Volume 4 Number 2 (2026)
July-December 2026
Page: 2408-2414

ISSN: 3031-2884
EDUJAVARE PUBLISHING
https://edujavare.com/index.php/edujavare

Development and Testing of an Android-Based Cybersecurity Awareness Educational Application for Students of SMP 4 Fatuleu Barat

Bonie Empy Giri
Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Citra Bangsa, Indonesia;
bonieangi28@gmail.com

Article history Submitted: 2026/08/01; Revised: 2026/09/11; Accepted: 2026/11/08

Abstract

The rapid development of digital technology has increased the use of the internet and mobile devices among students, while simultaneously exposing them to various cybersecurity threats, such as phishing, malware, identity theft, and personal data misuse. Therefore, cybersecurity awareness needs to be introduced from an early age through accessible and engaging educational media. This study aims to develop and test an Android-based cybersecurity awareness educational application for students of SMP 4 Fatuleu Barat. The application is designed to provide interactive learning materials covering basic cybersecurity concepts, types of cyber threats, password security, personal data protection, phishing awareness, and safe internet practices. The development of this application is expected to provide an alternative learning medium that enables students to understand digital security concepts more effectively. Application testing is conducted to evaluate its functionality and suitability as an educational medium. The expected outcome of this study is an Android-based educational application that is functional, accessible, and appropriate for supporting cybersecurity awareness among junior high school students. This application is also expected to contribute to strengthening students' digital literacy and encouraging responsible behavior when using digital technology.

Keywords Android Application, Cybersecurity Awareness, Digital Literacy, Educational Media, Junior High School Students

© 2026 by the authors. This is an open-access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY SA) license,https://creativecommons.org/licenses/by-sa/4.0/.

INTRODUCTION

The development of information and communication technology has brought significant changes to various aspects of life, including education. The widespread use of the internet, computers, and smartphones has made it easier for people to access information, communicate, and utilize various digital services. In the educational environment, digital technology provides opportunities for students to expand their knowledge and skills through more interactive learning resources. However, these technological advances are also accompanied by increasing digital security risks, particularly for users who lack sufficient knowledge of how to protect themselves when engaging in online activities. Threats such as phishing, malware, identity theft, account hacking, and personal data misuse have become serious concerns that require attention, including among junior high school students.

Junior high school students represent a group of digital technology users who need to

develop cybersecurity awareness from an early age. At this stage, students are increasingly active in using digital devices and the internet to support their learning activities and interact through various digital platforms. However, frequent technology use does not necessarily correspond to the ability to identify cyber threats and implement safe digital practices. Limited understanding of password security, personal data protection, suspicious links, and the risks of online interactions may increase students' vulnerability to cybercrime. Therefore, cybersecurity education needs to be introduced as an essential component of strengthening digital literacy in schools.

Cybersecurity awareness refers to an individual's understanding and awareness of cybersecurity threats, as well as the ability to implement preventive measures when using digital technology. Information security is generally based on three fundamental principles: confidentiality, integrity, and availability, commonly known as the CIA Triad. These principles serve as the foundation for maintaining the security of information and digital systems. In the educational context, cybersecurity awareness involves not only understanding technical concepts but also developing positive attitudes and responsible digital habits. These include protecting personal information, creating strong passwords, avoiding unfamiliar links, and critically evaluating information received through the internet.

Education plays a strategic role in developing cybersecurity awareness through structured learning processes that are appropriate to students' characteristics. Cybersecurity education can be delivered through theoretical and practical approaches, including instructional materials, simulations, case studies, and interactive learning media. These approaches enable students not only to understand cybersecurity concepts but also to recognize potential threats and determine appropriate responses when encountering them. The integration of technology into learning activities also provides opportunities to deliver educational content in more engaging, accessible, and relevant ways that correspond to students' learning habits.

One technology with considerable potential for developing cybersecurity educational media is the Android operating system. Android-based applications allow learning materials to be delivered through mobile devices, making them easily accessible via smartphones. Educational applications can incorporate instructional materials, illustrations, real-life examples, and quizzes to evaluate users' understanding. Through interactive presentation, such applications are expected to help students understand cybersecurity concepts more effectively than conventional instructional methods that rely solely on lectures or printed materials. Furthermore, mobile applications can serve as alternative learning media that support both independent learning and teacher-assisted instruction.

The development of a cybersecurity awareness educational application should consider the learning needs and comprehension levels of junior high school students. The materials should be presented using simple language, examples related to students' everyday experiences, and an intuitive user interface. Relevant topics include an

introduction to cybersecurity, types of cyber threats, account and password security, personal data protection, phishing awareness, and internet ethics. The presentation of these topics is expected to help students recognize potential risks when using digital devices while developing appropriate habits for protecting themselves in cyberspace.

In addition to the development process, application testing is an essential stage to ensure that the application functions according to user requirements. Testing is conducted to determine whether each feature operates properly, whether the application is easy to use, and whether its content and interface are appropriate for the intended users. Therefore, application testing should not focus exclusively on technical functionality but also consider the application's suitability as an educational medium. The results of testing can provide a basis for identifying weaknesses, implementing improvements, and refining the application before it is introduced into learning activities.

Based on these considerations, this study focuses on the development and testing of an Android-based cybersecurity awareness educational application for students at SMP 4 Fatuleu Barat. The application is designed to provide an informative, interactive, and user-friendly educational medium that helps students understand fundamental cybersecurity concepts. Specifically, this study aims to develop an Android-based cybersecurity awareness educational application and evaluate its functionality and suitability as a learning medium for junior high school students. The findings are expected to provide an alternative educational resource that supports the improvement of digital security awareness in the school environment and contributes to strengthening students' digital literacy in responding to various risks associated with the use of information technology.

METHOD

This study adopts a descriptive qualitative approach using a literature review and conceptual analysis design to explore the role of education in increasing cybersecurity awareness amid the growing complexity of digital threats. The study focuses on an in-depth analysis of the integration of digital security topics into formal education curricula, the effectiveness of various non-formal training programs, such as professional certifications and workshops, and partnership models involving government institutions, educational institutions, and the technology industry. Data were collected from scientific literature, program documents published by national and international institutions, and relevant implementation case studies. All collected data were analyzed thematically to identify key patterns, concepts, and findings related to cybersecurity education. The analysis was intended to formulate an educational model that could promote digital literacy and encourage more security-conscious behavior among individuals across various social environments.

RESULTS AND DISCUSSION

Implementation of Cybersecurity Education Across Various Institutions

The commitment of formal educational institutions to integrating cybersecurity topics into their curricula has become increasingly evident, particularly at the secondary and higher

education levels. This initiative represents a response to the growing complexity of risks in the digital environment. Learning materials covering data protection, cyber threat identification, password management, and ethical technology use have gradually been incorporated into information and communication technology subjects to foster cybersecurity awareness from an early age. At the university level, several institutions have introduced specialized courses or modules covering encryption, privacy policies, and digital forensic investigations as part of information technology, computer science, and cyber law programs.

Meanwhile, non-formal education also plays an important role in reaching broader communities that have limited access to formal cybersecurity education. Professional certifications such as Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), and CompTIA Security+, offered by international organizations such as EC-Council and CompTIA, provide more practical and technically oriented training. These programs generally include simulated cyberattacks, case studies, and practice-based assessments to help participants understand real-world threat patterns. In addition, self-paced online training through platforms such as Coursera, Udemy, and CISA provides an increasingly popular alternative due to its flexibility in terms of time, cost, and accessibility.

In industrial and organizational contexts, information security training has become an integral part of risk management procedures and internal governance systems. Many companies require cybersecurity training for newly recruited employees as part of their orientation programs and conduct regular follow-up training for all staff members. These programs cover phishing awareness, internal security policies, and assessments of organizational preparedness for cyberattacks. In the public sector, several government ministries and agencies have established partnerships with educational institutions and industry stakeholders to develop training guidelines tailored to the specific needs of their respective sectors. The implementation of cybersecurity education becomes more effective when supported by a cross-sector collaborative approach involving educational institutions, government agencies, industry, and technology user communities. Such collaboration not only expands access to cybersecurity education but also ensures that learning materials remain relevant to continuously evolving cyber threats. In practice, collaborative initiatives have contributed to the development of more adaptive curricula that respond to technological advancements while establishing competency standards aligned with current professional and industry requirements.

Advantages and Challenges of Cybersecurity Education

Public awareness of the importance of digital security continues to grow alongside the implementation of systematic and goal-oriented cybersecurity education programs. Education plays a significant role in equipping individuals with the ability to recognize digital threats and developing safe and responsible technology usage behaviors. Learning materials covering password management, two-factor authentication, phishing attacks, and social engineering are essential components of both theoretical and practical learning

processes. Individuals' ability to anticipate digital attacks reflects the effectiveness of security literacy developed through structured educational approaches.

At the organizational level, the benefits of cybersecurity education can be observed through improvements in internal security management and reductions in data breaches caused by human error. By providing training across all organizational levels, institutions can establish collective awareness of the importance of maintaining data integrity. This enables potential security incidents to be identified and addressed more promptly and efficiently. In addition to protecting information infrastructure, such initiatives strengthen public confidence in an organization's commitment to safeguarding the data of its users and business partners. Nevertheless, the implementation of digital security education programs continues to face significant challenges. These include the absence of standardized national cybersecurity curricula, which means that implementation often depends on local initiatives. The limited availability of educators with specialized cybersecurity expertise also represents a major obstacle, particularly in areas with restricted access to professional training. Furthermore, low public interest and limited participation in training programs indicate that awareness of cybersecurity issues has not yet been evenly established across society.

To address these challenges, innovative educational approaches have increasingly been developed to reach broader audiences. Gamification makes learning more engaging and accessible, while simulations based on realistic scenarios allow participants to experience the potential consequences of unsafe digital practices. In addition, artificial intelligence (AI)-based technologies are being utilized to personalize learning materials according to individual needs and capabilities. These innovations demonstrate that, with appropriate strategies and technological support, efforts to improve digital security literacy can become more progressive, inclusive, and effective.

Implications for Individuals and Organizations and Implementation Strategies

Cybersecurity education makes a significant contribution to improving individual awareness of increasingly complex digital risks. Individuals who participate in structured educational programs tend to demonstrate better abilities to identify various cyber threats, including phishing, malware, and social engineering attacks. They also become more disciplined in adopting safe digital practices, such as creating strong passwords, activating two-factor authentication, and carefully verifying information before engaging in online activities. Digital literacy acquired through educational processes plays an important role in developing more cautious, ethical, and responsible technology usage behaviors. Furthermore, cybersecurity education increases individuals' confidence in utilizing digital services effectively without neglecting security considerations.

At the organizational level, human resources equipped with knowledge of information security principles and practices represent a crucial asset in addressing the evolving cybersecurity landscape. Through internal training programs, organizations can establish a security-conscious working culture in which all employees actively participate in protecting systems and information. The positive impacts of such education extend beyond

operational efficiency to include regulatory compliance, increased stakeholder confidence, and stronger institutional reputations. In this context, education serves not merely as a means of developing technical skills but also as a strategic instrument for internalizing security values across all organizational levels, from leadership to operational staff.

The implementation of cybersecurity education strategies should be adapted to the backgrounds, levels of digital understanding, and specific needs of each target group. Therefore, learning materials should be contextualized to ensure their relevance and accessibility. In educational settings, project-based learning supported by micro-credentials can strengthen students' understanding of the practical application of cybersecurity in everyday activities. Meanwhile, in the industrial sector, risk-analysis-based training tailored to specific organizational conditions and vulnerabilities can accelerate the internalization of security policies and improve responses to actual threats. The selection of educational methods should also consider technological developments and continuously changing cyberattack patterns.

To ensure the optimal implementation of these strategies, strong public policies, cross-sector collaboration, and innovation in learning methods are essential. Governments are expected to establish national policy frameworks that encourage the integration of cybersecurity into both formal and professional education. Meanwhile, the industrial sector can contribute expertise, facilities, and experience-based training scenarios as part of its corporate social responsibility and long-term business interests. Such collaboration will strengthen an inclusive, adaptive, and sustainable digital security literacy ecosystem, ensuring that education becomes a fundamental foundation for building a resilient digital society capable of responding effectively to evolving cyber threats.

CONCLUSION

Addressing the growing challenges in the rapidly evolving field of cybersecurity has become increasingly important. The integration of information security education into formal educational systems, from primary schools to higher education institutions, contributes to improving students' digital literacy. Similarly, public awareness campaigns and non-formal training programs help broaden society's understanding of digital security issues. The findings indicate that a comprehensive and sustainable educational approach plays an important role in developing critical thinking skills, promoting safe digital practices, and strengthening the resilience of individuals and institutions against various cyber threats. However, several challenges remain in Indonesia, including disparities in access to educational resources, unequal teaching quality across regions, and the limited integration of cybersecurity literacy into the national curriculum. Addressing these challenges requires adaptive learning approaches, contextualized instruction, and collaboration among government agencies, educational institutions, industry stakeholders, and digital communities to establish a secure, resilient, and sustainable digital environment.

The development of cybersecurity education should be implemented systematically, comprehensively, and with a long-term perspective. The government and educational

institutions are encouraged to develop relevant and accessible learning materials, strengthen teachers' competencies through continuous training, and establish policies that support the integration of cybersecurity literacy into educational programs. Furthermore, private-sector organizations, technology communities, and civil society organizations should actively contribute through collaborative learning initiatives, free digital learning resources, and community-based educational campaigns. Future research is also recommended to examine the effectiveness of adaptive learning approaches and develop educational models that correspond to users' characteristics and local needs across various sectors. Through integrated and sustainable implementation, education can serve as a fundamental strategy for building a digitally literate, critical, ethical, and resilient society capable of recognizing and responding to evolving cybersecurity threats.

REFERENCE

Budi, E., Wira, D., & Infantono, A. (2024). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO), 3, 223–234.

CISA. (2023). Cybersecurity Education and Training Assistance Program (CETAP).

Cybersecurity Intelligence. (2025). The Evolution Of Cybersecurity Education.

Ginanjar, Y. (2022). STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA. Jurnal Dinamika Global, 7(02), 291–312.

Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning. University of Wollongong.

Permana, A. (2022). Indonesia’s Cyber Defense Strategy in Mitigating the Risk of Cyber Warfare Threats. Vol. 3, Issue 1.

Sudarmadi, D.A. & Runturambi, A.J.S. (2024). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2), 157–178.