

## Enhancing Personal Data Security Awareness and Vigilance on Social Media Platforms

Anrie Suryaningrat<sup>1,a)</sup>, Desi Ramayanti<sup>1,b)</sup> Bias Yulisa Geni<sup>1,c)</sup>, C Achmad Fahrudin<sup>2,d)</sup>, Christian Hovel Simanjuntak<sup>1,e)</sup>, Samuel Aras Michael<sup>1,f)</sup>

<sup>1</sup>Informatics Engineering Study Program, Faculty of Engineering and Informatics, Dian Nusantara University, Jakarta, Indonesia

<sup>2</sup>Informatics Engineering Study Program, Faculty of Engineering and, Muhammadiyah University of Banten, Tangerang, Indonesia

<sup>a)</sup>Corresponding author: anrie.suryaningrat@dosen.undira.ac.id

<sup>b)</sup>desi.ramayanti@undira.ac.id

<sup>c)</sup>bias.yulisa.geni@undira.ac.id

<sup>d)</sup>achmad.fahrudin@umbanten.ac.id

<sup>e)</sup>411211094@mahasiswa.undira.ac.id

<sup>f)</sup>411211123@mahasiswa.undira.ac.id

---

### ABSTRACT

As the demand for personal information protection grows, vigilance and awareness regarding data and privacy security have become paramount concerns in social media platform usage. While studies indicate rising awareness levels, there remains a deficit in understanding the risks and effective methods for safeguarding personal data. Factors such as inadequate education, constrained privacy controls, and uncertainties surrounding platform privacy policies impede users' efforts to bolster personal data security. This activity aims to educate on the significance of digital privacy and foster vigilance and awareness of data and privacy security on social media platforms. The implementation of activity planning involved a national seminar combining material presentations and interactive discussions with cybersecurity practitioners from the Indonesia Honeynet Project (IHP) and the Indonesia Artificial Intelligence Society (IAIS), high school students, university students, teachers, lecturers, and the surrounding community. The success of this activity was marked by the successful dissemination of knowledge and understanding among the audience, both online and offline. This is expected to provide insights and mitigate risks associated with data and privacy security, promoting safer and more responsible platform usage

---

---

### ARTICLE INFO

**Article History:**

*Submitted/Received 30 Apr 2024*

*First Revised 1 Mei 2024*

*Accepted 1 Mei 2024*

*First Available online 1 Mei 2024*

*Publication Date 30 Apr 2024*

---

**Keyword :**

*Awareness*

*Data Privacy*

*Social Media*

*Education*

*Privacy Control*

## INTRODUCTION

The advent of the digital era has revolutionized how we communicate and exchange information. Social media platforms have emerged as primary venues for social interaction, opening up new avenues for connection, sharing, and community building. Platforms like Facebook, Instagram, and Twitter have become an integral part of daily life for millions worldwide. Social media empowers users to connect with friends and family, stay abreast of news and current affairs, and discover communities with shared interests.

However, despite its conveniences and benefits, social media presents a double-edged sword. On one hand, it offers seamless communication, rapid and comprehensive access to information, and the ability to forge connections with individuals across the globe. On the other hand, social media platforms also open up avenues for personal data misuse. Personal information such as names, addresses, phone numbers, and other sensitive details shared on social media can be exploited by malicious actors.

Cases like Cambridge Analytica, which exploited Facebook user data for political purposes (Hinds et al., 2020), highlight the vulnerability of user privacy on social media platforms. Other instances of privacy breaches include the exploitation and misuse of user data by Facebook (Scheele, 2021) and the unauthorized use of personal data for marketing purposes by Instagram (Darmaningrat et al., 2020). These cases underscore the fragility of user privacy on social media.

The consequences of privacy breaches can be detrimental to users, giving rise to privacy concerns in social media, a phenomenon known as the privacy paradox (Halama et al., 2022; Hirschprung, 2023). This paradox manifests as a contradiction between individuals' expressed concerns about data privacy and their actions that contradict these concerns. While individuals voice their apprehensions about data privacy and its potential misuse, they willingly share personal information on social media and other online platforms. This behaviour can stem from factors such as a lack of understanding of risks and consequences, social pressures, a perceived sense of convenience in sharing information rather than keeping it private, and a belief that the platforms they use adequately safeguard their data (Prince et al., 2023).

Protecting personal data on social media is a critical issue that demands serious attention from governments and other stakeholders. Specific regulations are needed to safeguard user data and ensure its security on social media platforms. While Indonesia has the Information and Electronic Transactions Law (UU ITE), which governs privacy rights and legal protection for data owners in case of leaks, it lacks specific regulations tailored to the social media realm (Faridah Faridah et al., 2022; Pertiwi et al., 2022). Therefore, effective and efficient tactics and strategies are required, not only for addressing privacy breaches but also for prevention and anticipation.

Research efforts have delved into user perceptions and the impacts of privacy breaches on social media, examining concerns and online privacy management strategies (Sholikhatin et al., 2023). Further analysis is needed to assess awareness and vigilance regarding personal data protection on social media and how users can manage these concerns. In light of these prevailing conditions, the authors and their team have organized a national seminar inviting cybersecurity experts as speakers, fulfilling the university's tri dharma, particularly community service.

## METHOD

The research employed a qualitative descriptive method, aimed at in-depth analysis of social occurrences, phenomena, or circumstances (Rusandi & Muhammad Rusli, 2021). The activity took the form of a national seminar incorporating a combination of talks and interactive discussions. Cybersecurity experts from Indonesia Honeynet Project (IHP) and Indonesia Artificial Intelligence Society (IAIS) served as speakers. Approximately 150 attendees, including high school students, university students, teachers, and lecturers from various schools and universities, along with community representatives from the DKI Jakarta

region, participated both online and offline. Speakers delivered interactive presentations, providing empirical field data, explanations of causes and effects, impacts, and preventive measures for the audience to adopt. The audience engaged in direct interaction through discussions related to prevailing conditions and challenges. As depicted in Figure 1 (a and b), the audience demonstrated enthusiasm during the question-and-answer session with the speakers.



FIGURE 1: (a,b) Presentation and Interaction between Speakers and Participants

## DISCUSSION

The community service activity conducted in the form of a national seminar has yielded positive qualitative and quantitative impacts on fostering awareness and vigilance regarding personal data on social media platforms. These impacts are summarized as follows: 1. Heightened Awareness of Risks Associated with Social Media Usage: the seminar highlighted the urgency and importance of recognizing the risks associated with using social media platforms. Users often overlook the potential risks, such as privacy breaches, identity theft, and the spread of misinformation, due to the growing internet and social media penetration; 2. Collaborative Efforts to Enhance Data Privacy Awareness : the seminar emphasized the need for collective efforts from various stakeholders, including universities, research institutions, and civil society organizations, to promote awareness and vigilance regarding personal data security issues; 3. Exemplary Collaboration between Institutions: The partnership between Dian Nusantara University, Indonesia HoneyNet Project (IHP), and Indonesia Artificial Intelligence Society (IAIS) serves as a concrete example of collaborative efforts, as depicted in Figure 2; 4. Effective Dissemination of Information and Safe Practices.

The seminar's implementation demonstrated positive impacts and benefits in providing deeper information and understanding about safe practices on social media platforms. The speakers' presentations covered crucial aspects such as the "who, what, when, where, and why" of personal data protection and prevention measures; 5. Broadened Reach and Effective Messaging: The involvement of diverse community members, ranging from lecturers and teachers to students and the general public, is crucial. By targeting these groups, the message about the importance of personal data security awareness and vigilance can be conveyed more effectively and reach a wider audience.



FIGURE 2. Collaboration between Dian Nusantara University, Indonesia HoneyNet Project (IHP), and Indonesia Artificial Intelligence Society (IAIS)

The community service activity, conducted in the form of a national seminar, can be deemed a success. This is evident from the coverage and dissemination of the event across various online media outlets. Despite its success, there remains ample scope for expanding the topic and audience reach. The limited time allocation, coupled with the high interest and enthusiasm from the audience, presents an opportunity for improvement in future endeavors. Diversifying the speaker panel could also be considered, potentially including psychology professionals, government representatives as regulators, and other relevant stakeholders.

## CONCLUSION

In the face of personal data security challenges on social media platforms, the national seminar organized by Dian Nusantara University has proven successful in providing information, understanding, and practical skills to participants. Through close collaboration with IHP and IAIS, and the support of competent cybersecurity experts, the event has delivered a thorough understanding of how to protect personal data on social media platforms.

The combination of seminar and talk show formats effectively eliminated the barrier between speakers and the audience, facilitating productive interactive discussions. The involvement of diverse stakeholders, ranging from lecturers and teachers to students, schoolchildren, parents, and the general public, ensured that the activity reached a broad audience, aiming to raise awareness and vigilance regarding personal data security issues on a wide scale. Through comprehensive presentations and constructive Q&A sessions, the objectives of enhancing understanding and implementation were successfully achieved. Additionally, by integrating physical attendees with online participants via Google Meet and YouTube streaming, the event effectively reached its target audience, making a significant positive impact in raising awareness about the importance of personal data security in the digital age.

## REFERENCES

- Darmaningrat, E. W. T., Astuti, H. M., & Alfi, F. (2020). Information Privacy Concerns Among Instagram Users: The Case of Indonesian College Students. *Journal of Information Systems Engineering and Business Intelligence*, 6(2), 159.
- Faridah Faridah, Muhammad Yusuf, & Nur Setiawati. (2022). Etika Keterbukaan dan Perlindungan Privacy di Media Sosial. *Jurnal An-Nasyr: Jurnal Dakwah Dalam Mata Tinta*, 9(1), 36–47.
- Halama, J., Frenzel, T., Hofmann, L., Klose, C., Seifert, N., Telega, K., & Bocklisch, F. (2022). Is There a Privacy Paradox in Digital Social Media Use? The Role of Privacy Concerns and Social Norms. *Open Psychology*, 4(1), 265–277.
- Hinds, J., Williams, E. J., & Joinson, A. N. (2020). “It wouldn’t happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143, 102498.
- Hirschprung, R. S. (2023). Is the Privacy Paradox a Domain-Specific Phenomenon. *Computers*, 12(8), 156.
- Pertiwi, E., Delvina Nuraldini, D., Tri Buana, G., & Arthacseses, A. (2022). Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, 3(3), 10–16.
- Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2023). Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns. *IEEE Transactions on Engineering Management*, 70(10), 3553–3570.

- Rusandi, & Muhammad Rusli. (2021). Merancang Penelitian Kualitatif Dasar/Deskriptif dan Studi Kasus. *Al-Ubudiyah: Jurnal Pendidikan Dan Studi Islam*, 2(1), 48–60. <https://doi.org/10.55623/au.v2i1.18>
- Scheele, R. (2021). Facebook: From Data Privacy to a Concept of Abuse by Restriction of Choice. *Journal of European Competition Law & Practice*, 12(1), 34–37.
- Sholikhatin, S. A., Pribadi, P., Pratiwi, A., & Anggara, D. A. (2023). SOSIALISASI SECURITY AWARENESS DAN PERLINDUNGAN DATA PRIBADI DI MEDIA SOSIAL PADA SMK MAARIF NU 1 CILONGOK. *SELAPARANG: Jurnal Pengabdian Masyarakat Berkemajuan*, 7(3), 1517.