PUBLISHER
YAYASAN PENDIDIKAN DAN PENGEMBANGAN HARAPAN ANANDA

JURNAL
WAWASAN DAN AKSARA

Juwara | p-issn: 2797-2097 | e-issn: 2797-2119 | **Vol. 6 No. 1 (2026)**
https://doi.org/10.58740/juwara.v6i1.777

Digital Security Awareness Level of Boarding School Based Islamic Junior High School Students in Central Lampung

Radinal Fadli[1(✉)], Dwi Wahyudi[2], Fivia Eliza[3]
[1,2]Universitas Lampung, Indonesia
[3]Universitas Negeri Padang, Indonesia

✉Correspondence Author:
radinalfadli@fkip.unila.ac.id

Abstract
The increasing use of the internet and information technology devices among students has made digital security awareness an important issue in educational environments. This study aims to analyze the level of digital security awareness among students of a boarding school–based Islamic junior high school in Central Lampung. A descriptive quantitative approach was employed, with the population consisting of all active students in grades VII–IX who had used the internet for at least one year. The study involved 40 students selected through purposive sampling. The research instrument was an objective multiple-choice test covering several aspects of digital security. The results show that students' awareness is not evenly distributed across all aspects. Awareness of Viruses and Malware (75%) and Cyberbullying (70%) fell into the Sufficient category, indicating a basic understanding but still requiring reinforcement. In contrast, awareness of Artificial Intelligence (40%), Online Grooming (44%), and Phishing & Scams (47%) was categorized as Poor, highlighting the need for serious attention and targeted educational interventions. These findings emphasize the importance of implementing digital security literacy programs, particularly concerning contemporary digital threats, to better prepare boarding school students for the increasingly complex risks of cyberspace. Academically, this study contributes to the growing literature on digital security awareness within Islamic educational settings and highlights the need for integrating structured cybersecurity literacy into boarding school curricula. Furthermore, the findings may serve as a reference for future studies and educational policymakers in developing more contextual and sustainable digital security education programs.

Keywords
Boarding School; Cybersecurity Education; Digital Literacy; Digital Security Awareness

INTRODUCTION

Digital technology has become an inseparable part of modern education and adolescent life worldwide. Globally, adolescents are among the most active internet users and are increasingly dependent on digital platforms for learning, communication, and entertainment activities. Junior high school students are increasingly familiar with various digital platforms, whether for learning activities, communication, or entertainment (N. Hidayat et al., 2024). However, alongside the growing access to the digital world, the risks of cyber security are also rising (setiawan et al., 2024). Threats such as personal data theft, cyberbullying, harmful content, and online exploitation pose serious challenges for the younger generation, who often lack adequate preparedness to navigate the digital world safely (Hendrawan et al., 2025). Several international studies have further highlighted that adolescents remain highly vulnerable to cyber threats due to limited digital security awareness and insufficient supervision in educational environments (Lopez & Gatica, 2025). Therefore, strengthening students' digital security awareness has become an important concern for educational institutions in creating safer and more responsible digital learning environments.

Digital security is not merely a technical issue but also involves aspects of literacy, awareness, and user behaviour (F. Hidayat et al., 2025). This perspective aligns with the Chheang et al. (2026) Digital Literacy Framework which emphasizes that digital literacy encompasses not only technical skills but also cognitive, socio-emotional, and critical thinking abilities in navigating digital environments. In this context, adolescents, including junior high school students, represent a vulnerable group facing various forms of digital threats due to their limited knowledge and experience (Subni et al., 2024). The environment of Islamic boarding school–based institutions creates unique dynamics in how students interact with the digital world (Sri et al., 2024). Within boarding schools, supervision of students' digital activities is often limited, as educators and caretakers tend to prioritize spiritual and academic development Furthermore, the absence of internal policies on digital literacy and the lack of guidance when students access the internet may exacerbate the risks of exposure to harmful content (Rahman, 2024), unsafe interactions (Alamin et al., 2024), or inappropriate digital practices (Rahmawati et al., 2024). In other words, the closed boarding school system may inadvertently create blind spots in digital

supervision, leaving students more vulnerable to digital security threats without the awareness of their surrounding environment.

Accordingly, schools—including Islamic boarding school–based institutions—are expected not only to function as centers of academic and spiritual development but also to provide safe digital environments that support the comprehensive enhancement of students' digital literacy (Syahid et al., 2024). In line with the concept of digital literacy and cybersecurity awareness, students should be equipped with the knowledge, attitudes, and practical skills necessary to use technology wisely, safely, and responsibly (Yeyendra et al., 2024). Therefore, internet use within school environments should ideally be supported by clear institutional policies (Eliza et al., 2024), adequate supervision mechanisms (Surdjono et al., 2025), and the integration of digital security content into the learning process (Manik, 2022). Such measures are important for establishing structured internal control and continuous guidance, particularly considering the high intensity of gadget use and internet access among students outside classroom hours. Through these efforts, schools can play a strategic role in fostering students' digital security awareness and minimizing potential cyber risks within educational environments.

Several previous studies have highlighted the importance of digital security awareness. For instance, research by (Agung Al Affan et al., 2025) demonstrated that low levels of digital literacy among students increase their vulnerability to cyberbullying and the misuse of personal data. Similarly (Idris & Rukli, 2025), emphasized that students' understanding of digital security practices remains limited to technical aspects, such as password usage, while behavioral and ethical dimensions of digital engagement have not been adequately addressed. Another study by (Alam et al., 2025), found that integrating digital security content into the school curriculum has a significant impact on enhancing students' awareness at the secondary education level. However, to date, no research has specifically examined the level of digital security awareness among students in boarding school–based Islamic junior high schools. Therefore, this study was conducted to address this gap and to contribute to the development of more targeted digital security literacy strategies within Islamic boarding school environments.

Based on this research gap, this study aims to analyze the level of digital security awareness among students in boarding school–based Islamic junior high schools in Central Lampung. By focusing on the distinctive characteristics of Islamic boarding school

environments, this study is expected to contribute to the existing literature on digital security literacy and cybersecurity awareness within Islamic educational settings. Furthermore, the findings are anticipated to provide practical recommendations for schools, teachers, and policymakers in designing more targeted and sustainable digital security education interventions to promote safer and more responsible digital behavior among students.

METHOD

This study employed a descriptive quantitative approach aimed at providing an objective overview of the level of digital security awareness among junior high school students. This approach was chosen as it is suitable for measuring variables that can be expressed numerically and statistically analyzed to identify tendencies, frequencies, and general patterns within the population.

Population and Sample

The population of this study consisted of all students enrolled in boarding school–based Islamic junior high schools in Central Lampung. The sampling technique employed was purposive sampling, in which participants were selected based on specific criteria while ensuring equal opportunity for eligible members of the population to be included (Sari et al., 2023). The criteria applied were active students from grades VII to IX who had used the internet or information technology devices for at least one year. A total of 40 students were selected as the sample, of the target population. Sample size of 40 students was sufficient for descriptive quantitative analysis, as this study primarily aimed to identify general patterns and levels of digital security awareness among students in the selected educational setting.

Data Collection Techniques

The data in this study were collected using a multiple-choice test designed to measure students' understanding of digital security. The test consisted of 20 items with four answer options, of which only one was correct. The instrument was developed to assess students' comprehension of several key aspects of cybersecurity. The test was administered directly to the respondents, with a completion time of approximately 45 minutes. The results of the

test served as the primary data source for assessing students' levels of digital security awareness.

Research Instruments

The research instrument used in this study was an objective test in the form of multiple-choice questions with four answer options (A, B, C, D), of which only one was correct. The test was designed to measure students' level of understanding of digital security across five main aspects, as presented in Table 1 below.

Table 1. Digital Security Awareness Level Test Instrument Grid

No	Aspek	Objective	No. Question
1	Virus dan Malware	About malicious software threats	1,2,3,4
2	Phising and Scam	Recognizing forms of digital fraud	5,6,7,8
3	Cyberbullying	Awareness of Cyberbullying	9,10,11,12
4	Online Grooming	Understanding the threat of interacting with strangers on the internet	13,14,15,16
5	Artificial Intelligence (AI):	Understanding in recognizing the misuse of AI technology for information manipulation.	17,18,19,20

Prior to its use in the study, the instrument underwent a content validity test by soliciting evaluations from experts in the fields of information technology and education. In addition, a pilot test was conducted with respondents outside the research sample to assess the validity and reliability of the test items. Item validity was examined using point-biserial correlation analysis between individual item scores and the total score, while reliability was calculated using the Kuder-Richardson Formula 20 (KR-20), yielded a coefficient of 0.82, indicating that the instrument had high internal consistency and was reliable for measuring students' digital security awareness.

Data Analysis Techniques

The data obtained from the multiple-choice test were analyzed using descriptive statistics. Each student's total score was calculated to determine their individual level of understanding. The scores were then converted into percentages using the following formula:

$$\text{Percentages} = \frac{\text{number of answered correctly}}{\text{Total respondent}} x100\%$$

The percentage results were used to categorize students' levels of digital security awareness into several groups. The categorization criteria were determined based on the following percentage intervals:

Table 2. Cybersecurity Awareness Level Standards

Level	Range Score	Recomendation
Good	80 - 100	Need to Maintain
Sufficient	60 - 79	Need Improvement
Poor	< 60	Need Treatment

RESULT AND DISCUSSION

Result

After the test was administered to the students, the average score for each aspect of digital security awareness was obtained. The results were then categorized according to the Standard Level of Cybersecurity Awareness to determine the students' awareness levels and the follow-up recommendations required. The average scores and recommendations for each aspect are presented in Figure 1 below.

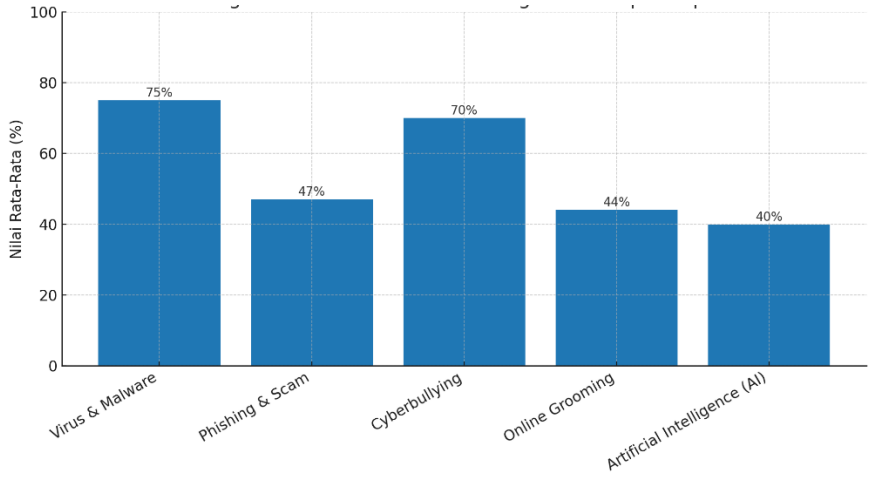

Figure 1. Average Digital Security Level Test Results

Based on Figure 1, it can be observed that students' levels of digital security awareness are not evenly distributed across all aspects. The highest scores were found in the areas of Viruses and Malware (75%) and Cyberbullying (70%), both categorized as *Sufficient* with the recommendation of *Need Improvement*. This finding supports the perspective of Yoram Eshet-Alkalai that students' digital experiences contribute to the development of operational digital literacy skills through repeated interaction with digital technologies. These findings also suggest that students' daily experiences in interacting

with digital devices contribute to their awareness. Although their level of understanding falls within the *Sufficient* category, further reinforcement is still required through more systematic and integrated learning within the curriculum. Thus, the current achievements can serve as a solid starting point but still demand additional interventions to elevate students' digital security awareness to a more optimal level.

Conversely, the lowest levels of awareness were found in the aspect of Artificial Intelligence (AI), with an average score of only 40% (*Poor* category), followed by Online Grooming (44%) and Phishing & Scam (47%). These three aspects all fall into the *Poor* category, thus requiring serious attention and specific interventions (*Need Treatment*). This condition indicates that students are still unable to recognize more modern forms of digital threats, such as AI-based manipulation through deepfakes and voice cloning, and they tend to be less vigilant against potentially harmful interactions with strangers online as well as increasingly complex online fraud schemes. The low awareness regarding AI-based threats and online grooming also reflects the behavioural dimension of cybersecurity awareness proposed by Kathryn Parsons, particularly students' limited ability to recognize and respond to emerging cyber risks. To further clarify the distribution of research findings, the data were also visualized using a heatmap. This visualization illustrates the variation in students' digital security awareness levels across different aspects through color gradations, as shown in Figure 2 below.

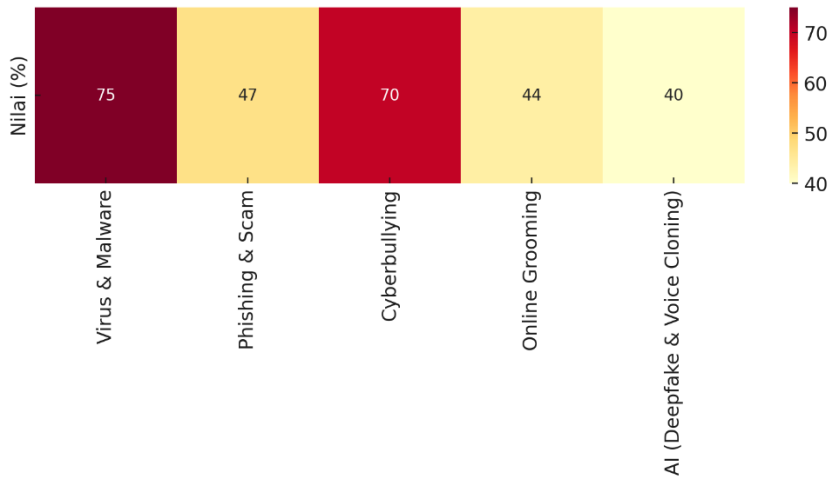

Figure 2. Digital Security Awareness Level Heatmap

Based on the heatmap in Figure 2, it can be seen that the aspects of Viruses & Malware (75%) and Cyberbullying (70%) are represented by darker colours, indicating relatively higher levels of awareness compared to the other aspects. In contrast, lighter colours appear in the aspects of Phishing & Scam (47%), Online Grooming (44%), and particularly Artificial Intelligence (AI: Deepfake & Voice Cloning) (40%), which reflects students' low levels of awareness regarding these topics. This visualization reinforces the finding that students tend to be more prepared to deal with traditional digital threats but remain vulnerable to more complex contemporary digital threats. Therefore, there is a need to strengthen digital literacy efforts that not only emphasize classical aspects of cybersecurity but also specifically equip students with the ability to recognize and anticipate emerging threats in cyberspace.

Discussion

The findings of this study indicate variations in students' levels of digital security awareness across different aspects. The aspects of Viruses and Malware (75%) and Cyberbullying (70%) were categorized as *Sufficient*, suggesting that students relatively possess a basic understanding of traditional digital threats. This may be attributed to the high exposure to issues related to viruses, malware, and cases of online bullying in their daily lives as well as through media. Consistent with the study of (Fachrin, 2025), students' digital literacy tends to be stronger in areas that frequently emerge within their social environment, which explains why awareness of these aspects is relatively higher compared to more complex digital threats.

Conversely, the aspects of Phishing & Scam (47%), Online Grooming (44%), and Artificial Intelligence (AI: Deepfake & Voice Cloning) (40%) were categorized as *Poor*, indicating significant weaknesses in students' awareness of contemporary digital threats. This finding is consistent with the study of (Keamanan et al., 2024), which revealed that students still tend to perceive digital security in terms of simple technical practices, such as password usage, but remain unfamiliar with the increasingly diverse modes of digital fraud. Furthermore, research by (Effendy & Oktiani, 2024), emphasized that integrating digital security content into the curriculum can enhance students' awareness, particularly regarding emerging topics that are rarely addressed in formal education. Thus, the low

scores in the areas of phishing, grooming, and AI are most likely influenced by students' limited access to specific education on these threats.

In the context of boarding schools, the low level of awareness in certain aspects can also be understood as a consequence of limited digital supervision and the absence of comprehensive internal digital literacy policies. The boarding school environment, which tends to prioritize academic and spiritual development, often results in digital security education receiving insufficient attention. Consequently, students may lack adequate opportunities to learn about emerging digital threats that are less visible but potentially harmful. This condition underscores the need for more structured digital literacy policies in boarding school settings, involving teachers, caretakers, and parents in a collaborative manner.

Practically, the findings of this study provide several important implications for educational institutions, particularly Islamic boarding schools. First, the aspects of phishing, online grooming, and Artificial Intelligence (AI)-based threats should become priority topics in students' digital literacy programs, as these represent the areas least understood by students. Second, the findings highlight the importance of integrating structured cybersecurity literacy into boarding school curricula through contextual learning materials, awareness campaigns, and supervised digital practices. Such integration may include topics related to online fraud prevention, safe social media interaction, digital ethics, privacy protection, and the identification of AI-based manipulation such as deepfakes and voice cloning. Furthermore, collaboration among teachers, boarding school caretakers, and parents is essential to ensure continuous guidance and monitoring of students' digital activities. Therefore, this study not only enriches the literature on adolescents' digital security awareness, particularly within Indonesian Islamic boarding school settings, but also provides a practical foundation for policymakers and educational institutions to design more targeted and sustainable cybersecurity education interventions.

CONCLUSION

This study concludes that the level of digital security awareness among students of boarding school–based Islamic junior high schools uneven across different aspects. The aspects of Viruses and Malware as well as Cyberbullying indicating a relatively adequate basic understanding of traditional digital threats, although further reinforcement is still

needed. In contrast, the aspects of Phishing & Scam, Online Grooming, and Artificial Intelligence (AI: Deepfake & Voice Cloning) reflecting students' low awareness of contemporary digital threats and the need for more targeted educational interventions. These findings highlight the importance of integrating structured cybersecurity education into boarding school–based Islamic junior high schools curricula to strengthen students' digital literacy and preparedness in facing evolving cyber risks. However, this study was limited by its relatively small sample size and the use of quantitative data only. Therefore, future research is recommended to involve broader samples and mixed-method approaches to obtain more comprehensive findings regarding students' digital security awareness in Islamic boarding school environments.

REFERENCES

Agung Al Affan, M., Fronita, M., Saputra, E., Luthfi Hamzah, M., Islam Negeri Sultan Syarif Kasim, U., & Soebrantas No, J. H. (2025). Measuring The Level of Cybersecurity Awareness of Social Media Users Among Students. *INOVTEK Polbeng - Seri Informatika*, *10*(1), 134–145. https://doi.org/10.35314/VYCQ9T65

Alam, H. S., Putra, A. A. G. A. M., Wiguna, A. A. G. B. A., Putra, I. G. A. H. J., & Adnyana, I. K. S. (2025). Peningkatan Literasi Dan Keamanan Digital Siswa SMP Negeri 3 Bangli Melalui Pelatihan Interaktif. *Joong-Ki : Jurnal Pengabdian Masyarakat*, *4*(4), 1330–1337. https://doi.org/10.56799/JOONGKI.V4I4.10487

Alamin, Z., Khairunnas, Larosae, T. A., Rofikah, U., Missouri, R., Sutriawan, & Alimin, M. (2024). Membangun Kecerdasan Digital Melalui Integrasi Literasi Digital dan Keamanan Digital. *Journal of Excellence Humanities and Religiosity*, *1*(2), 59–70. https://doi.org/10.34304/JOEHR.V1I2.247

Chheang, S., Phin, K., Hok, C., Rin, R., Tep, P., Loch, S., Phan, K., & Huot, S. (2026). Empowering Early Learners: Building Digital Literacy in Childhood Education. *Coresource 4*, 191–220. https://doi.org/10.4018/979-8-3373-6269-4.CH008

Effendy, M. Y., & Oktiani, H. (2024). Literasi Digital Keamanan Siber pada Remaja menghadapi Social Engineering. *Wacana Publik*, *18*(1), 35–42. https://doi.org/10.37295/WP.V18I1.67

Eliza, F., Fadli, R., Hidayah, Y., Surjono, H. D., & Sari, R. C. (2024). Enhancing cybersecurity awareness through mobile learning: a study on vocational accounting

and finance students. *International Journal of Advanced Technology and Engineering Exploration*, *11*(121), 1714–1731. https://doi.org/10.19101/IJATEE.2024.111101097

Fachrin, M. (2025). Tinjauan Sistematis Strategi Literasi Digital dan Keamanan Online untuk Siswa Sekolah Dasar: Mengusulkan Kerangka LOKAL. *FONDASI: Jurnal Pendidikan Dasar*, *1*(2), 53–59. https://doi.org/10.71094/FONDASI.V1I2.134

Hendrawan, F. R., Rahma, D. W., Ramadhan, Y. Z., Siregar, S. D., Naufal, F., Marza, M., & Muhtar, A. Y. (2025). Peningkatan Literasi Digital dalam Keamanan Siber bagi Siswa SMK Telekomunikasi Telesandi Bekasi. *SOROT : Jurnal Pengabdian Kepada Masyarakat*, *4*(2), 74–79. https://doi.org/10.32699/SOROT.V4I2.9534

Hidayat, F., Ramadhan, A., Cahya, G. I., Zayni, A., Ilyasya, A., Putra, I. J., Algifari, I., Azis, F., Farhansyah, M., & Akbar, D. (2025). Keamanan Siber Dan Etika Berinternet Di Kalangan Pelajar Era Digital. *APPA : Jurnal Pengabdian Kepada Masyarakat*, *2*(6), 752–758. https://jurnalmahasiswa.com/index.php/appa/article/view/2234

Hidayat, N., Paccagnnelae, N., & Paramithaswari, D. (2024). Peningkatan Keterampilan Keamanan Digital pada Siswa SMK Ananda Bekasi di Era Disrupsi Digital. *Jurnal Pengabdian Masyarakat Waradin*, *4*(3), 234–242. https://doi.org/10.56910/WRD.V4I3.432

Idris, H., & Rukli, R. (2025). EKSPLORASI PEMAHAMAN KEAMANAN DIGITAL OLEH SISWA SD DALAM AKTIVITAS ONLINE. *ELEMENTARY: Jurnal Inovasi Pendidikan Dasar* , *5*(2), 252–259. https://doi.org/10.51878/ELEMENTARY.V5I2.5574

Keamanan, K., Pada, D., Desa, M., Di, J., Hidayatussalamah, E. D., & Widyatama, R. (2024). KESADARAN KEAMANAN DIGITAL PADA MASYARAKAT DESA JIMBAR DI ERA DISRUPTIF. *Jurnal Ilmiah Wahana Pendidikan*, *10*(22), 584–590. https://doi.org/10.5281/ZENODO.14574171

Lopez, F. A., & Gatica, G. (2025). The Impact of Fear of Cyberattacks on Cybersecurity Behaviour in Young College Students. *Lecture Notes in Networks and Systems*, *1449 LNNS*, 82–92. https://doi.org/10.1007/978-3-031-93103-1_9

Manik, J. S. (2022). Peran Guru dalam Menjaga E-Safety Peserta Didik di Era Teknologi Digital di Indonesia. *EDUKATIF : JURNAL ILMU PENDIDIKAN*, *4*(4), 5098–5108. https://doi.org/10.31004/EDUKATIF.V4I4.3085

Rahman, Z. A. (2024). Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(6), 82–90. https://doi.org/10.61132/MERKURIUS.V2I6.399

Rahmawati, Y., Yuliani, M., & Hariyati, F. (2024). Pelatihan Literasi Digital Anak untuk Edukasi Keamanan dan Etika Digital Pelajar SD Muhammadiyah 12 Setia Budi Pamulang. *Inovasi Jurnal Pengabdian Masyarakat*, *2*(2), 275–282. https://doi.org/10.54082/IJPM.528

Sari, M., Desy Susiaty, U., Irvandi, W., Matematika, P., Pontianak, P., Ampera, J., 88 Kota, N., & Pontianak, B. (2023). Implementasi Model Pembelajaran Inquiry Berbantuan Quizizz terhadap Kemampuan Pemahaman Konsep Matematis SPLTV. *Juwara: Jurnal Wawasan Dan Aksara*, *3*(1), 57–67. https://doi.org/10.58740/JUWARA.V3I1.61

setiawan, R., Anjani, A. G. P., Putra, B. A., Febrianti, A., Cahyani, P., & Nastifa, D. (2024). PENTINGNYA PENDIDIKAN DIGITAL DALAM MENINGKATKAN KESADARAN DAN KETERAMPILAN ANAK DALAM MENGHINDARI CYBERCRIME. *Pendas : Jurnal Ilmiah Pendidikan Dasar*, *9*(04), 438–453. https://doi.org/10.23969/JP.V9I04.20558

Sri, E., Herawati, B., Mustofa, Z., Sari, M. N., Mirsa, R. P., Widiyan, A. P., Astuti, Y., Studi, P., Pendidikan, A., Pendidikan, I., Psikologi, D., & Yogyakarta, U. N. (2024). Edukasi Digital Safety Dalam Meningkatkan Kecakapan Bermedia Digital Siswa. *Lamahu: Jurnal Pengabdian Masyarakat Terintegrasi*, *3*(1), 47–54. https://doi.org/10.37905/LJPMT.V3I1.24090

Subni, M., Warman, W., & Yahya, M. (2024). MENINGKATKAN KESADARAN KEAMANAN DATA DIGITAL DI KALANGAN GURU: PERAN DAN TANTANGAN. *Jurnal Pengabdian Kreativitas Pendidikan Mahakam (JPKPM)*, *4*(1), 38–46. https://jurnal.fkip-uwgm.ac.id/index.php/jpkpm/article/view/1682

Surdjono, H. D., Fadli, R., Sari, R. C., Eliza, F., Yassin, A., Kulanthaivel, G., Ramadhan, M. A., Mukhaiyar, R., Hamid, M. A., Ridwan, M. R., Purnomo, S., & Asnimawati. (2025). Effectiveness of Cybersecurity Awareness Program Based on Mobile Learning to Improve Cyber Hygiene. *International Journal of Information and Education Technology*, *15*(2), 220–229.

https://doi.org/10.18178/IJIET.2025.15.2.2235

Syahid, A., Hamid, F. H. S., Jannah, M., Fitriani, N., Rahmadaniati, N., Saumi, R. I., Lukman, R. A. I., & Kusumaningrum, T. A. (2024). Edukasi Keamanan Digital dan Penggunaan Media Sosial di SMP Negeri 3 Palangka Raya: Bahasa Pengantar Bahasa Inggris. *KALANDRA Jurnal Pengabdian Kepada Masyarakat*, *3*(3), 125–133. https://doi.org/10.55266/JURNALKALANDRA.V3I3.384

Yeyendra, Y., Hajar, I., Darmanto, D., & Junaidi, E. (2024). Profil Keterampilan Literasi Digital Siswa SMA di Era Teknologi Digital. *Biology and Education Journal*, *4*(2), 111–119. https://doi.org/10.25299/BAEJ.2024.19988