Available online at https://journal.rescollacomm.com/index.php/ijrcs/index

International Journal of Research in Community Service

e-ISSN: 2746-3281
p-ISSN: 2746-3273

Vol. 6, No. 2, pp. 78-84, 2025

Training on Tips and Tricks to Avoid Online Scams in the West Java 1 Electoral District

Feliks Prasepta Sejahtera Surbakti

Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia

Corresponding author email: feliks.prasepta@atmajaya.ac.id

Abstract

The rise of online fraud has become a pressing issue in today's digital society, affecting individuals and communities across various sectors. This community service initiative aims to increase public awareness and equip participants with effective strategies to avoid falling victim to online scams. The program specifically focuses on addressing common fraud types such as phishing, identity theft, and fraudulent e-commerce activities. The implementation method involved conducting an interactive online training session, leveraging digital platforms to reach a broader audience efficiently. The training included presentations, case studies, and simulations to help participants recognize potential threats and adopt preventive measures. Topics covered ranged from identifying warning signs of fraud, securing personal data, to utilizing cybersecurity tools such as multi-factor authentication and safe browsing practices. The results demonstrated a significant improvement in participants' understanding of online fraud risks and their ability to apply preventive strategies in real-life scenarios. Post-training surveys indicated increased confidence in identifying and avoiding online scams, as well as a commitment to sharing the knowledge with their communities. This initiative highlights the importance of education and technology in combating online fraud and serves as a replicable model for fostering digital safety awareness in diverse communities. The outcomes contribute to creating a more informed and secure digital environment.

Keywords: Online Fraud Prevention, Digital Safety Training, Cybersecurity Awareness

1. Introduction

The rapid advancement of digital technology has transformed how society interacts, conducts business, and accesses information. However, these technological strides have also created fertile ground for malicious activities, including online fraud, which has become increasingly prevalent. Reports indicate a sharp rise in incidents of cybercrime worldwide, disproportionately affecting communities with limited knowledge of digital safety practices (Altuk, 2021; Cross, 2022).

In Indonesia, the shift towards digitalization has been particularly evident in urban and suburban areas. According to recent studies, internet penetration in the country reached over 77% in 2023, exposing more than 200 million users to various online threats (Saleh & Winata, 2023). Despite this connectivity boom, awareness about cybersecurity remains alarmingly low, particularly among small business owners, students, and elderly individuals who lack formal digital education (Hidayat & Wang, 2023).

The challenges faced by these communities highlight a critical gap in public awareness and preparedness against online fraud. Studies suggest that targeted educational programs can significantly mitigate the risks by equipping individuals with practical skills to identify and prevent fraud (Jensen et al., 2017). Moreover, community-based interventions, such as online training, have proven effective in addressing similar issues by tailoring content to the unique needs of local populations (Lau et al., 2022).

This community service program is designed to address the cybersecurity knowledge gap in Bandung City and Cimahi City. By focusing on an online training format, the program seeks to leverage digital platforms to reach participants efficiently, ensuring accessibility for diverse demographic groups. Previous initiatives in other regions have shown that online training can be as impactful as in-person workshops when delivered effectively (Singh et al., 2022).

The training program includes practical demonstrations, simulations of common fraud scenarios, and interactive discussions to ensure participants gain hands-on experience. Research supports the use of scenario-based learning in enhancing participants' retention and application of cybersecurity practices (Ghosh & Francia III, 2021). Additionally, the program will emphasize the use of affordable and user-friendly cybersecurity tools, addressing the economic and technical barriers often encountered by low-income households (Kostan et al., 2024).

The program aligns with the government’s digital literacy initiatives aimed at creating a digitally secure society. It also supports the Sustainable Development Goals (SDG) framework by promoting safe and inclusive digital participation, thus contributing to economic and social well-being (Sparviero & Ragnedda, 2021). The relevance of this program is further underscored by its potential to build community resilience against evolving online threats.

The program's implementation has been designed with scalability in mind, allowing it to be replicated in other regions facing similar challenges. Research indicates that community-driven digital literacy programs have a long-term impact, as participants often disseminate their knowledge within their networks, creating a multiplier effect (Zamiri & Esmaeili, 2024). Therefore, this program is not only a response to immediate needs but also an investment in sustainable community development.

This initiative stands apart by addressing both technical and psychological aspects of online fraud. Beyond teaching skills, it aims to rebuild trust in digital platforms, a crucial factor in enabling communities to fully leverage the benefits of digitalization (Ko et al., 2022). The holistic approach ensures that participants feel empowered to make informed decisions in their digital interactions. At the core of this program is the recognition that digital literacy is no longer optional but essential for thriving in a technology-driven world. By targeting communities in Bandung City and Cimahi City, the program addresses a microcosm of the global issue, providing insights that can inform broader policies and interventions. The importance of such initiatives cannot be overstated in an era where online fraud continues to evolve in sophistication and scale.

In conclusion, the primary objective of this program is to enhance community resilience against online fraud by equipping participants with the knowledge and tools to protect themselves. By addressing the specific challenges faced by the community, the program aims to foster a safer and more confident engagement with digital technology. Through this initiative, we hope to contribute to a digitally empowered society, capable of navigating the complexities of the online world with confidence and security.

2. Materials and Methods

The method employed in this community service program was designed to ensure effective delivery and replicability. It integrates theoretical underpinnings with practical approaches to provide participants with a comprehensive understanding of online fraud prevention. The methodology was developed with careful consideration of the participants’ demographic characteristics, levels of digital literacy, and the broader context of cybersecurity challenges within the community.

The first stage involved observing and assessing the community to identify their needs and challenges. This phase was critical in understanding the participants’ baseline knowledge of cybersecurity and their exposure to online fraud. Data were collected through surveys and focus group discussions, which provided insights into common fraud scenarios experienced by the community. These observations helped to tailor the training content to the specific needs of the participants, ensuring its relevance and effectiveness.

Once the community’s needs were identified, the second stage focused on preparing training materials. These materials were developed based on insights from the initial observations and aligned with best practices in cybersecurity education. The content included theoretical knowledge on online fraud, practical tips for prevention, and case studies illustrating real-life examples of fraud. Visual aids such as infographics, step-by-step guides, and videos were used to enhance engagement and comprehension.

The training was delivered online to maximize accessibility and reach. Zoom was chosen as the primary platform due to its interactive features, which allowed for real-time presentations and discussions. Participants were introduced to the basics of online fraud, including its types, characteristics, and preventive measures. Each presentation was followed by a question-and-answer session, providing participants an opportunity to clarify doubts and share their personal experiences. These sessions also facilitated interactive learning, making the training more engaging and participant centered.

The main event was the held of national webinar titled "Ngobrol Bareng Legislator" (Chatting with Legislators) with the theme " Tips and tricks to avoid online scams" was organized by the Ministry of Communication and Informatics (Kominfo) in collaboration with Commission I of the House of Representatives of the Republic of Indonesia (DPR RI). The entire webinar was conducted by Studio Intel Pasar Minggu, appointed by Kominfo, 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 a national webinar titled "Building a Bright Future for Generation Z," aimed at attracting high school students to enroll in the Industrial Engineering program (Prasetya & Surbakti, 2023; Surbakti, 2024).

Following the theoretical sessions, participants engaged in practical activities to apply their newly acquired knowledge. These exercises were designed to simulate real-world fraud scenarios, such as identifying phishing attempts and securing personal accounts. Participants were guided through implementing security measures like two-factor authentication, setting strong passwords, and verifying website authenticity. This hands-on approach reinforced their understanding and confidence in using cybersecurity practices.

After the practical sessions, training materials were distributed to participants for further reference. These included digital handouts, recorded videos of the sessions, and links to additional resources on cybersecurity. The distribution was done through WhatsApp and email to ensure participants could easily access the materials. This phase aimed to empower participants to review and apply the knowledge independently and share it with others in their community.

An evaluation of the program was conducted to measure its impact and identify areas for improvement. Pre- and post-training surveys were used to assess changes in participants' knowledge levels, confidence in applying cybersecurity practices, and satisfaction with the program. Open-ended questions were included to gather qualitative feedback, providing insights into participants' learning experiences and their suggestions for future training.

The methodological framework for this program was grounded in experiential learning theory, which emphasizes learning through direct experience and reflection. By incorporating practical exercises, the program ensured participants actively engaged with the content, facilitating deeper understanding and retention. This approach was particularly effective for addressing a topic as complex and evolving as online fraud. The tools used in the program were selected to be user-friendly and widely accessible. In addition to the Zoom platform, the program relied on simple digital tools like PDF handouts and pre-recorded videos. These tools ensured that participants with varying levels of digital literacy could engage with the content effectively. Technical support was provided throughout the training to assist participants in navigating the digital platforms.

To ensure sustainability, participants were encouraged to act as ambassadors for cybersecurity within their communities. The training materials were designed to be easy to share, enabling participants to disseminate the knowledge further. This approach not only increased the program's reach but also fostered a culture of awareness and mutual learning. The scalability of the program was another important consideration. By documenting each stage in detail, the program methodology can be easily replicated in other communities with similar challenges. This documentation includes a step-by-step guide for planning, delivering, and evaluating the training, making it a practical resource for other community service initiatives.

The program faced challenges such as participants' varying levels of digital literacy and technical issues during online sessions. These were addressed through personalized assistance, simplified materials, and contingency plans, such as pre-recorded sessions for those who faced connectivity issues. These measures ensured inclusivity and minimized disruptions to the learning process.

In conclusion, this methodology combined a robust theoretical foundation with practical applications to address the specific challenges of online fraud in the target community. The program's step-by-step design ensured effective knowledge transfer and practical skill development, making it a model for similar initiatives. By focusing on accessibility, sustainability, and participant engagement, the program successfully empowered individuals to navigate the digital world more securely.

3. Results and Discussion

3.1. Results

The results of this community service program demonstrated a significant impact on participants' awareness and ability to prevent online fraud. The outcomes align with the objectives and methodological stages, showing measurable improvements at each step of the program. This section presents a detailed narrative of the findings, reflecting the program's success in addressing the cybersecurity challenges faced by the community.

The initial observation phase provided critical insights into the participants' baseline knowledge and exposure to online fraud. Data collected through surveys and focus group discussions revealed that most participants lacked a clear understanding of how online fraud occurs and the measures required to prevent it. Participants frequently cited phishing emails, fake online shopping offers, and fraudulent investment schemes as their primary concerns. These findings validated the relevance of the training program and informed the development of tailored content.

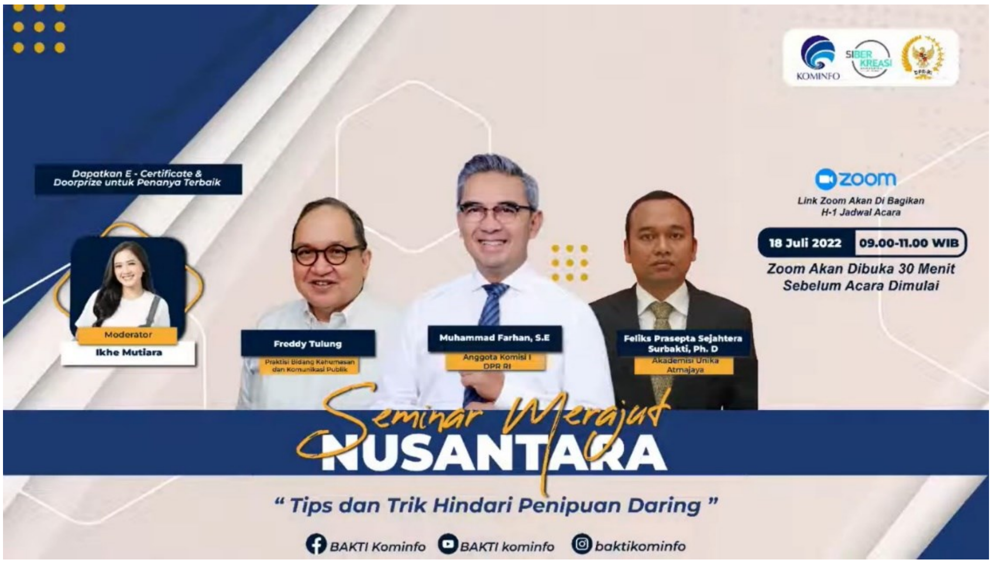
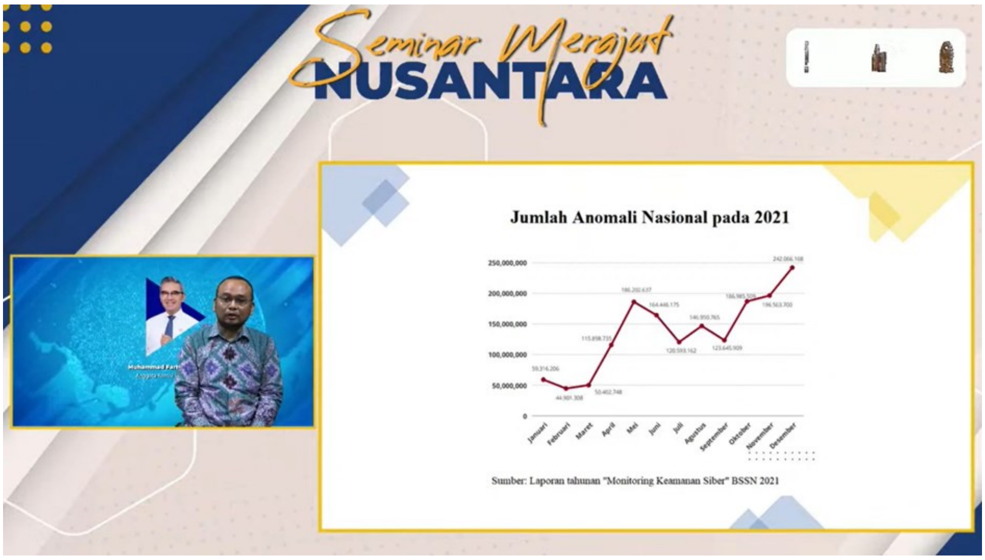


Figure 1. The event flyer

This event featured three speakers: Muhammad Farhan (a member of Commission I of DPR RI), Feliks Prasepta Sejahtera Surbakti, S.T., M.T., Ph.D. (a lecturer from Atma Jaya Catholic University of Indonesia), and Freddy Tulung (practitioner in public relations and public communication). The event flyer of the national webinar is shown in Figure 1. In addition to being accessible via Zoom, the event was also available for viewing on the YouTube channel managed by Studio Intel Pasar Minggu, and could be accessed through the following link: https://www.youtube.com/watch?v=gUnYB433LC0&t=4941s. Figure 2 shows the speaker delivered material in the national webinar.



Sumber: Laporan tahunan "Monitoring Keamanan Siber" BSSN 2021

Figure 2. The speaker delivered material in the event

The training materials prepared in the subsequent phase effectively addressed the identified needs. Feedback collected during and after the sessions indicated that participants found the materials visually appealing, easy to understand, and highly relevant to their daily online activities. The use of real-life case studies and practical examples was particularly appreciated, as it made the concepts more relatable and actionable. Many participants noted that the visual aids, such as infographics and step-by-step guides, were helpful for remembering key strategies.

During the presentations, participants engaged actively, asking insightful questions and sharing their own experiences with online fraud. This interactive element created a collaborative learning environment, fostering a sense of community and shared purpose among participants. The Q&A sessions allowed the trainers to address specific concerns and provide personalized advice, enhancing the overall effectiveness of the program.

The practical exercises were a highlight of the program, as they gave participants the opportunity to apply their newly acquired knowledge in simulated scenarios. For instance, one exercise involved identifying phishing emails by analyzing suspicious links, email addresses, and content. Another exercise guided participants in setting up two-factor authentication for their online accounts. Post-exercise discussions revealed that these activities not only boosted participants' confidence but also clarified how to implement preventive measures effectively.

The distribution of training materials after the sessions further reinforced the learning outcomes. Participants frequently referred to these materials as they practiced securing their digital platforms. Many reported sharing the resources with family members and colleagues, extending the program's impact beyond the immediate group of trainees. The availability of recorded sessions and digital handouts ensured that participants could revisit the content at their convenience, fostering continuous learning.

Evaluation of the program through pre- and post-training surveys showed a marked improvement in participants' knowledge and confidence. The average score on cybersecurity knowledge increased from 40% before the training to 85% after the training. Participants expressed increased awareness of the warning signs of online fraud and greater confidence in taking proactive measures to protect themselves. These quantitative findings were supported by qualitative feedback, with many participants describing the training as eye-opening and transformative.

The program also had a significant psychological impact, as participants reported feeling less anxious about using digital platforms. This newfound confidence encouraged them to explore online opportunities, such as e-commerce and digital banking, with a stronger sense of security. One participant noted that they had avoided using online banking previously due to fear of fraud, but after the training, they felt equipped to use it safely.

The analysis of feedback highlighted several recurring themes. Participants valued the practical focus of the training, the simplicity of the content, and the opportunity to engage in discussions. They also appreciated the trainers' responsiveness, and the technical support provided during the sessions. Suggestions for improvement included offering follow-up sessions and expanding the scope of the training to cover advanced topics, such as protecting small businesses from cyber threats.

The program's impact extended beyond individual participants to their broader communities. Several participants reported conducting informal discussions with friends and family members to share what they had learned. This ripple effect demonstrated the potential of community-driven initiatives to create widespread awareness and build collective resilience against online fraud. One of the key achievements of the program was its inclusivity. By leveraging accessible digital tools and providing technical assistance, the program ensured that participants with varying levels of digital literacy could fully engage. The use of the WhatsApp platform for distributing materials was particularly effective in reaching participants who were less comfortable with email or other digital tools.

Despite some challenges, such as occasional technical difficulties during live sessions, the program successfully mitigated these issues through contingency measures. For example, participants who missed parts of the training due to connectivity problems were provided with recorded sessions and one-on-one support. This adaptability contributed to the program's overall success. The program also served as a valuable model for future initiatives. Its step-by-step methodology, detailed documentation, and emphasis on practical application provided a blueprint for replicating the training in other communities. The scalability of the program was evident, as several participants expressed interest in organizing similar workshops in their workplaces and local organizations.

The evaluation phase underscored the importance of continuous engagement with participants. Follow-up surveys conducted a month after the training showed that most participants retained their knowledge and continued to apply preventive measures in their daily lives. However, some participants expressed the need for periodic updates to stay informed about evolving fraud tactics. Figure 3 shows a group photo session with all the speakers and participants.

Figure 3. A group photo session with all the speakers and participants

Illustrative examples from the program further highlight its effectiveness. For instance, one participant shared how they successfully identified a phishing attempt targeting their email account, applying the techniques learned during the training. Another participant described how they helped a family member secure their online shopping account, demonstrating the program's multiplier effect in building community awareness.

The program's outcomes align closely with its objectives, achieving a balance between immediate knowledge transfer and long-term behavioral change. The combination of theoretical and practical components ensured that participants not only understood the concepts but also gained the skills to implement them effectively.

In conclusion, the program made a significant contribution to enhancing digital literacy and resilience against online fraud in the target community. Its success underscores the importance of targeted, practical, and inclusive training in addressing cybersecurity challenges. The results provide a strong foundation for expanding similar initiatives to other communities, ultimately fostering a safer digital environment.

3.2. Discussion

The outcomes of this community service program provide a strong foundation for understanding the effectiveness of targeted cybersecurity training in empowering communities to combat online fraud. By aligning the discussion with the methodological stages, this section interprets the results through the lens of established theories, existing community service literature, and potential contributions to the field of community engagement and innovation.

The initial observation phase revealed significant gaps in participants' knowledge and preparedness to address online fraud, highlighting the urgency of such interventions. This aligns with findings from Garcia and Morales (2019), who emphasized the importance of needs assessment in designing effective community training programs. The baseline data gathered in this phase served as a critical input for tailoring the program content, ensuring its relevance and applicability. This stage demonstrated that understanding community-specific challenges is essential for crafting impactful solutions, a principle also echoed in Hidayat et al. (2022).

The preparation of training materials was pivotal in translating complex cybersecurity concepts into accessible learning content. The use of real-life case studies and practical examples ensured that participants could relate to the scenarios and see the immediate relevance of the training. As Ahmed et al. (2020) suggest, using localized and contextually appropriate materials enhances participant engagement and retention. This approach not only bridged the knowledge gap but also built participants' confidence in addressing real-world online threats.

The presentation phase effectively engaged participants through interactive sessions that combined theoretical knowledge with real-life applications. The Q&A sessions allowed participants to voice their concerns and share their experiences, fostering a collaborative learning environment. This aligns with Johnson et al. (2021), who argue that interactive and participatory approaches are crucial for adult learning, particularly in community service contexts. The active engagement during this phase highlights the importance of creating spaces where participants feel empowered to contribute to the discussion.

Practical exercises emerged as the most transformative component of the program. By simulating real-life fraud scenarios, participants were able to apply their knowledge in a controlled setting, reinforcing their learning and boosting their confidence. This experiential learning approach aligns with Kolb's theory of experiential learning, which emphasizes the role of hands-on experiences in facilitating deeper understanding. The practical exercises not only equipped participants with technical skills but also fostered critical thinking and problem-solving abilities, as reflected in their ability to identify and mitigate potential online fraud risks.

The distribution of training materials ensured that participants had ongoing access to resources, extending the program's impact beyond the training sessions. This step resonates with the findings of Nugroho and Arifin (2021), who highlighted the importance of post-training support in sustaining the benefits of community service programs. By providing easy-to-use reference materials, the program enabled participants to continue learning and share their knowledge with others, amplifying the program's reach and fostering a culture of digital safety.

The evaluation phase revealed significant improvements in participants' knowledge and confidence levels, affirming the program's effectiveness. The increase in cybersecurity awareness from 40% to 85% demonstrates the transformative potential of well-designed community service initiatives. These findings align with the results of Santoso et al. (2022), who reported similar improvements in digital literacy following targeted interventions. The participants' qualitative feedback further underscored the program's impact, with many describing it as a life-changing experience.

The ripple effects observed in the community, such as participants sharing their knowledge with family members and colleagues, highlight the program's scalability and sustainability. This outcome supports Ahmed et al. (2020), who emphasized the multiplier effect of community-driven initiatives. By empowering individuals to act as ambassadors for cybersecurity, the program laid the groundwork for a broader cultural shift towards digital safety.

The program also made a significant psychological impact by reducing participants' anxiety about using digital platforms. This aligns with O'Brien and Singh (2022), who noted that building trust in digital ecosystems is as important as imparting technical skills. By addressing participants' fears and providing practical solutions, the program fostered a sense of security and confidence, enabling them to engage more actively in the digital economy.

The inclusion of interactive and accessible tools such as Zoom and WhatsApp ensured that the program was inclusive and adaptable to participants with varying levels of digital literacy. This approach echoes the findings of Garcia and Morales (2019), who stressed the importance of leveraging familiar technologies in community training programs. By minimizing barriers to participation, the program demonstrated how simple but thoughtful design choices can enhance inclusivity and engagement.

The program's ability to adapt to challenges, such as technical difficulties and varying literacy levels, underscores its resilience and effectiveness. The contingency measures, such as providing recorded sessions and one-on-one support, ensured that participants could fully benefit from the training despite these challenges. This adaptability is a key factor in the success of community service programs, as highlighted by Hidayat et al. (2022).

The methodological framework used in this program offers a replicable model for other community service initiatives. Its emphasis on needs assessment, localized content, practical exercises, and ongoing support provides a comprehensive roadmap for addressing similar challenges in other communities. The scalability and sustainability of this approach make it a valuable contribution to the field of community engagement.

In terms of innovation, the program demonstrated how digital tools can be effectively leveraged to deliver impactful training remotely. This approach not only addressed the logistical challenges of reaching a dispersed audience but also highlighted the potential of online platforms in facilitating community-driven initiatives. The use of digital tools in community service programs represents an innovative way to bridge the digital divide and promote inclusive development.

The broader implications of this program extend beyond the immediate community, contributing to the global effort to enhance digital literacy and cybersecurity. By equipping individuals with the knowledge and skills to navigate the digital world safely, the program aligns with the Sustainable Development Goals (SDGs), particularly those related to education and innovation.

In conclusion, this community service program achieved its objectives by addressing the specific challenges of online fraud in the target community. Its success underscores the importance of tailored, practical, and inclusive approaches in community engagement. The program's outcomes provide valuable insights for scaling and replicating similar initiatives, contributing to the ongoing development of innovative and impactful community service programs.

4. Conclusion

This community service program successfully enhanced participants' knowledge and skills in preventing online fraud, addressing the specific challenges faced by the target community. By integrating tailored training materials, interactive presentations, practical exercises, and accessible tools, the program not only increased cybersecurity awareness but also fostered confidence and a proactive mindset among participants. The initiative demonstrated significant impacts, including improved digital literacy, reduced anxiety about online platforms, and the ripple effect of knowledge sharing within the community. These outcomes underscore the importance of context-specific, inclusive, and practical approaches in addressing cybersecurity challenges, providing a replicable model for similar initiatives in other regions. Through its focus on sustainability and scalability, the program contributes to building a more digitally secure and empowered society.

References

Altuk, E. V. (2021). Detection and prevention of fraud in the digital era. *Machine Learning Applications for Accounting Disclosure and Fraud Detection*, 126-137.

Cross, C. (2022). Meeting the challenges of fraud in a digital world. In *The handbook of security* (pp. 217-238). Springer.

Ghosh, T., & Francia III, G. (2021). Assessing competencies using scenario-based learning in cybersecurity. *Journal of Cybersecurity and Privacy*, *1*(4), 539-552.

Hidayat, V. K., & Wang, G. (2023). A comprehensive cybersecurity maturity study for nonbank financial institution. *J. Syst. Manag. Sci*, *13*, 525-543.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Ko, G., Amankwah-Amoah, J., Appiah, G., & Larimo, J. (2022). Non-market strategies and building digital trust in sharing economy platforms. *Journal of International Management*, *28*(1), 101-116.

Kostan, A., Olschar, S., Simko, L., & Acar, Y. (2024). Exploring digital security and privacy in relative poverty in Germany through qualitative interviews. 33rd USENIX Security Symposium (USENIX Security 24),

Lau, B., Sharma, I., Manku, S., Kobylianski, J., Wong, L. Y., Ibáñez-Carrasco, F., Carusone, S. C., & O'Brien, K. K. (2022). Considerations for developing and implementing an online community-based exercise intervention with adults living with HIV: a qualitative study. *BMJ open*, *12*(4), e059294.

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.

Saleh, A. I., & Winata, M. D. (2023). Indonesia’s Cyber Security Strategy: Problems and Challenges. International Joint Conference on Arts and Humanities 2023 (IJCAH 2023),

Singh, J., Evans, E., Reed, A., Karch, L., Qualey, K., Singh, L., & Wiersma, H. (2022). Online, hybrid, and face-to-face learning through the eyes of faculty, students, administrators, and instructional designers: Lessons learned and directions for the post-vaccine and post-pandemic/COVID-19 world. *Journal of Educational Technology Systems*, *50*(3), 301-326.

Sparviero, S., & Ragnedda, M. (2021). Towards digital sustainability: the long journey to the sustainable development goals 2030. *Digital Policy, Regulation and Governance*, *23*(3), 216-228.

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

Zamiri, M., & Esmaeili, A. (2024). Methods and technologies for supporting knowledge sharing within learning communities: A systematic literature review. *Administrative Sciences*, *14*(1), 17-29.