Journal of
Information Technology,
Cybersecurity, and Artificial Intelligence

(RESEARCH)

Cybersecurity Education in K–12 Schools: A Thematic Analysis of Pandemic-Era Literature

Dr. Ian Matthew Herzing

Herzing University, Department of Business & Legal Studies

Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2026, 3(1), 27–38

Article DOI: https://doi.org/10.70715/jitcai.2026.v3.i1.048

Abstract

The COVID-19 pandemic (2020–2025) accelerated digitalization in K–12 education, exposing students, educators, and families to heightened cybersecurity risks. This systematic review synthesizes more than 60 peer-reviewed studies, reports, and policy documents to examine how cybersecurity education initiatives evolved during and after the pandemic and what evidence exists regarding their effectiveness. Using Braun and Clarke's (2006) thematic analysis supplemented by an evidence-strength assessment, eight themes emerged: evolving cyber risks; cyberbullying and digital safety; teacher preparation; equity and access; curricular innovation; governance and policy; socio-emotional wellbeing; and AI-based interventions. Interventions included digital citizenship curricula, gamified learning tools, AI-supported safety monitoring, teacher professional development, and national policy frameworks. While AI-based tools were increasingly deployed for content filtering and threat detection, empirical evidence of their effectiveness in K–12 settings remains limited. Findings indicate that initiatives are most effective when embedded within socio-technical systems aligning pedagogy, technology, and governance. However, uneven implementation, equity gaps, and limited teacher capacity constrained impact. The review highlights the need for sustained professional development, equity-focused policy, holistic digital wellbeing, and longitudinal, cross-cultural research emphasizing student agency and rigorous evaluation of AI-enhanced interventions.

Keywords: COVID-19, cybersecurity, digital citizenship, qualitative study, curriculum development

1. Introduction

The rapid digitalization of education during the COVID-19 pandemic fundamentally transformed how young people engaged with technology. As schools shifted abruptly to remote learning, millions of students required constant internet access for educational continuity, exposing significant gaps in cybersecurity preparedness among students, teachers, and families (Ibrahim et al., 2024; Johnson et al., 2022). The blurring of boundaries between school and home environments amplified existing digital risks, increasing vulnerability to threats such as phishing, platform disruptions, and online grooming (Ling et al., 2021; Finkelhor et al., 2022). Parental oversight challenges identified prior to the pandemic became more pronounced as homes functioned as primary learning spaces (Ahmad et al., 2018).

Pre-pandemic cybersecurity education largely emphasized general awareness, but pandemic conditions created urgent, context-specific challenges that existing curricula were not designed to address (Catota et al., 2019; Mee, 2020). In response, education systems rapidly implemented emergency safeguards while rethinking longer-term digital safety strategies. This systematic literature review examines cybersecurity education initiatives in K–12 settings during and after the COVID-19 pandemic (2020–2025).

The study addresses the research question: How did cybersecurity education in K–12 settings evolve during and after the COVID-19 pandemic, and what thematic lessons emerge regarding implementation, challenges, and effectiveness? The paper outlines the review methodology, presents emergent themes and initiatives across global contexts, discusses key challenges and gaps, and concludes with directions for future research in post-pandemic cybersecurity education.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i1.048

2. **Methodology**

This study employed a systematic literature review guided by PRISMA 2020 to ensure transparent, reproducible identification, selection, and synthesis of relevant studies (Page, 2021). Academic sources were drawn primarily from ERIC, supplemented by grey literature identified through Google searches, including government reports and international frameworks, allowing integration of empirical and policy perspectives. To strengthen rigor, the PICO framework was applied to align the research question and search strategy (Methley et al., 2014). The population focused on K–12 students and educators; interventions included cybersecurity education initiatives; comparisons examined pre-, during-, and post-pandemic contexts; and outcomes addressed awareness, competencies, and implementation effectiveness. Table 1 outlines the Boolean search strategy translating PICO elements into population, intervention, context, and outcome terms.

Table 1 Search Strategy for K-12 Cybersecurity Education Post-Pandemic (2015-2025)

Component	Search Terms	Boolean Operators
Population	"K-12" OR "primary school*" OR "elementary school*" OR "secondary school*" OR "high school*" OR "middle school*" OR "junior high" OR "student*" OR "pupil*" OR "learner*" OR "child*" OR "adolescent*" OR "teen*" OR "youth"	OR
Intervention	"cybersecurity education" OR "cyber security education" OR "cyber safety" OR "digital safety" OR "online safety" OR "information security education" OR "cyber awareness" OR "digital security education" OR "cyber hygiene" OR "cyber literacy"	AND
Context	"COVID-19" OR "coronavirus" OR "pandemic" OR "SARS-CoV-2" OR "remote learning" OR "distance learning" OR "online learning" OR "virtual learning" OR "hybrid learning" OR "emergency remote teaching" OR "school closure*"	AND
Outcomes	"curriculum" OR "intervention*" OR "program*" OR "initiative*" OR "framework*" OR "competenc*" OR "skill*" OR "awareness" OR "behaviour" OR "behavior" OR "knowledge" OR "practice*" OR "implementation" OR "evaluation" OR "assessment"	AND

Table 2 details the database-specific search strategies, including Google Scholar, ERIC, and Semantic Scholar. Each database required slight adjustments in syntax and filters. For example, Google Scholar searches emphasized title, abstract, and keywords, while ERIC applied peer-review and education-level filters. These adjustments ensured coverage of relevant literature within the 2020–2025 timeframe.

Table 2 Primary Database Search Strategy

Database	Search String	Filters/Limiters
Google Scholar	("K-12" OR "primary school" OR "elementary school" OR "secondary school" OR "high school" OR "middle school") AND ("cybersecurity education" OR "cyber security education" OR "cyber safety" OR "digital safety" OR "online safety") AND ("COVID-19" OR "coronavirus" OR pandemic OR "remote learning" OR "distance learning")	• 2015-2025 • Language: English
ERIC	(title:"cybersecurity" OR abstract:"cybersecurity" OR title:"cyber safety" OR abstract:"cyber safety" OR title:"digital safety" OR abstract:"digital safety") AND (title:"K-12" OR abstract:"K-12" OR abstract:"elementary" OR abstract:"secondary" OR abstract:"school") AND (abstract:"pandemic" OR abstract:"COVID-19" OR abstract:"remote learning")	• Publication Date: 2015-2025 • Peer reviewed, dissertations, GAO reports • Educational level: Elementary, Middle, High School • Language: English
Semantic Scholar	("K-12" OR "primary school" OR "elementary school" OR "secondary school" OR "high school" OR "middle school")	• Year: 2015–2025 • Language: English

	AND ("cybersecurity education" OR "cyber safety" OR "digital safety" OR "online safety" OR "digital citizenship") AND ("COVID-19" OR pandemic OR "remote learning" OR "distance learning")	

Table 3 outlines the targeted grey literature sources. These included U.S. Department of Education resources, CISA reports, and UNESCO pandemic education analyses. The rationale for including grey literature was to capture practical guidance, emerging frameworks, and implementation evidence not always available in peer-reviewed sources. This complemented the academic literature and provided real-world context for K-12 cybersecurity education initiatives.

Table 3 Focused Grey Literature Sources

Source Type	Specific Targets	Rationale
Government Education	• US Department of Education COVID-19 resources • CISA K-12 Cybersecurity resources • State education department pandemic reports	Direct policy and implementation documentation
International Organizations	• UNESCO digital education reports (2020-2025) • OECD pandemic education responses	Cross-national comparative data
Preprints	• EdArXiv (education-focused) • SSRN education/technology sections	Recent studies not yet in peer review

Table 4 summarizes the inclusion and exclusion criteria. Only studies published between 2015 and 2025, focused on K-12 populations, and tied to pandemic-related contexts were included. Higher education-focused studies, purely technical security papers without an educational lens, or opinion-based pieces without empirical evidence were excluded. This ensured relevance and consistency across the body of evidence analyzed.

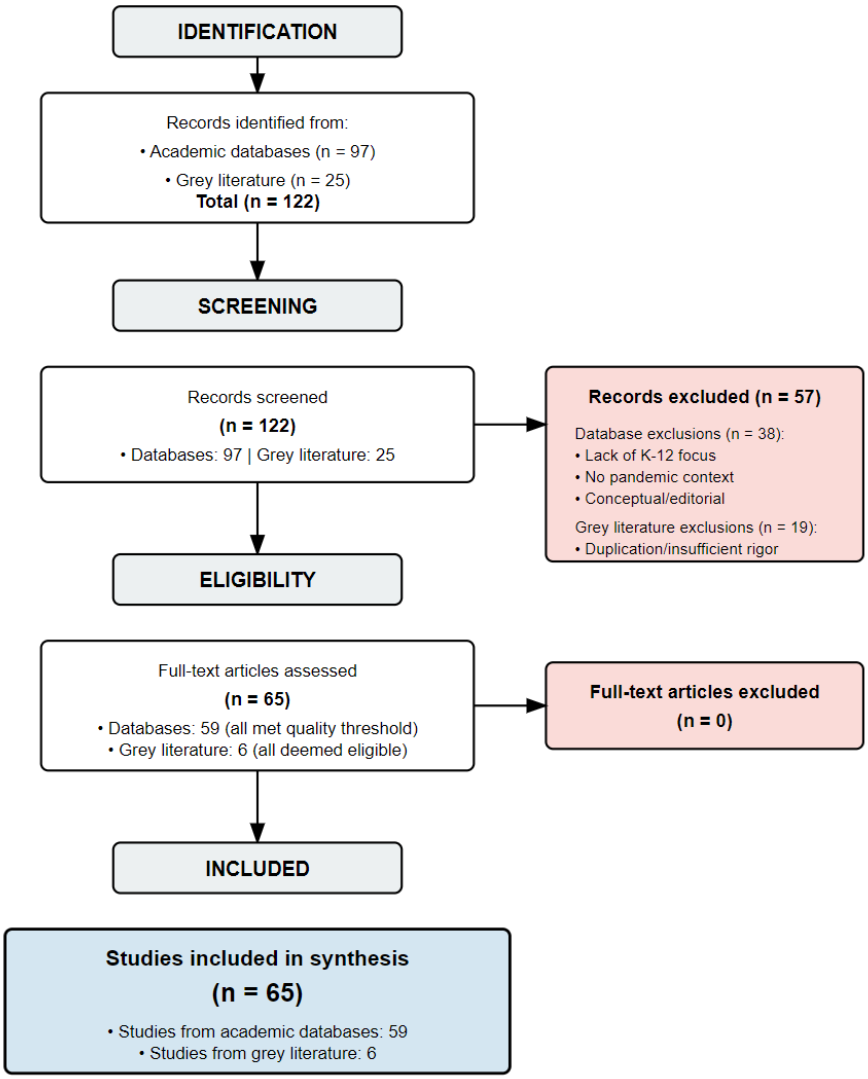
Table 4 Inclusion/Exclusion Criteria

Criteria	Inclusion	Exclusion
Time Period	January 2015 - December 2025	Before 2015
Population	K-12 students, teachers, schools	Higher education only, adult learners
Study Focus	Cybersecurity education initiatives, curricula, interventions	Pure technical security papers without educational component
Context	Pandemic-related or post-pandemic adaptations	Pre-pandemic studies without COVID-19 context
Language	English (or other languages you read)	Non-accessible languages
Publication Type	Peer-reviewed articles, conference papers, government reports, grey literature	Opinion pieces without data, news articles

In accordance with PRISMA 2020, the identification phase involved systematic searches across multiple sources. Database searches yielded 24 records from ERIC, 33 from Semantic Scholar, and 40 from Google Scholar, with an additional 25 documents identified through grey literature sources, totaling 122 records. During screening, 97 academic records were reviewed, and 38 were excluded based on relevance and scope, leaving 59 eligible full texts. Of the grey literature, 19 were excluded due to duplication or limited rigor, and six were retained. In total, 65 studies were included in the synthesis, as summarized in the PRISMA flow diagram (Figure 1).

DOI: https://doi.org/10.70715/jitcai.2026.v3.i1.048

Figure 1 ***PRISMA Diagram***



This study applied Braun and Clarke's (2006) thematic analysis to synthesize findings across the reviewed literature. Following the six-phase process, articles were repeatedly read to support familiarization, after which initial codes captured recurring patterns related to teacher capacity, digital safety, equity, and policy. Codes were grouped into candidate themes that were iteratively reviewed for coherence and distinction. Themes were then defined and aligned with the research question, clarifying their analytic contribution. Finally, the themes were integrated into a narrative explaining how K–12 cybersecurity education evolved between 2020 and 2025. This reflexive approach supported rigorous, transparent synthesis across diverse empirical and policy sources.

To address methodological heterogeneity across sources, a simplified evidence-strength rubric was applied during synthesis. Sources were classified into three tiers based on methodological rigor: (1) high-rigor sources included peer-reviewed empirical studies with experimental or quasi-experimental designs, validated instruments, and clearly defined samples (e.g., Ivy et al., 2020; Nguyen et al., 2024; Gaffney et al., 2021); (2) moderate-rigor sources included peer-reviewed qualitative studies, systematic reviews, and policy analyses with transparent methods (e.g., Sorrentino et al., 2023; Ibrahim et al., 2024; Martin et al., 2023); and (3) lower-rigor sources included grey literature, descriptive reports, and dissertations without peer review (e.g., Project Tomorrow, 2021; CISA, 2022; Couch, 2024). During thematic synthesis, findings supported by high-rigor sources were weighted more heavily, while claims derived primarily from lower-rigor sources were flagged as preliminary or requiring further validation. This stratified approach enhances transparency regarding the evidentiary basis of each theme.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i1.048

3. Results

Between 2020 and 2025, the COVID-19 pandemic marked a transformative period for K–12 education as schools rapidly shifted to digital learning environments, exposing significant vulnerabilities in cybersecurity infrastructure, teacher preparedness, and student safety. An inductive thematic analysis of more than sixty sources, stratified by methodological rigor, identified eight themes: evolving cyber risks; cyberbullying and digital safety; teacher capacity and professional development; digital equity and structural barriers; pedagogical innovation and curricular integration; policy, governance, and system-level responses; socio-emotional impacts and digital wellbeing; and AI-based interventions. The analysis followed Braun and Clarke's six-phase framework, organizing initial codes into higher-order themes. Cross-cutting issues, including leadership, parental involvement, and international variation, further contextualized the findings, producing a data-driven and theoretically robust synthesis of K–12 cybersecurity education during and after the pandemic.

Table 5 Codes and Corresponding Themes from the Thematic Analysis

Initial Codes	Corresponding Theme
Cyberbullying incidents; Online grooming; Harassment via social media/gaming	Cyberbullying and Digital Safety Challenges
Teacher preparedness; Professional development gaps; Preservice training deficits	Teacher Preparation and Professional Development
Equity of access; Rural–urban disparities; Device/bandwidth shortages; Competition access gaps	Digital Equity and Access
Gamified learning; Serious games; Digital comics/apps; Curricular integration	Pedagogical Frameworks and Curricular Innovation
Policy fragmentation; Federal coordination gaps; Leadership awareness; Principal digital leadership	Governance, Policy, and System-Level Responses
Pandemic-driven risks; Data breaches; Ransomware; Phishing attacks	Evolving Risks and Cyber Vulnerabilities
Student anxiety/depression; Digital wellbeing; Online habits; Dual digital identities	Socio-Emotional Consequences and Digital Wellbeing
Parent awareness gaps; Community support structures; Cross-sector collaboration	Cross-Cutting: Parental and Community Involvement
AI content filtering; Adaptive learning platforms; Automated threat detection; Algorithmic monitoring	AI-Based Interventions (Cross-Cutting)

3.1. Theme 1: Evolving Risks and Cyber Vulnerabilities

Schools' digital infrastructures have become attractive targets for malicious actors. The U.S. Government Accountability Office (2020, 2022) documented 99 cyber breaches in K–12 systems between 2016 and 2020, with ransomware and phishing attacks causing prolonged disruptions. Howard (2021) reported a 60 percent increase in incidents during 2020, attributing many breaches to human-factor vulnerabilities such as weak passwords and unsafe clicking behaviors. The Council of the Great City Schools (2017) emphasized the need for holistic security across identity, networks, applications, and endpoints, while CISA (2022, 2024) promoted layered digital and physical defenses through the School Security Assessment Tool. International comparisons further show that governance structures shape resilience, with centralized systems offering consistency and decentralized models amplifying inequities (Fernández Nieto et al., 2025; OECD, 2020).

3.2. Theme 2: Cyberbullying and Digital Safety Challenges

Cyberbullying has emerged as one of the most persistent risks. Nguyen et al. (2024) identified behavioral predictors of electronic bullying in U.S. high schools, while Marinoni et al. (2024) observed gendered differences: girls were more vulnerable on social media, boys in gaming. Sorrentino et al. (2023) synthesized global data and found that prevalence shifted regionally during COVID-19, with increases in Asia and Australia but some declines in Western contexts. Khalid (2017) had previously examined how students used Facebook for collaborative learning, establishing a baseline understanding of educational social media use before these platforms became vectors for harassment during the pandemic.

Paul (2022) reported Indian students experiencing online grooming and harassment, often concealing incidents due to stigma. Dahal (2023) documented similar harms in Nepal, with Facebook-based bullying producing anxiety and school disengagement. Intan et al. (2023) identified demographic, family, and societal determinants of vulnerability across 27 studies.

Gaffney et al. (2021) argued that IT tools (filters, AI-based monitors) must be combined with awareness programs to reduce risks. Martin et al. (2023) showed U.S. elementary teachers frequently confronted privacy and safety concerns but lacked structured guidance. Zulqadri et al. (2022) recommended active adult supervision, stronger ethics instruction, and student-centered awareness campaigns during online learning. Together, the evidence demonstrates cyberbullying's resilience across contexts and the inadequacy of fragmented school-level interventions.

3.3. Theme 3: Teacher Preparation and Professional Development

Teacher capacity consistently emerges as a critical gap in K–12 cybersecurity education. Studies across multiple contexts show that educators often feel underprepared to teach digital safety, with disparities by gender, age, and program level (Ivy et al., 2020; Latorre-Medina & Tnibar Harrus, 2023; Guillén-Gámez et al., 2024). Teachers frequently recognize the importance of cybersecurity but report low confidence and limited formal training, relying instead on informal sources (Dambrosio, 2021; Ravichandran et al., 2025). Promising initiatives demonstrate that targeted professional development can improve teacher confidence and instructional practice. Programs such as GenCyber Knights strengthened inquiry-based learning and classroom readiness (Ivy et al., 2020), while cross-sector and youth-inclusive frameworks emphasize shared responsibility and sustained capacity building (Ng, 2025; Alaofin, 2025). These findings underscore that sustainable cyber literacy depends on systematic, ongoing professional development embedded within teacher preparation and school leadership structures.

3.4. Theme 4: Digital Equity and Access

The digital divide magnifies cybersecurity risks. Anakwe et al. (2021) described African American families' "sink or swim" experiences during COVID-19, with poor device access, bandwidth shortages, and low institutional support intensifying stress. Amundson and Ko (2021) found remote learning disproportionately harmed marginalized U.S. students, with rising failure rates.

OECD (2020) documented how disadvantaged children lacked private study spaces, parental support, and secure devices. The U.S. Department of Education's National Educational Technology Plan (2024) reframed the divide into access, design, and use, arguing that while device access improved, meaningful use remained inequitable.

Jacob (2024) and Jiang et al. (2022) noted cybersecurity courses existed in only 192 U.S. schools across 11 states, with rural communities most excluded. Participation in competitions like CyberPatriot was uneven, further entrenching inequities. Fernández Nieto et al. (2025) showed how fragmented U.S. initiatives exacerbated disparities compared to China's universalized policies. Together, these findings illustrate that without equity, cybersecurity initiatives risk reproducing privilege: underserved communities face both reduced protection and diminished opportunities for future cyber careers.

3.5. Theme 5: Pedagogical Frameworks and Curricular Innovation

A major theme is the shift toward embedding cybersecurity education within K–12 curricula rather than relying on isolated interventions. Amankwa (2021) argued that cybersecurity must span all grade levels to address risks such as fraud and online exploitation, while Ondrušková and Pospíšil (2023) found one-off programs had minimal impact without systematic integration. Ayeyemi (2023) highlighted weak evaluation practices and advocated for project-based and game-based learning. Evidence strongly supports game-based approaches, with studies showing improved understanding of phishing, privacy, passwords, and online safety through serious games and interactive tools (Bassi et al., 2022; Amin, 2025; Arishi et al., 2024). Recent frameworks extend beyond technical skills to include digital wellbeing, literacy, and policy alignment, underscoring the importance of holistic, curriculum-embedded approaches for long-term resilience.

3.6. Theme 6: Governance, Policy, and System-Level Responses

Governance and leadership are central to effective cybersecurity education. U.S. Government Accountability Office (2022) criticized the U.S. Department of Education for failing to coordinate sector-wide cybersecurity. Project Tomorrow (2021) found that only 39% of technology leaders perceived superintendents as highly aware of cybersecurity risks, revealing leadership gaps. Karakose et al. (2021) found principals' digital leadership strongly influenced teachers' adoption of safe practices.

CISA advanced systems-based frameworks for integrating physical and cyber defenses. The SSAT guides schools in evaluating layered measures, communication capabilities, and training (CISA, 2022, 2024). The U.S. Department of Education (2021) linked digital safety to school reopening, while its National Educational Technology Plan (2024) emphasized privacy, design, and equity.

Internationally, Fernández Nieto et al. (2025) highlighted structural differences: centralized governance in China improved consistency, while the EU balanced local flexibility with shared standards. Sadaghiani-Tabrizi (2023) stressed that leadership vision, governance, and continual awareness were essential to resilience during disruptions. Together, these findings confirm that cybersecurity requires multi-level coordination spanning governance, funding, and institutional culture.

3.7. Theme 7: Socio-Emotional Consequences and Digital Wellbeing

Cybersecurity is also a matter of wellbeing. Paul (2022) and Dahal (2023) documented severe psychological harms from online harassment, including depression and withdrawal. King et al. (2018) highlighted risks of gaming addiction and maladaptive digital behaviors. Rad and Demeter (2019) showed that digital identity dualities influenced emotional regulation in adolescents.

Cowling et al. (2025) emphasized that digital wellbeing, encompassing balanced habits, healthy online relationships, and literacy, was essential to learning outcomes. Palalas and Doran (2023) linked safety to wellness, arguing that attention and agency were core components. Sadaghiani-Tabrizi (2023) emphasized the need for resilience and holistic support during crises. These findings illustrate that cybersecurity interventions cannot be divorced from socio-emotional supports. Protecting students requires integrating mental health, digital citizenship, and resilience into cybersecurity pedagogy.

3.8. Cross-Cutting Analysis: AI-Based Interventions in K–12 Cybersecurity Education

Across the reviewed literature, artificial intelligence emerged as a supporting rather than central element in K–12 cybersecurity education. AI-based interventions appeared in three primary forms: AI-supported content filtering and monitoring systems, adaptive learning platforms, and automated threat detection tools. Gaffney et al. (2021) noted that AI-enhanced content filters were increasingly deployed alongside educational programs to detect cyberbullying and inappropriate content in real time. Similarly, CISA (2022, 2024) referenced layered digital defenses incorporating AI-based threat detection, though implementation details and efficacy data remained sparse.

However, critical gaps limit the analytical contribution of AI within this literature. First, most references to AI-based tools were descriptive rather than evaluative; few studies provided empirical evidence of effectiveness in K–12 contexts. Second, ethical considerations—including student privacy, algorithmic bias, and the balance between surveillance and safety—were largely unaddressed. Third, the reviewed sources did not distinguish between AI as an educational topic (teaching students about AI and its cybersecurity implications) and AI as an intervention mechanism (using AI tools to enhance safety). This ambiguity limits the precision of conclusions regarding AI's pedagogical role.

Future research should rigorously evaluate AI-based interventions through controlled studies that assess impact on student knowledge, behavior, and safety outcomes. Additionally, research designs should address ethical dimensions including informed consent, transparency in algorithmic decision-making, and equitable access to AI-enhanced protections across socioeconomically diverse school districts.

4. Limitations

This study has several limitations. First, the thematic analysis was coded by a single researcher following Braun and Clarke's (2006) six-phase approach. Without multiple coders, the analysis is more susceptible to subjective interpretation, and themes may reflect individual bias. Reflexive journaling and transparency mitigated this risk, but inter-coder validation would have enhanced reliability.

Second, the review was limited to English-language, published, and accessible sources. Interventions documented in other languages or in unpublished internal reports were excluded, potentially biasing findings toward anglophone and higher-income contexts (OECD, 2020). Publication bias is also likely, as unsuccessful or less formal interventions were underreported.

Third, methodological quality across sources varied widely. While some interventions were evaluated with rigorous experimental designs (e.g., Ivy et al., 2020), others relied on descriptive or anecdotal reporting (Project Tomorrow, 2021). To address this heterogeneity, a simplified evidence-strength rubric was applied during synthesis, stratifying sources into high-, moderate-, and low-rigor categories. However, this approach remains less rigorous than formal risk-of-bias tools and could not fully compensate for the underlying variability. Moreover, many interventions were implemented rapidly during pandemic disruptions, meaning long-term outcomes remain uncertain (GAO, 2020; GAO, 2022).

Finally, the extraordinary circumstances of COVID-19 shaped much of the evidence. Some interventions reflected emergency responses rather than sustainable practices. As such, while the findings highlight important directions for cybersecurity education, their generalizability to stable, post-pandemic contexts must be considered with caution.

5. **Findings and Discussion**

During the COVID-19 pandemic and its aftermath, K–12 schools implemented diverse cybersecurity education interventions to protect students in rapidly expanding online learning environments. These included digital safety and citizenship training, curriculum integration of cybersecurity topics, cyberbullying prevention, teacher professional development, and new policy frameworks. Evidence indicates these efforts improved awareness and resilience and, in some cases, reduced online safety incidents, though outcomes varied by context, implementation quality, and institutional support (GAO, 2020, 2022; Howard, 2021).

Digital safety and citizenship education emerged as a core intervention, with structured curricula improving student knowledge of social media use, scams, and digital footprints (Ivy et al., 2020; Martin et al., 2023). Sustained, culturally responsive instruction and family involvement proved more effective than isolated lessons (Palalas & Doran, 2023; Couch, 2024). Curriculum integration advanced unevenly despite national and international frameworks and game-based approaches that increased engagement (Bassi et al., 2022; Fernández Nieto et al., 2025). Disadvantaged schools and underprepared teachers faced persistent barriers (Jacob, 2024; Ayeyemi, 2023).

Cyberbullying rose during lockdowns, with combined educational and monitoring approaches showing the strongest reductions (Gaffney et al., 2021). Policy analyses emphasize that cybersecurity education is most effective when treated as a socio-technical system integrating pedagogy, technology, and governance, supported by sustained investment and equity-focused leadership (GAO, 2022; U.S. Department of Education, 2024).

6. **Conclusion and Future Work**

This review shows that the COVID-19 pandemic functioned both as a stress test and a catalyst for K–12 cybersecurity education. Schools rapidly implemented digital safety training, integrated cybersecurity concepts into curricula, expanded cyberbullying prevention, and adopted new policies addressing privacy and digital wellbeing. Evidence indicates that effectiveness depended heavily on teacher professional development, leadership support, and sustained implementation, while equity gaps and underfunded mandates constrained access in many communities. Overall, cybersecurity education proved most effective when treated as a socio-technical system integrating pedagogy, technology, and governance. To sustain progress, schools should embed cybersecurity competencies within national standards, ensure equitable resource allocation, and balance technical literacy with holistic digital wellbeing. Future research should prioritize longitudinal and cross-cultural studies, examine student agency in program design, evaluate scalable teacher professional development models, and rigorously assess emerging approaches such as gamification, AI-supported monitoring, and family engagement to determine their long-term impact.

7. **References**

[1] Ahmad, N., Asma' Mokhtar, U., Fauzi, W. F. P., Othman, Z. A., Yeop, Y. H., & Abdullah, S. N. H. S. (2018). Cyber Security Situational Awareness Among Parents. In *2018 Cyber Resilience Conference* (pp. 1-3). IEEE. https://doi.org/10.1109/CR.2018.8626830

[2] Alaofin, B. A. (2025). Cybersecurity: Empowering K-12 Teachers and Administrators to Protect Children from Online Risks [Preprint]. East Tennessee State University. https://www.researchgate.net/publication/390569110_Cybersecurity_Empowering_K_-12_Teachers_And_Administrators_To_Protect_Children_From_Online_Risks

[3] Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, 12(4), 233-249. https://doi.org/10.4236/jis.2021.124013

[4] Amin, S. (2025). Play and Protect: Exploring Game-Based Learning for Cyber Safety in Primary Education [Master's thesis, UNSW Canberra]. UNSWorks. https://doi.org/10.26190/unsworks/30903

[5] Amundson, K., & Ko, A. (2021). The Role of Technology in Reimagining School. *State Education Standard*, 21(2), 13-18.

[6] Anakwe, A., Majee, W., Noel-London, K., Zachary, I., & BeLue, R. (2021). Sink or Swim: Virtual Life Challenges Among African American Families During COVID-19 Lockdown. *International Journal of Environmental Research and Public Health*, 18(8), 4290. https://doi.org/10.3390/ijerph18084290

[7] Arishi, A. A., Kamarudin, N. H., Bakar, K. A. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences. *International Journal of Advanced Computer Science and Applications*, 15(12), 467-473. https://doi.org/10.14569/IJACSA.2024.0151260

[8] Ayeyemi, B. M. (2023). A Systematic Review of Cybersecurity Education in K-12 Context [Master's thesis, University of Eastern Finland]. UEF eRepository. https://erepo.uef.fi/server/api/core/bitstreams/3053fee6-cadb-4d0d-a616-a93cc30f36df/content

[9] Bassi, G., Fabbri, S., & Vaccarelli, A. (2022). Cybersecurity Education: A Gamification Approach. In *Conference Proceedings of the 12th International Conference on The Future of Education 2022* (pp. 403-409). Filodiritto Editore.

[10] Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

[11] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cybersecurity*, 5(1), Article tyz001. https://doi.org/10.1093/cybsec/tyz001

[12] Couch, V. (2024). Investigating the Impact of Cybersecurity Awareness in K-12 Context: A Quantitative Research Method [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations Publishing. https://eric.ed.gov/?q=risk&pg=130&id=ED651485

[13] Council of the Great City Schools. (2017). Cyber-Security in Today's K-12 Environment. Baltimore City Public Schools.

[14] Cowling, M., Sim, K. N., Orlando, J., & Hamra, J. (2025). Untangling Digital Safety, Literacy, and Wellbeing in School Activities for 10 to 13 Year Old Students. *Education and Information Technologies*, 30(1), 941-958. https://doi.org/10.1007/s10639-024-13183-z

[15] Cybersecurity and Infrastructure Security Agency. (2022). K-12 School Security Assessment Tool User Guide. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2022-11/ssat_user-guide-022022-508.pdf

[16] Cybersecurity and Infrastructure Security Agency. (2024). K-12 School Security Guide Companion Product for School Business Officials. https://www.cisa.gov/resources-tools/resources/k-12-school-security-guide-3rd-edition

[17] Dahal, B. K. (2023). Secondary Level Students' Experiences of Cyberbullying Through Facebook. *Journal of NELTA Gandaki*, 6(1-2), 78-88. https://doi.org/10.3126/jong.v6i1-2.59714

[18] Dambrosio, R. (2021). Student Online Safety and Security: Middle School Teacher Perspectives Concerning Safe Internet Use in the Classroom [Master's thesis, California State University, Stanislaus]. https://scholarworks.calstate.edu/downloads/1v53k324t

[19] Fernández Nieto, B., Romanini, D., & Zhu, Y. (2025). Cybersecurity Education Showdown: A Comparative Analysis of K-12 Education Systems in the United States, the European Union, and China. In *CEUR Workshop Proceedings*, 3962. https://ceur-ws.org

[20] Fezzey, T., Batchelor, J. H., Burch, G. F., & Reid, R. (2023). Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic. *Journal of Cybersecurity Education, Research and Practice*, 2022(2), Article 4. https://doi.org/10.32727/8.2023.3

[21] Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of Online Sexual Offenses Against Children in the US. JAMA Network Open, 5(10), e2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471

[22] Gaffney, H., Ttofi, M. M., & Farrington, D. P. (2021). Effectiveness of school-based programs to reduce bullying perpetration and victimization: An updated systematic review and meta-analysis. *Campbell systematic reviews*, *17*(2), e1143. https://doi.org/10.1002/cl2.1143

[23] Guillén-Gámez, F. D., Tomczyk, Ł., Ruiz-Palmero, J., & Connolly, C. (2024). Digital Security in Educational Contexts: Digital Competence and Challenges for Good Practice. *Computers in the Schools*, 41(3), 257-262. https://doi.org/10.1080/07380569.2024.2390319

[24] Howard, C. D. (2021). Development of a Pilot Training Program for Middle School Students to Reduce End-User Cyber Vulnerabilities [Doctoral study, Walden University]. Walden Dissertations and Doctoral Studies Collection. https://scholarworks.waldenu.edu/dissertations/10919

[25] Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A Systematic Review of K-12 Cybersecurity Education Around the World. *IEEE Access*, 12, 59726-59738. https://doi.org/10.1109/ACCESS.2024.3393425

[26] Intan, D., Ismail, I. A., & Zairul, M. (2023). Cybersecurity Issues Among High School Students: A Thematic Review. *International Journal of Academic Research in Business and Social Sciences*, 13(14), 101-118. http://creativecommons.org/licences/by/4.0/legalcode

[27] Ivy, J., Kelley, R., Cook, K., & Thomas, K. (2020). Incorporating Cyber Principles into Middle and High School Curriculum. *International Journal of Cybersecurity Education Studies*, 4(2). https://doi.org/10.21585/ijcses.v4i2.101

[28] Jacob, J. (2024). Examining the Divide: Measuring the Inequitable Penetration and Access to K-12 Cybersecurity Education [Doctoral dissertation, University of Texas at San Antonio]. UTSA Repository. https://hdl.handle.net/20.500.12588/6909

[29] Jiang, B., Li, X., Liu, S., Hao, C., Zhang, G., & Lin, Q. (2022). Experience of Online Learning from COVID-19: Preparing for the Future of Digital Transformation in Education. *International Journal of Environmental Research and Public Health, 19*(24), 16787. https://doi.org/10.3390/ijerph192416787

[30] Johnson, N., Ibrahim, A., Sikos, L., & Glowrey, C. (2022). Cyber Security Curriculum in Western Australian Primary and Secondary Schools: Interim Report: Curriculum Mapping. https://doi.org/10.25958/x9r3-d254

[31] Karakose, T., Polat, H., & Papadakis, S. (2021). Examining Teachers' Perspectives on School Principals' Digital Leadership Roles and Technology Capabilities During the COVID-19 Pandemic. *Sustainability*, 13(23), 13448. https://doi.org/10.3390/su132313448

[32] Khalid, F. (2017). Understanding University Students' Use of Facebook for Collaborative Learning. *International Journal of Information and Education Technology*, 7(8), 595-600. https://doi.org/10.18178/ijiet.2017.7.8.938

[33] King, D. L., Delfabbro, P. H., Doh, Y. Y., Wu, A. M. S., Kuss, D. J., Pallesen, S., Mentzoni, R., Carragher, N., & Sakuma, H. (2018). Policy and Prevention Approaches for Disordered and Hazardous Gaming and Internet Use: An International Perspective. *Preventive Medicine*, 114, 152-159. https://doi.org/10.1007/s11121-017-0813-1

[34] Latorre-Medina, M. J., & Tnibar Harrus, C. (2023). Digital Security in Educational Training Programs: A Study Based on Future Teachers' Perceptions. *Information Technologies and Learning Tools*, 95(3), 102-118. https://doi.org/10.33407/itlt.v95i3.5204

[35] Ling, C., Balcı, U., Blackburn, J., & Stringhini, G. (2021, May). A First Look at Zoombombing. In *2021 IEEE Symposium on Security and Privacy* (pp. 1452-1467). IEEE. https://doi.org/10.1109/SP40001.2021.00061

[36] Marinoni, C., Rizzo, M., & Zanetti, M. A. (2024). Social Media, Online Gaming, and Cyberbullying During the COVID-19 Pandemic: The Mediation Effect of Time Spent Online. *Adolescents*, 4(2), 297-310. https://doi.org/10.3390/adolescents4020021

[37] Martin, F., Bacak, J., Polly, D., Wang, W., & Ahlgrim-Delzell, L. (2023). Teacher and School Concerns and Actions on Elementary School Children Digital Safety. *TechTrends*, 67, 561-571. https://doi.org/10.1007/s11528-022-00803-z

[38] Mee, P. (2020, March). We Need to Start Teaching Cybersecurity in Elementary School. World Economic Forum. https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity

[39] Methley, A. M., Campbell, S., Chew-Graham, C., McNally, R., & Cheraghi-Sohi, S. (2014). PICO, PICOS and SPIDER: A Comparison Study of Specificity and Sensitivity in Three Search Tools for Qualitative Systematic Reviews. *BMC Health Services Research*, 14, Article 579. https://doi.org/10.1186/s12913-014-0579-0

[40] Ng, W. A. (2025). Strengthening Digital Safety Education Through Cross-Sector Collaboration. In *Mobile Technology and Teens Workshop*, CHI 2025. https://sciety.org/articles/activity/10.31234/osf.io/9rvy7_v1

[41] Nguyen, T. H., Shah, G. H., Kaur, R., Muzamil, M., Ikhile, O., & Ayangunna, E. (2024). Factors Predicting In-School and Electronic Bullying Among High School Students in the United States: An Analysis of the 2021 YRBSS. *Children*, 11(7), 788. https://doi.org/10.3390/children11070788

[42] Ondrušková, D., & Pospíšil, R. (2023). The Good Practices for Implementation of Cyber Security Education for School Children. *Contemporary Educational Technology*, 15(3), ep435. https://doi.org/10.30935/cedtech/13253

[43] Organization for Economic Co-operation and Development (OECD). (2020). Education Responses to COVID-19: Embracing Digital Learning and Online Collaboration. OECD Publishing. https://doi.org/10.1787/d75eb0e8-en

[44] Page, M. J. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. International *Journal of Surgery*, 88, Article 105906. https://doi.org/10.1016/j.ijsu.2021.105906

[45] Palalas, A., & Doran, M. (2023). Digital Wellness Framework for Online Learning. *Canadian Journal of Learning and Technology*, 49(3), 1-25. https://doi.org/10.21432/cjlt28581

[46] Paul, M. (2022). A Study on the Cyber Safety of High School Students During the Pandemic in Ernakulam [Master's dissertation, St. Teresa's College, Mahatma Gandhi University]. http://117.239.78.102:8080/jspui/bitstream/123456789/2237/1/MARIA%20PAUL.pdf

[47] Project Tomorrow. (2021). Creating a Common Culture of Action Around Cybersecurity: Results from the 2021 Project Tomorrow–iboss National K-12 Education Cybersecurity Report. https://files.eric.ed.gov/fulltext/ED619717.pdf

[48] Rad, M., & Demeter, M. (2019). Youth Digital Well-Being: Exploring Online Duality and Emotional Regulation Across Europe. *Journal of Youth Studies*, 22(8), 1062-1078. https://doi.org/10.18662/po/9

[49] Ravichandran, R., Singh, S., & Sasikala, P. (2025). Exploring School Teachers' Cyber Security Awareness, Experiences, and Practices in the Digital Age. *Journal of Cybersecurity Education, Research and Practice*, 2025(1), Article 1. https://doi.org/10.62915/2472-2707.1214

[50] Sadaghiani-Tabrizi, A. (2023). Revisiting Cybersecurity Awareness in the Midst of Disruptions. *International Journal for Business Education*, 163(1), Article 6. https://doi.org/10.30707/IJBE163.1.1675491516.833197

[51] Sorrentino, A., Sulla, F., Santamato, M., di Furia, M., Toto, G. A., & Monacis, L. (2023). Has the COVID-19 Pandemic Affected Cyberbullying and Cybervictimization Prevalence Among Children and Adolescents? *A Systematic Review. International Journal of Environmental Research and Public Health*, 20(10), 5825. https://doi.org/10.3390/ijerph20105825

[52] U.S. Department of Education. (2021). ED COVID-19 Handbook, Volume 1: Strategies for Safely Reopening Elementary and Secondary Schools (OPEPD-IO-21-01). https://www2.ed.gov/documents/coronavirus/reopening.pdf

[53] U.S. Department of Education. (2024). National Educational Technology Plan. Office of Educational Technology. https://tech.ed.gov

[54] U.S. Government Accountability Office (GAO). (2020). Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm (GAO-20-644). https://www.gao.gov/products/gao-20-644

[55] U.S. Government Accountability Office (GAO). (2022). Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity (GAO-23-105480). https://www.gao.gov/products/gao-23-105480

[56] Voogt, J., & Knezek, G. (2021). Teaching and Learning with Technology During the COVID-19 Pandemic: Highlighting the *Need for Micro-Meso-Macro Alignments. Canadian Journal of Learning and Technology*, 47(4). https://doi.org/10.21432/cjlt28150

[57] Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, L., Tournas, P., & Spanos, T. (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, Article 100474. https://doi.org/10.1016/j.ijcci.2022.100474

[58] Zulqadri, D. M., Mustadi, A., & Retnawati, H. (2022). Digital Safety During Online Learning: What We Do to Protect Our Students? *Journal Iqra': Kajian Ilmu Pendidikan*, 7(1), 178-191. https://doi.org/10.25217/ji.v7i1.1746