Abdi Jurnal Publikasi **ISSN : 2963-3486**
Vol. 4, No. 5, Mei 2026 (17-21)

CYBERSECURITY EDUCATION FOR YOUNG GENERATIONS: THREATS, RISKS, AND SELF-PROTECTION STRATEGIES IN THE DIGITAL WORLD

Satrya Mahardika[1], Abdul Saboor[2], Kautsar Hilmi[3], M. Heru Prayogo[4], Wildan Hilmy[5], H. Apridelson Manurung[6], Ahmad Zulfikar A.[7]*

[1]Master Program in Informatics Engineering, Universitas Pamulang, Tangerang Selatan, Indonesia, 15417
*e-mail: zulfikar.khalwaniev@gmail.com

Abstract

The rapid growth of digital technology has increased internet use among young people, especially students who actively use social media, messaging applications, online games, and learning platforms. However, this participation is not always accompanied by adequate cybersecurity literacy. As a result, young users may be exposed to phishing, account takeover, malware, online fraud, personal data leakage, identity misuse, and cyberbullying. This community service activity aimed to introduce practical cybersecurity awareness and self-protection strategies for students and teachers. The activity was conducted at SMA Al Wafi Islamic Boarding School, Depok, on 10 April 2026 from 08.00 to 11.00 WIB, involving approximately 300 participants consisting of senior high school students, grade 9 students, and teachers. The method combined interactive presentation, case-based explanation, simple threat-identification simulation, open discussion, and qualitative evaluation through observation and participant feedback. The materials covered common cyber threats, digital privacy, phishing-link recognition, strong password habits, two-factor authentication, one-time password protection, and responsible social media behavior. The results indicated increased awareness based on participant engagement, questions, and observed ability to restate basic cybersecurity practices. The activity also produced practical learning materials and recommendations for sustainable cybersecurity literacy programs in the school environment.

Abstrak

Perkembangan teknologi digital telah meningkatkan intensitas penggunaan internet di kalangan generasi muda, khususnya siswa yang aktif menggunakan media sosial, aplikasi pesan instan, permainan daring, dan platform pembelajaran. Namun, aktivitas digital tersebut belum selalu diimbangi dengan literasi keamanan siber yang memadai. Kondisi ini membuat generasi muda berisiko menghadapi phishing, peretasan akun, malware, penipuan daring, kebocoran data pribadi, penyalahgunaan identitas, dan cyberbullying. Kegiatan pengabdian kepada masyarakat ini bertujuan memperkenalkan kesadaran keamanan siber dan strategi perlindungan diri yang praktis bagi siswa dan guru. Kegiatan dilaksanakan di SMA Al Wafi Islamic Boarding School, Depok, pada 10 April 2026 pukul 08.00-11.00 WIB, dengan melibatkan sekitar 300 peserta yang terdiri atas siswa SMA, siswa kelas 9, dan guru. Metode kegiatan menggabungkan presentasi interaktif, penjelasan berbasis kasus, simulasi sederhana identifikasi ancaman, diskusi terbuka, dan evaluasi kualitatif melalui observasi serta umpan balik peserta. Materi meliputi ancaman siber umum, privasi digital, pengenalan tautan phishing, kebiasaan kata sandi kuat, autentikasi dua faktor, perlindungan OTP, dan perilaku bermedia sosial yang bertanggung jawab. Hasil kegiatan menunjukkan indikasi peningkatan kesadaran berdasarkan keterlibatan peserta, pertanyaan yang diajukan, dan kemampuan peserta mengulang kembali praktik dasar keamanan digital.

Keywords: cybersecurity education; digital literacy; phishing; digital privacy; two-factor authentication; community service

Kata kunci: edukasi keamanan siber; literasi digital; phishing; privasi digital; autentikasi dua faktor; pengabdian kepada masyarakat

1. INTRODUCTION

Digital transformation has changed how young people communicate, learn, search for information, and build social interaction. Internet access, mobile applications, social media, online games, and digital learning platforms have become common parts of students' daily routines. These technologies provide educational opportunities, but they also create exposure to digital threats when students do not have adequate cybersecurity awareness. In the Indonesian education context, digital literacy is also an important foundation for responsible technology use because it includes the ability to access, evaluate, protect, and communicate information safely in digital environments [15].

Cybersecurity is not only a technical issue handled by specialists. It is also shaped by user behavior, because many incidents begin with human mistakes such as clicking suspicious links, sharing one-time passwords, reusing weak passwords, or exposing private information on social media. Prior studies on cybersecurity awareness and training show that the human factor remains an important vulnerability and that structured awareness programs can help improve safe digital behavior [1], .

ISSN : 2963-3486

For young users, the risk is critical because digital communication often happens quickly, informally, and emotionally. A fake prize notification, a message that appears to come from a friend, or a login page imitating a real platform can deceive users who are not trained to verify digital signals. Recent studies also indicate that phishing attacks have become more convincing with generative artificial intelligence, which increases the need for user-centered education and continuous awareness development [2], [3], [4].

The school environment is an appropriate place for preventive cybersecurity education because students are still forming their digital habits. Early education can help them understand that account security, digital privacy, online ethics, and critical verification are parts of responsible technology use. For teachers, the same knowledge is useful for guiding students, managing class communication, and reducing risks related to online learning activities [5], [6].

Based on this situation, the community service team from the Master Program in Informatics Engineering, Universitas Pamulang, conducted a cybersecurity education program at SMA Al Wafi Islamic Boarding School. The program focused on three practical objectives: introducing basic cybersecurity concepts, explaining real digital risks faced by teenagers, and training participants to apply simple self-protection strategies in daily digital activities.

2. METHOD

This community service activity used an educational and participatory method. The activity combined socialization, interactive presentation, practical simulation, and open discussion. This method was selected because cybersecurity awareness is more effective when participants are not only given definitions, but are also shown examples of threats that resemble their daily digital experiences [7].

The activity was conducted on Friday, 10 April 2026, from 08.00 to 11.00 WIB at SMA Al Wafi Islamic Boarding School, Jalan Raya Pengasinan, Kecamatan Pengasinan, Sawangan, Depok, West Java 16518. The participants consisted of senior high school students, grade 9 students, and teachers, with approximately 300 participants attending the activity.

The problem-solving framework was built from the condition that young users intensively use digital platforms but may not understand the security consequences of sharing private information, using weak passwords, ignoring suspicious links, or responding to fraudulent messages. The intervention was therefore designed to connect cybersecurity concepts with everyday online behavior.

Problem	Response and expected output
Low cyber-threat awareness	Interactive explanation of phishing, malware, account takeover, online fraud, and cyberbullying so participants can recognize common threats.
Weak digital-privacy understanding	Explanation of personal data, identity misuse, digital footprint, and privacy settings so participants understand why private information must be protected.
Limited self-protection skills	Guidance on strong passwords, 2FA, suspicious-link checking, and OTP protection so participants can mention basic protection steps.
Need for school follow-up	Teacher involvement and open discussion to create a basis for future cybersecurity education in the school environment.

Table I. Problem-solving framework of the PKM activity

Table II summarizes the implementation agenda used during the community service activity.

Time	Main agenda
07.30-08.00	Preparation by the PKM team
08.00-08.30	Opening, supervising lecturer remarks, and school remarks
08.30-08.40	Plaque handover to the school
08.40-09.30	Main material delivery by Universitas Pamulang lecturer
09.30-10.30	Cybersecurity education and self-protection strategies
10.30-10.50	Question-and-answer session and souvenir distribution
10.50-11.00	Closing and group photo

Table II. Schedule of the community service activity

The main materials consisted of: (1) introduction to cybersecurity and common threats; (2) real digital risks such as data leakage, account takeover, identity misuse, cyberbullying, and online fraud; and (3) self-protection strategies including strong passwords, two-factor authentication, suspicious-link recognition, one-time password protection, limited personal data exposure, and responsible social media behavior [8], [9], [10], [11], [12].

 ISSN : 2963-3486

The threat-identification simulation was conducted by showing examples of suspicious messages, fake prize notifications, and phishing-style links. Participants were guided to identify warning signs such as unknown senders, unusual domains, urgent language, shortened or suspicious URLs, and requests for OTP or password information. The purpose of the simulation was to train participants to perform simple verification before clicking links or responding to online messages.

Because no structured questionnaire was administered, the evaluation was conducted qualitatively through observation of participant attention, discussion dynamics, questions raised by participants, and direct feedback from the school community. The evaluation focused on engagement, relevance of questions, ability to restate basic protection steps, and response from teachers and school representatives. This approach was appropriate for the available activity design, but it became a limitation because the impact could not be expressed as a numerical percentage.

3. RESULTS

The program was implemented successfully and received a positive response from both the school and participants. The activity began with preparation and coordination, followed by formal opening, material presentation, practical explanation, interactive discussion, souvenir-based appreciation for active participants, and closing documentation. Figure 1 presents the school location documentation used in the activity preparation stage.

Figure 1. Location documentation of SMA Al Wafi Islamic Boarding School

The implementation followed six major stages: proposal and administrative preparation, logistical preparation, schedule confirmation with the school, activity execution, monitoring and evaluation, and final reporting. During the execution stage, the PKM team delivered materials using examples that were close to participants' daily activities, such as social media login security, suspicious messages, fake prize links, and misuse of personal information. Figure 2 shows the delivery of cybersecurity education material in the school hall.

Figure 2. Delivery of cybersecurity education material during the PKM activity

Participants showed strong attention during the explanation of phishing, password security, and privacy settings. The question-and-answer session indicated that many students were familiar with digital platforms but had not previously connected everyday online habits with cybersecurity risk. Figure 3 shows participant involvement during the classroom-based discussion.

Figure 3. Participant involvement during classroom-based discussion

To make the results more concrete, the discussion outputs were grouped into several observed indicators. These indicators do not represent questionnaire-based percentages, but they summarize qualitative evidence collected during the activity.

Observed evidence	Interpretation
Questions about suspicious links, account recovery, OTP protection, and social media safety	The topic was directly relevant to students' daily digital experience.
Participants could mention not sharing OTP, checking sender identity, using stronger passwords, and enabling 2FA	The activity indicated basic awareness-building.
Teachers supported follow-up digital literacy topics in school guidance	Teacher involvement can strengthen sustainability.
Slides, case examples, threat checklist, and practical self-protection messages were delivered	The activity produced reusable education material.

Table III. Qualitative evidence observed during the activity

 ISSN : 2963-3486

Based on qualitative observation, the activity indicated that participants were able to identify several common cybersecurity threats and mention basic preventive actions, particularly related to phishing links, OTP protection, password security, and social media account safety. The strongest participant interest appeared during examples related to social media account security and suspicious links. This indicates that the selected topic matched the everyday digital behavior of teenagers.

Reward-based participation was used to encourage students to ask questions and respond during the discussion session. This approach created a more active learning atmosphere and helped the team observe whether participants could connect the material with real digital problems. Figure 4 shows documentation of participant appreciation during the activity.

Figure 4. Reward-based participation during the question-and-answer session

Several operational obstacles were identified during the activity. Some female students arrived late because their dormitory location was relatively far from the activity venue. The large number of participants created crowding during snack distribution. In addition, the activity was held on Friday, so the available time was limited by the Friday prayer schedule in the same building. These constraints did not prevent the activity from being completed, but they should be considered in future planning.

4. DISCUSSION

The results show that cybersecurity education is relevant for school communities. The participants' active responses during the discussion confirmed that cyber threats are not abstract issues, but practical risks that can occur in students' daily digital routines. Phishing, URL spoofing, and social engineering are especially important because they exploit user trust rather than only technical system weaknesses and may create legal as well as social consequences when personal data or identity is misused [2], [3], [8], [13].

The use of interactive examples helped participants connect technical concepts with real-life situations. The explanation of phishing was linked to messages, links, login pages, and account recovery problems that students may encounter. This approach is consistent with cybersecurity culture and awareness literature, which emphasizes behavioral and contextual learning rather than purely technical explanation [7].

The absence of a numerical questionnaire means that this activity cannot claim statistical improvement in knowledge. The safer interpretation is that participant engagement, questions, and direct responses indicated increased awareness of basic cybersecurity practices. This limitation should be treated as an important methodological note rather than hidden from the manuscript.

Another important finding is the strategic role of teachers. Students may learn digital safety in one event, but sustainable behavior requires reinforcement in daily school routines. Teachers can help integrate basic cybersecurity habits into classroom guidance, digital assignments, and school communication practices. This is aligned with child online protection guidance that encourages schools and educators to support safe and empowering online environments for young users [5], [6].

For sustainability, the activity should not stop as a one-time socialization. The school can develop a simple cybersecurity habit checklist for students, such as using unique passwords, enabling two-factor authentication when available, avoiding public sharing of personal information, checking sender and domain identity, and reporting suspicious messages to teachers or trusted adults [9], [10], [11], [12]. The university team can also prepare follow-up modules, including phishing simulation, password manager introduction, privacy-setting workshop, and incident reporting procedures.

5. CONCLUSION

Based on the implementation of the community service activity, it can be concluded that the program was successfully conducted at SMA Al Wafi Islamic Boarding School on 10 April 2026 with approximately 300 participants consisting of senior high school students, grade 9 students, and teachers. The activity introduced various common cyber threats such as phishing, malware, online fraud, account takeover, data leakage, cyberbullying, identity misuse, and social engineering. The results showed an increase in cybersecurity awareness, reflected through active participant engagement, relevant discussions, and the ability of participants to identify basic preventive measures including the use of strong passwords, two-factor authentication, suspicious-link recognition, OTP protection, and privacy management. However, the activity still had limitations due to the absence of structured pre-test

and post-test instruments, so the evaluation results were presented qualitatively rather than statistically. Therefore, future programs are recommended to include quantitative evaluation methods, smaller discussion groups, hands-on phishing simulations, privacy-setting workshops, and follow-up modules related to network security, digital ethics, and the safe use of artificial intelligence in education.

ACKNOWLEDGEMENT

The authors express their gratitude to Universitas Pamulang, the Postgraduate Program, and the Master Program in Informatics Engineering for supporting this community service activity. The authors also thank SMA Al Wafi Islamic Boarding School, the teachers, staff, and all student participants for their cooperation and active participation. Appreciation is also extended to the supervising lecturers and all parties who contributed to the preparation, implementation, and documentation of the activity.

DOCUMENTATION OF ACTIVITY

The main documentation of the activity has been embedded in the Results section as Figures 1-4 so that every image is connected directly to the corresponding activity narrative. The documentation shows the location, material delivery, participant involvement, and reward-based participation during the question-and-answer session.

REFERENCES

[1] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks," *Educ. Inf. Technol. (Dordr).*, vol. 27, no. 4, pp. 4729–4752, 2022, doi: 10.1007/s10639-021-10806-7.

[2] C. Natasya, I. Irvin, and A. A. S. Gunawan, "A systematic literature review: Cyber attack: Phishing environments, techniques, and detection mechanism," *International Journal of Computer Science and Humanitarian AI*, vol. 1, no. 1, pp. 9–13, 2024, doi: 10.21512/ijcshai.v1i1.12155.

[3] R. Jabir, J. Le, and C. Nguyen, "Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors," *AI*, vol. 6, no. 8, p. 174, 2025, doi: 10.3390/ai6080174.

[4] S. Sajid, A. W. Fazil, and M. Hakimi, "AI-based phishing attacks on university networks: A systematic literature review and defense framework," *Journal of Advanced Computer Knowledge and Algorithms*, vol. 3, no. 2, pp. 62–75, 2026, doi: 10.29103/jacka.v3i2.26650.

[5] I. T. Union, *Guidelines for Parents and Educators on Child Online Protection*. Geneva, Switzerland: International Telecommunication Union, 2020.

[6] E. U. A. for Cybersecurity, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," ENISA, Heraklion, Greece, 2018.

[7] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2024. doi: 10.6028/NIST.CSWP.29.

[8] F. T. Commission, "How to recognize and avoid phishing scams," 2024. [Online]. Available: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[9] C. and I. S. Agency, "Recognize and report phishing," 2024. [Online]. Available: https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

[10] C. and I. S. Agency, "More than a password," 2024. [Online]. Available: https://www.cisa.gov/MFA

[11] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020. doi: 10.6028/NIST.SP.800-63b.

[12] B. Ulum, Taryo, and D. Sudarno, "Klasifikasi phishing URL pada website berbasis metode ensemble," *Jurnal Teknologi Informasi dan Komputer*, vol. 3, no. 1, 2025.

[13] M. Purwadi, M. Makhfud, and A. Jamaludin, "Legal accountability and policy gaps in social engineering-based phishing cybercrimes," *Research Horizon*, vol. 5, no. 3, pp. 797–806, 2025, doi: 10.54518/rh.5.3.2025.580.