Indonesia Berdaya, 6(1) 2025: 115-126
https://doi.org/10.47679/ib.20251004

P-ISSN 2502-4825
E-ISSN 2502-9495

Introduction to Cybersecurity for Teachers and Students in Indonesia in the Digital Era

Pengenalan Keamanan Siber bagi Guru dan Siswa di Indonesia di Era Digital

Cut Susan Octiva[1,*], Novi Rahayu[2], Mitranikasih Laia[3], Dikky Suryadi[4], Muhammad Lukman Hakim[5]

Published online: 1 Desember 2024

ABSTRACT

This Community Service (PKM) activity aims to increase cybersecurity literacy among teachers and students as part of efforts to support digital transformation in education. The training was conducted online with an interactive approach, involving 50 participants from various schools in Indonesia. The material includes an introduction to cyber threats, mitigation strategies, and daily digital security practices. The evaluation was done through pre-test and post-test, accompanied by a participant satisfaction questionnaire. The results showed a significant improvement in participants' understanding, with an average score increase of 73%. The level of satisfaction of participants with the training reached the "excellent" category with an average score of 4.75 on a scale of 5. These findings reflect the effectiveness of the designed training methods. However, the limitations of digital infrastructure are the main challenge in implementing activities. This Activity has contributed positively to building cybersecurity awareness and literacy in the education sector. In addition to providing direct benefits to participants, this program is expected to be a model for similar training that supports the sustainable strengthening of digital literacy in Indonesia.

Keywords: Cyber Security, Digital Literacy, Education, Community Service, Digital Transformation

Abstrak. Kegiatan Pengabdian Kepada Masyarakat (PKM) ini bertujuan untuk meningkatkan literasi keamanan siber di kalangan guru dan siswa sebagai bagian dari upaya mendukung transformasi digital dalam pendidikan. Pelatihan dilakukan secara daring dengan pendekatan interaktif, melibatkan 50 peserta dari berbagai sekolah di Indonesia. Materi yang diberikan meliputi pengenalan ancaman siber, strategi mitigasi, dan praktik keamanan digital sehari-hari. Evaluasi dilakukan melalui pre-test dan post-test, disertai dengan kuesioner kepuasan peserta. Hasil penelitian menunjukkan adanya peningkatan pemahaman peserta yang signifikan, dengan peningkatan skor rata-rata sebesar 73%. Tingkat kepuasan peserta terhadap pelatihan mencapai kategori “sangat baik” dengan skor rata-rata 4,75 dari skala 5. Temuan ini mencerminkan efektivitas metode pelatihan yang dirancang. Namun, keterbatasan infrastruktur digital menjadi tantangan utama dalam pelaksanaan kegiatan. Kegiatan ini telah memberikan kontribusi positif dalam membangun kesadaran dan literasi keamanan siber di sektor pendidikan. Selain memberikan manfaat langsung kepada peserta, program ini diharapkan dapat menjadi model pelatihan serupa yang mendukung penguatan literasi digital di Indonesia secara berkelanjutan.

[1] Universitas Amir Hamzah Medan

[2] STIA Bengkulu

[3] Universitas Nias Raya

[4] STMIK Al Muslim

[5] Universitas Mandiri Bina Prestasi Medan

*) *corresponding author*

Cut Susan Octiva
Universitas Amir Hamzah Medan

Email: cutsusan875@gmail.com

Kata Kunci: Keamanan Siber, Literasi Digital, Pendidikan, Pengabdian Masyarakat, Transformasi Digital

INTRODUCTION

The development of information and communication technology (ICT) has had a significant impact on various aspects of life, including the world of education. ICT improves

access to educational resources by providing information beyond traditional textbooks' confines, allowing students to explore a wide range of relevant knowledge. Digital platforms also offer flexibility in learning, which can be tailored to different individual learning styles and preferences (Anastasopoulou et al., 2024). In addition, ICT integration encourages the implementation of active learning strategies, where students become the center of the educational process (Bajac & Fišer, 2024). Educators use digital tools to create interactive and engaging learning experiences, proven to improve student engagement and academic outcomes (Jamal et al., 2024).

Furthermore, ICT also promotes inclusivity and equality in education. ICT-enabled assistive technology allows students with disabilities to get support tailored to their needs. In addition, the potential of ICT in bridging the education gap in underserved areas shows its essential role in expanding access and realizing educational equality (Anastasopoulou et al., 2024). Nevertheless, challenges like the digital divide remain barriers, exacerbating inequalities in access to technology and resources. Therefore, it is essential to address this problem to maximize the benefits of ICT in education.

In the digital era, the need to understand cybersecurity is becoming increasingly important, especially for teachers and students involved in technology-based learning (Ahyani & Dhuhani, 2024; Rewara et al., 2024; Sani, 2024). Data shows that cyberattacks on educational institutions continue to increase every year, ranging from the threat of data hacking to the misuse of personal information (Akor et al., 2024). For example, BlueVoyant reports ransomware attacks against colleges increased by 100% between 2019 and 2020. Additionally, Arctic Wolf reports that 68% of cyberattacks against schools and colleges come from external sources. This condition shows the urgency of introducing and understanding cybersecurity in the educational environment.

Previous studies have discussed the importance of digital literacy and cybersecurity among educators and students. Previous studies highlight low levels of cybersecurity awareness in secondary schools (Quayyum et al., 2021; Zhang-Kennedy & Chiasson, 2022), while other research by Ahyani & Dhuhani (2024) emphasizes the need for continuous training for teachers to understand cyber threats. In Indonesia, research by (Rahman et al., 2020) found that many teachers still do not have basic knowledge about digital data security measures. In addition, some previous community service programs focused more on digital literacy in general, without any particular emphasis on cybersecurity aspects (Asy'hary et al., 2023; Syafuddin et al., 2023).

However, there is still a significant research gap, especially in the context of the systematic introduction of cybersecurity for teachers and students in Indonesia. Community service activities that integrate the introduction of cybersecurity with a practical approach that suits the needs of schools are still minimal. This Community Service article aims to fill this void by introducing a cybersecurity program specifically designed for teachers and students.

The existence of this Community Service article is essential because cybersecurity not only serves as a protector of personal and institutional data but also as a foundation for creating a safe digital learning environment. With the increasing reliance on technology during the COVID-19 pandemic, the threat to cybersecurity among educators and students is becoming more and more apparent (Jalil et al., 2024; Mandadi et al., 2024; Wagman et al., 2023; Whitty et al., 2024). Therefore, this program is expected to be the first step in building sustainable cybersecurity awareness.

This Community Service article aims to describe the implementation of community service activities that focus on introducing cybersecurity for teachers and students in Indonesia, as well as to evaluate the effectiveness of the approach used in improving their understanding of cyber threats and mitigation strategies. Thus, this article makes a practical contribution and enriches the literature in the field of digital literacy and cybersecurity in the education sector.

LITERATURE OR CONCEPTUAL REVIEW

The Importance of Cybersecurity in Education

Cybersecurity is becoming an increasingly relevant topic in line with the rapid digital transformation in the education sector (Fernández et al., 2023). Educational institutions' reliance on digital platforms for teaching and learning activities not only improves accessibility and collaboration but also opens the door to various cyber threats. Due to their extensive digital infrastructure, higher education institutions now face increased vulnerabilities, such as data breaches and ransomware attacks (Siphambili, 2024). In addition, the lack of awareness among students is a serious challenge, as many do not have adequate cybersecurity knowledge, making them more vulnerable to cyberattacks (Jagadeesan et al., 2023).

To overcome these challenges, cybersecurity education is essential. One of the steps that must be taken is integrating cybersecurity training into the educational curriculum, especially for non-technical majors, to bridge the digital literacy gap (Ghazali et al., 2024; Hussain et al., 2024). Additionally, practical learning emphasizing hands-on experience can enhance students' problem-solving skills and prepare them for real-world challenges (Hussain et al., 2024).

Mitigation strategies must also be implemented by educational institutions, including adopting advanced technologies and strategies to build resilient digital infrastructure to cyber threats (Rangavittal, 2024). Partnerships with industry stakeholders can be an effective solution in addressing cybersecurity education challenges and developing a workforce that is ready to face these threats (Hussain et al., 2024). Nonetheless, it is essential to realize that the rapid pace of technological change can outpace educational institutions' ability to adapt, potentially creating gaps in knowledge and readiness.

Technology-based learning, such as e-learning and hybrid learning, has become an integral part of the education system in recent years. However, the adoption of this technology also carries risks, including the threat of hacking, data misuse, and exposure to inappropriate content (Farid et al., 2023; Javaid et al., 2023). Cybersecurity literacy among educators and learners is considered the first step in preventing these threats and creating a secure educational ecosystem (Ibrahim et al., 2024).

Cybersecurity: A Conceptual Review

Cybersecurity is a set of practices to protect data, systems, and networks from digital threats such as malware, phishing, and hacking (Kumar, 2023; Perwej et al., 2021). These threats are increasingly complex, requiring a multi-faceted approach integrating technology solutions, legal frameworks, and organizational strategies. One of the critical solutions in cybersecurity is firewalls, which act as a barrier to control network traffic. Advancements such as next-generation firewalls (NGFWs) further enhance security with more in-depth packet inspections (Kumar, 2023). In addition, the Intrusion Detection and Prevention System (IDPS) has evolved to take advantage of AI technology, which improves threat detection capabilities. However, challenges such as false positives are still a problem (Roopesh, 2024). Encryption also plays a crucial role in keeping data confidential, with modern algorithms such as AES that can handle computational complexity. Multi-factor authentication (MFA) is increasingly being introduced to strengthen security, although its implementation often faces resistance from users (Roopesh, 2024).

In addition to technology solutions, legal and institutional frameworks are crucial in protecting digital assets and privacy rights. Cybersecurity law focuses on the principles and regulations necessary to ensure these protections, highlighting the tension between the need for security and individual rights (Andraško et al., 2021). The institutional role, especially of global technology companies and governance bodies, is no less important in setting cybersecurity norms and practices (Savaş & Karataş, 2022).

Cyber threats have evolved rapidly, especially since the COVID-19 pandemic, triggering increased attacks and necessitating new protection measures (Choudhary et al., 2022). To that end, organizations are encouraged to adopt a holistic management approach that aligns cybersecurity with their business goals. Advanced technologies such as machine learning are also expected to reinforce this strategy (Abrahams et al., 2024). While focusing on technical solutions is essential, organizations must also consider the broader ethical and legal dimensions that shape cybersecurity practices. In education, cybersecurity includes protecting devices used for learning, students' data, and technology-based education management systems. Without a basic understanding of cybersecurity, educational institutions are vulnerable to digital threats that can disrupt the learning process.

RESEARCH DESIGN

Activity Design

This community service activity uses an interactive online workshop method, accompanied by training and evaluation, to improve cybersecurity literacy in teachers and students. The implementation of the Activity is focused on a participatory approach, where participants receive material passively and are actively involved in simulations and discussions.

Activity Stages

a. Activity Preparation

1. Needs Analysis

An initial survey was conducted on participants, including teachers and students, to identify the level of cybersecurity literacy, specific needs, and challenges faced in protecting digital data in schools. This survey is conducted online using platforms such as Google Forms.

2. Preparation of Training Modules

The training material is designed based on the survey findings, including an introduction to cybersecurity, types of cyber threats, mitigation measures, and best practices in maintaining digital data security.

3. Technical Preparation

Online platforms such as Zoom and Google Classroom are used as an implementation medium. Training modules, learning videos, and additional teaching materials are uploaded to Google Drive for participant access.

b. Implementation of Activities

The implementation of this online workshop consisted of several main sessions: 1) Opening session (30 minutes), namely a) Remarks and introductions from the implementation team, and b) Explanation of the objectives and benefits of the training. 2) Cybersecurity introduction session (60 minutes), namely a) Explanation of basic cybersecurity concepts; b) Identify common cyber threats such as phishing, malware, and hacking. 3) Cybersecurity practice session (90 minutes), i.e., a) Simulation of cyber threat recognition through real examples (e.g., phishing emails); b) Practice creating strong and secure passwords; and c) Group discussion on case studies of cybersecurity violations in the educational environment. 4) There will be a question-and-answer session and discussion (30 minutes), where participants will be invited to ask questions and share experiences about the challenges they face related to cybersecurity. 5) Evaluation and closing session (30 minutes), namely a) Training evaluation using online quizzes to measure the improvement of

participants' understanding; and b) Submission of evaluation results and provision of follow-up recommendations.

c. Evaluation and Follow-up

The evaluation was carried out through 1) questionnaires to assess participants' satisfaction with the Activity; 2) online tests to measure material understanding before and after training; 3) Participants who show the best evaluation results will be rewarded in the form of a special e-certificate; 4) Online discussion groups via WhatsApp or Telegram are created to facilitate post-activity communication, information sharing; and 5) answering participants' questions.

Supporting Tools and Media

The online platform uses Zoom, Google Classroom, Google Forms, and WhatsApp/Telegram. Furthermore, the training materials use PowerPoint presentations, simulation videos, and PDF modules. Meanwhile, the evaluation uses online quizzes with applications such as Kahoot! or Google Forms.

Target Participants

The target participants are teachers and high school students in Indonesia who have minimal access to devices and internet connections. The selection of participants is carried out through coordination with partner schools that are willing to participate.

Expected Results

The expected results of this Community Service activity are a) Increasing cybersecurity literacy among teachers and students, b) Awareness of the importance of protecting digital data in the educational environment, and c) Forming a continuous learning community to share information related to cybersecurity. With this method, service activities are expected to be helpful in a practical way and the first step in building a safe digital literacy culture in Indonesian education.

RESULTS

The implementation of the Activity was carried out according to the method that had been designed, with the following results:

Participant Profile

The number of participants who participated in the Activity was 50, consisting of 30 teachers and 20 students from several secondary schools in Indonesia.

Table 1. Participant Profile

No.	Participant Profile	Amount (n)	Percentage (%)
1	Teachers	30	60%
2	Students	20	40%
	Total	50	100%

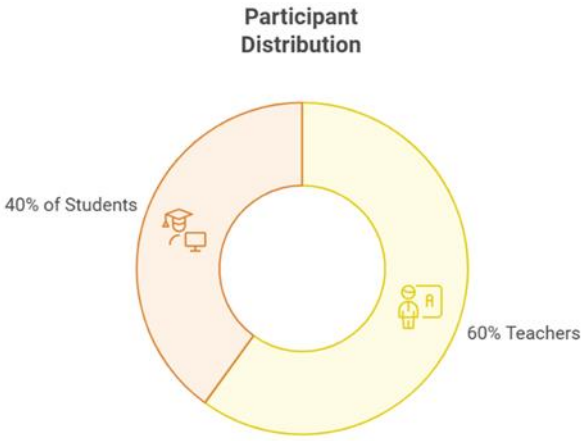

Figure 1. Distribution of Community Service Activities Participants

Evaluation of Material Comprehension

The increase in participants' understanding of cybersecurity was measured through tests before and after the training. This test consists of 10 multiple-choice questions.

Table 2. Evaluation of Material Comprehension

No.	Category	Average Score Before (Pre-test)	Average Score After (Post-test)	Increase (%)
1	Teachers	50	85	70%
2	Student	45	80	78%
3	Average Total	48	83	73%
4	Category	Average Score Before (Pre-test)	Average Score After (Post-test)	Increase (%)

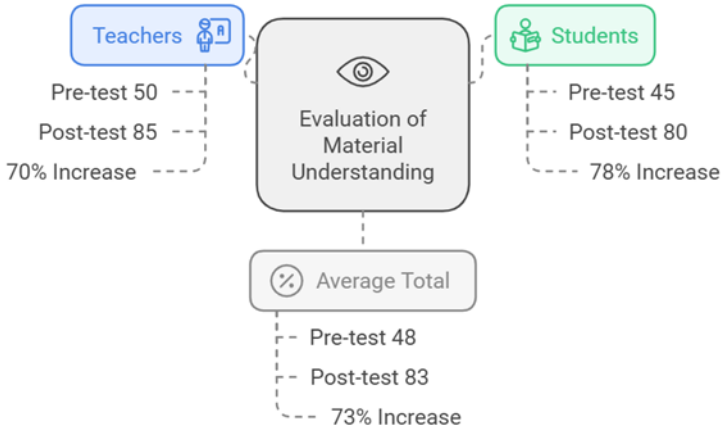

Figure 2. Results of Evaluation of the Understanding of Community Service Activity Participants on the Material

Participant Satisfaction Level

The participants' satisfaction level with the training was assessed using a questionnaire with a Likert scale (1–5).

Table 3. Participant Satisfaction Level

No.	Assessed Aspects	Average Score (1–5)	Category
1	Material Suitability	4.8	Excellent
2	Relevance to Needs	4.7	Excellent
3	Training Interactivity	4.6	Excellent
4	Presentation by the Speaker	4.9	Excellent
5	Average Total	4.75	Excellent

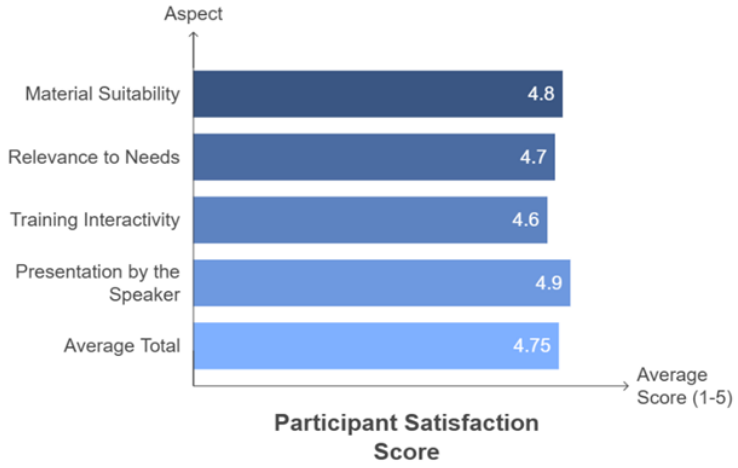

Figure 3. Satisfaction Level Score of Community Service Activity Participants

DISCUSSION

The results of Community Service (PKM) activities that focus on introducing cybersecurity to teachers and students show a significant increase in understanding and awareness of the importance of digital literacy. Based on pre-test and post-test data, there was an average increase of 73% in participants' comprehension scores. This indicates the effectiveness of the interactive-based online training method used. This increase is in line with the findings of Ouahidi (2020), which shows that a technology-based approach to education can improve students' digital literacy skills.

In addition, the increased distribution of scores indicates that teachers and students have successfully understood basic cybersecurity concepts, such as types of cyber threats and mitigation measures. This is an essential first step in reducing the vulnerability of educational institutions to cyberattacks, as suggested by AlDaajeh et al. (2022), which emphasizes the importance of cybersecurity literacy education in the academic environment to face increasing digital threats.

Participant satisfaction with the training was also in the "outstanding" category, with an average score of 4.75 on a scale of 5. This reflects the success of a participatory-based training approach that actively engages participants through simulations and discussions. A study by Harahap et al. (2022) and Susanti et al. (2022) also supports that interactivity in online learning is vital in increasing participant satisfaction and engagement.

However, although the results show success, there are several challenges to implementing this Activity. One is limited internet access for some participants in certain regions, which can affect participation and the quality of the training experience. Similar challenges were also reported by Berliyanto & Santoso (2018) and Hadiningrat et al. (2024), who found that technological infrastructure barriers are still the main obstacle in implementing online training in Indonesia. Therefore, efforts to expand access and digital infrastructure should be a concern in the following service program.

This Activity also has the potential to be further developed through advanced training that focuses on the practical application of cybersecurity technology in the school environment. A study by Heena & Nidhi (2022) emphasized that continuous training can have a long-term impact on integrating digital literacy into the educational curriculum. Overall, this PKM activity provides direct benefits for participants and contributes to strengthening the digital literacy culture in the education sector. This Activity can be a widely applied model to support digital transformation in Indonesia.

CONCLUSIONS

Community Service Activities (PKM) that focus on introducing cybersecurity for teachers and students in Indonesia have increased participants' digital literacy. Based on the pre-test and post-test results, there was an average increase in understanding by 73%, which shows the effectiveness of the interactive-based online training method. The level of satisfaction of participants in the "excellent" category also indicates the relevance of the material and the success of the training approach used. This Activity proves that cybersecurity literacy can be improved through technology-based education designed systematically and interactively.

However, challenges in implementation, such as limited internet access in some regions, are a reminder of the importance of strengthening digital infrastructure in Indonesia. By overcoming these constraints, similar programs can be expanded and developed to support digital transformation in the education sector. Therefore, this Activity provides direct benefits to participants and becomes a strategic step in building a sustainable digital literacy culture in the educational environment.

REFERENCES

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). a Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection. *Computer Science & IT Research Journal*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

Ahyani, E., & Dhuhani, E. M. (2024). Transformasi Digital dalam Manajemen Perkantoran Pendidikan: Sebuah Kajian Literatur. *Jurnal Visionary : Penelitian Dan Pengembangan Dibidang Administrasi Pendidikan*, *12*(1), 205. https://doi.org/10.33394/vis.v12i1.10785

Akor, S. O., Nongo, C., Udofot, C., & Oladokun, B. D. (2024). Cybersecurity Awareness: Leveraging Emerging Technologies in the Security and Management of Libraries in Higher Education Institutions. *Southern African Journal of Security*. https://doi.org/10.25159/3005-4222/16671

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Anastasopoulou, E., Angeliki Tsagri, Eleni Avramidi, Konstantina Lourida, Evangelia Mitroyanni, Danai Tsogka, & Ioannis Katsikis. (2024). The Impact of ICT on Education. *Technium Social Sciences Journal*, *58*, 48–55. https://doi.org/10.47577/tssj.v58i1.11144

Andraško, J., Mesarčík, M., & Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. *AI & SOCIETY*, *36*(2), 623–636. https://doi.org/10.1007/s00146-020-01125-5

Asy'hary, A., Arsyad, J., Sulistyo, L., Rahayu, W., & Fatmawati, E. (2023). Upaya Peningkatan Literasi Digital Masyarakat Melalui Program Pelatihan Komputer Di Desa Terpencil. *Communnity Development Journal*, *4*(1), 654–661.

Bajac, M., & Fišer, M. (2024). Digital Transformation and New Educational Paradigm. *Social Informatics Journal*, *3*(1), 1–8. https://doi.org/10.58898/sij.v3i1.01-08

Begamudra Rangavittal, P. (2024). Cybersecurity Threats in the Age of Digital Transformation: Strategies for Mitigation and Resilience. *International Journal of Science and Research (IJSR)*, *13*(7), 1279–1285. https://doi.org/10.21275/SR24721221003

Berliyanto, & Santoso, H. B. (2018). Indonesian perspective on massive open online courses: Opportunities and challenges. *Journal of Educators Online*, *15*(1). https://doi.org/10.9743/jeo2018.15.1.11

Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J., & Dragoni, N. (2022). Emerging Cyber Security Challenges after COVID Pandemic: A Survey. *Journal of Internet Services and Information Security*, *12*(2), 21–50. https://doi.org/10.22667/JISIS.2022.05.31.021

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*. https://doi.org/10.1177/01655515231160026

Fernández, A., Gómez, B., Binjaku, K., & Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. *Education and Information Technologies*, *28*(10), 12351–12382. https://doi.org/10.1007/s10639-022-11544-0

Ghazali, N., Ab Rahim, I. S., & Syed Idrus, S. Z. (2024). Challenges and Opportunities of Cybersecurity Education for Non-technical Majors. *Journal of Communication in Scientific Inquiry (JCSI)*, *6*(1), 47–55. https://doi.org/10.58915/jcsi.v6i1.873

Hadiningrat, K. P. S. S., Silalahi, V. A. J. M., & Wardani, F. P. (2024). Opportunities and Challenges in Implementing Information Technology Innovations in the Indonesian Education Sector. *East Asian Journal of Multidisciplinary Research*, *3*(8). https://doi.org/10.55927/eajmr.v3i8.10686

Harahap, F. M., Ulinniam, Sitinjak, L., Urath, S., & Alfiyanto, A. (2022). Pelaksanaan Pembelajaran Daring pada Masa Pandemi Covid-19 di SMPN 23 Palembang. *Pendidikan Tambusai*, *06*(02), 8501–8508. https://doi.org/https://doi.org/10.31004/jptam.v6i2.3697

Heena, C., & Nidhi, B. (2022). Barriers Affecting the Effectiveness of Digital Literacy Training Programs (DLTPs) for Marginalised Populations: A Systematic Literature Review. *Journal of Technical Education and Training*, *14*(1), 110–127. https://doi.org/10.30880/jtet.2022.14.01.010

Hussain, S. M., Tummalapalli, S. R. K., & Chakravarthy, A. S. N. (2024). CYBER SECURITY EDUCATION: ENHANCING CYBER SECURITY CAPABILITIES, NAVIGATING TRENDS AND CHALLENGES IN A DYNAMIC LANDSCAPE. In *Advances in Cyber*

Security and Digital Forensics (pp. 9–33). Iterative International Publishers, Selfypage Developers Pvt Ltd. https://doi.org/10.58532/nbennurch254

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

Jagadeesan, S., Sameer, Singh, D., Ojha, R., Ibrahim, R. K., & Alazzam, M. B. (2023). Application of Cybersecurity in E-Learning Education. *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)*, 932–937. https://doi.org/10.1109/AECE59614.2023.10428587

Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaiah, M. A. (2024). Cybersecurity Awareness among Secondary School Students Post Covid19 Pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115–127. https://doi.org/10.37934/araset.37.1.115127

Jamal, B., Ain, Q. ul, Dara, D., Shabbir, A., & Shaikh, G. M. (2024). Impact of ICT on the Academic Performance of Students at University Level. *Bulletin of Business and Economics (BBE)*, *13*(2), 719–722. https://doi.org/10.61506/01.00385

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

Kumar, I. (2023). Emerging Threats in Cybersecurity: A Review Article. *International Journal of Applied and Natural Sciences Journal Homepage*. http://bluemarkpublishers.com/index.php/IJANS

Mandadi, S., Gochhayat, S. P., Torremocha, V., & Kethar, J. (2024). Cybersecurity Risks in Remote Work and Learning Environments and Methods of Combating Them. *Journal of Student Research*, *13*(2). https://doi.org/10.47611/jsrhs.v13i2.6808

Ouahidi, L. M. (2020). Constraints on Developing Digital Literacy Skills in Higher Education. *International Journal of Linguistics, Literature and Translation (IJLLT)*, *3*(2), 197–205. https://creativecommons.org/licenses/by/4.0/

Perwej, D. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

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

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Rewara, N., Faridah, N. A., Wijay, T. T., & Wijay, T. (2024). Inhibiting factors of metaverse adoption in Indonesian education: A literature review. *Hipkin Journal of Educational Research*, *1*(1), 75–86. http://ejournal-hipkin.or.id/index.php/hipkin-jer/

Roopesh, M. (2024). CYBERSECURITY SOLUTIONS AND PRACTICES: FIREWALLS, INTRUSION DETECTION/PREVENTION, ENCRYPTION, MULTI-FACTOR AUTHENTICATION. *ACADEMIC JOURNAL ON BUSINESS ADMINISTRATION, INNOVATION & SUSTAINABILITY*, *4*(3), 37–52. https://doi.org/10.69593/ajbais.v4i3.90

Sani, M. R. (2024). ANALISIS KINERJA DAN PENGGUNAAN WEBSITE SEKOLAH DALAM MENINGKATKAN KUALITAS PELAYANAN PENDIDIKAN: TINJAUAN SISTEMATIS. *Scientica: Jurnal Ilmiah Sains Dan Teknologi*, *3*(1).

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Siphambili, N. (2024). Exploring Cybersecurity Implications in Higher Education. *European Conference on Cyber Warfare and Security*, *23*(1), 526–531. https://doi.org/10.34190/eccws.23.1.2306

Susanti, Y., Guntur, M., Jaya, R., Rais, R., Alfiyanto, A., & Hidayati, F. (2022). Pengorganisasian Kelas dalam Pembelajaran Daring Masa Pandemi di MI. *At-Tafkir*, *15*(1), 82–97. https://doi.org/10.32505/at.v15i1.4352

Syafuddin, K., Jamalullail, & Rafi'i. (2023). Peningkatan Literasi Keamanan Digital Dan Perlindungan Data Pribadi Bagi Siswa Di Smpn 154 Jakarta. *Eastasouth Journal of Impactive Community Services*, *1*(03), 122–133. https://doi.org/10.58812/ejimcs.v1i03.119

Wagman, K. B., Blinder, E. B., Song, K., Vignon, A., Dworkin, S., Clegg, T., Vitak, J., & Chetty, M. (2023). "We picked community over privacy": Privacy and Security Concerns Emerging from Remote Learning Sociotechnical Infrastructure During COVID-19. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2), 1–29. https://doi.org/10.1145/3610036

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: considering the human factors. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyae001

Zhang-Kennedy, L., & Chiasson, S. (2022). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, *54*(1), 1–39. https://doi.org/10.1145/3427920