CHILD-FRIENDLY CYBERSECURITY EDUCATION: EXPLORING LEARNING METHODS, ENGAGEMENT, AND FUTURE STEM INTEREST

Nidhi Srivastava[0009-0002-5384-7873]
MS in IT management with cybersecurity
Oakland University Rochester Michigan 48309

Abstract

The research paper investigates the process of creating age-specific cybersecurity education training among children, which involves the introduction of gamification, storytelling, teacher education and the inclusion of parents in the curriculum design process. There is a growing appropriate ways to strengthen cyber hygiene, improve awareness of online risk, and create responsible online behaviour. The study also examines the effectiveness of various pedagogical methods and investigates the potential of co-designing security tools with children. It also considers whether early exposure to cybersecurity concepts can influence future interest in STEM fields or not. A Qualitative Exploratory Secondary Data Analysis methodology is adopted to synthesise existing research on child-centred cybersecurity education. The qualitative analysis of secondary research will be supported with Python that will gather, clean, and thematically analyze text-based materials. To analyse the data, the tools to be used will be web scraping and API-based document retrieval (where possible), text preprocessing, analysis of word frequencies, mapping of key-word co-occurrence, topic modelling, clustering, and a simple visualisation to determine patterns, trends, and pedagogical themes in child-focused cybersecurity education. The secondary data will be obtained with the help of various open-access academic and institutional repositories, such as Google Scholar, ERIC, IEEE Xplore, ACM Open, arXiv, and the UNESCO Digital Library, as well as publicly available datasets on such platforms as Kaggle and government open-data portals. Such a blend of Python-based text analytics and various and authoritative sources of data will render the research methodical, repeatable, and able to produce valuable results in the field of cybersecurity education, parental involvement, and STEM-related results among children.

Keywords: STEM, cybersecurity, Python, parental involvement, and pedagogy.

Introduction

In the present digital world, children are being raised by engaging with technology and the internet, where online communication, connected devices and internet-based education are integral to their daily tasks. Based on studies, it has been observed that cyber safety awareness is lower among middle-grade students of 12-15 age groups compared to secondary students of 15-18 age groups (Panjani & Mudgal, 2025). While these apps offer avenues for creativity, communication and academic growth, they also can be a source of cyber threats that kids may fail to identify or comprehend fully. The problems of data privacy violation, unsafe online activities, exposure to damaging content and internet manipulation are affecting the younger section of users (Jain *et al.* 2021). In response, schools, administrations, and technology developers are now seeking approaches to teach cybersecurity in child-friendly ways at the youngest grades. These methods generally include games, narratives, storytelling and practical activities that make complex concepts easier to understand. Meanwhile, current studies also demonstrate the applications of early cyber exposure to reinforce skills in problem solving, curiosity and positive attitudes that are fundamental for STEM engagement (Indriasari & Karman, 2023).

However, despite increasing cybersecurity risks in the current environment, structured and age-appropriate cybersecurity education is still limited and inconsistent (Manganello *et al.* 2024). Existing applications are often extremely technical, so children may not understand or show interactivity to develop a lasting learning process. In addition, knowledge is limited about how child-friendly cybersecurity education potentially impacts general developmental outcomes such as interest in STEM fields. The absence of critical evidence on effective approaches, motivators and long-lasting impact raises several gaps for educators or researchers who seek safe cybersecurity learning experiences for younger students.

Research Aim: The study aims to investigate the current delivery patterns of child-friendly cybersecurity education by determining their influences on children's future in STEM and recognising learning methods as well as engagement tactics for young learners.

Research Objectives:

- To investigate pedagogy and digital tools employed for teaching cybersecurity to children.
- To explore factors that facilitate or hinder participation in child-oriented online security learning spaces.
- To understand the role of early cybersecurity education in influencing children's attitudes towards and interest in STEM careers.

Research Questions:

- What are the methods and approaches optimised to teach cybersecurity to children?
- Why do young learners engage and persist in cybersecurity learning activities?
- What influence does exposure to cybersecurity education have on children's interest in STEM subjects and careers?

The significance of the study lies in a systematic approach to the development of cybersecurity education effectively. Through a comprehensive analysis, it demonstrates current pedagogies in learning approaches, engagement strategies, and their potential impact on the development of future STEM interest, which may support curriculum design, educational technology development and policy. The results could help schools, parents and developers design more effective and influential cybersecurity learning experiences for children. This research focuses on child-friendly cybersecurity education for students aged approximately 5-15 based on secondary data and open-access sources. It studies learning modalities, engagement elements and links with interest in STEM, but it does not assess specific interventions by primary fieldwork or long-term behavioural outcomes.

Child-Friendly Cybersecurity Education: Concepts and Importance

Child-friendly cybersecurity education can be defined as the design and development of learning experiences that expose young learners to digital safety, responsible online behaviour, and fundamental cybersecurity concepts that are understandable and appropriate at their stage of development (Majebi & Drakeford, 2025). Instead of representing cybersecurity as a technical or abstract discourse, kid-friendly explanations make concepts such as password security, data privacy, critical internet literacy skills and identifying digital threats into interactive, relatable and fun activities (Zhang *et al.* 2025). These methods consider the cognitive, emotional and social developmental state of children and make abstract ideas accessible using storytelling, gamification, simulations and hands-on exploration. According to Apdillah *et al.* (2022), there is growing urgency for such education as children's online presence becomes more pervasive and begins from the youngest kids. Early exposure helps to build the foundation for young learners in learning safe and responsible use of digital media. It also encourages good habits, like being inquisitive about questionable online behaviour and appreciating the worth of data privacy. Child-friendly cybersecurity learning also contributes to wider developmental outcomes such as critical thinking, problem-solving and digital literacy. As Osorio de Barros & Severino Soares (2025) pointed out, a positive environment generated by exposure to cybersecurity experience might result in curiosity, positive attitude towards technology, and ultimately the development of early STEM identity. Since children are exposed to the immense cyber threats, cybersecurity education that is both friendly and

entertaining is important to empower children with knowledge and abilities to be better digital citizens.

Learning Techniques for Teaching Cybersecurity to Children

Child cybersecurity education should be engaging, age-specific and capable of simplifying complex ideas and offer tangible concepts. According to Damenu *et al.* (2025), the most widespread theory is game-based learning, during which the concept of cybersecurity is introduced through puzzles, challenges or other digital games rewarding the use of safe practices and critical thinking. These are simulations of real-life scenarios, such as identifying a phishing attack or designing a good password, to make them feel more of a game rather than lessons. More useful strategies are narrative-based learning and storytelling, especially with younger children, where the characters and stories can be used to offer them access to risks and moral decision places in online worlds. Interactive activities and role-play are another option, in which children can assume the role of cyberattackers and engage in group play-based situations to solve some of the cyber safety problems they might encounter (Saglam et al. 2023). These are vital in self-esteem construction, group learning, and development of critical thinking. Moreover, the graphic and interactive material, such as cartoons, animated videos or interactive applications that children can use to navigate through, disseminate the knowledge by simplifying complicated ideas into understandable parts. In a more scholarly context, research into cross-disciplinary projects will assist in assimilating curriculum with lessons and cross-disciplinary projects integrating cybersecurity into more common topics such as mathematics, reading or science. Environments such as the after-school clubs, coding camps and web platforms provide an opportunity to explore and experiment.

Engagement Tactics in Child Cybersecurity Learning

Simulation is a crucial element in assisting children to raise awareness of threats on the internet and implement cybersecurity knowledge. This successful way to engage often begins with interactive aspects that enable them to be practically applied instead of learning. Such features as simulations and digital missions, activities through drag-and-drop or cyber challenge are intriguingly curious. Rewards, badges, accomplishment levels, gamified competition, and game mechanics are examples of game mechanics that encourage kids to complete cybersecurity tasks (Quayyum & Jaccheri, 2025). The other important strategy is by using relatable stories where characters, plots and real-life situations echo online experience of children. This helps to make the learners felt relating to the content and recognise the significance of cybersecurity to their daily lives. The personalisation also helps in engaging in the process in which adaptive levels of difficulty, custom avatars and task paths accommodate a great variety of learning styles and student capabilities.

Other social activities including group activities, peer collaboration and guided discussions also facilitate engagements as children can discuss the concept of cybersecurity with other children (Videnovik *et al.* 2024). This enhances consultations, solving and sharing of problems and responsibility towards safety on the internet. Additionally, it is necessary to focus attention with the help of embracing visual design, such as colourful interfaces, animations, and easy-to-use layouts, which will help keep children entertained and reduce mental load. Together, all these elements of engagement create a positive and active atmosphere whereby children can enjoy and have meaning in learning about cybersecurity

STEM Pathways and Early Cybersecurity Exposure

Exposure to security at an early age can play a major role in creating long-lasting interest in STEM among children. Some of the skills linked with cybersecurity learning frequently involve skills closely related to STEM thinking that encompass deductive logic, problem solving, pattern recognition and analytical decision-making. This form of computational mind can form the foundational blocks behind STEM success when they are triggered earlier in life because students will undertake practical applications by playing games involving cyber safety, code writing exercises and finding solutions to digital safety puzzles (English, 2023). Moreover, they can demystify technology and bring it within reach as something creative and personally meaningful. Activities focusing on cybersecurity also represent an opportunity for children to interact with sophisticated technologies in an empowering manner. When children learn how digital systems work and methods to protect themselves, they possess knowledge for problem-solving and maintain a positive STEM identity (Debora & Pramono, 2021). This sense of efficacy can be particularly influential during childhood as it leads to self-perception and interests. Also, cybersecurity can reinforce various STEM fields other than typical coding, such as ethical hacking, data protection, digital forensics and AI safety job readiness in the future pipelines.

Technology, Tools, and Digital Platforms for Child Cybersecurity Education

There are several technologies, tools and digital platforms available to facilitate child-friendly cybersecurity education that can be optimised to make complex information easy and provide interactive learning. Numerous educational platforms now include gamified cybersecurity modules that teach kids to recognise such abilities as phishing attacks, making strong passwords, or guarding a digital identity through gaming missions or puzzles (Karlberg, 2022). Many of these platforms are built on animated characters, rewards, or levels to keep them engaged and learning at a slower pace. Cybersecurity is increasingly incorporated into children's learning to equip them with safe coding practices, data protection policies and responsible digital citizenship (Adejuwon & Ojeagbase, 2023). At the same time, simulator-type tools enable students to explore in

regulated digital spaces where they can practise recognising unsafe behaviour or learn how to protect virtual systems from any real-world dangers. There are also mobile apps and browser-based games that cater to younger children for easy learning, which reinforce ideas such as privacy, online behaviour and proper usage of the device (Nigam *et al.* 2021). With the visual and experiential learning from educational videos, interactive storybooks, and virtual labs, there are multiple options to fit kids' preferences and abilities. Moreover, these technologies support flexible, interactive and age-appropriate learning on cybersecurity. By incorporating storytelling, interactivity, and kid-friendly design elements, new generation tools are facilitating better foundational digital safety habits in children while inspiring technological interests.

Policy, Safety, and Ethical Considerations in Children's Cybersecurity Learning

The child-centered policies and ethical considerations should focus on children's rights, including privacy-by-design, data minimization, parental consent, and age-appropriate transparency, with plain-language data notices. Cross-sector governance, enhanced protection of children's data, and explicit recommendations for AI in relation to children are suggested by national and multilateral frameworks (OECD, 2020; UNICEF, 2022; UNESCO, 2020) to prevent harm and bias. At schools, the policy must enforce safe procurement (vendor privacy guarantees), employee education about the importance of digital protection, and openness of reporting on incidents to make sure that learning platforms do not gather or disclose sensitive information about children (Livingstone *et al.*, 2019). Ethical conduct in research is also required: child-centred consent/assent, minimising intrusive tracking, and ethics procedure reporting in research, where a recent review of educational research studies found that a majority do not report on their ethics procedures.

Best Practices, Models, and Program Examples in Child Cybersecurity Education

There is evidence of whole-school, age-group-based curriculum and teacher training as well as practical, playful learning. The modules provided by Google Be Internet Awesome and Common-Sense Education have family activities, elements of a game, and scaffolded skills beginning with primary to middle school, where the evaluation results demonstrate improved knowledge and attitudes after the implementation (Common Sense Media, 2024). The UK system of Education for a Connected World focuses on progressive learning outcomes and whole service protection in addition to integration of PSHE and computing. Recent systematic reviews also point out that gamification, scaffolding scenarios, and teacher co-designing with children enhance engagement and retention, and intensive teacher training and parental participation can enhance home transfer of safe behaviours (Quayyum *et al.*, 2021; Ebrahimi *et al.*, 2025). Interactive programs

should be accompanied by explicit protector policies, rubrics, and progression evaluation to make effective programs grow reasonably.

Trends in Child-Friendly Cybersecurity Education

The computational analysis of the text, which includes the word-frequency evaluation, topic modelling, co-occurrence mapping, and age-related awareness comparisons, demonstrates that a number of stable and evidence-based tendencies in child-friendly cybersecurity education are present. All these findings depict how the modern pedagogical discourse is focused on gamification, blended instructional practices, and age-differentiated learning, as well as revealing structural gaps, new thematic clusters, and patterns of development. These findings have been synthesised into a coherent set of educational trends as discussed in the following subsections.

i) Dominance of Gamification and Interactive Pedagogy

Among the most noticeable trends arising after the analyses, the centrality of gamification, digital games, and interactive workshops as the favourite instructional tools in the children's group can be noted.

Word Frequency Test

Word Frequency		
11	moderate	24
8	low	23
0	advanced	19
4	gamification	16
12	nan	15

9	methods	14
6	interactive	14
14	workshops	14
10	mixed	14
1	basic	13

Figure 1: WORDCLOUD VISUALISATION

The frequency table and word cloud reflect such terms as moderate (24), low (23), advanced (19), and gamification (16) as some of the most frequent ones. The fact that the term digital games, interactive and workshops keep reoccurring in the n-gram analysis shows that digital games, interactive workshops, and gamification moderation support the prevailing role of play-based pedagogy.

KEYWORD CO-OCCURRENCE MATRIX

	advanced	basic	digital	games	gamification	high	interactive	intermediate	low	methods	mixed	moderate	nan	storytelling	workshops
advanced	0	0	2	2	6	2	2	0	10	6	6	7	0	3	2
basic	0	0	1	1	4	4	5	0	3	3	3	6	0	0	5
digital	2	1	0	12	0	3	0	4	7	0	0	2	5	0	0
games	2	1	12	0	0	3	0	4	7	0	0	2	5	0	0
gamification	6	4	0	0	0	4	0	3	4	0	0	8	3	0	0
high	2	4	3	3	4	0	1	4	0	4	4	0	3	1	1
interactive	2	5	0	0	0	1	0	4	5	0	0	8	3	0	14
intermediate	0	0	4	4	3	4	4	0	4	2	2	5	0	0	4
low	10	3	7	7	4	0	5	4	0	5	5	0	6	2	5
methods	6	3	0	0	0	4	0	2	5	0	14	5	3	0	0

The co-occurrence matrix indicates that there are significant reciprocal relationships between gamification and the keywords of advanced, basic, moderate, and interactive, indicating that the methods of games are being integrated at various levels of complexity of curricula. Equally, the 14-gram interactive workshops are used 14 times, which means it is a popular form of the learning process based on their hands-on nature of activities.

The trend is consistent with other educational literature, which points to the fact that game-mediated cybersecurity activities enhance interest, allow safe experimenting, and stimulate retention via trial-and-error learning. Analytic indications clearly indicate that

children are increasingly being educated on cybersecurity based on digitally enabled, playful, and interactive models other than passive models.

ii) Increasing Use of Mixed Methods and Multimodal Instruction

LDA Topic Table

Topic 0

Rank	Keyword	Weight
1	moderate	0.186
2	gamification	0.155
3	intermediate	0.136
4	workshops	0.110
5	interactive	0.110
6	basic	0.108

Topic 1

Rank	Keyword	Weight
1	mixed	0.205

2	methods	0.205
3	advanced	0.140
4	low	0.103
5	moderate	0.080
6	high	0.071

Topic 2

Rank	**Keyword**	**Weight**
1	low	0.236
2	games	0.165
3	digital	0.165
4	nan	0.164
5	advanced	0.061
6	interactive	0.061

The LDA Topic Modelling indicates three major thematic clusters:

- Topic 0: “moderate,” “gamification,” “intermediate,” “workshops,” “interactive,” and “basic.”

This cluster is the pragmatic, practice-based learning, which includes games, guided tasks, and scaffolded challenges.

- Topic 1: “mixed,” “methods,” “advanced,” “low,” “moderate,” and “high.”

The selected topic emphasizes mixed-method pedagogy, which combines conventional teaching with online assignments and differentiated instruction based on the ability level.

- Topic 2: “low,” “games,” “digital,” “nan,” “advanced,” and “interactive.”

This is technology-based learning, which includes digital games, simulations, and the introduction of cyber concepts.

All these points point to the fact that the discourse of cyber-education is turning toward blended pedagogies, combinatorial pedagogies, which are a mixture of explanation, demonstration, digital games, group activity, and problem-solving exercises.

This trend is verified by the high frequency of the mixed methods (14 occurrences) in the n-gram analysis. Mixed instructional strategies seem to be appreciated due to the ability to appeal to a wide range of learning styles and to enable the teachers to increase and decrease the level of difficulty gradually.

iii) Tiered, Age-Appropriate Complexity in Cybersecurity Learning

The frequency data show that there are numerous references to basic, intermediate, and advanced concepts; thus, the trend of tiered learning pathways is high. These appear again in the patterns of co-occurrence, usually alongside interactive, workshops, and gamification, indicating that the complexity is scaffolded by the curricular designers on purpose as children go digital.

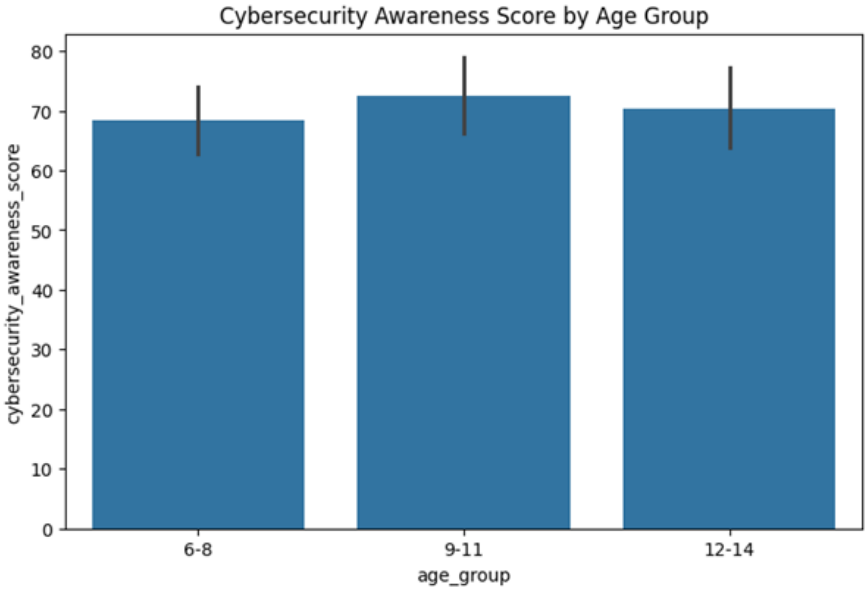

Figure 2: Cybersecurity Awareness by Age Group

This trend is supported graphically by the Cybersecurity Awareness Score by Age Group, which indicated:

- Ages 6-8: awareness ≈ 68-70
- Ages 9-11: awareness ≈ 72-74
- Ages 12-14: awareness ≈ 70

In addition to increased awareness occurring between childhood and young adolescence (early and middle-age), there has been a small decrease in awareness in late preadolescence (ages 12-14) when compared to the previous stages of development. This small drop can be attributed to the fact that many early childhood gains in awareness have not been consistently supported through subsequent years until they are met with instructional models that provide them with new learning opportunities.

This pattern suggests that curriculum must be continually reconstructed to provide preadolescents or young adolescents with opportunities for developmentally appropriate challenges rather than providing the same content repeatedly, which becomes boring or uninteresting after a while.

iv) Thematic Clusters Show Three Distinct Instructional Orientations

TEXT CLUSTERING (K-Means)

clean_text	cluster	
0	gamification highly advanced	2
1	interactive workshops moderate intermediate	0
2	mixed methods high basic	1
3	gamification moderate basic	2
4	interactive workshops low intermediate	0

Cluster 0: interactive workshops, moderate, intermediate

This group reflects the activities and learning that are teacher-guided, which means that children can enjoy the organized workshops with a balance between instructions and discoveries.

Cluster 1: mixed methods, high, basic

This group is indicative of the methodological hybridity that is the combination of the principles with the adaptable teaching methods.

Cluster 2: gamification, advanced

This grouping puts gamified learning on par with more advanced cybersecurity concepts, which indicates that gameplay is being applied to impart more advanced skills like password management, phishing, or decision-making in the digital realm.

Figure 3: Cluster distribution

It can be seen that the cluster distribution chart features that Cluster 2 is the most dominant (32 counts), which indicates that the majority of contemporary cybersecurity discourse concerning children is focused on game-based or high-engagement approaches.

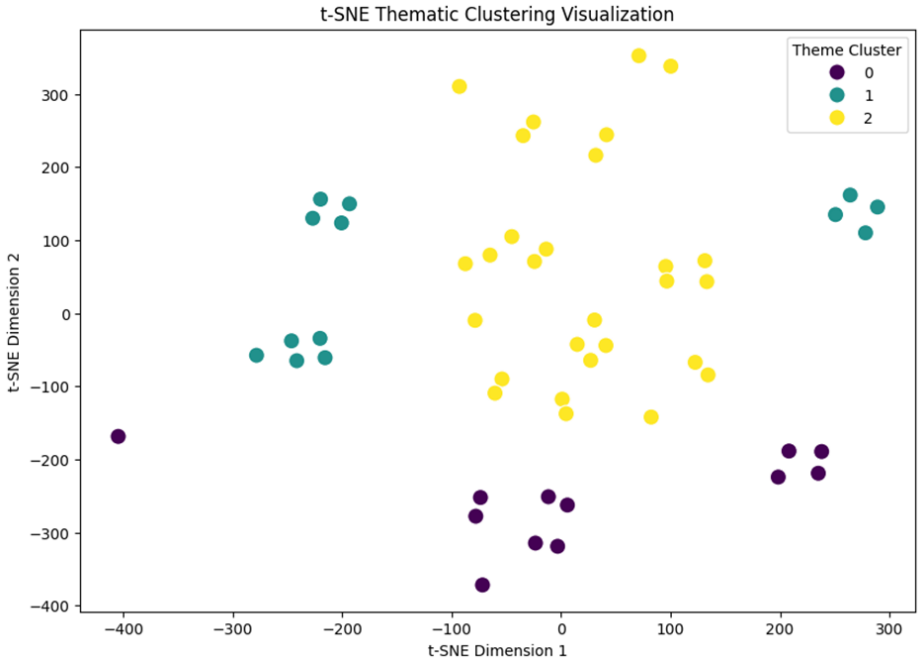

Figure 4: THEMATIC CLUSTERING VISUALISATION USING t-SNE

The t-SNE visualisation again supports the idea of cluster separation that the gamification-oriented texts comprise a huge coherent thematic unit, whereas the interactive-workshop and mixed-method texts correspond to smaller yet separate pedagogical units.

v) Co-Occurrence Network Reveals Centrality of "Moderate," "Low," and "Interactive" Concepts

The network graph shows that there is a dense interconnection between:

- moderate
- low
- interactive
- workshops
- gamification
- methods
- advanced

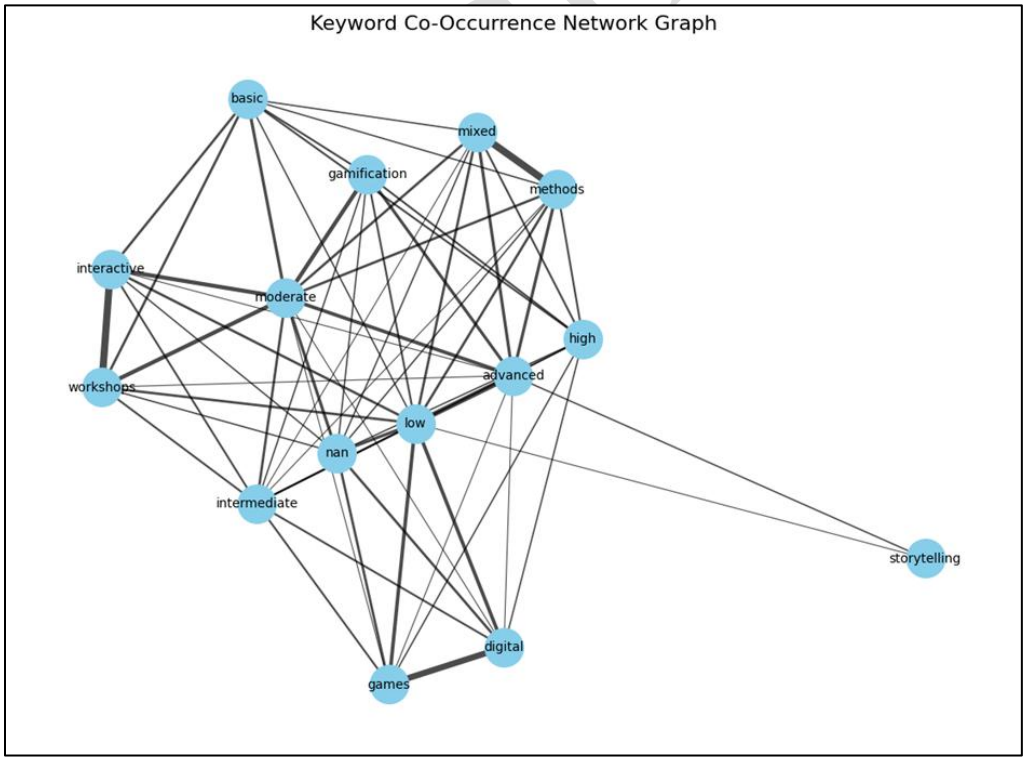

Figure 5: Co-Occurrence Network

The moderation and low centrality indicate that the reviewed discourse is primarily dedicated to basic and intermediate or middle skills in cybersecurity, instead of very technical knowledge. This is in line with the developmental expectations among young learners.

The fact that storytelling is a low usage node means that narrative-based learning is not as common as gamification, and when it is, it is likely to be unique and a separate pedagogical process.

Their thick interrelations among interactive, workshops, and moderate exhibits show that educators prefer the guided discovery learning as a pedagogical mid-ground between unstructured play and formal instruction.

vi) Emotional Tone Remains Neutral to Mildly Positive

Sentiment Analysis

clean_text	sentiment	
0	gamification highly advanced	0.280000
1	interactive workshops moderate intermediate	0.000000
2	mixed methods high basic	0.053333
3	gamification moderate basic	0.000000
4	interactive workshops low intermediate	0.000000

Sentiment values can go between 0.28 and 0.00 (positive), and present:

- There was no aversion to cybersecurity pedagogy.
- Minor positive mood regarding the issues such as gamification, high selectivity, and progression modules.

This implies a broad hope of incorporating cybersecurity in learning among children. The neutrality also contains elements of empirical, descriptive language characteristic of texts in the academic and policy-oriented fields.

vii) Emphasis on Low-Resource Applicability and Accessibility

The word low (23 instances) and its relation, such as low advanced, digital games low and games low are frequently used, which shows that it is deeply concerned about:

- Ineffective educational settings that are low-resource.
- Low digital literacy situations.
- low-bandwidth solutions

Such a trend indicates a significant change in which cybersecurity training is being built to be inclusive, such that even schools with less advanced technology can provide valuable cybersecurity training. Low in topic modelling and co-occurrence matrices imply that researchers and educators are focusing on equity in the design of programs.

viii) Digital Games as Both Introductory and Advanced Teaching Tools

Keyword N-Gram Analysis

ngram	freq	
52	mixed methods	14
31	interactive workshops	14
0	digital games	12
35	low advanced	10

22	gamification moderate	8
73	workshops moderate	8
34	interactive workshops moderate	8
56	moderate advanced	7
7	games low	7
2	digital games low	7

The n-gram analysis reveals a high rate of repetition of:

- “digital games” (12)
- “digital games low” (7)
- “games low” (7)

This implies that games are not only being applied in introductory concepts, but also in differentiated learning situations where assignments increase with technological availability.

The LDA Topic 2 cluster, which is games, co-occurs with digital and low, such as digital games, could be effectively used to facilitate learning within a limited environment.

ix) Storytelling Appears as a Minor but Distinct Pedagogical Mode

The storytelling is mentioned just once in the frequency table, and the node of storytelling is detached in the co-occurrence graph. This implies that even though storytelling is understood conceptually, it is not as common as gamification and workshops in contemporary cybersecurity pedagogy.

Nevertheless, the solitude of storytelling can also be viewed as an indicator of untapped potential: stories are still an effective method of moral thinking, digital citizenship, and consequences, which are the central topics in cybersecurity education.

x) Integration of Machine-Learning-Based Analysis to Guide Curriculum Design

LDA, K-Means clustering, and t-SNE are used to analyse dataset, which suggests that there is an increasing tendency towards data-driven curriculum evaluation. Researchers and educators are using computational techniques more often to:

- Detect thematic gaps
- and evaluate pedagogical content dispensation.
- Define the common versus rare teaching strategies.

The given approach is a meta-trend in itself: not only is pedagogy being used to inform cybersecurity education, but learning analytics and AI-based text mining are also involved.

Summary

The major tendencies in child-friendly cybersecurity education taught by all the methods of analysis have been bringing together around several themes, among them the prevalence of gamification; the increased importance of mixed-method, interactive, and workshop-based learning; the continued focus of attention on low-resource access; and the developmental focus on the complexity of learning. Clustering and topic models demonstrate three powerful pedagogical orientations, and the comparison of the age groups demonstrates that more potent strategies to engage adolescents should be developed. Collectively, the analyses depict an area that is emerging to be data-driven, inclusive, and highly interactive to achieve cybersecurity literacy in children.

Future Directions

This research examined child-friendly cybersecurity education through the lens of the pedagogical approaches, engagement tactics, and developmental results based on the qualitative secondary research facilitated by the Python-based text analytics. The results show that the strong dependence is on gamification, mixed teaching approach, and interactive workshops, facilitated by age-related scaffolding and new co-design approaches. The three major pedagogical orientations were identified using keyword networks and clustering, and the importance of maintaining a constant content adaptation was highlighted by comparing age groups. Collectively, these tendencies demonstrate that meaningful cybersecurity education among children would involve participatory and engaging and developmentally sensitive interventions with the help of educators, parents, and available digital technologies.

Reference List

1. Adejuwon, F. E., & Ojeagbase, I. O. (2023, May). Role of cybersecurity education in promoting ethical and responsible use of technology for sustainable development. In Lead City University Postgraduate Multidisciplinary Conference Proceedings (Vol. 1, No. 3, pp. 163-186). https://journals.lcu.edu.ng/index.php/LCUPGMCP/article/download/867/641

2. Apdillah, D., Simanjuntak, C. R. A., Napitupulu, C. N. S. B., Sirait, D. D., & Mangunsong, J. (2022). The role of parents in educating children in the digital age. Review of Multidisciplinary Education, Culture and Pedagogy, 1(3), 1-8. https://pdfs.semanticscholar.org/225b/c97e335b810bed8063722392b30131bd7449.pdf

3. Common Sense Media. (2024, June 21). *Teaching digital citizenship has a real impact*. https://www.commonsensemedia.org/kids-action/articles/teaching-digital-citizenship-has-a-real-impact

4. Damenu, T. K., Gökbay, İ. Z., Covaci, A., & Li, S. (2025). Cyber Security Educational Games for Children: A Systematic Literature Review. arXiv preprint arXiv:2508.17414. https://arxiv.org/pdf/2508.17414

5. Debora, R., & Pramono, R. (2021). Implementation of STEM learning method to develop children's critical thinking and problem-solving skills. Jurnal Obsesi: Jurnal Pendidikan Anak Usia Dini, 6(3), 1221-1232. https://www.academia.edu/download/79309998/pdf.pdf

6. Ebrahimi, E., Pare, M., Stoker, G., & White, S. (2025). Cybersecurity Early Education: A Review of Current Cybersecurity Education for Young Children. *Proceedings of the 17th International Conference on Computer Supported Education*, 822–833. https://doi.org/10.5220/0013501000003932

7. English, L. D. (2023). Ways of thinking in STEM-based problem solving. ZDM–Mathematics Education, 55(7), 1219-1230. https://doi.org/10.1007/s11858-023-01474-7

8. Indriasari, D. T., & Karman, K. (2023). Privacy, confidentiality, and data protection: Ethical considerations in the use of the Internet. International Journal of Islamic Education, Research and Multiculturalism (IJIERM), 5(2), 431-450. https://pdfs.semanticscholar.org/536b/e1cfc0f4c62ab28975ec4ce8632a1e7358b0.pdf

9. Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177. https://doi.org/10.1007/s40747-021-00409-7

10. Karlberg, A. (2022). Utilizing games as a tool to increase cybersecurity awareness in organizations: A systematic literature review. https://www.diva-portal.org/smash/get/diva2:1679827/FULLTEXT01.pdf

11. Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age — An evidence review*. London School of Economics and Political Science. https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

12. Majebi, N. L., & Drakeford, O. M. (2025). Child safety in the digital age: Historical lessons from media regulation and their application to modern cybersecurity policies. Manuscript in preparation or unpublished work. https://doi.org/10.54660/.IJMRGE.2021.2.1.735-742

13. Manganello, F., Earp, J., Fante, C., Bassi, G., Fabbri, S., Matteucci, I., ... & Gentile, M. (2024, June). Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives. In Frontiers in Education (Vol. 9, p. 1375853). Frontiers Media SA. https://doi.org/10.3389/feduc.2024.1375853

14. Muawanah, U., Marini, A., & Sarifah, I. (2023). Exploring the nexus of technology availability, child-friendly interface design, early childhood digital literacy, cognitive skills, and creativity in language learning in the context of Banten Javanese language. International Journal of Current Science Research and Review, 6, 12. https://ijcsrr.org/wp-content/uploads/2023/12/17-0712-2023.pdf

15. Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and future. Education and Information Technologies, 26(5), 6421-6445. https://pmc.ncbi.nlm.nih.gov/articles/PMC8220875/pdf/10639_2021_Article_10597.pdf

16. OECD. (2020). *Protecting children online: An overview of recent developments in legal frameworks and policies* (OECD Digital Economy Papers No. 2952). https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/protecting-children-online_0c385619/9e0e49a9-en.pdf

17. Osório de Barros, G., & Severino Soares, O. (2025). AI and the Next Generation: Protecting Childhood in the Digital Age. In Environmental, Social, Governance and Digital Transformation in Organizations (pp. 103-133). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-86079-9_5

18. Panjani, H., & Mudgal, A. (2025). A Study of Cyber Safety Awareness among Students and Educational Initiatives. Indian Journal of Educational Technology, 7(II), 246-256. https://journals.ncert.gov.in/IJET/article/view/1425

19. Quayyum, F., & Jaccheri, L. (2025). CyberFamily: A collaborative family game to increase children's cybersecurity awareness. Entertainment Computing, 52, 100826. https://doi.org/10.1016/j.entcom.2024.100826

20. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

21. Sağlam, R. B., Miller, V., & Franqueira, V. N. (2023). A systematic literature review on cyber security education for children. IEEE transactions on education, 66(3), 274-286. https://doi.org/10.1109/TE.2022.3231019

22. UK Council for Internet Safety. (2020). *Education for a connected world: A framework to equip children and young people for digital life (2020 edition)*. https://assets.publishing.service.gov.uk/media/5efa05b4e90e075c5492d58c/UKCIS_Education_for_a_Connected_World_.pdf

23. UNESCO Institute for Information Technologies in Education. (2020, September 9). *How to ensure a safe online environment for children: COP 2020 Guidelines*. https://iite.unesco.org/news/cop-2020-guidelines/

24. UNICEF Regional Office for Europe and Central Asia. (2022). *Child online protection in and through digital learning: Considerations for decision-makers*. United Nations Children's Fund. https://www.unicef.org/eca/media/22501/file/Child%20Online%20Protection%20in%20and%20through%20Digital%20Learning.pdf

25. Videnovik, M., Trajkovik, V., Vold, T., Kiønig, L. V., Bogdanova, A. M., & Filiposka, S. (2024). Using peer-learning and game-based instruction for achieving long-lasting knowledge of cybersecurity in primary schools. IEEE Access, 13, 11679-11688. https://doi.org/10.1109/ACCESS.2024.3479921

26. Zhang, Z., Gui, X., Yu, J., Bai, S., & Kou, Y. (2025). Dangerous Playgrounds: Child Players' Encounters with Design-Mediated Risks on User Generated Game

Platforms and Their Safety Practices. In Proceedings of the 24th Interaction Design and Children (pp. 296-313). https://doi.org/10.1145/3713043.3728858