Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

Digital Safety Education for the Constituents of West Nusa Tenggara Electoral District 2

Feliks Prasepta Sejahtera Surbakti
Industrial Engineering Department, School of Bioscience, Technology, and Innovation, Universitas Katolik Indonesia Atma Jaya, Indonesia.
*Corresponding Author. Email: feliks.prasepta@atmajaya.ac.id

Abstract: This community service aims to provide the public with practical knowledge and skills in cybersecurity, focusing on securing digital devices, digital identities, and managing digital footprints. The method used involved interactive seminar-based training and case simulations. Participants were trained to understand various types of cyber threats, recognize digital scams, and implement security measures such as using strong passwords, two-factor authentication, full encryption, and antivirus software. Additionally, participants were encouraged to manage their digital footprints responsibly to minimize the risk of privacy violations. To evaluate the effectiveness of the program, a structured instrument in the form of pre-test and post-test questionnaires was used. The instrument measured participants' understanding of key cybersecurity concepts and safe digital practices. The data collected were analyzed using descriptive statistics, specifically by comparing the average scores before and after the training to determine the extent of knowledge improvement. The results of this program showed a significant improvement of 35% in participants' awareness and understanding of digital security. In conclusion, this program successfully enhanced participants' digital literacy in cybersecurity and contributed to building a safer digital ecosystem in Indonesia.

Article History:
Received: 02-06-2025
Reviewed: 11-07-2025
Accepted: 28-07-2025
Published: 25-08-2025

Key Words:
Cybersecurity; Data Protection; Digital Literacy; Digital Security Awareness; Online Scams.

How to Cite: Surbakti, F. P. S. (2025). Digital Safety Education for the Constituents of West Nusa Tenggara Electoral District 2. *Jurnal Pengabdian UNDIKMA*, *6*(3), 479-487. https://doi.org/10.33394/jpu.v6i3.16374

https://doi.org/10.33394/jpu.v6i3.16374

Introduction

In the increasingly advanced digital era, the use of information technology has become an integral part of the daily lives of Indonesian people. Activities such as communication, financial transactions, education, and entertainment are now largely carried out through digital platforms. However, along with the growing adoption of technology, threats to digital security have also become more complex and diverse (Sendjaja et al., 2024). Incidents such as personal data breaches, the spread of malware, and online fraud pose serious challenges that can harm both individuals and institutions.

Recent studies show that phishing and ransomware are the most prevalent cybercrime types in Indonesia, exploiting low levels of digital literacy and regulatory gaps (Khoirunnisa & Jubaidi, 2024). Furthermore, research among Indonesian college students reveals that 39.9% have experienced cyber victimization, including harassment, fraud, or identity theft (Nugroho et al., 2024). Despite a 79.5% internet penetration rate, the country's digital literacy index remains low, with scores averaging around 62% (Afrina et al., 2024), the lowest in ASEAN (Afrina et al., 2024). Therefore, digital literacy that emphasizes safe digital practices has become an urgent necessity to protect users from various cyber threats.

The main reason for conducting this community service is the high level of public vulnerability to cyberattacks due to a lack of knowledge and awareness about the importance

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

of safe digital practices. Many internet users do not yet understand how to protect their personal data or recognize signs of online fraud, making them easy targets for cybercriminals. By providing proper education, it is hoped that the public will become more proactive in safeguarding their digital security.

The literature review shows that digital literacy plays an important role in preventing cybercrime. According to Kurnia and Astuti (2017), the digital literacy movement in Indonesia has evolved by involving various actors and a range of activities targeting specific groups. This indicates that efforts to improve digital literacy must continue to be carried out on a large scale and in a structured manner.

In addition, Dwiyanto (2023) emphasizes the importance of implementing cybersecurity standards in Indonesian higher education institutions to uncover existing vulnerabilities. This highlights the strategic role of educational institutions in fostering digital security awareness among the younger generation. Monggilo et al. (2020), in their guide on digital media literacy and cybersecurity, stress that young people must be equipped with the knowledge and skills to be creative and resilient in cyberspace. This is essential so they can make the most of technology without compromising their personal security.

Hidayat et al. (2021) highlight that digital literacy and civic defense can serve as effective efforts to prevent the spread of hoaxes within the national defense system. This indicates that digital literacy is not only crucial for individual security but also for national stability. Napu et al. (2024), in their analysis of the role of cybersecurity and digital skills in the growth of small and medium enterprises (SMEs) in Indonesia's digital economy era, found that improving digital skills can drive economic growth and protect SMEs from cyber threats.

Nasrullah (2022), in his book on cyber media theory and research, emphasizes the importance of understanding cyber culture and digital communication to develop effective security strategies. Putri et al. (2020) discuss the mitigation of cybersecurity risk threats during the COVID-19 pandemic, a period marked by a significant increase in digital activity. This highlights that crisis situations can heighten vulnerability to cyberattacks, making digital literacy all the more essential.

Based on these various studies, it can be concluded that digital literacy, which emphasizes safe digital practices, is a key element in protecting society from cyber threats. Therefore, community service through education and training on digital security is a strategic step toward building a safe and trustworthy digital ecosystem in Indonesia. This community service aims to raise public awareness and understanding of the importance of digital security. Through educational and training programs, it is expected that the community will be able to recognize potential cyber threats and implement effective preventive measures. The anticipated benefit of this activity is the creation of a more responsive and prepared community in facing digital security challenges, thereby minimizing the risk of losses due to cybercrime.

Method

This community service was carried out using a structured method designed to address issues related to digital literacy in the context of cybersecurity and safe digital practices. The stages of the activity include needs assessment, program planning, implementation, and evaluation with impact analysis, following the framework proposed by Ghosh et al. (2023). Each stage is designed to ensure that the program is not only relevant but also delivers a significant impact to the target audience.

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

The first stage is the needs assessment, which was conducted through a preliminary survey of prospective participants. This survey aimed to understand participants' level of digital literacy, including their knowledge of cyber threats such as phishing, sniffing, and malware. Data was collected online using a simple questionnaire and then analyzed using descriptive statistics to provide an overview of participants' needs. The results of this analysis served as the basis for designing the training materials.

The second stage is program planning, in which the training modules were developed based on the needs analysis. The training materials covered key topics such as an introduction to digital threats, safe digital practices, management of digital footprints, and security measures such as two-factor authentication and the use of strong passwords. In addition, supporting tools such as infographics and case simulations were prepared to enhance participants' understanding.

The third stage is the implementation of activities, which was conducted through interactive training. The lecture method was used to deliver foundational theory in a structured manner. The trainer explained various cyber threats, case examples, and practical solutions. This lecture was followed by a Q&A session, where participants could ask questions related to the material presented. This method proved effective in clarifying points that were not well understood.

Group discussion sessions were an integral part of the training. Participants were divided into small groups and given case studies related to cyber threats that they had to analyze and solve. These discussions encouraged participants to collaborate, share perspectives, and apply the theories they had learned to real-life situations. The case studies also helped trainers evaluate the extent of participants' understanding of the material.

The fourth stage is evaluation and impact analysis, conducted using pre-tests and post-tests to measure the improvement in participants' understanding. The pre-test data provided an initial overview of participants' literacy levels, while the post-test results showed an increase in understanding after the training. This data was analyzed to provide additional insights that could be used for future program development.

The Merajut Nusantara Webinar Seminar with the theme "Cybersecurity: Safe Digital Practices" was organized by the Ministry of Communication and Information Technology (Kominfo) in collaboration with Commission I of the House of Representatives of the Republic of Indonesia (DPR RI). The entire webinar event was facilitated by Studio Intel Pasar Minggu, appointed by Kominfo, and located at Jalan Tlk. Peleng No.B/32, RT.4/RW.8, Pasar Minggu, South Jakarta, Special Capital Region of Jakarta, 12520. Atma Jaya Catholic University of Indonesia had previously collaborated with Studio Intel Pasar Minggu in organizing another national webinar titled "Building a Bright Future for Generation Z," which targeted high school students enrolled in the Industrial Engineering Study Program (Prasetya & Surbakti, 2023), as well as several similar webinar activities (Surbakti, 2024a, 2024b).

This community service event featured three speakers: H. Bambang Kristiono, S.E. (member of Commission I of the House of Representatives of the Republic of Indonesia), Feliks Prasepta Sejahtera Surbakti, S.T., M.T., PhD (lecturer at Atma Jaya Catholic University of Indonesia), and Freddy Tulung (Public Relations and Public Communication Practitioner), with M. Irsal Nurhuda serving as the moderator. The event flyer (a) and the presentation materials (b) delivered by Feliks Prasepta Sejahtera Surbakti, S.T., M.T., PhD, are shown in Figure 1. The event involved coordination with all speakers, the moderator, and participants from the general public. The majority of participants were constituents of H. Bambang Kristiono, S.E., representing the NTB 2 electoral district.

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

The training method used in this community service was not only aimed at increasing knowledge but also at providing practical skills that participants could immediately apply. The use of case simulations and visual aids such as infographics proved effective in enhancing participant engagement and making the material easier to understand.

Figure 1. Flyer and presentation materials

This activity was designed to be flexible and inclusive, making it accessible to participants with varying levels of digital literacy. By combining lectures, Q&A sessions, and group discussions, the training offered a comprehensive and practical learning experience. Overall, the community service method implemented successfully addressed the target audience's needs while making a tangible contribution to improving digital literacy. With a practice-based approach, participants not only understood the theory but were also able to apply it in their daily lives, thereby fostering a safer digital ecosystem.

Result and Discussion

The main outcome of this community service activity was the successful organization of the Merajut Nusantara seminar with the theme "Cybersecurity: Safe Digital Practices," which was attended primarily by participants from the NTB 2 electoral district. This national webinar was broadcast live via the Zoom platform (Figures 2, 3, and 4). As one of the keynote speakers, the author also delivered a presentation titled "Cybersecurity: Safe Digital Practices." In addition to Zoom, the event was also available for viewing on the YouTube channel: https://www.youtube.com/watch?v=hX339MM6y9c&t=5118s.

This community service activity successfully engaged 130 participants from various backgrounds, including students, professionals, and the general public. The program was designed to enhance digital literacy related to safe digital practices through interactive training and simulation-based education. The pre-test results showed that the participants' average level of understanding of digital security was 50, indicating limited basic knowledge of cyber threats and protective measures. After the training, the average post-test score increased to 85. The results of the pre-test and post-test calculations can be seen in Table 1.

One of the key findings from this activity was the participants' low initial awareness of simple practices such as using strong passwords and implementing two-factor authentication. Before the training, most participants used easily guessed passwords, such as

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

combinations of birthdates or names. After the training, participants began to understand the importance of using complex character combinations in passwords and the need to change them regularly. This finding is consistent with the studies by Monggilo et al. (2020), Kurnia and Astuti (2017), and Abdullah and Ikasari (2023), which highlight the importance of digital literacy in reducing the risk of cyberattacks.

Table 1. Evaluation of Community Service Program – Digital Literacy and Cybersecurity

Digital Skills Indicator	Pre-test (%)	Post-test (%)	Improvement (%)
Awareness of the importance of personal data protection	48	88	40
Understanding common cyber threats (phishing, malware)	50	85	35
Ability to secure devices and accounts	52	87	35
Use of strong and unique passwords	55	90	35
Safe internet usage practices	47	83	36
Knowledge of recovery steps after cyber incidents	48	84	36
Average across all indicators	**50**	**85**	**35**

The results presented in Table 1 indicate a significant improvement in participants' digital literacy related to cybersecurity following the training. The average score increased from 50% in the pre-test to 85% in the post-test, demonstrating a 35% gain across key digital skills. Notable improvements were observed in areas such as understanding cyber threats, securing accounts and devices, and practicing safe internet behavior. These findings suggest that the structured, simulation-based training method was highly effective in enhancing participants' knowledge and awareness of digital safety, making them more prepared to navigate and respond to cybersecurity risks in their daily lives.

The outcomes of this activity include a practical guide in the form of a digital module on safe digital practices, as well as recordings of the training sessions that participants can revisit. This guide is designed to help participants recall the security steps they have learned and apply them in their daily lives. In addition, the activity has led to a better understanding of the cyber threats commonly faced by the public, such as phishing and pharming.

The results of this training were also compared with previous literature. A study by Farid (2023) indicated that digital literacy combined with hands-on training can significantly enhance participants' awareness and technical capabilities. The outcomes of this activity support those findings, as participants not only understood the theory but were also able to apply security measures such as using password manager apps and regularly backing up data. However, the program also revealed some limitations. One of them was the limited training time, which prevented all topics from being discussed in depth. Some participants stated that they needed more time to grasp technical aspects such as data encryption and software security settings. Moreover, the varying levels of technological literacy among participants posed a challenge in delivering relevant materials to all groups.

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

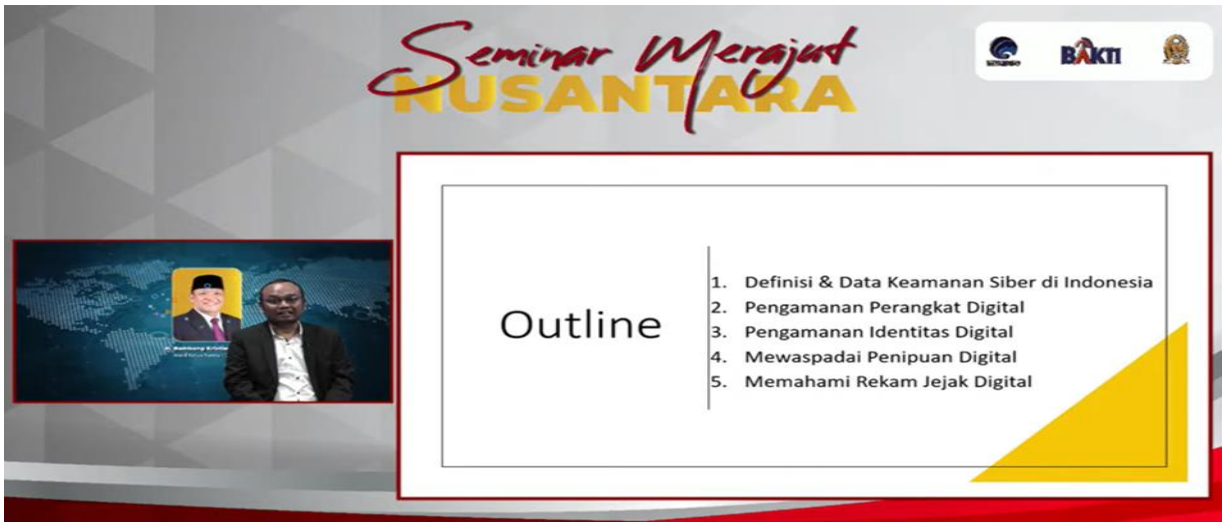

Figure 2. Delivering material in the national webinar

Figure 3. Screenshot view of participants

The discussion also highlights that safe digital practice training should be tailored to the specific needs of target groups. For example, students require a more visual and hands-on approach, while professionals may need more in-depth materials on digital risk management in the workplace. Such adjustments can improve the effectiveness of future training sessions. In terms of impact, the activity successfully boosted participants' confidence in facing digital security challenges. Most participants stated that they felt more prepared to recognize and avoid online scams after completing the training. This aligns with the research by Napu et al. (2024) and Lubis et al. (2023), which emphasize the importance of digital skills in supporting individual and community security.

This program also contributed to creating a safer digital ecosystem. With increased awareness among participants about the importance of digital security, it is hoped that they can become agents of change in their respective communities, spreading information and best practices they have learned. Research by Risdiana et al. (2024) supports this idea, showing that educated individuals can have a positive impact on their surroundings. Recommendations for future activities include expanding the program's reach to broader community groups, such as MSMEs and marginalized communities that may be more vulnerable to cyber threats.

Jurnal Pengabdian UNDIKMA:
Jurnal Hasil Pengabdian & Pemberdayaan kepada Masyarakat
https://e-journal.undikma.ac.id/index.php/jpu/index
Email: pengabdian@undikma.ac.id

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

Additionally, developing gamified training modules could be an engaging alternative to boost participant involvement and motivation.

It is also recommended to involve more institutions, such as schools and non-governmental organizations, in the implementation of this program. Such collaborations can increase the program's reach and impact. A study by Alfiana et al. (2023) shows that cross-sector collaboration is key to creating sustainable digital literacy programs. Overall, this community service activity has succeeded in improving participants' digital literacy in terms of security and safe digital practices. These findings provide a strong foundation for the development of future programs that can be more in-depth and reach wider community groups. With continuous evaluation and innovation, such programs have great potential to build a more resilient and digitally aware society in Indonesia.

Conclusion

This community service program successfully achieved its objective of enhancing participants' digital literacy, particularly in practicing safe digital behavior. The results of the activity showed a significant improvement in participants' understanding of cyber threats and preventive measures. The average post-test score increased from 50 to 85, reflecting the effectiveness of the training methods used, such as lectures, Q&A sessions, discussions, and case simulations. In addition, participants began to adopt basic security practices, such as using two-factor authentication and improving password management. Another finding from this activity was the initially low awareness among participants regarding the importance of protecting personal data and securing their digital devices. However, after the training, participants became more confident in facing cyber threats and more proactive in securing their information. The practical guide and training recordings provided as program outputs also received positive responses and are expected to assist participants in implementing the security steps they have learned.

Recommendation

To ensure the sustainability of the knowledge gained during the training, participants are encouraged to regularly apply safe digital practices in their daily online activities, such as using strong and unique passwords, enabling two-factor authentication, and being vigilant against phishing attempts. It is also recommended that participants stay updated on the latest cybersecurity threats by following credible sources and attending refresher sessions or webinars. In addition, participants can serve as digital literacy ambassadors within their communities by sharing key insights and encouraging others to adopt safe online behaviors. For long-term impact, it is advisable to periodically assess personal digital security practices and implement data backup routines to minimize the risk of data loss or breaches. For future community service programs, it is recommended to expand the program's scope by involving more community groups, such as students, MSMEs, and marginalized communities, who may be more vulnerable to cyber threats. Advanced training focusing on specific topics, such as data encryption and software security, can also be designed to enhance participants' technical understanding. In addition, the use of gamified training modules and interactive visual aids can increase participant engagement. Collaboration with educational institutions and local organizations is also essential to broaden the program's reach. With continuous evaluation and innovation in training methods, this community service initiative is expected to have a broader and more sustainable impact in creating a safer and more digitally responsive society.

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

Acknowledgements
The author expresses appreciation to the Ministry of Communication and Informatics and Commission 1 of the Indonesian House of Representatives (DPR RI) for the invitation to serve as a speaker.

References
Abdullah, M. S., & Ikasari, I. H. (2023). Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan. *JRIIN: Jurnal Riset Informatika dan Inovasi*, *1*(1), 96-98.

Afrina, C., Zulaikha, S. R., & Jumila. (2024). Low digital literacy in Indonesia: Online media content analysis. *Record and Library Journal*, *10*(2), 374-387.

Alfiana, A., Mulatsih, L. S., Kakaly, S., Rais, R., Husnita, L., & Asfahani, A. (2023). Pemberdayaan Masyarakat Dalam Mewujudkan Desa Edukasi Digital Di Era Teknologi. *Community Development Journal: Jurnal Pengabdian Masyarakat*, *4*(4), 7113-7120.

Dwiyanto, A. R. (2023). Prevalensi Penerapan RFC 9116 untuk Membantu Pengungkapan Kerentanan Keamanan Siber di Perguruan Tinggi Indonesia. *Jurnal Greenation Ilmu Teknik*, *1*(2), 52-59.

Ghosh, A., Diyasi, S., & Dey, D. (2023). Cybersecurity Literacy Programs for Marginalized Communities: Bridging the Gap in Digital Security. *Int. J. HIT. TRANSC: ECCN. Vol. 9*(1A), 29-44.

Hidayat, N., Widyaningrum, N., & Sarjito, A. (2021). Literasi Digital Dan Bela Negara: Sebuah Upaya Untuk Mencegah Hoax Dalam Sistem Pertahanan Negara. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(1), 32-41.

Khoirunnisa, K., & Jubaidi, D. (2024). Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. *Politeia: Journal of Public Administration and Political Science and International Relations*, *2*(2), 62-82.

Kurnia, N., & Astuti, S. I. (2017). Peta gerakan literasi digital di Indonesia: studi tentang pelaku, ragam kegiatan, kelompok sasaran dan mitra. *47*(2), 149-166.

Lubis, P., Mardianto, M., & Nasution, M. I. P. (2023). Gerakan Literasi Sekolah: Tantangan Literasi Di Era Digital Dan Cara Mengatasinya. *Jurnal Media Infotama*, *19*(2), 487-496.

Monggilo, Z. M. Z., Kurnia, N., & Banyumurti, I. (2020). Panduan Literasi Media Digital dan Keamanan Siber: Muda, Kreatif, dan Tangguh di Ruang Siber. *Jakarta: Badan Siber dan Sandi Negara*.

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha Kecil Menengah di Era Ekonomi Digital di Indonesia. *Sanskara Ekonomi dan Kewirausahaan*, *2*(03), 156-167.

Nasrullah, R. (2022). *Teori dan riset media siber (cybermedia)*. Prenada Media.

Nugroho, S., Fadhlia, T. N., Rahmat, W., Napitupulu, L., & Arief, Y. (2024). Model of cyber victimization: Study on college students in Indonesia. *The Open Psychology Journal*, *17*(1), 21-32.

Prasetya, W., & Surbakti, F. P. (2023). Pelaksanaan Kegiatan Pengabdian Masyarakat Webinar Nasional Building Bright Future for Generation Z bagi Siswa-Siswi SMA Jabodetabek. *Jurnal Pengabdian Masyarakat Charitas*, *3*(02), 45-52.

Vol. 6, No. 3 (August 2025)
E-ISSN : 2722-5097
Pg : 479-487

Putri, N. I., Komalasari, R., & Munawar, Z. (2020). Pentingnya keamanan data dalam intelijen bisnis. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(02), 41-48.

Risdiana, R., Setiawan, R., & Afrizal, S. (2024). Partisipasi Netizen pada Kesadaran Literasi Digital di Kecamatan Ciledug. *Edu Sociata: Jurnal Pendidikan Sosiologi*, *7*(1), 400-411.

Sendjaja, T., Irwandi, E. P., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity in the digital age: Developing robust strategies to protect against evolving global digital threats and cyber attacks. *International Journal of Science and Society*, *6*(1), 1008-1019.

Surbakti, F. P. S. (2024a). Edukasi Keamanan Siber Berdigital dengan Aman. *Prima Abdika: Jurnal Pengabdian Masyarakat*, *4*(4), 868-878.

Surbakti, F. P. S. (2024b). Edukasi Tantangan Transformasi Digital di Dunia Bisnis pada Masyarakat Dapil Sumatera Selatan 2. *Jurnal Abdimas Ekonomi dan Bisnis*, *4*(2), 175-182.