frequently show only a superficial awareness of issues, including phishing, social engineering, and malware attacks, many educators report having received fewer than six hours of formal cybersecurity training [7]. This cognitive gap makes people less prepared and more vulnerable in learning environments.

2. Practical Implementation (Application) Is Limited by Program Design and Evaluation Gaps: Higher levels of engagement and information retention are shown by cybersecurity education programs that include real-world, practical scenarios, such as gamification, simulations, and case-based learning. These benefits, however, are frequently fleeting since few programs monitor long-term behavioural change through longitudinal reviews. Program comparison and efficacy measurement are made more difficult by the absence of standardised instruments for evaluating cybersecurity literacy [13].

3. Participation and Engagement are influenced by Curriculum Integration and Collaboration: Effective cybersecurity initiatives encourage stakeholder collaboration and cross-subject integration. School-government-industry cooperation improves curricular relevance and resource accessibility. Participation is unequal due to institutional support, lack of structured activities, and poor teacher preparation [1].

4. Empowerment Gaps and Structural Barriers Undermine Long-Term Impact: Both educators and students frequently exhibit insufficient confidence and capability to serve as advocates for cybersecurity. Restricted professional development, obsolete curricula, and the lack of contextualised resources impede empowerment. Furthermore, the majority of research concentrates on Western educational systems, resulting in considerable knowledge gaps concerning the cultural, regional, and socio-economic factors that influence cybersecurity behaviour. The swift advancement of technology, encompassing risks associated with AI and IoT, exacerbates this empowerment gap [10].

5. Strategic Recommendations Align with the CAPE Model for Future Progress

The literature supports a multi-dimensional approach to strengthening cybersecurity literacy. Recommended strategies include:

- **Enhancing cognition** through targeted awareness campaigns and digital literacy modules
- **Facilitating application** via hands-on training and immersive learning tools
- **Expanding participation** through policy-backed collaboration between education, government, and industry
- **Fostering empowerment** by investing in continuous teacher development and culturally relevant content

8. IMPLICATIONS

This study's findings have important implications for educators, policymakers, curriculum designers, and stakeholders involved in developing a cyber-resilient society. Cybersecurity literacy has

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

transitioned from a peripheral skill to a fundamental aspect of contemporary education, crucial for the protection of individuals, institutions, and national infrastructure in a progressively digitised environment.

1. **Educational practice should extend beyond mere awareness:** The CAPE Framework demonstrates that mere awareness (Cognition) is inadequate. Cybersecurity education should be integrated into daily learning contexts via practical, scenario-based applications. Educators require systematic and continuous professional development to enhance their content knowledge and teaching methodologies for the effective delivery of cybersecurity education.
2. **Institutional and policy-level support is essential for participation:** To ensure cybersecurity literacy remains a sustained priority, educational institutions must incorporate it throughout curricula rather than treating it as an optional supplement. Participation will increase only when governments and educational systems institutionalise cybersecurity education through national standards, dedicated funding, and collaboration with industry experts and cybersecurity professionals.
3. **Empowerment fosters a culture characterised by collective responsibility:** True digital resilience is attained not by passive knowledge acquisition but through active empowerment. Students and educators should be motivated to serve as advocates and exemplars of secure online practices. This necessitates the cultivation of confidence, digital agency, and a culture of collective responsibility within educational institutions and beyond.
4. **Research and innovation are essential to address existing gaps,Further research is urgently required on:**
    - Longitudinal effects of cybersecurity education initiatives.
    - Curricula that are adapted to cultural and regional contexts.
    - Standardised metrics for evaluating cybersecurity literacy in various contexts.
    - Curriculum design innovation, through the integration of gamified tools, AI-assisted learning platforms, and real-time simulations, enhances relevance and adaptability.

9. LIMITATIONS OF THE RESEARCH

This work is limited by the availability and regional focus of existing literature, with most research originating from North America and Europe, and a few Indian studies making global generalization challenging. There is also a lack of longitudinal data, so the long-term effects of cybersecurity literacy programs remain unclear. Additionally, inconsistencies in assessment tools and metrics across studies hinder direct comparison and synthesis of results. Finally, rapid technological changes mean that some findings may quickly become outdated as new threats and tools emerge.

10. CONCLUSION

The literature on cybersecurity literacy reflects that a problem exists and that it's no small task to educate people to function in an ever-more digital, ever-riskier world. Throughout the literature, one key message becomes clear: a gap exists between increased awareness about cybersecurity risks and actual literacy, inclusive of knowledge, skills, and routine safe behavior, especially among students and teachers. The discussion highlights critical and complex aspects of cybersecurity literacy in the rapidly evolving digital space. Even though the level of consciousness about the topic of cyber threats is growing, there is still a large gap between the knowledge level and its implementation, and between the theory and the use of safe practices. This shortfall is especially noticeable in schools where those learning and teaching there are quite often not equipped with the training, tools, and assistance required to responsibly participate in and encourage online security.

In this paper, we propose the CAPE Framework (Cognition, Application, Participation, Empowerment) to evaluate and promote cybersecurity literacy as a holistic process through integrating insights from the existing literature and best practices. It highlights a need for our work in cybersecurity education to move beyond mere knowledge transfer toward hands-on skill development, greater community involvement, and increased confidence in our users. Awareness-only efforts, that do not help to apply in a practical sense nor serve to maintain ongoing engagement, likely will not bring about sustainable change.

The lack of longitudinal studies, consistent measures, and international inclusion acts as an obstacle in the field. In response to these deficiencies, the following future actions should be taken. These will involve ongoing teacher training, flexible lesson planning, and supply-side initiatives. School systems need to form strategic alliances with industry and government to ensure that learning resources are current, relevant, and scalable.

In conclusion, understanding cybersecurity is not some kind of one-off educational objective but a consistent, adaptive process that should continue to progress along technological developments and societal demands. Keep It Simple By taking a holistic, inclusive, and proactive security approach--based on frameworks such as CAPE-we can create a cyber-resilient community in which members understand the threats against them and are prepared, positioned, and enabled to respond efficiently.

REFERENCES

1. *Abrahams, N. T. O., Farayola, N. O. A., Kaggwa, N. S., Uwaoma, N. P. U., Hassan, N. A. O., & Dawodu, N. S. O. (2024). CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY. Computer Science & IT Research Journal, 5(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708.* ***[16]***

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 6| June 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

2. *Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 27(3), 393–410. https://doi.org/10.1108/ics-07-2018-0080.* ***[1]***
3. *Bandura, A. (1977). Social Learning Theory. Englewood Cliffs, NJ: Prentice-Hall.* ***[20]***
4. *Bandura, A. (1997). Self-Efficacy: The Exercise of Control. New York: W. H. Freeman.* ***[21]***
5. *Bloom, B.S. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York: Longmans, Green.* ***[18]***
6. *Charlie, Sander. (2023). The effectiveness of cybersecurity awareness programs in schools — The Learning Counsel. (n.d.-b). The Learning Counsel. https://thelearningcounsel.com/articles/the-effectiveness-of-cybersecurity-awareness-programs-in-schools/.* ***[12]***
7. *Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information, 13(4), 192. https://doi.org/10.3390/info13040192.* ***[2]***
8. *Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001.* ***[4]***
9. *Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Bataineh, M. A., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports, 16, 100501. https://doi.org/10.1016/j.chbr.2024.100501.* ***[9]***
10. *Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. Information, 12(10), 417. https://doi.org/10.3390/info12100417.* ***[5]***
11. *Kolb, D. A. (1984). Experiential Learning: Experience as the Source of Learning and Development. Englewood Cliffs, NJ: Prentice Hall.* ***[19]***
12. *Manganello, F., Earp, J., Fante, C., Bassi, G., Fabbri, S., Matteucci, I., Vaccarelli, A., Olesen, N., De Vibraye, A., Callaghan, P., & Gentile, M. (2024). Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives. Frontiers in Education, 9. https://doi.org/10.3389/feduc.2024.1375853* ***[3]***
13. *Mishra, S. (2024). Integrating Cybersecurity education into the curriculum: best practices and implementation challenges. In Digital Parenting. Bluerose. https://www.researchgate.net/publication/383846506_Integrating_Cybersecurity_Education_into_the_Curriculum_Best_Practices_and_Implementation_Challenges.* ***[8]***
14. *Mukherjee, M., Le, N. T., Chow, Y., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A study of Educational models and Outcomes. Information, 15(2), 117. https://doi.org/10.3390/info15020117.* ***[6]***
15. *Ondrušková, D., & Pospíšil, R. (2023). The good practices for implementation of cyber security education for school children. Contemporary Educational Technology, 15(3), ep435.*
16. *https://doi.org/10.30935/cedtech/13253.* ***[7]***
17. *Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: national level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756.* ***[10]***
18. *Taherdoost, H. (2024). Towards an innovative model for cybersecurity awareness training. Information, 15(9), 512. https://doi.org/10.3390/info15090512.* ***[11]***
19. *Tamrakar, A., & Patra, B. (2018). CYBERSECURITY THREATS AND COUNTERMEASURES: A REVIEW. Türk Bilgisayar Ve Matematik Eğitimi Dergisi, 9(3), 1400–1404. https://doi.org/10.61841/turcomat.v9i3.14598.* ***[17]***
20. *What is cyber literacy, and why is it important? (2027, May 27). https://www.cyberlutions.com.au/what-is-cyber-literacy-and-why-is-it-important#:~:text=The%20word%20%E2%80%9Ccyber%20literacy%E2%80%9D%20refers,effectively%2C%20safely%2C%20and%20ethically.* ***[15]***
21. *Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys, 54(1), 1–39. https://doi.org/10.1145/3427920.* ***[13]***
22. *Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269.* ***[14]***