



BUILDING STUDENTS' DIGITAL SECURITY AWARENESS THROUGH PRACTICAL EDUCATION AND TRAINING AT SMA SEMINARI MERTOYUDAN MAGELANG

Melda Rumia Rosmery Simorangkir^{1*}, Bernadetha Nadeak², Edison Siregar³, Risma Uly Manalu⁴, A Dan Kia⁵, Melya Dyanasari Sebayang⁶, Lolom Evalita Hutabarat⁷, Pius Pari⁸, Bania Bastanta Tarigan⁹

Universitas Kristen Indonesia, Jakarta, Indonesia

*meldasimorangkir82@gmail.com

E-ISSN : 3109-9777

Received: Oktober 2026

Accepted: Oktober 2026

Published: Oktober 2026

Abstract :

The increasing engagement of adolescents in digital environments presents various risks, including cyberbullying, the dissemination of unverified information, personal data theft, account hijacking, and the unauthorized use of photos and videos. These conditions highlight the importance of strengthening digital security beyond technical skills to include awareness, decision-making, and responsible technology use. This Community Service Program aimed to provide education and practical training to strengthen students' digital security awareness at SMA Seminari Mertoyudan Magelang. The program involved 207 students and was implemented through instructional sessions, interactive discussions, case studies, simulations, practical exercises, and a post-test followed by program evaluation. The training covered digital threats, account security, personal data protection, cyberbullying, the role of the school environment, and digital pressure and adolescent mental health. The results indicated strengthened students' understanding of digital security risks and basic account protection measures. Students' active participation in discussions, case studies, and simulations also demonstrated that a practical approach helped them relate digital security concepts to their everyday technology use. In the context of SMA Seminari Mertoyudan, digital security also has an ethical dimension that aligns with the values of honesty, discipline, responsibility, and respect for others embedded in the formation process. Thus, digital security education and practical training that integrate knowledge, skills, and ethical responsibility represent a relevant approach to fostering safe, wise, and responsible digital behavior among students.

Keywords: digital security; cyberbullying; digital literacy; students.

INTRODUCTION

The development of digital technology has become an inseparable part of adolescents' lives. The use of social media, instant messaging applications, information-sharing platforms, and various digital services provides students with greater convenience in communicating, accessing information, learning, and building social networks. However, the intensity of interaction in digital spaces also presents various risks that need to be anticipated. Adolescents are not only required to be able to use technology but also need to develop the awareness and skills necessary to protect themselves, safeguard their privacy, and behave responsibly in digital environments (Arisanty et al., 2025). One of the growing concerns associated with increasing digital activity is cyberbullying. Online bullying refers to aggressive behavior repeatedly carried out through digital



media in verbal, psychological, or social forms that may demean, humiliate, or harm others (Tanjung, Suciptaningsih, & Asikin, 2024). Such practices may occur through social media, messaging applications, email, and various other digital platforms. They are not limited to insulting comments or messages but may also involve the dissemination of harmful information, social exclusion in digital spaces, and the distribution of a person's photos or videos without consent (Arifin, 2025).

Digital security risks among adolescents are also associated with their ability to protect personal information and manage content shared online. The use of weak passwords, openly sharing personal information, accessing unfamiliar links, and disseminating information without verification may increase students' vulnerability to various forms of technology misuse (DS & Isroqunnajah, 2026). Similarly, sharing photos and videos without permission is not merely a matter of digital ethics but also concerns individual privacy and security. In this context, digital security needs to be understood as the ability to recognize risks, make informed decisions, protect personal data and identity, and use technology safely and responsibly. These concerns are increasingly important because the negative consequences of digital interactions can extend to adolescents' psychological and social well-being. Cyberbullying, for example, may be associated with anxiety, stress, reduced self-confidence, and other psychosocial problems. The characteristics of digital spaces allow content to spread rapidly and reach a broad audience. In addition, anonymous accounts may make it difficult to identify perpetrators and may prolong victims' exposure to harmful content. These conditions indicate that the use of digital technology without adequate knowledge and security skills may place adolescents in vulnerable situations.

An indication of such vulnerability can be seen in a 2020 UNICEF survey involving 2,777 Indonesian adolescents aged 14–24 years. Approximately 45% of respondents reported having experienced cyberbullying. The reported forms included harassment through chatting applications (45%) and the distribution of photos or videos without permission (41%) (Riswanto & Marsinun, 2020; Rachmayanti & Candrasari, 2022). These findings indicate that risks in digital spaces are not limited to negative verbal communication but also involve the misuse and dissemination of personal content. Meanwhile, data from Statistics Indonesia (Badan Pusat Statistik) in 2021 indicated that experiences of bullying occurred among students at various levels of education, with male students reported to have experienced bullying more frequently. These findings demonstrate the need to address safety and security issues in digital spaces within educational settings. Schools have a strategic position in developing students' digital security awareness because their role extends beyond academic knowledge to include character development, responsibility, and life skills (Hidayat, Sari, & Noviani, 2025). Digital security education should therefore be delivered through approaches that are closely connected to students' experiences so that learning does not remain at the conceptual level. Students need opportunities to identify risky situations, understand the consequences of digital

behavior, and practice simple measures to protect their accounts, personal data, digital identities, and interactions in cyberspace (Noor & Khasanah, 2025; Palupi et al., 2026).

An educational approach combined with practical training is relevant because digital security is a competency that requires application in real-life situations. Through education and hands-on practice, students can learn to identify the characteristics of suspicious messages or links, understand the importance of strong passwords, maintain the confidentiality of personal information, manage account privacy settings, verify information, and understand the consequences of sharing other people's photos or videos without permission (Sulianta, 2026). Such learning is expected to encourage a shift from merely knowing about digital risks toward developing awareness and habits that support safer digital behavior. Based on these conditions, this Community Service Program was conducted at SMA Seminari Mertoyudan Magelang as a form of higher education's contribution to strengthening students' capacity to face challenges in the digital environment. The program was designed through education and practical training addressing digital security situations relevant to students' everyday lives. The materials focused on recognizing risks in cyberspace, protecting accounts and personal data, maintaining security in digital communication, being alert to suspicious information and links, and practicing ethical behavior when sharing digital content.

Through this program, students were expected not only to understand various forms of digital security risks but also to apply self-protection measures in their everyday digital activities. Accordingly, this Community Service Program aimed to build students' digital security awareness through education and practical training, thereby promoting safer, more responsible, and ethical use of technology both within the school environment and in everyday life.

RESEARCH METHOD

The Community Service Program was conducted at SMA Seminari Mertoyudan Magelang in the form of digital security education and training aimed at all students. The activity began with coordination between the PKM team and the school, particularly the principal, vice principal for student affairs, and guidance and counseling (BK) teacher. The coordination was conducted to establish a shared understanding of the objectives, materials, schedule, venue, and technical aspects of the program. The school was responsible for coordinating the participation of all students, providing the venue and supporting facilities, and accompanying students throughout the activity. The training materials and supporting instruments were prepared based on students' needs, taking into consideration various risks commonly encountered in everyday digital activities.

The program was implemented through interactive training and hands-on practice integrating instructional sessions, discussions, question-and-answer sessions, case examples, and simulations. The training materials covered digital security risks, account and password protection, data and personal information

security, awareness of suspicious messages and links, information sharing, cyberbullying, and ethics in sharing photos and videos. Students were presented with situations closely related to their everyday digital activities and guided to identify potential risks and determine appropriate responses. A practical approach was adopted to ensure that students not only understood the concepts of digital security but also developed skills that could be applied in their use of technology and digital media.

Throughout the program, students received support and guidance from the principal, vice principal for student affairs, and BK teacher. The involvement of school personnel was intended to strengthen the sustainability of the training outcomes within the school environment. The BK teacher played a specific role in supporting student guidance by connecting digital security with behavior, social interaction, responsibility, and self-protection. Meanwhile, the vice principal for student affairs supported participant coordination and activity management, while the principal provided institutional support for the program. Collaboration between the PKM team and the school was expected to foster an environment that supports the implementation of safe and responsible behavior in digital spaces.

Evaluation was conducted to assess the implementation of the program, students' responses, and participants' understanding of the training materials. The evaluation involved observation of student engagement, question-and-answer sessions, discussions, case-based exercises, and a post-training evaluation instrument. The assessed aspects included students' ability to recognize digital security risks, understand the importance of protecting personal data and accounts, and determine appropriate actions when encountering risky situations in digital spaces. The evaluation results served as a basis for assessing the achievement of the program objectives and providing input for the school to strengthen and sustain digital security education and student support.

RESULTS AND DISCUSSION

Results of the Community Service Program

The Community Service Program (PKM) conducted by Universitas Kristen Indonesia was held on **September 18, 2026, at SMA Seminari Mertoyudan Magelang**, under the theme *"Digital Account Security Education and Training as an Effort to Prevent Cybercrime among Students of SMA Seminari Mertoyudan Magelang."* The program was attended by all students and supported by the principal, vice principal for student affairs, and guidance and counseling (BK) teacher. The activity was implemented in a structured sequence, beginning with the opening and welcoming remarks, followed by three main instructional sessions, interactive simulations and discussions, and a *post-test* and program evaluation. The program received a positive response from participants, as reflected in their active engagement in discussions, questions, responses to case studies, and participation in simulations. The approach extended beyond the delivery of instructional materials by connecting digital security issues with students' experiences in using technology and interacting in digital spaces.



Figure 1. Universitas Kristen Indonesia Community Service Program at SMA Seminari Mertoyudan Magelang

The first session, *"Recognizing Digital Threats: From Hacking to Cyberbullying,"* provided students with an understanding of various threats that may arise in digital activities. Through instructional materials, case examples, and discussions, students were introduced to risks such as *phishing*, personal data theft, account hijacking, the dissemination of unverified information, *cyberbullying*, and the misuse of photos and videos without consent. Case-based discussions helped students recognize that digital threats do not always involve sophisticated technical attacks but may begin with simple actions, such as opening suspicious links, providing personal information to unknown parties, using easily guessed passwords, or sharing content without considering the rights and privacy of others. Thus, students began to understand that digital security is an integral part of everyday behavior when using technology.

The second session, *"The Role of Teachers in Improving Students' Digital Security,"* broadened the discussion by positioning the school as an important environment for fostering safe digital behavior. The session emphasized that protecting students in digital spaces is not solely an individual responsibility but also requires support from the educational environment. In this context, the involvement of the principal, vice principal for student affairs, and BK teacher was important in providing guidance, establishing communication with students, and responding to issues related to technology use. Students were encouraged to understand that when facing threats, pressure, or problems in digital spaces, they can seek assistance and communicate their concerns to trusted school personnel. This approach reinforced the understanding that digital security is a shared responsibility involving students, teachers, schools, and the broader social environment.

The third session, *"Digital Pressure and Mental Health: How Adolescents Can Navigate the Online World,"* directed students' attention to the psychological and social impacts of digital engagement. The session addressed pressures that may arise from online interactions, negative comments, *cyberbullying*, the dissemination of content without consent, and the perceived need to remain continuously engaged in social media activities. Students were guided to recognize situations that may generate digital-related pressure and to understand the importance of setting boundaries in technology use, maintaining healthy communication, and seeking support when experiencing harmful digital interactions. This discussion was particularly relevant to the students' lives within the Seminari Mertoyudan environment, which emphasizes communal

living, discipline, responsibility, and character formation.

During the simulation and question-and-answer session, students were given opportunities to respond to various situations related to digital security. The activity indicated that students were able to connect the training materials with their everyday experiences of technology use. Key issues discussed included identifying suspicious messages or links, protecting personal data, securing digital accounts, sharing information, and determining appropriate responses to harmful digital behavior. The interactions during the activity indicated that case-based and simulation methods provided a practical means of developing students' understanding, as participants were able to discuss concrete issues that were closely connected to their daily lives.

In terms of **knowledge and skills**, the program strengthened students' understanding of basic measures for maintaining account and personal data security. Participants were introduced to the importance of using strong and different passwords for different accounts, exercising caution when encountering suspicious links and messages, and managing privacy settings on digital accounts. In terms of **attitudes and awareness**, the program emphasized honesty, responsibility, respect for privacy, and caution in using technology. Students were encouraged not to disseminate unverified information, use or share other people's data without permission, or upload and forward content without considering its potential consequences.

The distinctive characteristics of SMA Seminari Mertoyudan as an educational and *formatio* environment for prospective priests provided a specific context for the implementation of the program. Values such as honesty, discipline, responsibility, communal life, and respect for others provide a relevant foundation for developing safe and ethical digital behavior. In this context, digital security is understood not merely as a technical ability to protect accounts but also as part of the moral responsibility involved in using technology. The ability to maintain the confidentiality of personal data, respect the privacy of others, verify the accuracy of information, and avoid actions that may harm others represents an application of these values in digital life.



Figure 2. Handover of the Universitas Kristen Indonesia Certificate and Plaque

The program concluded with a *post-test* and evaluation to obtain an overview of participants' understanding after the training and their responses to the implementation of the program. The evaluation was also used to identify the materials considered most relevant and the learning experiences perceived by participants during the activity. Overall, the PKM strengthened

students' **knowledge, basic digital security skills, and ethical awareness** in using technology safely and responsibly. The program also demonstrated the importance of collaboration between higher education institutions and schools in developing educational environments that are responsive to the development and risks of digital spaces. For students at SMA Seminari Mertoyudan Magelang, strengthening digital security represents an important component of developing individuals who are not only capable of using technology but are also able to protect themselves, respect others, and take responsibility for their activities in digital spaces.

Discussion of the Community Service Program Implementation

The implementation of the Community Service Program (PKM) at SMA Seminari Mertoyudan Magelang demonstrates that digital security should be understood as a competency encompassing **knowledge, skills, and ethical responsibility**, rather than merely as a technical ability to secure digital accounts. Students are generally familiar with technology and various digital platforms; however, such familiarity does not automatically translate into the ability to recognize risks and make safe decisions. Therefore, digital security education is important for bridging the gap between the ability to use technology and the ability to protect oneself and others while using it. This perspective is particularly relevant in the SMA Seminari Mertoyudan environment, where the *formatio* process and communal life constitute important components of students' personal development.



Figure 3. Universitas Kristen Indonesia PKM Training Session

1. Building Awareness of Digital Risks

The implementation of the program demonstrated that experience with technology needs to be accompanied by a more critical understanding of risks in digital spaces. Through discussions and case studies, students were able to identify various forms of digital threats, ranging from *phishing*, identity theft, account hijacking, misuse of personal data, and the dissemination of unverified information to *cyberbullying* and the use of photos or videos without consent. This understanding is important because some digital risks arise not from technological limitations but from users' insufficiently cautious decisions. The use of cases closely related to students' everyday experiences played an important role in developing such awareness. Students were not merely introduced to the concepts of "safe" and "unsafe" behavior but were encouraged

to consider the consequences of their digital actions. Thus, digital security shifted from a purely technical understanding toward conscious decision-making: whether information should be shared, whether a link can be trusted, whether personal data needs to be provided, and whether an action respects the rights and privacy of others. This shift in perspective represents an important component of developing responsible digital behavior.

2. From Knowledge to Account Protection Skills

The training also demonstrated the importance of a practical approach to digital security education. Knowledge of cyber threats has limited value if students do not know what concrete actions to take when facing potential risks. Therefore, the program provided hands-on experiences involving the use of strong passwords, account privacy settings, and the identification of suspicious messages and links. The practical approach enabled students to connect the training materials with their everyday digital activities. Students not only gained information about **what** actions should be taken but also learned **when** protective measures are necessary and **why** they are important. This strengthened the understanding that account security is an ongoing process requiring consistent habits rather than an action taken only after a security problem occurs. Accordingly, digital security education needs to focus on developing protective habits that students can apply independently in their daily digital activities.

3. Digital Security as Part of Ethics and *Formatio*

An important aspect emerging from the program is that digital security has a strong ethical dimension. In the life of the Seminari Mertoyudan community, values such as honesty, discipline, responsibility, respect for others, and communal life are integral to the *formatio* process. These values should not be limited to face-to-face interactions but should also be applied when students engage in digital spaces. From this perspective, digital security can be positioned as part of character development rather than merely as a technological skill. Its application can be observed through simple yet meaningful actions. Protecting passwords and accounts represents responsibility for one's own security. Maintaining the confidentiality of other people's personal data demonstrates respect for privacy. Verifying information before sharing it reflects caution and responsibility. Likewise, refraining from *cyberbullying*, avoiding the distribution of photos or videos without consent, and not using other people's personal information carelessly demonstrate respect for human dignity. Thus, ethical values developed in everyday life need to be continuously reflected in digital behavior.

4. The Role of the School in Sustaining Digital Security

The implementation of the program also demonstrated that strengthening digital security cannot be placed entirely on students. The involvement of the principal, vice principal for student affairs, and BK teacher highlights the importance of school-level support in fostering safe digital behavior. In particular, the BK teacher has a strategic role in integrating digital security issues into student support and guidance, including when students experience digital

pressure, conflict, *cyberbullying*, data misuse, or other problems arising from digital interactions.

The sustainability of the program cannot rely solely on a one-time training activity. Further strengthening can be developed through continuous practice, integration of digital security topics into school activities, guidance and counseling support, and the provision of consultation opportunities for students experiencing problems in digital spaces. A sustainable approach can help transform the knowledge acquired during training into more consistent habits and behaviors.

CONCLUSION

Overall, the implementation of the PKM demonstrates that digital security education becomes more meaningful when it integrates **knowledge of digital risks, account protection skills, decision-making abilities, and ethical responsibility**. The combination of education, discussion, case studies, simulations, and practical activities provided students with opportunities to connect digital security issues with real-life experiences. In the context of SMA Seminari Mertoyudan, this strengthening has broader significance because digital security can be positioned as part of students' personal *formatio*: developing individuals who are not only capable of using technology but also able to use it **safely, wisely, responsibly, and with discipline and respect for the dignity of others**. The sustainability of the program, as indicated by the evaluation, can subsequently focus on strengthening digital security literacy, personal data protection, digital media ethics, the ability to recognize cyber threats, and mechanisms for supporting students when they encounter challenges in digital spaces.

REFERENCES

- Arifin, N. (2025). Pendidikan karakter di era digital. Penerbit Tahta Media.
- Arisanty, M., Riady, Y., Kharis, S. A. A., Permatasari, S. M., & Sukatmi, S. (2025). Cerdas dan aman bermedia digital: Peningkatan kesadaran keamanan siber di era hoaks dan phishing.
- DS, E. J., & Isroqunnajah, I. (2026). Hukum Mengambil Foto Orang di Era AI: Fikih Kontemporer, Privasi, dan Etika Digital. *An-Nahdloh: Journal of Education and Islamic Studies*, 1(3), 890-900.
- Hidayat, T., Sari, I., & Noviani, D. (2025). Pengaruh literasi digital terhadap kemampuan berpikir kritis peserta didik di era Society 5.0. *Jurnal Multidisiplin West Science*, 4(08), 1404-1415.
- Noor, I. F. D., & Khasanah, N. (2025). Peran Sekolah dalam Pembentukan Kepribadian Anak di Tengah Krisis Nilai Moral di Era Digital. *Insan Cendekia: Jurnal Studi Islam, Sosial Dan Pendidikan*, 4(2), 32-42.
- Palupi, T. N., Ninasari, A., Saksana, J. C., Sholeh, M., & Fajriyah, E. (2026). Membangun Etika Digital Siswa MI/SD: Sinergi Pendidikan Karakter dan

- Literasi Teknologi Pada Pendidikan Dasar. *Jurnal Pendidikan Dasar Islam*, 4(3), 467-477.
- Rachmayanti, A., & Candrasari, Y. (2022). Perilaku cyberbullying di instagram: Perilaku cyberbullying di instagram. *Linimasa: Jurnal Ilmu Komunikasi*, 5(1), 1-12.
- Riswanto, D., & Marsinun, R. (2020). Perilaku cyberbullying remaja di media sosial. *Analitika: Jurnal Magister Psikologi UMA*, 12(2), 98-111.
- Sulianta, F. (2026). DOXING: Ancaman di Balik Jejak Digital. Feri Sulianta.
- Tanjung, A. Q., Suciptaningsih, O. A., & Asikin, N. (2024). Urgensi etika dalam literasi digital di era globalisasi. *WASIS: Jurnal Ilmiah Pendidikan*, 5(1), 34-41.