Jurnal Bhakti Karya dan Inovatif

e-ISSN: 2775-5002
p-ISSN: 3025-3985
Volume 6 No. 2 August 2026

Strengthening Cybersecurity Literacy and Personal Data Protection for Students and Educators

Muhamad Fathur Fawaz[1)], Galih Abdul Fatah Maulani[2)], Fahmi Al Ghiffari[1)], Muh Aqil Safaat Nugraha[1)], Vina Septia Anggraeni[1)]

[1)] Institut Pendidikan Indonesia Garut

[2)] Universitas Garut

Email: fathur38@institutpendidikan.ac.id; galihafm@uniga.ac.id; fahmi_al_ghifari_mhs@institutpendidikan.ac.id.

Accepted:	Accepted After Revision:	Published:
12 August 2026	28 August 2026	3 September 2026

Abstract

This community service program aimed to strengthen the digital resilience of students, teachers, and education staff at SMP Negeri 5 Tarogong Kidul, Garut Regency, through practice-based training on cybersecurity literacy and personal data protection, delivered to 65 participants (34 teachers, 30 students, and 1 school operator) on April 29, 2026. The program combined a cybersecurity-ecosystem literacy session with a controlled, ethically-bounded simulation of fake-link and phishing traps, and its effectiveness was measured through a pre-test–post-test design, a paired t-test, an N-Gain analysis, and a satisfaction survey. The results showed a significant increase in understanding, from an average pre-test score of 65.38 to a post-test score of 87.08 (a gain of 21.70 points; paired t-test $p < 0.001$), with an average N-Gain of 0.61 (61.44%), categorized as moderately effective. The participant satisfaction index reached 91.67% (very satisfied). These findings indicate that practice-based, simulation-supported cybersecurity training adapted to the school context can improve personal data security literacy and encourage safer digital behavior, while also highlighting the need for such training to be delivered regularly and evaluated for its longer-term retention effect.

Keywords: Personal Data Security, Digital Resilience, Cybersecurity Literacy, Students, Education Staff.

1 INTRODUCTION

Personal data security has become one of the critical issues in digital life, as nearly all educational, communication, administrative, and learning activities are now connected to online systems. Technological development provides convenience for school communities, but it also increases exposure to cyber risks such as data theft, account misuse, hacking, phishing, fake links, and the spread of unsafe information. In this context, personal data security is not merely a technical matter but is also closely related to users' awareness, habits, and ability to recognize digital threats [1], [2].

The educational environment is one of the spaces most vulnerable to information security threats, as students, teachers, and education staff use various digital platforms for learning, communication, document storage, and academic data management. The increasingly widespread use of educational technology has not always been accompanied by adequate understanding of cybersecurity. Several studies indicate that cybersecurity education at the school level is important so that students and educators can understand digital risks early and not merely become passive technology users [3], [4].

Many digital-literacy or cybersecurity-awareness activities conducted in school settings are still delivered as one-time lectures or seminars, with content that is largely conceptual and rarely accompanied by a systematic measurement of learning outcomes. What distinguishes the present program is a combination of elements that are still rarely implemented together at the junior secondary school level: (1) a structured cybersecurity-ecosystem literacy session paired with a hands-on, ethically-bounded simulation of fake-link and phishing traps, so that participants do not merely receive theory but also directly experience how such attacks are constructed and how to recognize them; (2) a rigorous pre-test–post-test evaluation design supported by a paired t-test and N-Gain analysis, rather than relying solely on participant satisfaction as an indicator of success; and (3) a specific focus on a public junior secondary school in a non-metropolitan regency (Garut), a context that remains underrepresented compared with studies conducted at the university level [8] or in schools in more digitally mature regions [9]. This combination positions the program not only as a literacy activity but

also as an evidence-based intervention whose effectiveness can be measured and replicated.

SMP Negeri 5 Tarogong Kidul, Garut Regency, is the partner school that needs to improve its community's understanding of personal data security. Based on the initial assessment, students, teachers, and education staff actively use digital technology, but not all of them fully understand how to recognize fake links, safeguard account credentials, avoid phishing traps, or apply safe habits when using digital devices and services. This condition has the potential to create risks for both individuals and educational institutions, particularly if the personal data of students, teachers, or school administration is not managed securely.

This community service program was implemented in response to that need through education, training, mentoring, and evaluation. The program was designed so that participants would not only receive theoretical explanations but also gain learning experience through case studies, educational simulations, discussions, and reinforcement of a personal digital security checklist. The objective of this program was to improve participants' understanding of the cybersecurity ecosystem, digital threats, the impact of cybercrime, the identification of fake links, and preventive measures for safeguarding personal data. In addition, this program aimed to build critical awareness so that school communities can apply safer digital behavior in their daily lives.

1 METHODS

This community service program used an educational-participatory approach. The educational approach was used to provide a basic understanding of cybersecurity and personal data protection, while the participatory approach was used to actively engage participants through discussions, question-and-answer sessions, educational simulations, and reflection on cases relevant to everyday life. The activity was held on Wednesday, April 29, 2026, at SMP Negeri 5 Tarogong Kidul, Garut Regency, with a total of 65 participants consisting of 34 teachers, 30 students, and 1 education staff/school operator.

The program consisted of three main stages: pre-implementation, implementation, and post-activity. In the pre-implementation stage, the team coordinated with the school regarding the program's needs, technical arrangements, participants, schedule, venue, and event structure. In the implementation stage, the activity began with participant registration, opening remarks from the program leader and the school principal, pre-test completion, material delivery, educational simulation, discussion and question-and-answer sessions, post-test completion, satisfaction survey completion, closing, and documentation. In the post-activity stage, the team processed the pre-test, post-test, and participant satisfaction survey data.

The first material was presented by Muhamad Fathur Fawaz, M.Kom., with the topic "Cybersecurity Literacy: Understanding the Ecosystem, Threats, and Impact of Digital Crime in Cyberspace." This material emphasized a basic understanding of the cyber world, forms of threats, the impact of digital crime, and real case studies as material for participant reflection. In this session, participants also received a Personal Digital Checklist handbook as a practical guide for personal digital security.

Figure 1. Documentation of the Cybersecurity Literacy Session
Source: Community service results, 2026

The second material was presented by Muh Aqil Safaat Nugraha with the topic "Cyber Trap: The Secret Behind Fake Links Lurking Around Us." In this session, participants were guided to understand the characteristics of fake links, recognize fraudulent login pages, and analyze digital trap patterns. The demonstration was conducted as a controlled educational simulation to show how attack methods can occur, without providing technical instructions that could be misused. The simulation was thus focused on raising awareness and prevention.

Figure 2. Documentation of the Cyber Trap and Fake Link Session
Source: Community service results, 2026

Figure 3. Documentation of the Question and Answer Session
Source: Community service results, 2026

The program was evaluated using a one-group pre-test–post-test design. The pre-test and post-test each used an identical instrument consisting of 10 multiple-choice items, with both topics delivered in the program – the cybersecurity ecosystem and the impact of digital crime, and the identification of fake links and phishing – proportionally represented. The items were drafted based on the material delivered by the presenters, with the assistance of an AI-based writing tool; owing to time constraints, no formal content-validity procedure (e.g., expert judgment or piloting) was carried out at the time of data collection. A retrospective reliability check was subsequently performed on the retained pre-test item-level responses (n = 65), yielding KR-20 = 0.42, indicating low-to-questionable internal consistency; this is discussed as a limitation in Section 4.5. A self-administered satisfaction questionnaire consisting of nine items (Table 4) was distributed after the activity using a four-point Likert scale (1 = strongly disagree to 4 = strongly agree) to assess participants' evaluation of the material, presenters, and program organization. Quantitative data were analyzed by comparing pre-test and post-test scores, a paired-sample t-test, an N-Gain score following Hake's formula g = (post-test score – pre-test score) / (maximum score – pre-test score) [14], with categories of high (g > 0.7), medium (0.3 <= g <= 0.7), and low (g < 0.3), and a satisfaction index calculated as the percentage of the total score relative to the maximum possible score. Qualitative data were obtained from participant feedback, discussion results, and reflective notes recorded during the program. Participation was voluntary; because most student participants are minors, involvement was coordinated with and authorized by the school as the responsible institution, and all pre-test, post-test, and questionnaire data were anonymized prior to analysis to protect participants' personal data, consistent with the personal-data-protection principles promoted by the program itself.

2 RESULTS AND DISCUSSION

2.1 Improvement in Participants' Understanding

The evaluation results show that the community service program was able to improve participants' understanding of personal data security and cyber threats. Before the activity, participants' average pre-test score was 65.38. After participants received the material, simulation, and discussion, the average post-test score increased to 87.08. This represents an improvement of 21.70 points. The lowest score also increased from 50.00 to 80.00, while the highest score increased from 80.00 to 90.00. The paired t-test results showed p-value < 0.001, indicating that the improvement in participants' understanding was statistically significant.

Table 1. Summary of Pre-Test and Post-Test Results (N = 65)

Indicator	Pre-Test	Post-Test	Improvement
Average Score	65.38	87.08	+21.70
Lowest Score	50.00	80.00	+30.00
Highest Score	80.00	90.00	+10.00

Source: Community service results, 2026
Note: Based on the paired t-test, p-value < 0.001, indicating that the improvement is statistically significant.

2.2 Program Effectiveness Based on N-Gain

The program's effectiveness was also analyzed using the N-Gain score. Based on the data processing results, 18 participants (27.69%) fell into the high N-Gain category, while 47 participants (72.31%) fell into the medium category. No participants fell into the low category. The overall average N-Gain was 0.61 or 61.44%, indicating that the program can be categorized as moderately effective in improving participants' competence and understanding of cybersecurity and personal data protection.

Table 2. Effectiveness Analysis Using N-Gain Score

N-Gain Category	Value Range (g)	Number of Participants	Percentage (%)
High	g > 0.7	18	27.69%
Medium	0.3 <= g <= 0.7	47	72.31%
Low	g < 0.3	0	0.00%
Total	-	65	100.00%

Source: Community service results, 2026

Table 3. Pre-Test and Post-Test Performance Based on Participant Status

Participant Status	N	Average Pre-Test	Average Post-Test	Average N-Gain	Effectiveness Category
Teachers	34	69.71	88.53	0.60	Medium
Students	30	60.33	85.33	0.63	Medium
Operator	1	70.00	90.00	0.67	Medium

Source: Community service results, 2026

2.3 Participant Satisfaction with the Program

The participant satisfaction evaluation showed very positive results. The overall average satisfaction index reached 91.67%, categorized as very satisfied. The indicator with the highest score was the presenters' mastery of the material at 95.77%, followed by the cybersecurity literacy material at 95.00%, and the presenters' ability to answer discussion questions at 94.62%. These results indicate that participants considered the program relevant to their digital needs and delivered in an easily understandable manner.

Table 4. Participant Satisfaction Index for Program Implementation

Assessment Indicator	Total Score	Satisfaction Index	Category
The material delivered is relevant to participants' current needs	236	90.77%	Very Satisfied
The cybersecurity literacy material is easy to understand and useful	247	95.00%	Very Satisfied
The Cyber Trap/fake link material is practical and easy to apply	226	86.92%	Very Satisfied
The presentation slides are easy to understand and engaging	232	89.23%	Very Satisfied
The presenter mastered the material very well	249	95.77%	Very Satisfied
The presenter's language style is easy to understand and not boring	234	90.00%	Very Satisfied
The presenter answered discussion questions satisfactorily	246	94.62%	Very Satisfied
The program's implementation time matched the rundown	236	90.77%	Very Satisfied
The committee was friendly and helpful throughout the program	239	91.92%	Very Satisfied
Overall satisfaction index	238.3	91.67%	Very Satisfied

2.4 Participant Responses and Practical Relevance of the Material

Qualitatively, participants considered the most memorable material to be the explanation of the real impact of cyberattacks on financial, social, and personal aspects of life. Participants also showed strong interest in practical material on how to distinguish fake login pages, recognize trap links, and understand social engineering patterns commonly used in cyberattacks. This indicates that participants need material that is not only conceptual but also directly related to everyday digital experience.

The discussion and question-and-answer session showed that participants began to understand that personal data security is not solely the responsibility of technicians or system operators, but also the responsibility of every technology user. In the school context, this awareness is important because teachers, students, and education staff interact with academic data, digital accounts, personal devices, and various communication platforms. This shift in participants' understanding can therefore serve as a foundation for building a digital security culture within the school environment.

Participants also suggested that similar programs be conducted regularly and reach more schools, at both the junior and senior high school levels. Minor feedback related to the provision of refreshments and improved time management during implementation. Overall, these responses indicate that the community service program was well received and has the potential to be developed into a sustainable cybersecurity literacy program within educational settings.

2.5 Interpretation and Implications of the Findings

The overall pattern of results, a statistically significant increase in test scores, a moderate N-Gain, and a very high satisfaction index, suggests that the improvement in participants' understanding is more plausibly attributable to the program's practice-based design than to the delivery of information alone. Two elements of the program design appear to have contributed most directly to this outcome. First, the fake-link and phishing simulation session translated abstract cybersecurity concepts into a concrete, recognizable experience, which is consistent with the qualitative finding that participants found this material the most memorable and most directly linked to their everyday digital experience (Section 4.4). Second, the Personal Digital Checklist provided as a take-home reference reinforced the material beyond the session itself, supporting retention of practical guidance rather than conceptual knowledge alone. This pattern is consistent with survey evidence from Jordanian middle schools,

where cybersecurity education emerged as one of the strongest predictors of students' security awareness, second only to password-management knowledge [13], and with a nine-country European study reporting that most schools allocate cybersecurity only two to three hours per month within general computing courses, an amount the authors argue is insufficient and recommend expanding in both time and frequency [9]; this reinforces the broader argument that cybersecurity education is highly relevant at the school pedagogy level [4].

The moderate, rather than high, N-Gain category obtained in this program (0.61) indicates that although the intervention was effective within a single session, most participants (72.31%, Table 2) remained in the medium rather than the high category, suggesting that a single session is sufficient to build initial awareness but may not be sufficient to produce mastery-level understanding. This is consistent with recommendations in the literature that cybersecurity training rely on repeated, practice-based delivery, for instance through simulations and workshops, rather than a single lecture-style session [13], and with evidence that security-education programs are more effective when delivered through diversified, multi-channel formats rather than a single, one-time method [11]. It is also important to note the methodological limitations of this evaluation. The one-group pre-test–post-test design, without a comparison group, means that the observed improvement, although statistically significant, cannot be attributed to the program alone; maturation, familiarity with the test instrument on the second administration, and social-desirability bias in the self-reported satisfaction survey cannot be ruled out. A further limitation concerns the pre-test/post-test instrument itself: as noted in Section 3, its 10 items were drafted without formal content-validity or reliability testing. A retrospective reliability check on the retained pre-test data yielded KR-20 = 0.42, a low-to-questionable level of internal consistency. Item-level analysis indicates this was driven mainly by four items that all participants, including at pre-test, answered correctly, so these items contributed no discriminating variance; reliability could not be meaningfully re-estimated on the post-test administration for the same reason. This indicates that part of the observed 21.70-point gain should be interpreted with caution, and that item difficulty calibration should be prioritized when this instrument is revised for future use. The evaluation also measured only participants' knowledge and perceived satisfaction immediately after the activity, not their actual digital behavior over time, so whether participants continue to apply safer digital practices several weeks or months after the training remains untested, a limitation shared by comparable school-based cybersecurity-awareness surveys, which likewise report no empirical data on the retention of effects beyond a single point in time [13]. Because the program was implemented at a single school with a relatively small, non-randomly selected sample (N = 65, including only one school operator), the results should be interpreted as context-specific evidence of program feasibility and short-term effectiveness rather than as generalizable proof of cybersecurity-literacy improvement across schools.

For the partner school, these findings suggest that the program provides a workable model for building initial cybersecurity awareness among teachers, students, and staff, and that its practice-based components (the simulation and the digital checklist) are the elements most worth retaining if the program is scaled or repeated. Consistent with participants' own suggestion that similar programs be conducted regularly (Section 4.4), the results support institutionalizing this type of training, for example as a recurring component of the school's digital-safety curriculum, rather than treating it as a one-off activity, and pairing future iterations with a follow-up assessment to evaluate the retention of both knowledge and behavior over time. Future iterations should also budget time for formal instrument development – content validation by subject-matter experts and a reliability check – so that reported gains rest on a measurement instrument with demonstrated psychometric quality, not only on statistical significance.

3 CONCLUSION

The community service program on personal data security education and training at SMP Negeri 5 Tarogong Kidul, Garut Regency, successfully improved participants' understanding of cybersecurity, personal data protection, phishing, fake links, and safe practices in using digital technology. This improvement is reflected in the increase of the average pre-test score from 65.38 to 87.08 in the post-test, with a gain of 21.70 points and paired t-test results of p-value < 0.001. The N-Gain analysis of 0.61 or 61.44% indicates that the program falls into the moderately effective category. In addition, the participant satisfaction index of 91.67% shows that the program was very well received by participants. The educational, simulative, and contextual approach proved relevant for improving the digital resilience of school communities.

REFERENCES

[1] T. Xu, “Ethical Boundary Between Network Security and Personal Privacy in the Era of Big Data,” *International Journal of Information Security and Privacy (IJISP)*, vol. 19, no. 1, pp. 1–18, 2025.

[2] P. G. Chiara, "The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional" Security&Privacy" Surveys," *Eur. Data Prot. L. Rev.*, vol. 7, p. 18, 2021.

[3] W. Wei and M. R. B. A. Rahman, "Research on the Issues and Paths of Citizen Privacy Protection in China in the Era of Big Data," *SALUD, CIENCIA Y TECNOLOGÍA Учредители: Salud, Ciencia y Tecnologia*, vol. 4, 2024.

[4] E. Amankwa, "Relevance of cybersecurity education at pedagogy levels in schools," *Research Highlights in Mathematics and Computer Science Vol. 7*, vol. 7, pp. 21–37, 2023.

[5] H. H. M. A. Al-Fatlawi, "Awareness of cyber security aspects in distance education," *Journal of Pedagogical Sociology and Psychology*, vol. 6, no. 1, pp. 77–88, 2024.

[6] M. F. Fawaz and Y. Nugraha, "Security Audit for Detection and Mitigation of AMP Injection from Online Gambling Sites on the Wordpress Platform with a Code Analysis and Wordfence Scanning Approach," *RISTEC: Research in Information Systems and Technology*, vol. 6, no. 1, pp. 138–153, 2025.

[7] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity.," *Computer Systems Science & Engineering*, vol. 40, no. 3, 2022.

[8] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, p. 39, 2021.

[9] B. Jerman Blažič and A. Jerman Blažič, "Cybersecurity skills among European high-school students: a new approach in the design of sustainable educational development in cybersecurity," *Sustainability*, vol. 14, no. 8, p. 4763, 2022.

[10] S. Alrobaian, S. Alshahrani, and A. Almaleh, "Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. Big Data Cogn Comput 7 (2): 73," 2023.

[11] B. Zheng, D. Tse, J. Ma, X. Lang, and Y. Lu, "An Empirical Study of SETA Program Sustaining Educational Sector's Information Security vs. Information Systems Misuse," *Sustainability*, vol. 15, no. 17, p. 12669, 2023.

[12] Y. Deng, Z. Zeng, K. Jha, and D. Huang, "Problem-based cybersecurity lab with knowledge graph as guidance," *Journal of Artificial Intelligence and Technology*, 2021.

[13] M. H. M. Altarawneh, A. Althunibat, M. H. Almajali, N. Alzriqat, and S. Alazzam, "Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 1, pp. 1516–1529, 2025.

[14] R. R. Hake, "Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses," *American Journal of Physics*, vol. 66, no. 1, pp. 64–74, 1998.