IDENTITY SECURITY AND DIGITAL WORK TRAINING FOR PGRI HIGH SCHOOL STUDENTS

Loneli Costaner[1*], Lisnawita[2], Guntoro[3]
[1,2,3] Faculty of Computer Science, Lancang Kuning University, Riau, Indonesia
email (lonelicostaner@unilak.ac.id[1] , lisnawita@unilak.ac.id[2], guntoro@unilak.ac.id[3])

Abstract: This Community Service (PkM) activity aims to address the crucial cybersecurity literacy gap among students at PGRI Pekanbaru Senior High School. Along with the push to become creative content creators (through PkM partners focusing on Canva and copywriting), a pressing issue has emerged: students are not equipped with the skills to protect their digital identities and works. A situational analysis identified two key issues faced by partners: (1) a lack of cognitive understanding of modern cyber threat modes such as phishing and social engineering; and (2) a lack of psychomotor and technical skills in implementing basic security procedures, particularly the failure to activate Two-Factor Authentication (2FA) on essential accounts. The proposed solution is an interactive workshop method with hands-on assistance, designed to provide simultaneous cognitive and psychomotor impact. Implementation will include two main interventions: (1) case study-based threat detection training and interactive quizzes (using tools like Kahoot!) to train students' vigilance against phishing; and (2) A technical mentoring session where students will be guided step by step to activate 2FA directly on their smartphones (focusing on Google and Instagram accounts). The expected output of this activity is an increase in measurable cybersecurity knowledge (analyzed through pre-tests and post-tests), and most importantly, students have actually secured their accounts (2FA adoption). This PkM provides an essential digital "safety belt", making a fundamental contribution in shaping SMAS PGRI Pekanbaru students into content creators who are not only creative, but also smart, resilient, and safe in the cyber world.

Keyword: Cybersecurity, Digital Account, High School Students, Phishing, Two-Factor Authentication

1. Introduction

Digital transformation has brought society into an era in which Generation Z, who currently occupy senior high school classrooms, live as true digital natives. Preliminary observations at SMAS PGRI Pekanbaru confirm this condition; students actively interact with various digital media platforms. They are proficient users of communication and creative tools such as Instagram, TikTok, and Gmail (Google), which are no longer used merely for consumption but also for self-expression. SMAS PGRI Pekanbaru has responded positively to this trend by facilitating partner community service activities focused on creative soft skills, namely copywriting training and visual design using the Canva tool. This initiative is highly strategic because it encourages students to shift from passive consumers to active content creators.

Figure 1.The Environment of SMAS PGRI Pekanbaru

E-ISSN : 2774-7581

The solid building located in the city center, as shown in Figure 1, reflects a school environment that is strongly committed to expanding students' knowledge and insight. The spirit of creativity and innovation is highly important. However, understanding security challenges in cyberspace is equally essential. This condition indirectly creates a crucial gap between the enthusiasm for creativity and awareness of digital security. There is an imbalance between the acceleration of content creation skills and the literacy required to protect digital content and identity. Students are equipped with an "accelerator" (Canva), but they are not equipped with a "seat belt." They are encouraged to publish their work publicly without sufficient understanding of the risks that may arise on the platforms where they share their work on social media. This gap is not merely an assumption. A national report (APJII, 2024) consistently shows that although internet penetration among adolescents aged 13–18 years is close to 100%, their level of cybersecurity literacy remains low (R. P. Sari, 2024). The current condition of digital security at SMAS PGRI Pekanbaru is concerning, marked by a critical gap between students' proficiency in operating social media and their awareness of protecting personal data. Technically, most students still neglect basic security features such as Two-Factor Authentication (2FA) (Syahputri et al., 2023).

This neglect is not merely a matter of technical carelessness but also a form of digital apathy, in which students assume that their accounts have no value for hackers. In fact, within the cybercrime ecosystem, every active account is a valuable asset that can be used to spread broader harm.

The root of the main problem lies in psychological exploitation through highly organized social engineering techniques. Students, who sociologically are in a phase of seeking recognition and financial independence, become easy targets through fake endorsement schemes. These manipulative messages infiltrate highly personal daily communication channels, such as Instagram Direct Messages (DMs) or email. Due to their ambition to become content creators or influencers, students' critical reasoning is often weakened when they receive messages promising professional collaboration. At this point, perpetrators can easily direct students to click unfamiliar links that resemble official login pages or to download third-party applications containing malicious modules. The real impact of this vulnerability has resulted in various traumatic incidents within the school environment. Several students at SMAS PGRI Pekanbaru have reported losing full access to their social media accounts after falling into phishing traps. These cases became more serious when the hacked accounts were used by perpetrators to commit fraud against classmates and teachers in the victims' contact lists. The identified methods included distributing malicious application files disguised as "digital invitations" and sending urgent requests for money under the pretext of an emergency.

The systemic consequences of this phenomenon do not stop at material loss; they also create a crisis of trust within the school's digital ecosystem. Students who become victims often experience psychological burdens due to digital bullying or guilt because their accounts were used to deceive others. If this pattern is allowed to continue without systematic educational intervention, SMAS PGRI Pekanbaru will remain a fertile ground for hacking, where students' digital identities become commodities exploited by irresponsible parties, damaging both individual reputations and the overall security of the school community.

This finding is highly concerning because it aligns with findings from several previous studies. The case study documented by Garnita & Kuswandi (2025) confirms that account takeover practices most frequently target novice creators through social engineering

E-ISSN : 2774-7581

schemes disguised as fake offers (Pangaribuan et al., 2023; A. Putri et al., 2025). These incidents are often not purely technical failures but rather socio-technical failures. As stated by Ani et al. (2025), perpetrators exploit two aspects: (1) the victim's psychology, such as curiosity, FOMO, or greed, and (2) the victim's procedural negligence in utilizing existing security features or tools available on digital platforms. An analysis of various solutions previously implemented to address similar cases shows that passive lecture-based approaches are ineffective. D. N. Sari & Alfiyan (2023) found that active learning and simulation-based learning through gamification significantly improve students' ability to detect phishing (L. A. Putri et al., 2024). In addition, Azkiya et al. (2026) concluded that the most effective interventions are practical in nature and encourage the adoption of basic security procedures, such as direct workshops on activating 2FA (Subroto et al., 2026).

Based on this analysis, the approach required for SMAS PGRI Pekanbaru should be dual in nature. First, a technical-procedural approach is needed through hands-on practice in activating 2FA features on the Google and Instagram user interfaces (UI). Second, a cognitive-behavioral approach is required by training healthy skepticism through case studies and phishing simulations. To diagnose students' baseline conditions, a Google Forms questionnaire will be used, while Kahoot! will be used as an interactive simulation tool.

Based on the situational analysis, the fundamental problems faced by the partner are the low level of students' cognitive understanding of digital footprints and cyber threat modes, the limited psychomotor skills of students in implementing basic security measures such as 2FA, and the lack of students' affective awareness regarding the importance of ethics and digital work protection.

Therefore, the objective of this community service activity is to improve students' cognitive understanding of cyber risks and threats. Furthermore, this activity aims to provide practical psychomotor skills so that students are able to secure their accounts independently. Finally, this activity seeks to develop students' affective awareness so that they can become intelligent and responsible content creators.

2. Method

The method used in this community service activity was systematically designed to ensure the effectiveness of the training delivered to the partner. The approach consisted of several main stages, beginning with an analysis of the partner's situation and needs and continuing through to the evaluation of the training outcomes. Observations and interviews were conducted to identify the participants' initial level of understanding and the obstacles they faced in understanding cybercrime and configuring account security.

Subsequently, the training module was developed in accordance with the participants' needs by applying practice-based and simulation-based learning methods. The training was conducted in the school hall by utilizing the participants' smartphones and social media accounts, allowing the material to be practiced directly during the training session. To measure the effectiveness of the training, evaluation was carried out through a pre-test and post-test, as well as a final project that served as an indicator of the participants' skill achievement.

In addition, the implementation of the activity emphasized active participation through discussion, question-and-answer sessions, and guided practice. The facilitators provided direct assistance when participants encountered difficulties, particularly in understanding security features, recognizing suspicious digital activities, and applying account protection measures. This mentoring process was intended to ensure that participants did not only

E-ISSN : 2774-7581

receive theoretical knowledge but were also able to apply the material independently in their daily digital activities. Therefore, the method used in this activity combined conceptual understanding, technical practice, and reflective evaluation to strengthen participants' awareness and skills in maintaining digital security.

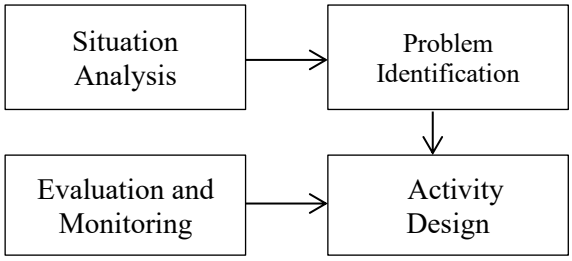

Figure 2 Stages of the Community Service Method

The stages presented in Figure 2 begin with an analysis of the partner's problems through observation and interviews. The next stage involves examining the partner's problems by considering the relevant technology and the partner's needs. Subsequently, the training activities are designed based on those needs. The final stage consists of evaluating the training delivered to the partner through questionnaires in the form of a pre-test and post-test.

3. Results and Discussion

The community service program conducted at PGRI School Pekanbaru was implemented through several stages, beginning with the delivery of material on digital literacy, cybercrime, and training on social media security configuration. This activity was carried out to improve students' understanding of how to configure security settings and identify user history on social media accounts.

The training delivered to the partner focused on understanding digital cyber literacy, configuration, and identification of account history using social media platforms and the prepared training module. This activity was expected to assist the partner in addressing potential errors or security-related problems. The training was conducted in the computer laboratory of the Faculty of Computer Science.

Figure 3 Opening Session of the Training

E-ISSN : 2774-7581

The training began with an opening session, as shown in Figure 3, followed by an introduction of the community service team and greetings to participants who had completed the attendance list. This initial interaction was intended to create an engaging and pleasant training atmosphere from the beginning to the end of the activity. As shown in the figure, the team provided guidance to the participants regarding digital literacy and social media security so that students would become more familiar with configuring security settings and identifying account user history. The training participants showed strong enthusiasm in joining the activity, as reflected in their active participation in following each step related to the components available in the application. The community service activity demonstrated how to configure security settings and identify user history on social media accounts.

Figure 4 Identity Security Training

As shown in Figure 4, the speaker provided instructions and demonstrated the training material, while the participants followed the directions enthusiastically. In the social media application training, participants were introduced to several features that are easy to use and can be accessed quickly through their smartphones, as shown in the following figure.

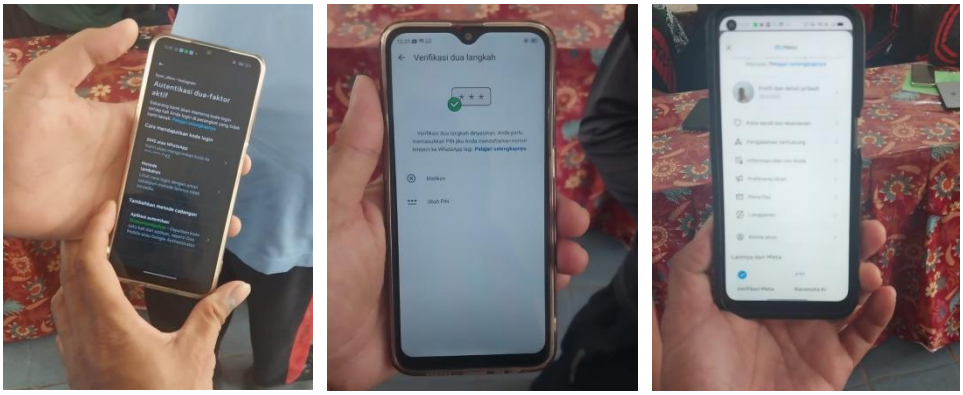

Figure 5 Social Media Configuration

E-ISSN : 2774-7581

Figure 5 shows that the training participants successfully configured social media identity security and mitigated accounts from various suspicious users. This process contributed to improving the security of user data and the digital works created by the participants.

To determine the extent to which the training participants understood the community service assistance activities that had been delivered, it was necessary to conduct an assessment of their understanding. Therefore, the implementation team administered a written test using a questionnaire consisting of 15 items, both before and after the training. The pre-test and post-test data were analyzed using the Guttman scale, which is a scale that requires firm and definite answers. The Guttman scale designed by the implementation team consisted of two clear response options: the first option, "Yes," was assigned a score of "1," while the second option, "No," was assigned a score of "0."

A total of 30 respondents participated in the activity until completion. These 30 participants provided the pre-test assessment data using the Guttman scale, as presented in Table 4.

Table 1. Pre-Test Results on Participants' Level of Understanding

No	Question	Yes Response	Percentage of Yes Responses (%)
1	Q1	6	20,0
2	Q2	0	0,0
3	Q3	10	33,3
4	Q4	1	3,3
5	Q5	5	16,7
6	Q6	1	3,3
7	Q7	9	30,0
8	Q8	0	0,0
9	Q9	3	10,0
10	Q10	5	16,7
11	Q11	2	6,7
12	Q12	2	6,7
13	Q13	4	13,3
14	Q14	4	13,3
15	Q15	24	80,0
Total :		76	253,3
Average :		5,07	16,9

Tabel 1 diatas dapat terlihat persentasi tingkat pengetahuan peserta sebelum melakukan pelatihan Keterampilan teknologi, dimana dari 15 pertanyaan guna mengukur pemahaman peserta terhadap proses pendampingan dengan jumlah nilai 253,2 dan jumlah persentasi tingkat pemahaman peserta baru sebesar 16,9 %. Jika dilihat tingkat persentasi pemahaman peserta terhadap materi pelatihan masih rendah.

Selanjutnya hasil quisioner peserta mengisi form evaluasi akhir yaitu setelah melakukan pelatihan, dimana hal ini dilakukan untuk mengetahui apakah tujuan dari pelatihan tercapai atau belum. Berikut data posttest yang sudah diolah pada tabel 2 dibawah ini.

Tabel 2. Posttest tingkat pemahaman peserta

E-ISSN : 2774-7581

No	Question	Yes Response	Percentage of Yes Responses (%)
1	Q1	30	100,0
2	Q2	30	100,0
3	Q3	29	96,7
4	Q4	28	93,3
5	Q5	29	96,7
6	Q6	28	93,3
7	Q7	27	90,0
8	Q8	30	100,0
9	Q9	28	93,3
10	Q10	30	100,0
11	Q11	28	93,3
12	Q12	30	100,0
13	Q13	30	100,0
14	Q14	30	100,0
15	Q15	30	100,0
Total :		437	1456,7
Average :		29,13	97,1

Based on Table 2, the percentage of participants' knowledge level after the technology training can be observed. The 15 questions used as instruments to measure participants' understanding of the training material showed a total understanding score of 1,456.7, with an overall percentage of participants' understanding reaching 96.9%. Based on this percentage, the level of participants' understanding indicates that the training was highly successful. This percentage also demonstrates a significant increase in participants' understanding, as illustrated in the following comprehension chart.

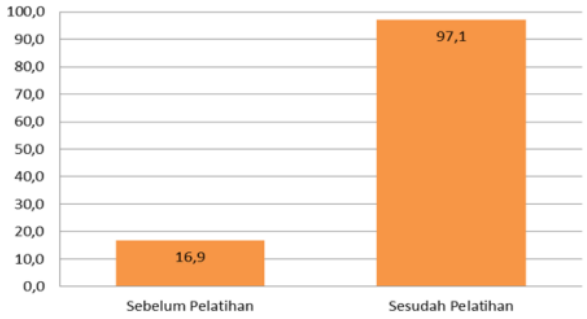

Figure 6 Chart of the Increase in Participants' Understanding during the Assistance Activity

As shown in Figure 6, the level of participants' understanding increased from 16.9% before the training to 97.1% after the training. Therefore, based on the difference between 97.1% and 16.9%, the increase in participants' understanding reached 80.2%.

4. Conclusion

Based on the series of community service activities conducted through training on cyber security and mitigation on social media, several conclusions can be drawn. Prior to the training, the partner's level of understanding of digital security and social media security configuration was still low, reaching only 16.9%. After receiving cyber security training on social media to protect digital works, the participants' level of understanding increased to 97.1%. This indicates a significant improvement of 80.2% in the participants' understanding.

E-ISSN : 2774-7581

Based on the evaluation results of the community service activity, it is recommended that future assistance programs be conducted by preparing more optimal devices and supporting facilities during practice sessions so that the results can be maximized and the benefits can reach a wider audience.

Acknowledgment
The authors would like to express their gratitude to the Institute for Research and Community Service (*LPPM*) of Universitas Lancang Kuning (*UNILAK*) for supporting this community service activity, enabling it to be carried out successfully.

References
Ani, U. D., Al-Mhiqani, M., Tuptuk, N., Tuptuk, | Nilufer, Hailes, I. S., & Watson, J. D. M. (2025). Socio-Technical Security Modelling and Simulations in Cyber-Physical Systems: Outlook on Knowledge, Perceptions, Practices, Enablers, and Barriers. *IET Cyber-Physical Systems: Theory & Applications*, 1–26. https://doi.org/10.1049/cps2.70017
Azkiya, A., Ichsan, Muhammad Budi Hasibuan, P., Nabil Azhari Putra Finula, Andrianti, R., & Maulana, I. (2026). Analisis Sistem Autentikasi Dua Faktor (2FA) Dan Efektivitasnya Dalam Meningkatkan Keamanan Akses. *JIKUM: Jurnal Ilmu Komputer, 2*(2), 1–7. https://doi.org/10.62671/jikum.v2i2.175
Garnita, C. F., & Kuswandi. (2025). Analisis Kriminologi dalam Tindak Pidana Pencurian Data Pribadi di Era Digital. *Jurnal Pubmedia*, *3*(2), 1–11. https://doi.org/10.47134/ijlj.v3i2.5288
Pangaribuan, L. J., Cahyadi, C. I., Banjarnahor, J., Barus, B., & Siahaan, B. N. (2023). Strategi Otentikasi Dokumen Pada Email Menggunakan Digital Signature dengan Algoritma Schnorr. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *3*(4), 1–9. https://doi.org/djournals.com/klik
Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, *6*(1), 1–10. https://doi.org/10.35870/jpni.v6i1.1097
Putri, L. A., Subair, M. A. F., & Marsuki, N. R. (2024). Strategi Pengguna Media Sosial Dalam Mengatasi Tantangan Privasi dan Keamanan Online di Era Digital. *Concept: Journal of Social Humanities and Education*, *3*(1), 1–8. https://doi.org/10.55606/concept.v3i1.949
Sari, D. N., & Alfiyan, A. R. (2023). Peran Adaptasi Game (Gamifikasi) dalam Pembelajaran untuk Menguatkan Literasi Digital: Systematic Literature Review. *UPGRADE: Jurnal Pendidikan Teknologi Informasi*, *1*(1), 1–9. https://doi.org/10.30812/upgrade.v1i1.3157
Sari, R. P. (2024). *APJII : Survei Penetrasi Internet Indonesia 2024*. Cisco Indonesia.
Subroto, D. E., Rahardian, R. L., Ventayen, C. O., Saputra, A. E., & Cahyono, B. (2026). Analisis Keamanan Privasi pada Media Sosial: Studi Kasus Penggunaan Data Pribadi di Facebook dan Instagram. *Journal of Innovative and Creativity*, *6*(1), 1–17. https://doi.org/10.31004/joecy.v6i1.6347
Syahputri, N. I., Herlina, H., & Nurohman, H. A. (2023). Penyuluhan Pentingnya Two Factor Authentication dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat*, *1*(6), 1–6.