Jurnal Pengabdian Masyarakat: Bisnis dan Iptek
Vol. 1 No. 2, October 2025, 73-85
ISSN Online: 3064 - 0415, https://doi.org/10.56447/jpmbistek
Published by LPMM, STMIK Mardira Indonesia, Bandung.

Preventing Cyber Threats Early: Cyber Crime Education for Students of SMKN 1 Katapang

Aisah Nur Endah Sari[1], Solehhudin[2] , Irwan Ardhiyanto[3], Vicky Muhammad A[4], Nabila Sri Gustina[5], Afifah[6], Muhamad Zaki[7], Ilham Hidayat[8], Andika Fazri F[9], Ari Ardiansyah[10], Regi Muhammad S[11]
[1,2,3,4,5,6,7,8,9,10,11] *STMIK Mardira Indonesia, Bandung*
Email: *aisahnurendah09@gmail.com[1], solehhhudinn@gmail.com[2], irwan.adhiyanto@gmail.com[3], vickymuhamad001@gmail.com[4], nabilasrigustina8047@gmail.com[5], afifahopi77@gmail.com[6], mhmdzaki213@gmail.com[7], ilhamm.hdyat@gmail.com[8], fazriandika82@gmail.com[9], arisyah085@gmail.com[10], regimuhammad753@gmail.com[11]*

Abstract

The community service team, comprising faculty and students, implemented initiatives to raise awareness about the rapid advancement of digital technology, which facilitates access to information, communication, and everyday tasks. Nevertheless, in conjunction with these conveniences, numerous cybercrime concerns have emerged, including phishing, hacking, cyberbullying, and the theft of personal data. The deficiency in awareness and understanding of these concerns, especially among students, underpins our community service activity. The events consisted of interactive outreach directed at 11th-grade students in the RPL program at SMKN 1 Katapang—the employed procedures comprised pre-tests, material presentations, phishing web simulations, conversations, and post-tests. The subjects addressed encompassed categories of cybercrime, its adverse effects, and preventive strategies employing security technology such as firewalls, two-factor authentication (2FA), and SSL. The findings indicated significant enthusiasm among participants and an enhanced comprehension of digital hazards and the significance of personal data protection. This effort demonstrates that early education on cybercrime is essential for cultivating a prudent and secure generation in the responsible use of digital technology.

Keywords: *Cyber Crime, Digital Literacy, Cyber Education, Phishing, Data Security*

Introduction

The advancement of information and communication technology (ICT) has transformed practically every facet of human existence, encompassing education, commerce, social connections, and entertainment. In recent decades, the advent of the internet, digital gadgets, and online applications has facilitated rapid and efficient access to information, communication, and numerous activities. This arrangement has substantially enhanced the quality of life for society. Nonetheless, the pervasive adoption of technology has given rise to other obstacles and concerns, including a surge in cybercrime.

Cybercrime denotes illicit activities conducted through digital technology and the internet, including hacking, identity theft, online fraud (phishing), dissemination of illegal content, digital harassment (cyberbullying), and social media account hijacking. These offenses persistently adapt as society increasingly relies on digital technology. Paradoxically, the awareness and comprehension of cybercrime threats remain comparatively inadequate, particularly among youth such as students who are frequent users of the internet and social media.

Students are a susceptible demographic for digital dangers, since they frequently engage on multiple online platforms without sufficient understanding of digital security. A multitude of pupils indiscriminately disclose personal information, employ inadequate passwords, or readily succumb to fraudulent websites and dubious links. This circumstance elicits significant worries, as the ramifications of cybercrime extend beyond money losses to include psychological and societal repercussions, such as trauma, mental distress, and reputational harm.

In response to this context, a group of students from the Informatics Engineering Program at STMIK Mardira Indonesia conducted a community service initiative entitled "Cyber Crime and Threats in the Digital Era." The event occurred at SMKN 1 Katapang in Bandung Regency, targeting 11th-grade students enrolled in the Software Engineering (RPL) program. The venue was selected due to its pertinence to the students' technological field of study and their requirement for a comprehensive understanding of digital security and ethical considerations in information technology usage.

This initiative is structured as an educational and interactive outreach program comprising several essential elements: a pre-test to evaluate students' prior knowledge of cybercrime, a presentation of materials utilizing visual aids and group discussions, a live simulation of phishing techniques to impart a practical understanding of digital criminal activities, and a post-test to serve as a conclusive assessment of students' grasp of the presented material. The subjects addressed encompass categories of cybercrime, their causes and effects, preventive strategies, and an overview of digital security systems, including firewalls, two-factor authentication (2FA), Secure Socket Layer (SSL), and the legal framework established by the Information and Electronic Transactions Law (UU ITE).

Prior community service initiatives have demonstrated that simulation-based teaching and real case studies are more efficacious in enhancing students' knowledge of the perils of the digital realm than traditional lecture techniques (Derian Shakti, 2022; Warjiono et al., 2022). Engaging participants in conversations and simulations renders the learning process more interactive and significant. This activity utilizes interactive ways to foster a robust understanding, encompassing both theoretical insights and practical experience.

This activity seeks to develop responsible digital citizens who understand their rights and obligations in the online realm, rather than simply disseminating information. It is anticipated that students would not only safeguard themselves but also serve as advocates for digital literacy within their schools and communities. Continuous education can mitigate the hazards of cybercrime and foster a robust digital culture from an early age.

This effort signifies a concrete commitment by students to society in tackling the issues of a progressively digitalized era. By employing a preventive and educative strategy, adolescents are prepared to navigate the complexities of the digital realm with intelligence, critical thinking, and safety. This aligns with cultivating exceptional human resources that are adaptable to technological progress and aware of associated risks.

Method

The community service team from STMIK Mardira Indonesia utilized a descriptive qualitative methodology in this initiative, incorporating a case study alongside an education-oriented participatory approach. The primary objective is to deliver digital literacy education and comprehension of cybercrime to students at SMKN 1 Katapang via interactive outreach initiatives. This program is both educational and exploratory, integrating simulations, conversations, and participant comments to examine their comprehension and experiences concerning the digital realm and its security.

The community service design employed is an educational case study utilizing a participatory learning methodology. This technique facilitates active participant involvement in comprehending the topic and offering feedback via practical exercises and conversations. The case study centers on a single vocational education institution, SMKN 1 Katapang, which serves as the site for implementing the activities.

The population for this study comprises all 11th-grade students enrolled in the Software Engineering (RPL) program at SMKN 1 Katapang. The sample was obtained using complete sampling, encompassing all students from two courses, XI RPL 1 and XI RPL 2, totaling roughly 60 participants. The selected students possess vocational backgrounds intimately aligned with the digital realm, rendering the information on cybercrime pertinent and significantly influential to their everyday endeavors.

Data collection methods encompassed direct observation of activities, the administration of pre-tests and post-tests, and the facilitation of discussion and Q&A sessions, all documented as field notes. Furthermore, visual documentation was employed as a component of triangulation to enhance data validity. The pre-tests and post-tests included inquiries regarding categories of cybercrime, their effects, and preventive strategies. The tools employed were created by the implementation team, grounded in measures of digital literacy and cybersecurity.

Data analysis using descriptive qualitative approaches to compare pre-test and post-test findings, evaluating the enhancement of participants' understanding. Additionally, observational notes recorded during the activities were utilized to assess the efficacy of the delivery modalities, participant engagement, and the success of simulations in enhancing students' practical comprehension. The outcomes of the student talks were thematically evaluated to assess their perceptions and awareness of cybercrime issues following participation in the activities.

This endeavor did not employ physical laboratory apparatus or sophisticated technology devices. For educational support, laptops and a projector were utilized to present materials, accompanied by a phishing simulation website created for demonstration purposes. A documentation camera was utilized to capture participants' activities during the event.

The community service engagement included a team of faculty and students serving as facilitators, resource individuals, and observers on-site. This presence was essential for facilitating reciprocal conversation with participants and assuring their active engagement in the educational process. The informants for this exercise comprised students, accompanying teachers, and the head of the vocational program, who offered supplementary insights into the digital literacy circumstances of the students at the school.

The community service occurred in the auditorium of SMKN 1 Katapang, situated in the Katapang District of Bandung Regency, West Java. The primary action happened on June 18, 2025, from 07:00 to 11:00 WIB, with planning, material preparation, and review activities taking place roughly two weeks earlier. The results were validated using data triangulation involving pre-test/post-test evaluations, participatory observations, and student discussion answers, which were meticulously evaluated to confirm the accuracy and validity of the conclusions.

This method was developed to produce empirical data that is both instructive and influential in enhancing participants' awareness of digital risks, while also demonstrating the efficacy of educational strategies within the realm of community service aimed at technological literacy.

Results and Discussion

On June 18, 2025, a community service initiative at SMKN 1 Katapang, executed by a cohort of students and instructors from STMIK Mardira Indonesia, effectively augmented pupils' comprehension of the perils and ramifications of cybercrime. This instruction was provided to around 60 participants in the 11th-grade Software Engineering (RPL) program. The campaign sought to enhance digital literacy and promote awareness of the significance of protecting personal data and utilizing the internet judiciously.

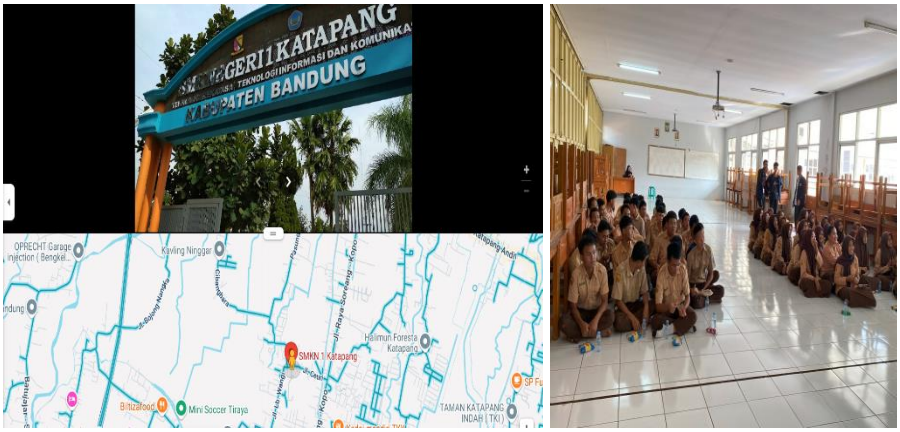


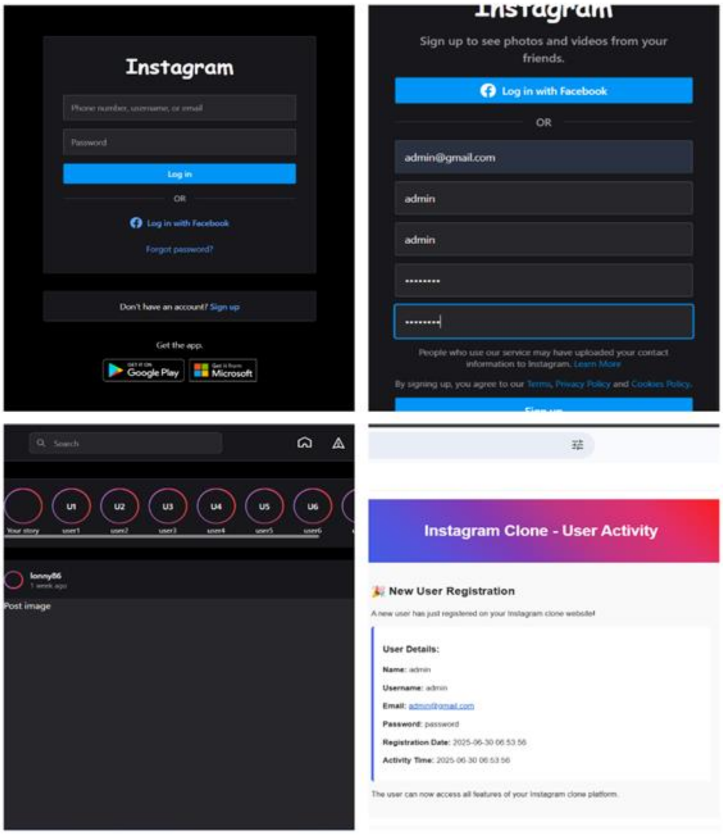
Figure 1. Location of Community Service Activities

Prior to the commencement of the activity, a pre-test was conducted to evaluate the students' preliminary comprehension of the subject of cybercrime. The pre-test findings revealed that the majority of participants lacked a thorough comprehension of many forms of cybercrime, including phishing, carding, cracking, and cyberbullying. Their comprehension was confined to broad concepts such as "hacker" or "account breach," lacking insight into the framework, methodologies, or legal ramifications of these activities.

Figure 2. RPL Students Conducting Pre-test

The information was systematically delivered, commencing with an introduction to cybercrime, its contributing reasons, various forms of digital offenses, prevention techniques, and the legal framework regulating it in Indonesia under the ITE Law. The presentation sessions were engaging and featured actual case studies, including the BPJS data breach and the compromise of the DPR RI account. This method facilitated students' connection of the curriculum to contemporary circumstances pertinent to their lives as a digital generation.

A crucial element of this activity was the phishing web simulation session. Students were shown how a counterfeit webpage can replicate the appearance of an authentic site to deceive people into disclosing important information. This simulation heightened pupils' awareness of dubious relationships and illustrated how crimes can transpire unbeknownst to them. Student feedback was overwhelmingly favorable, with numerous individuals articulating curiosity and recounting personal experiences about prior hacking incidents or dubious links they had encountered.



Sign up to see photos and videos from your friends.

admin@gmail.com

admin

admin

••••••••

••••••••

People who use our service may have uploaded your contact information to Instagram. Learn More

By signing up, you agree to our Terms, Privacy Policy and Cookies Policy.

🎉 New User Registration

A new user has just registered on your Instagram clone website!

User Details:

Name: admin

Username: admin

Email: admin@gmail.com

Password: password

Registration Date: 2025-06-30 06:53:56

Activity Time: 2025-06-30 06:53:56

The user can now access all features of your Instagram clone platform.

Figure 3. Phishing Web that has been created for Implementation

After the presentation and simulation, a post-test was administered, revealing substantial enhancement in student comprehension. The majority of participants successfully articulated the categories of cybercrime and offered concrete instances from the real world. They recognized the significance of preventive strategies, including the use of two-factor authentication (2FA), managing robust passwords, and exercising prudence in sharing information online.

Figure 4. RPL Students Conducting Post-test

These findings suggest that a pedagogical method centered on dialogue and simulation surpasses traditional lectures in efficacy. This approach facilitates students' comprehension of concepts in both theoretical and practical dimensions, corroborating the conclusions of the community service initiatives by Derian Shakti (2022) and Warjiono et al. (2022), which assert that context-based learning significantly enhances digital security awareness.

The conversations indicated that students lack comprehensive digital literacy while being engaged users of technology. This practice not only imparted new knowledge but also motivated them to become advocates of digital literacy in their environments. Comprehending cybercrime can enhance the principles of digital ethics and accountability in technological utilization.

This activity illustrates that educational interventions conducted via interactive outreach effectively meet students' needs in comprehending cybercrime. These findings can provide a foundation for the development of digital literacy courses at the secondary education level and the continuous implementation of analogous activities.

PKM
PENGABDIAN KEPADA MASYARAKAT
STMIK MARDIRA INDONESIA
PROGRAM STUDI TEKNIK INFORMATIKA

Figure 5. Documentation Session

Conclusion

The community service initiative centered on Cyber Crime and Threats in the Digital Era has effectively accomplished its primary goal: to augment the comprehension and awareness of students at SMKN 1 Katapang about many manifestations of cybercrime and the significance of digital security. Utilizing an interactive instructional methodology that encompassed material dissemination, participation dialogues, and phishing web simulations, students acquired both theoretical insights and practical experiences that enhanced their digital alertness in everyday life.

The primary findings reveal that students' digital literacy, despite their active engagement with the internet, is alarmingly inadequate. A significant number of individuals lack an adequate understanding of cyber threats and the necessary preventive measures. This activity revealed that contextual, practical outreach through direct simulations is significantly more effective than traditional one-way tactics. The findings offer factual proof that experience-based education substantially influences the cultivation of intelligent and responsible digital character.

This practice enhances the approach to digital literacy, especially within vocational education. This program not only enhances participants' understanding but also facilitates the development of a cybersecurity curriculum at the school level. This activity can serve as a prototype for creating digital education modules in other schools with analogous qualities, thus expanding its reach.

This practice substantiates the notions of digital literacy and digital citizenship by incorporating hands-on experience as a crucial component of the learning process. It illustrates that to tackle the difficulties of the digital age, the educational paradigm must transition from simple information dissemination to fostering reflective attitudes and awareness.

Analogous programs should be implemented continually, rather than as isolated events, and included in extracurricular activities or standard school curricula. Collaboration among universities, schools, and pertinent agencies is essential for the development of learning modules that educators can utilize in technology-driven character education.

Future community service programs may create more systematic digital literacy assessment tools, evaluate enduring shifts in digital perspectives, or analyze the effects of comparable education across diverse educational environments. This strategy enables community service to function as a vehicle for imparting intellectual and social ideals while simultaneously contributing to the establishment of a secure and ethical digital ecosystem.

References

Andrianto, A., Subekti, R., & Utami, A. (2023). Penguatan literasi digital dalam pencegahan cyberbullying di kalangan pelajar SMA. *Jurnal Pendidikan Teknologi dan Keamanan Digital*, 8(2), 145–157.

Derian Shakti. (2022). Model edukasi digital berbasis simulasi untuk peningkatan kesadaran keamanan siber. *Jurnal Teknologi dan Masyarakat Digital*, 10(1), 66–75.

Fadillah, S., & Nugroho, B. (2020). Analisis perilaku pengguna media sosial terhadap ancaman phishing. *Jurnal Ilmu Komputer dan Keamanan Siber*, 7(3), 199–207.

Firmansyah, R., & Syahputra, I. (2019). Pencegahan cybercrime melalui pendidikan karakter digital di sekolah menengah. *Jurnal Pendidikan dan Teknologi Informasi*, 5(2), 89–97.

Kamilah, N., & Ratsari, D. (2020). Evaluasi sistem informasi monitoring gizi balita berbasis web. *Jurnal Sistem Informasi dan Komputerisasi Kesehatan*, 4(1), 40–50.

Mahanani, D., & Kurniadi, Y. (2015). Penerapan teknologi informasi dalam layanan posyandu: Studi kasus di Kecamatan Jetis. *Jurnal Kesehatan Masyarakat Digital*, 3(2), 25–34.

Manik, A. A. dkk. (2022). Strategi peningkatan kesadaran keamanan data pribadi di kalangan remaja. *Jurnal Keamanan Digital dan Literasi Teknologi*, 9(2), 104–113.

Murdiani, A., & Hermawan, R. (2022). Perbandingan metode waterfall dan RAD dalam pengembangan sistem informasi pendidikan. *Jurnal Teknologi Informasi*, 12(1), 56–63.

Purwadi, T., & Hendrawan, M. (2020). Penerapan black box testing untuk pengujian aplikasi layanan kesehatan berbasis web. *Jurnal Riset Komputer dan Aplikasi*, 8(3), 220–227.

Purwati, L., Salim, H., & Wibowo, M. (2024). Sistem informasi terpadu untuk posyandu di wilayah perdesaan. *Jurnal Inovasi Pelayanan Publik Digital*, 6(1), 30–42.

Rahman, S., & Azizah, N. (2021). Cybersecurity awareness program untuk remaja sekolah menengah. *Jurnal Pendidikan Keamanan Siber*, 5(2), 100–109.

Sidharta, R., & Rahmahwati, D. (2023). Urgensi pendidikan etika digital dalam menghadapi era kejahatan siber. *Jurnal Moral dan Teknologi*, 11(1), 12–23.

Sukoco, R. dkk. (2022). Penerapan sistem informasi posyandu digital dalam meningkatkan efektivitas pelaporan. *Jurnal Komunitas Digital*, 7(4), 174–183.

Warjiono, T. dkk. (2022). Pengaruh simulasi phishing terhadap kesadaran mahasiswa mengenai keamanan siber. *Jurnal Keamanan Informasi dan Pendidikan Teknologi*, 6(2), 90–98.

Yuliana, D. (2020). Pemanfaatan internet aman pada kalangan remaja. *Jurnal Remaja Digital*, 4(2), 115–124.