International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

INTERNATIONAL JOURNAL OF MODERN EDUCATION (IJMOE)
www.ijmoe.com

GLOBAL ACADEMIC EXCELLENCE

CYBERSECURITY AWARENESS AND DIGITAL EDUCATION: A GLOBAL BIBLIOMETRIC ANALYSIS

Badariah Abdollah[1*], Nurul Izzati Mohd Zaki [2], Shazana Mustapa [3]

[1] Department of Mathematics, Science and Computer, Politeknik Banting Selangor, Malaysia
Email: badariah@polibanting.edu.my
[2] Department of Mathematics, Science and Computer, Politeknik Banting Selangor, Malaysia
Email: nurul.izzati@polibanting.edu.my
[3] Department of Aircraft Maintenance, Politeknik Banting Selangor, Malaysia
Email: shazana@polibanting.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 22.10.2025
Revised date: 11.11.2025
Accepted date: 01.12.2025
Published date: 17.12.2025

To cite this document:

Abdollah, B., Zaki, N, I, M., & Mustapa, S. (2025). Cybersecurity Awareness and Digital Education: A Global Bibliometric Analysis. *International Journal of Modern Education, 7* (28), 859-873.

DOI: 10.35631/IJMOE.728059

Abstract:

The increasing importance of cybersecurity in the digital era showcases the demand for enhancing cybersecurity awareness and strengthening digital education, particularly in academic and professional contexts where vulnerabilities often arise from human factors rather than purely technical weaknesses. In spite of the expanding body of literature, there remains a lack of systematic mapping to understand the trends, patterns, and global collaboration in this research domain. This research addresses the gap by performing a bibliometric analysis of publications related to cybersecurity awareness and digital education. Data were collected through Scopus advanced searching using the keywords "cybersecurity," "awareness," and "education," yielding a total of 1,107 documents. To ensure accuracy, OpenRefine was employed to clean and harmonize the dataset, while Scopus Analyzer provided statistical insights into publication growth, sources, authorship, and citation structures. For deeper visualization, the VOSviewer software was applied to generate co-authorship, co-occurrence as well as country collaboration networks. The analysis indicated a consistent increment in publications throughout the past decade, with notable contributions from leading countries like China, the United States, and the United Kingdom, forming distinct clusters of international collaboration. The thematic mapping indicated a strong emphasis on awareness training, educational strategies, and policy integration in digital learning environments. Nine main clusters were identified, reflecting the multidisciplinary nature of the field across computer science, social sciences, and education. These findings enrich the body of knowledge by offering a thorough overview of research progress, highlighting influential authors and institutions, and identifying gaps where future studies can integrate practical awareness frameworks into digital education systems.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

In conclusion, this study not only underscores the evolution of cybersecurity awareness in education but also offers a roadmap for policymakers, educators, and researchers to foster resilient digital ecosystems.

Keywords:

Cybersecurity, Awareness, Digital, Education, Literacy

Introduction

In the contemporary digital age, the integration of technology into daily life has become ubiquitous, leading to an increased dependence on digital platforms for communication, education, and commerce. This digital transformation, while beneficial, has also heightened the risk of cyber threats, making cybersecurity awareness a critical concern. Cybersecurity awareness involves understanding the potential threats and vulnerabilities in the digital environment and adopting practices to mitigate these risks. Digital education, on the other hand, refers to the use of digital tools and platforms to assist learning and teaching. The convergence of these two fields is vital, as it provides individuals with the essential knowledge and skills to engage with the digital environment in a safe and responsible manner. This paper examines the significance of cybersecurity awareness and digital education, analyzes the current developments in these areas, and identifies effective strategies for enhancing cybersecurity knowledge among various user groups.

The significance of cybersecurity awareness has been widely recognized, particularly in the context of education. Research indicates that human errors and behaviors often lead to vulnerabilities, making individuals susceptible to cyber threats (Alalawi et al., 2024). To address this, various educational initiatives have been developed. For instance, an AI-integrated mobile application has been designed to provide tailored cybersecurity education to different age groups, including children, teenagers, and adults. This application offers lessons, videos, stories, scenarios, and exercises to enhance individual awareness levels, leveraging AI to provide engaging responses and support users with chatbot assistance [1]. Such innovative approaches highlight the potential of technology in enhancing cybersecurity education.

University students, as a significant demographic in the digital landscape, have been the focus of several studies. One study emphasizes the importance of promoting cybersecurity awareness among university students to reduce risks and safeguard sensitive information. The research identifies key determinants of cybersecurity awareness and examines their implications for information security education (Halimnundjaja et al., 2024). Another study performed in Saudi Arabia highlights the importance of improving cybersecurity awareness among university students to foster a positive cybersecurity culture and safeguard critical information assets (Mohammed & Bamasoud, 2022). These studies collectively highlight the necessity of integrating cybersecurity education into higher education curricula to prepare students for the digital challenges they may face.

Adolescents, growing up in a hyper-connected digital environment, also require effective cybersecurity education. A pilot study aimed at designing a cyber-awareness teaching approach for Montessori middle schools in Italy demonstrates the effectiveness of participatory lectures and game-based activities in enhancing engagement and learning (Renieri et al., 2025).

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Likewise, incorporating engaging games has proven to be an effective method for teaching children complex cybersecurity concepts, enabling them to identify and avoid potential threats such as phishing scams and online predators (Ebrahimi et al., 2025). These findings imply that interactive and engaging teaching methodologies can significantly improve cybersecurity awareness among younger audiences.

The digital education role in fostering cybersecurity awareness goes beyond formal classroom environments. A study on the integration of cybersecurity awareness into higher education institutions in the Dominican Republic emphasizes the vital importance of such programs in protecting sensitive information and strengthening institutional resilience amid drastic digital transformation (Bueno, 2025). The study reveals notable discrepancies in cybersecurity knowledge between students and staff, underscoring the demand for targeted awareness initiatives to address these gaps. By cultivating a strong cybersecurity culture, educational institutions may safeguard their digital assets while promoting sustainable innovation and global collaboration.

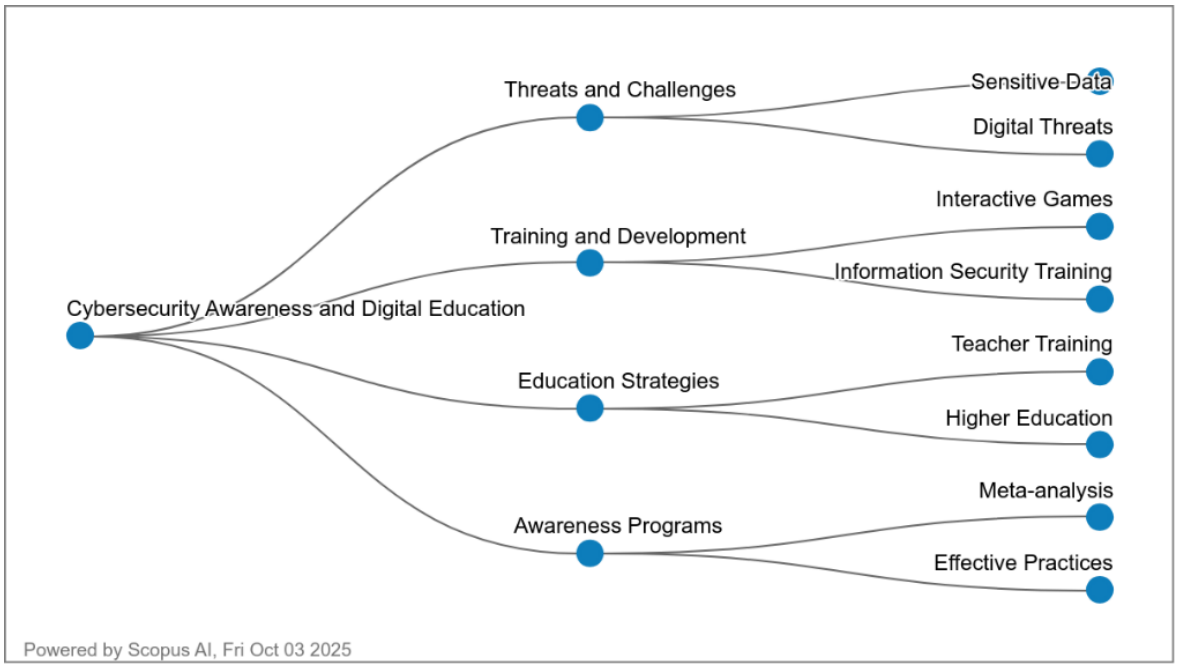

Figure 1: Concept Map Cybersecurity Awareness and Digital Education
Source: (Scopus AI, Fri Oct 03 2025)

Figure 1 illustrates 4 four major thematic clusters that shape the field: threats and challenges, training and development, education strategies, and awareness programs. Within threats and challenges, issues such as sensitive data protection and digital threats emerge as critical concerns, demonstrating the pressing need for robust cybersecurity frameworks. The training and development cluster emphasizes the importance of interactive games and information security training as innovative methods to enhance learners' engagement and skills. Meanwhile, education strategies connect strongly to teacher training and higher education, underscoring the role of institutions and educators in embedding cybersecurity literacy into curricula.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Finally, awareness programs focus on meta-analysis and effective practices, suggesting that evidence-based approaches and best practice models are essential for scaling impact. Collectively, these interrelated themes indicate that cybersecurity awareness in digital education requires a multifaceted approach: addressing technological threats, developing human capacity through innovative pedagogy, empowering educators and institutions, and grounding efforts in proven strategies. This synthesis confirms that successful digital education in cybersecurity must balance prevention, capacity-building, and evaluation to ensure sustainable resilience against the ever-evolving landscape of cyber risks.

In conclusion, the literature highlights the significance of cybersecurity awareness and digital education in today's digital age. Various studies highlight the effectiveness of innovative educational approaches, such as AI-integrated applications, game-based learning, and targeted awareness programs, in enhancing cybersecurity knowledge among different user groups. As digital threats continue to evolve, it is imperative to adopt proactive strategies in education and training to empower individuals with the essential skills to travere the digital world securely and responsibly.

Research Question

RQ1: What are the research trends in online learning studies according to the year of publication?
RQ2: What are the top 10 most cited articles?
RQ3: Which are the top 10 countries based on the number of publications?
RQ4: What are the most popular keywords related to the study?
RQ5: What are the patterns of co-authorship based on countries' collaboration?

Methodology

Bibliometrics represents a systematic method of gathering, organizing as well as analyzing bibliographic information from scientific publications (Alves et al., 2021; Assyakur & Rosa, 2022; Verbeek et al., 2002). While it incorporates descriptive indicators, for instance, identifying publishing journals, tracking annual publication outputs, and highlighting leading authors (Wu & Wu, 2017), bibliometrics also employs more advanced techniques, notably document co-citation analysis, to uncover intellectual structures and research frontiers within a field.

A successful literature review, therefore, requires a careful and iterative process that involves the selection of precise keywords, comprehensive searching of the literature, and detailed analytical evaluation. Such rigor ensures the compilation of a robust bibliography and the attainment of reliable research outcomes (Fahimnia et al., 2015). In this paper, special attention was given to high-impact publications provided that they give essential perspectives into the theoretical foundations that define the research domain. To maintain accuracy and consistency, SCOPUS was utilized as the main data source for data collection (Al-Khoury et al., 2022; di Stefano et al., 2010; Khiste & Paithankar, 2017). Moreover, to uphold academic quality, only peer-reviewed journal articles were included, while books and lecture notes were intentionally excluded (Gu et al., 2019). Publications indexed in Elsevier's Scopus from 2015 to October 2025 were systematically collected and analyzed for this study.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Data Search Strategy

In conducting the data collection process, the study employed the Scopus advanced search function to ensure both comprehensiveness and precision in retrieving relevant publications. The search string was carefully constructed, combined with filters to refine results by publication year and language (refer to Table 2). Specifically, the query was restricted to works published between 2015 and 2025 and limited exclusively to studies written in English, thereby guaranteeing accessibility and consistency in interpretation. The search was conducted with an access date of October 2025 (refer to Table 1), ensuring that the most recent and updated records available within the defined period were captured. Following the initial retrieval, a systematic screening procedure was applied based on pre-determined inclusion and exclusion criteria. Publications were included if they met two essential conditions: (i) written in English, and (ii) published within the 2015–2025 time frame. Conversely, works published prior to 2015 and non-English language articles were excluded, as they fell outside the scope of the study. This structured screening ensured the reliability, validity, and relevance of the dataset by removing irrelevant or linguistically inaccessible materials. As a result of this rigorous process, the final dataset comprised 1,107 publications, reflecting a substantial and representative body of scholarly work on cybersecurity awareness, literacy, and education. By adopting this methodologically robust strategy, the study ensured that the bibliometric analysis was grounded in high-quality data, accurately representing current trends, emerging themes, and influential contributions within the field.

Table 1: The Search String

Scopus	TITLE (("cybersecurity" OR "cyber-security" OR "cyber security") AND ("awareness" OR "literacy" OR "education")) AND PUBYEAR > 2014 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE , "English"))) Access date: October 2025

Table 2: The Selection Criterion Is Searching

Criterion	Inclusion	Exclusion
Language	English	Non-English
Time line	2015 – 2025	< 2015

Data Analysis

VOSviewer is an intuitive bibliometric software developed by Nees Jan van Eck and Ludo Waltman at Leiden University, Netherlands (van Eck & Waltman, 2010, 2017). It is extensively utilized for analyzing and visualizing scientific literature, providing capabilities such as generating clear network maps, grouping related elements, and producing density visualizations. Its versatility supports the examination of co-authorship, co-citation, and

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

keyword co-occurrence networks, giving researchers an in-depth view of research trends and relationships. With its interactive interface and ongoing software enhancements, the tool allows for dynamic and intuitive exploration of large-scale datasets. In addition, VOSviewer supports metric computations, customizable visualizations, and compatibility with multiple bibliometric data sources, establishing it as a valuable tool for examining complex scholarly domains. One of its distinctive features is the ability to transform complex bibliometric datasets into visually interpretable maps and charts, with particular strengths in keyword co-occurrence, clustering, and density visualization. Its intuitive interface makes it suitable for both beginner and advanced researchers, while ongoing updates ensure that the software continues to lead in bibliometric analysis (van Eck & Waltman, 2010, 2017).

In this study, datasets containing publication year, title, author names, journal, citations, and keywords in PlainText format were retrieved from the Scopus database for the period spanning 2015 to October 2025. These datasets were analyzed using VOSviewer version 1.6.20, employing VOS clustering and mapping techniques to produce bibliometric maps. In contrast to the traditional Multidimensional Scaling (MDS) method, which positions items based on similarity measures such as cosine or Jaccard indices, VOSviewer focuses on representing items in low-dimensional spaces to ensure that the distances between them accurately reflect their degree of relatedness (van Eck & Waltman, 2010; Appio et al., 2014). The software utilizes a more robust normalization technique known as association strength (AS_{ij}), defined as (Van Eck & Waltman, 2007):

$$AS_{ij} = \frac{C_{ij}}{w_i w_j}$$

in which C_{ij} denotes the observed number of co-occurrences of items i and j, while w_i and w_j resemble their respective total occurrences. This value expresses the ratio between the observed and expected number of co-occurrences under the assumption of statistical independence (Van Eck & Waltman, 2007). By integrating this approach, VOSviewer provides more accurate visualizations of bibliometric relationships, positioning it as a superior and indispensable tool in the field of research mapping and analysis.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Findings and Discussion

RQ1: What Are the Research Trends in Online Learning Studies According to The Year of Publication?

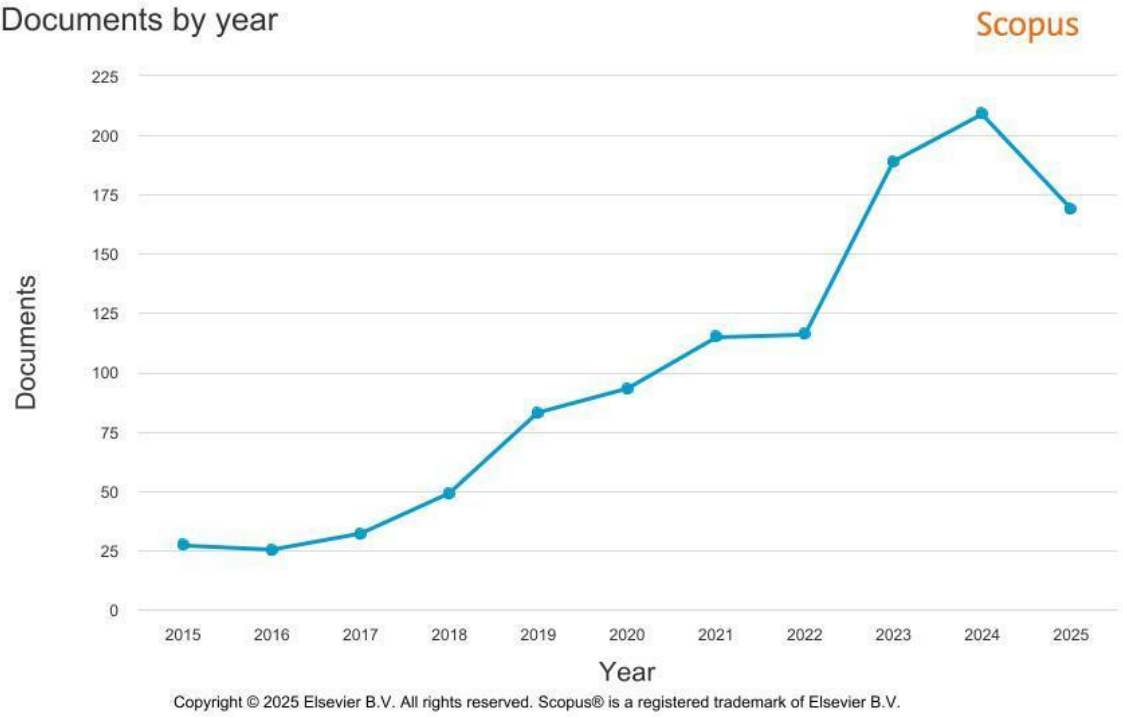

Figure 2: Number Of Documents Based on Year of Publication

Source: (Scopus, Fri Oct 03 2025)

The publication trend on Cybersecurity Awareness and Digital Education from 2015 to 2025 in Figure 2 above demonstrates a clear upward trajectory, with notable fluctuations across the years. In the early phase (2015–2017), the number of publications can be considered low, ranging between 25 and 32, reflecting the nascent stage of cybersecurity awareness research within the educational context. This period coincides with the gradual integration of digital technologies in teaching and learning, where cybersecurity concerns were present but had not yet gained prominence in academic discourse. A moderate increase is observed between 2018 and 2020, with publications rising from 49 to 93. This growth can be attributed to the worldwide push toward digital transformation in education and the parallel rise in cybersecurity threats, particularly phishing, data breaches, and privacy concerns among students and educators. The COVID-19 pandemic in 2020 acted as a catalyst, accelerating digital adoption in education and simultaneously elevating concerns about cybersecurity literacy, thus driving academic interest.

From 2021 onwards, the trend shows significant expansion, with publications increasing steadily to 115 in 2021, 116 in 2022, and a substantial jump to 189 in 2023. The peak occurs in 2024 with 209 publications, before a slight decline to 169 in 2025. This surge reflects growing recognition of cybersecurity as a critical component of digital education policies and

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

institutional practices, particularly as online learning, cloud platforms, and digital assessment systems have become deeply embedded in higher education. The peak in 2024 can be explained by intensified research funding, policy initiatives, and global collaborations on cybersecurity capacity building. The slight drop in 2025 may suggest that while the topic remains highly relevant, research has begun to consolidate, shifting focus toward specialized themes such as AI-driven cybersecurity tools, policy evaluation, and long-term implementation frameworks. Overall, the trend underscores the field's maturation and its alignment with global priorities in safeguarding digital education ecosystems.

RQ2: What Are the Top 10 Most Cited Articles?

Table 3: Most Cited Author

Authors	Year	Source title	Cited by
Zwilling et al. (2022)	2022	Journal of Computer Information Systems	282
Li et al., (2019)	2019	International Journal of Information Management	274
de Bruijn & Janssen, (2017)	2017	Government Information Quarterly	212
Hart et al., (2020)	2020	Computers and Security	176
Corallo et al. (2022)	2022	Computers in Industry	170
Aldawood & Skinner, (2019)	2019	Future Internet	145
Aldawood & Skinner (2018)	2018	IEEE International Conference on Teaching Assessment and Learning for Engineering Tale 2018	123
Quayyum et al., (2021)	2021	International Journal of Child-Computer Interaction	114

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Ulven & Wangen, (2021)	2021	Future Internet	109
Berkman et al.,(2018)	2018	Journal of Accounting and Public Policy	109

The top 10 cited articles by author in Table 3 above reveal that research on cybersecurity awareness and digital education is dominated by studies that combine behavioral, policy, and educational perspectives. The most cited article by author, Zwilling et al. (2022), with 282 citations, underscores the growing global concern with how awareness and knowledge influence cybersecurity behavior, aligning with the rapid rise of digital dependency during and after the COVID-19 pandemic. Similarly, Li et al. (2019) and de Bruijn & Janssen (2017) highlight the role of policy awareness and evidence-based strategies in shaping secure practices, explaining their high citation counts (274 and 212, respectively). These works resonate strongly with both academia and policymakers, as they provide actionable insights into human factors—the recognized weakest link in cybersecurity. The prominence of Hart et al. (2020) and Corallo et al. (2022) further indicates the significance of innovative pedagogical tools (serious games) and emerging contexts like the Industrial Internet of Things (IIoT) in cybersecurity education research.

Meanwhile, other highly cited works reflect more specialized niches within cybersecurity awareness, such as social engineering (Aldawood & Skinner, 2018; 2019), child-focused awareness (Quayyum et al., 2021), higher education (Ulven & Wangen, 2021), and even the economic implications of cybersecurity awareness (Berkman et al., 2018). The diversity of topics shows that awareness research is multi-dimensional, spanning education, workforce training, industry needs, and societal impacts. The relatively high citation numbers for recent works (2020–2022) suggest that cybersecurity awareness has become a particularly urgent research domain in the digital era, with new challenges driving rapid academic attention. Overall, the results demonstrate that impactful studies are those that bridge theory with practical application—offering strategies, frameworks, and evidence-based insights that stakeholders across sectors can adopt to strengthen cybersecurity resilience.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

RQ3: Which Are the Top 10 Countries Based on The Number of Publications?

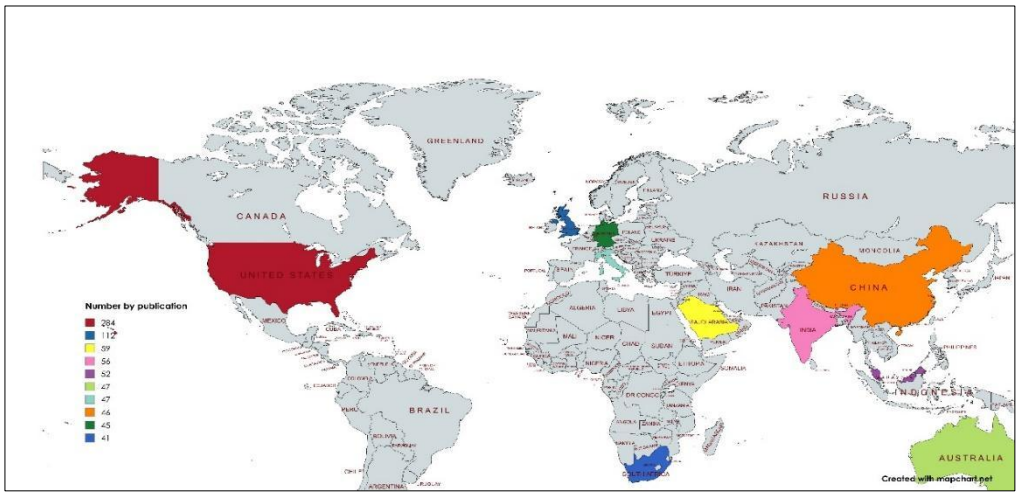

Figure 3: Country Mapping Based on Number of Publications

Source: (Scopus, Fri Oct 03 2025)

The global distribution of publications on Cybersecurity Awareness and Digital Education highlights that the United States emerged as the leading contributor, with 284 publications, far surpassing other countries. This dominance reflects the country's strong research ecosystem, significant investment in cybersecurity education, and early recognition of digital threats as a national priority. The United Kingdom follows with 112 publications, driven by its proactive policies in digital literacy and its academic institutions' strong engagement in cybersecurity research. Interestingly, Saudi Arabia (59), India (56), and Malaysia (52) emerge as prominent contributors among developing and transitional economies. Their growing output indicates national initiatives to strengthen cybersecurity capacity and integrate awareness programs into digital education, particularly as these countries experience rapid digitalization and expansion of online learning platforms.

Other countries such as Australia (47), Italy (47), China (46), Germany (45), and South Africa (41) demonstrate moderate but significant research activity. These outputs can be linked to regional needs: for example, Australia's focus on cyber resilience in education, China's large-scale digital transformation initiatives, and Germany's emphasis on data privacy and digital competencies. The presence of South Africa on the list reflects the rising importance of cybersecurity education in addressing the regional digital divide and cybercrime threats. The variation across countries may also be influenced by factors such as funding availability, government policy prioritization, and international research collaborations. Overall, the distribution shows that while Western nations dominate in absolute numbers, emerging economies in Asia and the Middle East are increasingly contributing, signaling a global recognition of the critical link between cybersecurity awareness and digital education.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

RQ4: What Are the Most Popular Keywords Related to The Study?

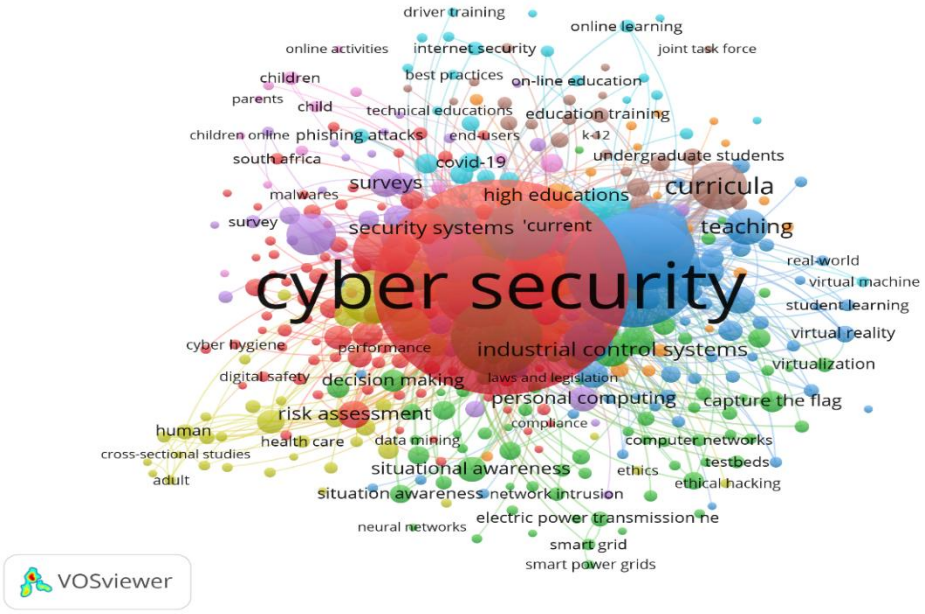

Figure 4: Network Visualization Map of Keywords' Co-Occurrence
Source: (Scopus, Fri Oct 03 2025)

The co-occurrence analysis of author keywords in VOSviewer examines how frequently specific keywords appear together across publications, thereby revealing thematic connections and research trends in the field. Using the full counting method with a minimum occurrence threshold of five, 401 keywords from a total of 2,825 met the criteria and were clustered into nine distinct groups, each representing a major research domain. The use of minimum cluster size ensures the inclusion of meaningful and interconnected terms, with highly frequent and strongly linked keywords such as "cyber security" (901 occurrences, 6,105 link strength), "cyber-security education" (327 occurrences, 2,630 link strength), and "students" (199 occurrences, 1,850 link strength) dominating the network. These clusters reflect not only the breadth but also the centrality of recurring research themes, including awareness, training, curricula design, threats, and technological innovations such as IoT and AI in education.

The findings make a substantial contribution to the body of knowledge by mapping how the academic community addresses cybersecurity awareness and digital education. The clustering underscores a growing interdisciplinary landscape where education and training intersect with technical domains like network security, data protection, and machine learning, as well as human-centered dimensions such as behavioral research, gamification, and awareness programs. The emergence of clusters on pedagogical methods (e.g., e-learning, serious games, curricula), advanced technologies (AI, IoT, industrial control systems), and societal concerns (cybercrime, digital literacy, children, higher education) highlights that research has evolved from narrowly technical issues to holistic frameworks that integrate human, institutional, and technological factors. This knowledge map not only shows the maturity of cybersecurity awareness research but also provides a roadmap for future studies. It identifies areas of high

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

concentration and gaps where further exploration is needed to strengthen digital resilience through education.

Rq5. What Are the Patterns of Co-Authorship Based on Countries' Collaboration?

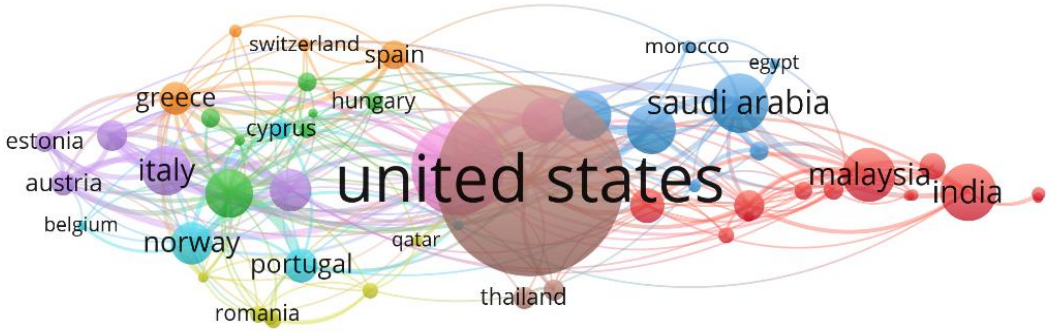

Figure 5: Network Visualization Map Of Co-Authorship By Countries' Collaboration
Source: (Scopus, Fri Oct 03 2025)

The concept of co-occurrence co-authorship by countries in VOSviewer is designed to map and visualize how different nations collaborate in research based on joint publications. Each country represents a node in the network, and the strength of links shows the frequency and intensity of collaborations. Countries with stronger co-authorship ties are placed closer, while weaker links appear farther apart, revealing global research patterns. In this study, the full counting method was used, where each co-authored publication is fully counted for all involved countries. With a minimum threshold of five publications, 54 out of 102 countries qualified, and by setting a minimum cluster size of five, nine clusters were generated. This clustering highlights distinct regional and cross-regional collaboration groups, with stronger nodes like the United Kingdom, the United States, and Germany serving as central hubs.

The findings add to the body of knowledge by showing both the strength and diversity of international collaborations in cybersecurity awareness and digital education. For example, the United States (285 documents, 2,539 citations) and the United Kingdom (111 documents, 1,425 citations) dominate not only in volume but also in citation impact, indicating their leadership roles. Emerging contributors such as Saudi Arabia, Malaysia, and South Africa reflect the growing interest from developing regions, which strengthens the global inclusivity of this research area. The presence of nine clusters suggests multiple centers of excellence and thematic orientations, from technical approaches to policy and education. This indicates that cybersecurity is no longer a localized concern but a shared global priority, where collaboration fosters knowledge exchange, capacity building, and innovative solutions. By identifying influential hubs and collaborative gaps, this analysis helps policymakers, researchers, and institutions strategize future partnerships to enhance both academic impact and practical applications in digital education and cybersecurity.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Conclusion

This study aimed to explore the research landscape on cybersecurity awareness and digital education through bibliometric analysis, aiming to identify publication trends, highly cited works, contributing countries, popular keywords, and international collaboration patterns. The analysis of 1,107 documents published between 2015 and 2025 highlights the growing significance of this field and reflects how academic interest has developed in response to evolving digital threats and the increasing role of technology in education.

The findings demonstrate a consistent growth in publications, with a peak observed in 2024, demonstrating heightened global attention toward integrating cybersecurity within digital learning environments. Highly cited works emphasize behavioral, policy, and educational perspectives, while the most productive countries, such as the United States, the United Kingdom, and China, play a central role in shaping global discourse. Keyword analysis identified major research themes, including awareness training, curricula development, cyber threats, and emerging technologies such as IoT and AI. Co-authorship patterns further underline the importance of international collaboration, with nine distinct clusters evidencing regional and cross-regional partnerships.

This study contributes to the field by showing a systematic overview of how cybersecurity awareness and digital education research have matured into a multidisciplinary area that bridges computer science, education, and social sciences. The results suggest that strengthening awareness through pedagogical innovation, policy integration, and global collaboration is essential for building digital resilience. While the study is restricted by its reliance on the Scopus database and English-language publications, it establishes a strong foundation for future investigations. Further research could expand the scope by integrating additional databases, non-English studies as well as longitudinal comparisons to capture broader perspectives.

In summary, bibliometric analysis proves to be an effective approach in mapping the intellectual structure, thematic focus, and collaborative networks in this domain. The evidence presented underscores the vital importance of cybersecurity awareness as a cornerstone of digital education and calls for continued scholarly efforts to align research with the pressing demands of the digital era.

Acknowledgements

The authors would like to express their sincere appreciation to Politeknik Banting Selangor for the continuous support and encouragement in completing this paper.

References

Al-Khoury, A., Hussein, S. A., Abdulwhab, M., Aljuboori, Z. M., Haddad, H., Ali, M. A., Abed, I. A., & Flayyih, H. H. (2022). Intellectual Capital History and Trends: A Bibliometric Analysis Using Scopus Database. Sustainability (Switzerland), 14(18). https://doi.org/10.3390/su141811615

Alalawi, M., Madathil, N. T., Darota, S. K., Abula, W., Alrabaee, S., & Melhem, S. B. (2024). Evaluating and Boosting Cybersecurity Awareness With an AI-Integrated Mobile App. Proceedings - Frontiers in Education Conference, FIE. https://doi.org/10.1109/FIE61694.2024.10893003

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059
Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review (M. J. W. Lee, S. Nikolic, M. Ros, J. Shen, L. C. U. Lei, G. K. W. Wong, & N. Venkatarayalu (eds.); pp. 62–68). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/TALE.2018.8615162

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future Internet, 11(3). https://doi.org/10.3390/fi11030073

Alves, J. L., Borges, I. B., & De Nadae, J. (2021). Sustainability in complex projects of civil construction: Bibliometric and bibliographic review. Gestao e Producao, 28(4). https://doi.org/10.1590/1806-9649-2020v28e5389

Appio, F. P., Cesaroni, F., & Di Minin, A. (2014). Visualizing the structure and bridges of the intellectual property management and strategy literature: a document co-citation analysis. Scientometrics, 101(1), 623–661. https://doi.org/10.1007/s11192-014-1329-0

Assyakur, D. S., & Rosa, E. M. (2022). Spiritual Leadership in Healthcare: A Bibliometric Analysis. Jurnal Aisyah : Jurnal Ilmu Kesehatan, 7(2). https://doi.org/10.30604/jika.v7i2.914

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Bueno, J. T. (2025). Cybersecurity Awareness in Higher Education: Aligning Technological Growth With Sustainable Innovation in the Dominican Republic. In Bridging Technology and Development for Sustainable Innovation and Geopolitical Dynamics (pp. 197–223). IGI Global. https://doi.org/10.4018/979-8-3693-9072-6.ch008

Chin, J. L. (2011). Women and Leadership: Transforming Visions and Current Contexts. *Forum on Public Policy: A Journal of the Oxford Round Table*, (2), 1–12.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137. https://doi.org/10.1016/j.compind.2022.103614

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

di Stefano, G., Peteraf, M., & Veronay, G. (2010). Dynamic capabilities deconstructed: A bibliographic investigation into the origins, development, and future directions of the research domain. Industrial and Corporate Change, 19(4), 1187–1204. https://doi.org/10.1093/icc/dtq027

Ebrahimi, E., Pare, M., Stoker, G., & White, S. (2025). Cybersecurity Early Education: A Review of Current Cybersecurity Education for Young Children. In du B. B., D. M. T., T. E., & M. C. (Eds.), International Conference on Computer Supported Education, CSEDU - Proceedings (Vol. 1, pp. 822–833). Science and Technology Publications, Lda. https://doi.org/10.5220/0013501000003932

Fahimnia, B., Sarkis, J., & Davarzani, H. (2015). Green supply chain management: A review and bibliometric analysis. In International Journal of Production Economics (Vol. 162, pp. 101–114). https://doi.org/10.1016/j.ijpe.2015.01.003

Gu, D., Li, T., Wang, X., Yang, X., & Yu, Z. (2019). Visualizing the intellectual structure and evolution of electronic health and telemedicine research. International Journal of Medical Informatics, 130. https://doi.org/10.1016/j.ijmedinf.2019.08.007

Halimnundjaja, D., Liman, R. F., Elysia Tandra, T., Gui, A., Sianipar, N. F., Apriani, S., & Suhartono, J. (2024). Factors and Impact Correlating to Awareness of Cybersecurity in

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 7 Issue 28 (December 2025) PP. 859-873
DOI: 10.35631/IJMOE.728059

Java. In W. F.W. (Ed.), 7th International Seminar on Research of Information Technology and Intelligent Systems: Advanced Intelligent Systems in Contemporary Society, ISRITI 2024 - Proceedings (pp. 866–871). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISRITI64779.2024.10963419

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers and Security, 95. https://doi.org/10.1016/j.cose.2020.101827

Khiste, G. P., & Paithankar, R. R. (2017). Analysis of Bibliometric term in Scopus. International Research Journal, 01(32), 78–83.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Mohammed, M., & Bamasoud, D. M. (2022). THE IMPACT OF ENHANCING AWARENESS OF CYBERSECURITY ON UNIVERSITIES STUDENTS: A SURVEY PAPER. Journal of Theoretical and Applied Information Technology, 100(15), 4756–4766. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138808067&partnerID=40&md5=f5409059905f855f94029d0526d10d6b

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

Renieri, M., Renieri, A., & Galletta, L. (2025). WalkthroughCyber: Teaching Cyber-Awareness in Montessori Middle Schools. In S. F., N. V., & D. S. B. (Eds.), Lecture Notes in Computer Science: Vol. 15999 LNCS (pp. 5–22). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-032-00644-8_1

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 1–40. https://doi.org/10.3390/fi13020039

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

van Eck, N. J., & Waltman, L. (2017). Citation-based clustering of publications using CitNetExplorer and VOSviewer. Scientometrics, 111(2), 1053–1070. https://doi.org/10.1007/s11192-017-2300-7

Van Eck, N. J., & Waltman, L. (2007). Bibliometric mapping of the computational intelligence field. International Journal of Uncertainty, Fuzziness and Knowldege-Based Systems, 15(5), 625–645. https://doi.org/10.1142/S0218488507004911

Verbeek, A., Debackere, K., Luwel, M., & Zimmermann, E. (2002). Measuring progress and evolution in science and technology - I: The multiple uses of bibliometric indicators. International Journal of Management Reviews, 4(2), 179–211. https://doi.org/10.1111/1468-2370.00083

Wu, Y. C. J., & Wu, T. (2017). A decade of entrepreneurship education in the Asia Pacific for future directions in theory and practice. In Management Decision (Vol. 55, Issue 7, pp. 1333–1350). https://doi.org/10.1108/MD-05-2017-0518

Zwilling, M., Klein, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basim, H. N. (2022). 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