Abdimas Umtas: Jurnal Pengabdian Kepada Masyarakat
LPPM-Universitas Muhammadiyah Tasikmalaya
Volume: 9, Issue: 1, January, 2026; pp: 239-249
E-ISSN: 2614 - 8544

Enhancing Digital Identity And Personal Data Security Literacy in The Digital Era: A Community Service Program at Rumah Gemilang Indonesia

Dede Handayani [a], Oke Hariansyah [b], and Ahmad Nursodiq [c]

Informatic Study Program, Universitas Pamulang, Tangerang Selatan, Indonesia

[a]Corresponding author: dosen02411@unpam.ac.id
[b]dosen00840@unpam.ac.id
[c]dosen02526@unpam.ac.id

ABSTRACT

The rapid advancement of information technology in the digital era offers convenience while simultaneously increasing risks related to digital identity and personal data security. Participants at Rumah Gemilang Indonesia (RGI), who are predominantly young and active users of digital platforms, exhibit relatively low levels of digital security literacy, making them vulnerable to cyber threats such as phishing, identity theft, and personal data misuse. This Community Service Program (PkM) aimed to enhance participants' knowledge, awareness, and practical skills in protecting digital identities and personal data. The program employed educational and participatory approaches, including lectures, discussions, hands-on practice, and case studies, with effectiveness evaluated through pre-test and post-test assessments. The activity was conducted face-to-face at Rumah Gemilang Indonesia, Depok, involving 24 participants. The results showed a substantial improvement in participants' understanding, with the average correct response rate increasing from 29.86% in the pre-test to 86.81% in the post-test. These findings indicate that structured digital security training is effective in improving digital security literacy among youth. Therefore, this program provides empirical evidence supporting the role of community-based digital security education in fostering safe and responsible digital behavior and enhancing participants' readiness for technology-driven education and employment environments.

ARTICLE INFO

Article History:
Submitted/Received: 26-12-2025
First Revised: 05 January 2025
Accepted: 10 January 2025
First Available online: 31 January 2026
Publication Date: 31 January 2026

Keyword :
Digital Identity
Personal Data
Digital Security
Digital Literacy
Community Service

https://doi.org/10.35568/abdimas.v9i1.7576

INTRODUCTION

The rapid development of information technology in the digital era has significantly transformed patterns of learning, communication, and work activities in society. While digital technologies provide efficiency and accessibility, they also introduce new risks related to digital identity and personal data security (Badan Siber dan Sandi Negara (Badan Siber dan Sandi Negara, 2021). These risks are increasingly relevant for young people, who are among the most active users of digital platforms.

At Rumah Gemilang Indonesia (RGI), most training participants are young individuals who frequently use the internet, social media, and application-based services to support learning, communication, and job searching (Setiawan, 2021). Despite this high level of digital engagement, participants generally demonstrate limited understanding of digital identity protection and personal data security. Previous studies indicate that high digital usage is not always accompanied by adequate digital security literacy, particularly among youth populations (Gasser & Maclay, 2020).

Low digital security literacy increases vulnerability to various cyber threats, including phishing, identity theft, online fraud, data misuse, and account hacking (Riyanto, 2023). In practice, these vulnerabilities are reflected in unsafe digital behaviors such as using weak passwords, sharing personal data without proper verification, and oversharing private information on social media platforms. Furthermore, young people who actively seek employment online are particularly exposed to cybercrime risks, including fraudulent job advertisements that request sensitive personal information such as identity cards or personal photographs (Komisi Perlindungan Anak Indonesia, 2022).

Another challenge faced by Rumah Gemilang Indonesia is the absence of structured educational programs specifically focused on digital security and personal data protection. Although RGI provides various vocational and skills-based training programs, digital security literacy has not been systematically integrated into its curriculum (O'Brien & Marakas, 2018). This condition aligns with national findings that emphasize the need for formal education and socialization related to personal data protection in response to increasing cyber threats in Indonesia (Kementerian Komunikasi dan Informatika Republik Indonesia, 2020).

The urgency of strengthening digital security education is further amplified by the tendency of young people to share personal information excessively on social media, such as identity photos, location data, travel information, and daily routines. Such practices may lead to privacy violations, identity misuse, and long-term reputational damage, which can negatively affect educational and professional opportunities (Wahyudi & Nurhadi, 2022).

Therefore, the main problem faced by Rumah Gemilang Indonesia is the low level of awareness and practical skills related to digital identity and personal data protection, combined with the lack of structured digital security education. To address this gap, systematic socialization and educational activities are essential. This Community Service Program (PkM) aims to enhance participants' knowledge, awareness, and practical skills in protecting digital identities and personal data, thereby fostering safe, responsible, and professional digital behavior in the modern digital era(Nasution, 2022).

https://doi.org/10.35568/abdimas.v9i1.7576

METHOD

To achieve the objectives of the activity effectively, the implementation of the socialization program was designed by combining educational, interactive, and practical approaches. The activity methods used are described as follows:

Lecture Method (Material Presentation)

This method was used to deliver fundamental concepts related to:

- Digital identity and personal data,
- Cybercrime risks,
- Mechanisms of digital attacks such as phishing, malware, and identity theft, and
- The importance of data security in daily digital activities

The material was delivered using presentation media to facilitate participants' understanding. This method was chosen to provide participants with essential knowledge regarding the importance of maintaining digital identity and personal data in the digital era, particularly in the context of education.

Discussion and Question-and-Answer Method

Following the material presentation, participants were allowed to engage in discussions and ask questions. The objectives of this method were to:

- Explore participants' experiences related to digital security,
- Address real problems encountered by participants, and
- Enhance interaction and deepen understanding of the material.

Through this method, participants at Rumah Gemilang Indonesia Training in Depok City were encouraged to actively explore information related to digital identity and data protection that they had not previously understood.

Practice Demonstration Methods

Participants were invited to engage in hands-on practice activities, including:

- Create a strong password
- Enable two-factor authentication
- Recognize examples of phishing messages
- Manage the security and privacy of social media accounts

This method is important to ensure participants not only understand the theory but are also able to apply it. This simulation method is given to all students to try to apply the importance of maintaining identity and data in the digital era, which has been explained.

Case Study Methods

Participants were provided with real case examples related to:

https://doi.org/10.35568/abdimas.v9i1.7576

- Identity theft
- Misuse of personal data
- Online scams

The purpose of this method was to enable participants to analyze situations, identify warning signs, and understand the potential impacts of cyber incidents on victims.

Activity Evaluation Method

The evaluation of the activity was conducted through:

- pre-test and post-test instruments to measure improvements in participants' knowledge
- observation of participant engagement during discussions and practical sessions
- collection of participant feedback regarding the material and the implementation of the socialization activities.

RESULTS

This Community Service Program (PkM) was implemented in the form of socialization activities aimed at increasing participants' knowledge regarding the importance of maintaining digital identity and personal data security in the digital era. The activity was conducted by the Community Service Team from the Information Technology Study Program at Rumah Gemilang Indonesia Training Center, Depok City. This program represents an important effort to prepare participants as future graduates who are ready to engage in educational and professional environments that increasingly rely on digital technologies. The activity was carried out over three days, from November 16 to November 18, 2025, through structured material delivery focused on digital identity protection and personal data security.

In this Community Service activity, positive results were observed based on participants' levels of understanding, as measured through pre-test and post-test surveys. The surveys were administered to 24 participants to assess their knowledge of digital identity and personal data security. The evaluation instruments consisted of six questions addressing key aspects of digital security literacy, including:

- What is a digital identity?
- What is included in personal data?
- Personal data that is sensitive and at high risk if leaked is?
- One of the main risks due to low digital security literacy is?
- RGI participants who are looking for work online are vulnerable to becoming victims of cybercrime because?
- Examples of unsafe digital behaviors are?

Each question was accompanied by multiple-choice answer options designed to reflect participants' level of understanding regarding the importance of maintaining digital identity and personal data security in the digital era. The comparison between pre-test and post-test results illustrates changes in participants' knowledge before and after the implementation of the program. From these questions, we have included answer choices to illustrate the extent to which participants understand the importance of maintaining identity and data in the digital era. From the results of the survey carried out, the results

https://doi.org/10.35568/abdimas.v9i1.7576

between before and after the implementation were obtained as follows:

Question 1

Before Delivering Material

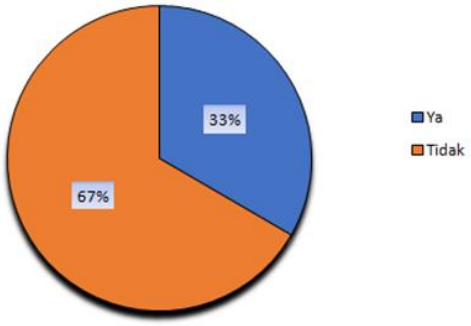

FIGURE 1. Evaluation of Participant Activity on the Fiverr Platform

From the questions given before the delivery of the material (Pre-test), the results obtained from 24 participants, the majority of whom did not have digital identities, were with a percentage of 33% answering "Yes" and 67% answering "No".

After the Presentation of the Material

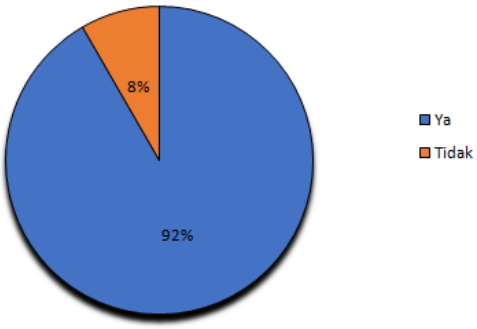

FIGURE 2. Question 1 After the Presentation of the Material

From the questions given after the delivery of the material (Post-test), we can see that there is a significant increase where the percentage of digital identity is increased to 92% answering "Yes", and 8% answering "No".

Question 2

Before Delivering Material

https://doi.org/10.35568/abdimas.v9i1.7576

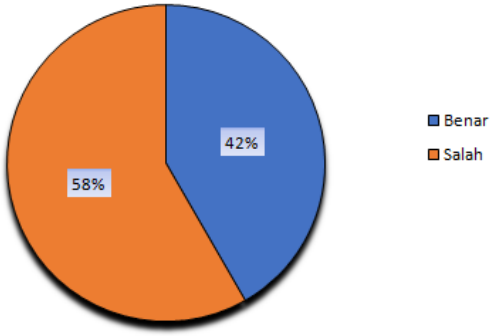

FIGURE 3. Question 2 Before Delivering Material

From the questions given before the submission of the material (Pre-test), the results obtained from 24 participants, the majority of whom did not know what personal data included was that with a percentage of 42% answering "True" and 58% answering "False".

After the Presentation of the Material

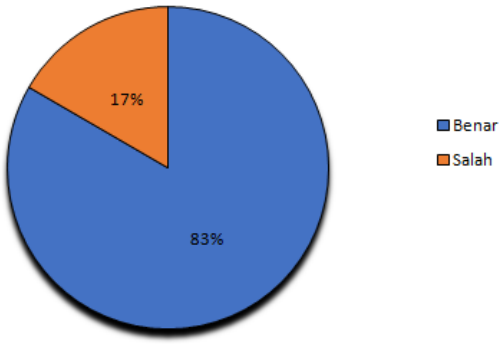

FIGURE 4. Question 2 After the Presentation of the Material

From the questions given after the submission of the material (Post-test), we can see that there is a significant increase where the percentage who know what is included in personal data is that it has increased to 83% answering "True", and 17% answering "False".

Question 3

Before Delivering Material

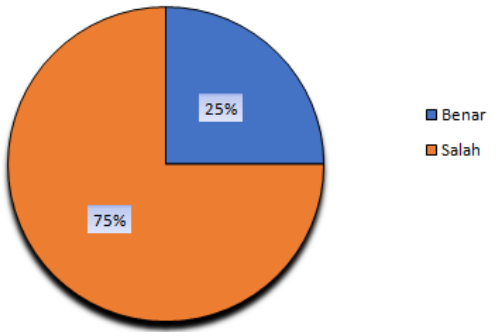

FIGURE 5. Question 3 Before Delivering Material

https://doi.org/10.35568/abdimas.v9i1.7576

From the questions given before the delivery of the material (Pre-test), the results obtained from 24 participants were partly unaware of personal data that is sensitive and at high risk if leaked is with a percentage of 25% answering "True" and 75% answering "False".

After the Presentation of the Material

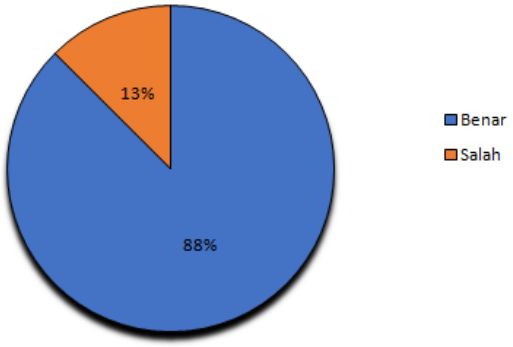

FIGURE 6. Question 3 After the Presentation of the Material

From the questions given after the submission of the material (Post-test), we can see that there is a significant increase where the percentage who know personal data that is sensitive and at high risk if leaked is increased to 88% answering "True", and 13% answering "False".

Question 4

Before Delivering Material

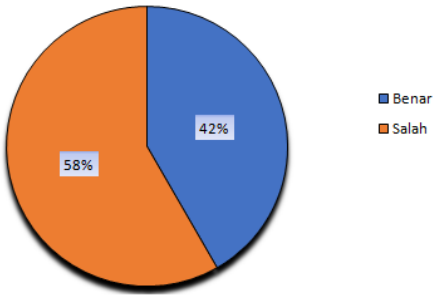

FIGURE 7. Question 4 Before Delivering Material

From the questions given before the delivery of the material (Pre-test), the results obtained from 24 participants were partly unknown One of the main risks due to low digital security literacy is with a percentage of 42% answering "True" and 58% answering "False".

After the Presentation of the Material

https://doi.org/10.35568/abdimas.v9i1.7576

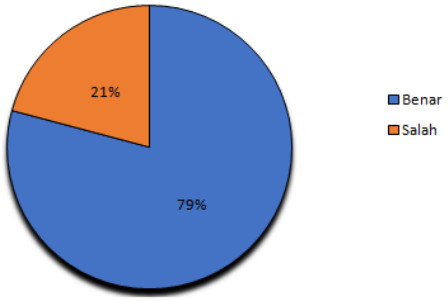

FIGURE 8. Question 4 After the Presentation of the Material

From the questions given after the delivery of the material (Post-test), we can see that there is a significant increase where the percentage who know One of the main risks due to low digital security literacy is that it increases to 79% answering "True", and 21% answering "False".

Question 5

Before Delivering Material

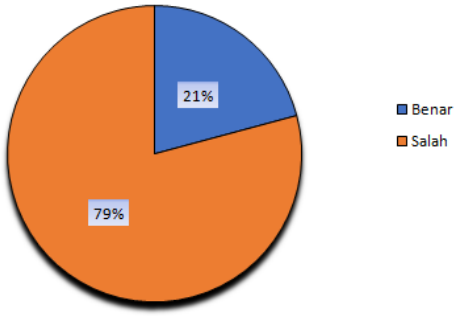

FIGURE 9. Question 5 Before Delivering Material

From the questions given before the submission of the material (Pre-test), the results obtained from 24 participants did not know that RGI participants who look for work online are vulnerable to becoming victims of cybercrime because with a percentage of 21% answering "True" and 79% answering "False".

After the Presentation of the Material

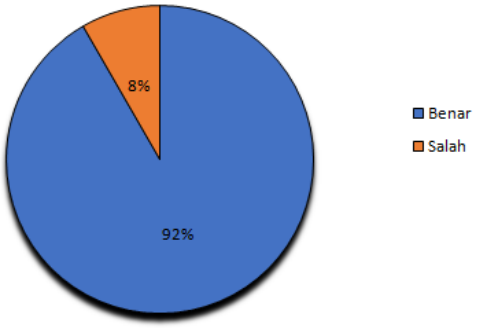

FIGURE 10. Question 5 After the Presentation of the Material

https://doi.org/10.35568/abdimas.v9i1.7576

From the questions given after the submission of the material (Post-test), we can see that there is a significant increase where the percentage who know that RGI Participants who are looking for work online are vulnerable to becoming victims of cybercrime increased to 92% answered "True", and 8% answered "False".

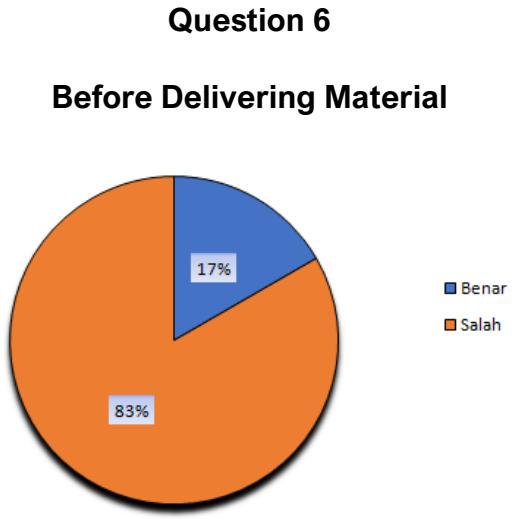

FIGURE 11. Question 6 Before Delivering Material

From the questions given before the delivery of the material (Pre-test), the results obtained from 24 participants were partly unknown Examples of unsafe digital behavior were with a percentage of 17% answering "True" and 83% answering "False".

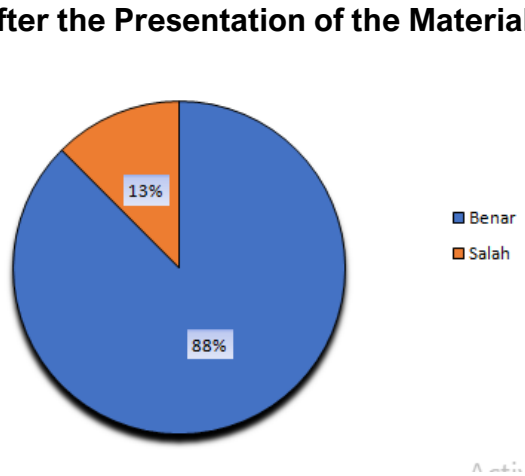

FIGURE 12. Question 6 After the Presentation of the Material

From the questions given after the delivery of the material (Post-test), we can see that there is a significant increase where the percentage who know Examples of unsafe digital behavior is increased to 88 Based on the results obtained, it is evident that prior to the implementation of this Community Service Program (PkM), many participants at Rumah Gemilang Indonesia Training Center in Depok City had limited awareness of the importance of maintaining digital identity and personal data security. After the implementation of the program, participants demonstrated a notable improvement in technological

https://doi.org/10.35568/abdimas.v9i1.7576

knowledge and understanding related to digital security, indicating increased readiness to adapt to digital transformation in educational contexts.

This improvement is supported by the results of the pre-test and post-test evaluations conducted with 24 participants. The pre-test results indicated low levels of correct responses across all question categories. In contrast, the post-test results showed a substantial increase in accuracy for each question, reflecting improved understanding after the socialization and training activities. The comparison of average scores demonstrates a significant increase from 29.86% before the activity to 86.81% after the activity, as presented in Table 1:

FIGURE 1. Comparative percentage

Question Types	Percentage of correct answers before socialization	Percentage of correct answers after socialization
Question 1	33%	92%
Question 2	42%	83%
Question 3	25%	88%
Question 4	42%	79%
Question 5	21%	92%
Question 6	17%	88%
Average Percentage	29.86%	86.81%

These results indicate that the scientific briefing and practical training provided through this program effectively enhanced participants' understanding of digital identity and personal data security. With improved digital security literacy, it is expected that graduates of Rumah Gemilang Indonesia Training Center in Depok City will be better prepared to pursue further education and contribute to the advancement of education in the field of Information Technology.

CONCLUSION

Based on the implementation of the activities and the evaluation results, it can be concluded that the educational program on digital identity security and personal data protection in the digital era had a positive impact on participants' understanding. Participants demonstrated improved knowledge regarding types of personal data, potential cybercrime risks, and preventive measures for maintaining information security when using the internet and digital media.

Throughout the activity, participants showed high enthusiasm and were able to actively engage in all stages of the program. The evaluation results indicated a clear improvement in participants' understanding from before to after the activity was conducted. Therefore, this Community Service Program successfully achieved its objective of enhancing digital security literacy, enabling participants to become more aware, cautious, and responsible in their activities within cyberspace.

REFERENCES

Badan Siber dan Sandi Negara. (2021). Panduan Keamanan Siber untuk Masyarakat. BSSN Press.

Gasser, U., & Maclay, C. (2020). Digital Literacy and Youth's Online Safety: A Framework of Protection. International Journal of Digital Society, 11(4), 56–70.

https://doi.org/10.35568/abdimas.v9i1.7576

Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). Perlindungan Data Pribadi di Era Digital. Kominfo.

Komisi Perlindungan Anak Indonesia. (2022). Ancaman Kejahatan Siber pada Anak dan Remaja di Indonesia.

Nasution, M. K. (2022). Literasi Digital dan Perlindungan Data Pribadi bagi Generasi Muda. Jurnal Teknologi Informasi, 15(2), 45–54. https://doi.org/10.1234/jti.2022.15.2.45

O'Brien, J. A., & Marakas, G. M. (2018). Management Information Systems (11th ed.). McGraw-Hill Education.

Riyanto, B. (2023). Keamanan Informasi dan Ancaman Siber: Upaya Pencegahan pada Generasi Muda. Jurnal Keamanan Siber Indonesia, 4(1), 12–25.

Setiawan, H. (2021). Kebijakan Perlindungan Data Pribadi dalam Perspektif Hukum di Indonesia. Jurnal Hukum \& Teknologi, 7(3), 33–44.

Wahyudi, A., & Nurhadi, D. (2022). Edukasi Keamanan Data bagi Pelajar sebagai Upaya Preventif Cybercrime. Jurnal Pendidikan Dan Teknologi, 8(1), 33–40.

https://doi.org/10.35568/abdimas.v9i1.7576