Vox Populi: Jurnal Umum Pengabdian Kepada Masyarakat
E-ISSN: 3032-3606
Vol 2, No 2, Juli 2025. pp. 70-76
DOI: doi.org/10.70308/voxpopuli.v2i2.117

Cybersecurity Education: Protecting Personal Data And Recognizing Fraud Modes On Facebook Social Media In Pkk Women In Bukit Subur Merangin Village

Edukasi Keamanan Siber: Melindungi Data Diri Dan Mengenali Modus Penipuan Di Media Sosial Facebook Pada Ibu-Ibu Pkk Desa Bukit Subur Merangin

[1]Ichsandi
[2]Hawari Alhaq
[3]Widja Yanto
[4]Lily Indria
[5]Adinda Maria Ulfa

[1,2,3,4,5]Fakultas Sains dan Teknologi, Universitas Merangin
Email Correspondence: Ichsandi.m.kom@gmail.com

*Correspondence Writer

ARTICLE INFO:

Article History:
Diterima: 15 Mei 2025
Direvisi: 28 Mei 2025
Diterima: 13 Juni 2025

Keywords:
Cybersecurity, Education, Online Fraud, Social Media, Facebook, PKK, Digital Literacy.

Kata Kunci:
Keamanan Siber, Edukasi, Penipuan Daring, Media Sosial, Facebook, PKK, Literasi Digital.

Abstract:
Cybersecurity is a crucial issue in the digital era, especially for communities actively using social media platforms such as Facebook. The PKK mothers of Bukit Subur Village, Merangin, represent a group vulnerable to fraud and misuse of personal data online. This community service activity aims to enhance the understanding and awareness of PKK mothers regarding the importance of protecting personal data and recognizing various fraud schemes prevalent on Facebook. The methods employed include interactive education through counseling, discussions, and case simulations. The results of the activity show an increase in participants' knowledge and vigilance towards cybersecurity risks, as well as their ability to identify and avoid fraud schemes on social media. This initiative is expected to foster a better digital literacy culture within the Bukit Subur Village community.

Abstrak:
Keamanan siber merupakan isu krusial di era digital, terutama bagi masyarakat yang aktif menggunakan platform media sosial seperti Facebook. Ibu-ibu PKK Desa Bukit Subur, Merangin, merupakan kelompok yang rentan terhadap penipuan dan penyalahgunaan data pribadi secara daring. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pemahaman dan kesadaran ibu-ibu PKK terhadap pentingnya melindungi data pribadi serta mengenali berbagai modus penipuan yang marak terjadi di Facebook. Metode yang digunakan meliputi edukasi interaktif melalui penyuluhan, diskusi, dan simulasi kasus. Hasil kegiatan menunjukkan peningkatan pengetahuan dan kewaspadaan peserta terhadap risiko keamanan siber, serta kemampuan mereka dalam mengidentifikasi dan menghindari skema penipuan di media sosial. Inisiatif ini diharapkan dapat menumbuhkan budaya literasi digital yang lebih baik di lingkungan masyarakat Desa Bukit Subur.

INTRODUCTION

The rapid development of information and communication technology has encouraged people to be more active in using social media as a means of communication, sharing information, and carrying out economic activities. One of the most widely used platforms in Indonesia is Facebook, which is not only used for socializing, but also for community activities such as the PKK at the village level. However, behind these conveniences and benefits, there are threatening cybersecurity risks, especially related to personal data protection and the rise of digital fraud modes (Rifqy et al., 2023).

Cases of leakage and misuse of personal data on social media are increasingly frequent, both due to users' negligence in maintaining the confidentiality of personal information and due to increasingly sophisticated cyber attacks. Research shows that the protection of personal data on social media is essential to prevent misuse that can harm users, such as identity theft, fraud, and the spread of false information (Lubis et al., 2023). Legal protection efforts against the misuse of personal data have indeed been implemented, but adequate awareness and education are still needed so that people are able to protect themselves independently.

In addition to the risk of data leakage, digital fraud modes that utilize social media are also increasingly diverse. Social media-based online fraud often targets groups of people who lack digital literacy, such as housewives, with various modes ranging from part-time job offers, fake lotteries, to unauthorized requests for personal data (Utomo et al., 2024). Lack of understanding of the characteristics of digital fraud and low digital literacy make the community, especially PKK women, a vulnerable group to become victims of cybercrime (Suryati et al., 2024).

Strong digital literacy is the main key to facing cybersecurity challenges in the digital era. Through structured education, people can be equipped with knowledge and skills to recognize and avoid various digital threats, including basic security practices such as using strong passwords, not carelessly sharing personal information, and being wary of suspicious links or messages (Qolbi & Kabetta, 2024). Cybersecurity education and socialization programs carried out directly in the community have proven to be effective in increasing participants' knowledge, awareness, and awareness of cybercrime risks (Kurniati et al., n.d.).

Based on this background, this community service activity aims to provide education related to cybersecurity, especially in protecting personal data and recognizing fraud modes on Facebook social media to PKK women in Bukit Subur Merangin Village. It is hoped that through this activity, the participants can improve digital literacy, understand the importance of personal data protection, and be able to identify and avoid various modes of fraud circulating on social media.

This community service activity is designed with the aim of having a real impact on PKK women in Bukit Subur Merangin Village in facing cybersecurity challenges. The goals to be achieved include:

1. Increase the understanding of PKK women about the importance of personal data protection when using Facebook in order to prevent the misuse of personal information.

2. Equip participants with practical skills to recognize various modes of online fraud, such as fake offers and fraudulent sweepstakes, so that they can independently identify and reject fraudulent attempts.
3. Fostering strong digital literacy awareness to strengthen critical attitudes and vigilance in interacting on social media.
4. Encourage the implementation of basic cybersecurity practices, including the use of strong passwords and two-factor authentication, in everyday online activities.
5. Building a support network between PKK members as a forum for sharing experiences and solutions related to cybersecurity issues in the village environment.

RESEARCH METHODS

The implementation method in the activity "Cyber Security Education: Protecting Personal Data and Recognizing Fraud Modes on Facebook Social Media in PKK Women in Bukit Subur Merangin Village" integrates several stages with theoretical and practical approaches to achieve comprehensive educational goals.

1. Preparation and Planning

(Idris et al., n.d.) (Idris et al., n.d.)

2. Interactive Lectures

The interactive lecture lasted 60 minutes by explaining the basic concepts of cybersecurity, the types of threats such as phishing, malware, and social engineering, and the importance of strong password management. The presentation was accompanied by real case studies to raise awareness among participants, followed by a short Q&A session every 15 minutes to maintain active participation.

3. Live Demonstrations

Unlike conventional lectures, the live demonstration was carried out by displaying a dummy Facebook account and demonstrating how to enable two-factor authentication, check privacy settings, and recognize phishing links in incoming messages. Participants are guided step by step while imitating on their respective devices.

4. Focus Group Discussions

Participants were divided into groups of 4–5 people to discuss case studies of fraud such as fake sweepstakes and personal data request modes. The facilitator provides criteria for fraud mode characteristics to help participants compile a list of security verifications before interacting online.

Gambar 1 Diskusi Kelompok

5. Phishing Case Simulation

Each group receives a phishing message scenario in the form of a text that resembles a bank notification or a gift invitation. The group was asked to identify

signs of suspicion, design a safe reply, and report attack patterns to the discussion group. This stage aims to train rapid detection and response skills to cyber threats.
6. Q&A and Mentoring

The open session provides 30 minutes for technical questions, such as Facebook's security settings and how to use the suspicious content reporting feature. Intensive mentoring allows participants to practice the steps described directly with mentor guidance.

Gambar 2 Sesi Tanya Jawab

7. Evaluation and Measurement of Results

The evaluation was carried out in three stages:

Pre-Test: A short multiple-choice question before the material is delivered to measure the participants' initial knowledge of cybersecurity.

Formative Assessment: Observation of discussion participation and simulation during activities to assess direct engagement and understanding.

Post-Test: A short test after the entire material is completed, comparing the score with the pre-test to quantitatively calculate knowledge improvement.

The results of the pre-test and post-test were analyzed to evaluate the effectiveness of the training method, with a target of a minimum score increase of 30% in participants.

8. Documentation and Reporting

All activities are documented in photos, videos, and discussion notes. The final report includes a graph of pre-test vs post-test score improvement, a summary of participant feedback, and follow-up recommendations in the form of digital health modules for advanced counseling in the village..

DISCUSSION

Result

1. Participant Demographics

The socialization activity was attended by 30 PKK women from Bukit Subur Merangin Village with an age range of 35-60 years and an elementary to high school education background. All participants actively use Facebook as their primary social media in their daily activities.

2. Evaluation Results (Pre-test and Post-test)

The evaluation was carried out through a pre-test and post-test in the form of 20 multiple-choice questions that included basic cybersecurity concepts, password management, phishing recognition, and how to report suspicious content. The following table summarizes the results of participant scores:

Table 1. Participant Score Results

Score	Pre-test (n=30)	Post-test (n=30)	Change (%)

20–40	8 participants	1 participant	–
41–60	15 participants	4 participants	–
61–80	6 participants	16 participants	–
81–100	1 participant	9 participants	–
Average	52,3	73,8	↑ 41%

From the table, it can be seen that the average score of participants increased by 21.5 points (41%) which indicates the effectiveness of the training method in improving cybersecurity knowledge.

Discussion

1 Knowledge Enhancement

The average post-test score increased significantly compared to the pre-test, especially in terms of phishing feature recognition and Facebook's privacy settings. As many as 83% of participants who initially scored below 60, rose to the range of 61–100 after the training, demonstrating their understanding of personal data security materials.

Gambar 3 Sesi Post-test dan Pre-test

2 Readiness to Identify Fraud Modes

Before the training, 27% of participants had never heard of the term "phishing" and only 10% were able to name the basic characteristics of digital fraud. After the training, 93% of participants managed to identify at least three characteristics of phishing messages, such as suspicious links, requests for personal data, and urgent language.

3 Practical Implementation

Participants directly activate two-step verification on the dummy Facebook account. In the simulation session, 90% of participants were able to disable the "login from unknown device" feature and update passwords with criteria of at least 8 characters, numbers, and symbols. This indicates a good transfer of practical skills.

4 Obstacles and Solutions

Some participants faced internet network problems so that the online simulation was not smooth. The proposed solution is to reschedule online practice sessions at a location with a stable connection and provide a print module for self-pacers.

5. Follow-Up

Continuous Mentoring: Hold follow-up sessions every three months to strengthen understanding and update the module according to the development of fraud mode.

Formation of Peer-Learning Groups: Facilitate WhatsApp groups between members to share experiences and remind each other of security practices.

Digital Module Creation: Compile interactive modules in PDF format and video tutorials to facilitate access to information outside of face-to-face sessions.

With positive evaluation results, this activity has been proven to increase digital literacy and readiness of PKK women in Bukit Subur Merangin Village in facing cybersecurity threats on Facebook, so that it is expected to strengthen the digital resilience of the village community.

CONCLUSION

Based on the results of the evaluation and discussion of cybersecurity education activities for PKK women in Bukit Subur Merangin Village, it can be concluded that this program has succeeded in increasing digital literacy and practical skills of participants in protecting personal data and recognizing fraud modes on Facebook significantly. The average post-test score increased by 41%, demonstrating the effectiveness of interactive and applicable training materials and methods in facilitating the understanding of cybersecurity concepts. Hands-on practices such as phishing simulations and privacy settings demonstrations were shown to strengthen skills transfer, with 93% of participants able to identify at least three characteristics of phishing messages after training. In addition, the implementation of two-step verification and stronger password management by the majority of participants signaled the adoption of basic security practices in everyday digital life.

Technical constraints such as unstable internet connectivity can be overcome through print modules and rescheduling online sessions in locations with better signals, so that material accessibility is maintained for all participants. Peer-learning support through WhatsApp groups also supports sustainability, raising awareness and sharing solutions related to cybersecurity challenges. For follow-up, it is recommended to hold periodic reinforcement sessions every three months and develop digital-based interactive modules to adjust to the development of new fraud modes.

Overall, this activity has succeeded in building a stronger foundation of cybersecurity literacy among PKK women in Bukit Subur Merangin Village, so that it can increase the digital resilience of the village community in facing cyber threats in the future.

BIBLIOGRAPHY

Idris, H., Anwar, A., Dunakhir, S., & Idrus, M. (n.d.). *PKM Sosialisasi Keamanan Berinternet dan Potensi Pencurian Data Bagi Pelajar Pada SMA Negeri 1 Tinambung Sulawesi Barat*. www.ncsi.ega.ee.

Kurniati, I., Dharmalau, A., Suryantoro, H., Sari, J., Ningtyas, S., Khoriyah, K., Winarno, H., & Ar-Rasyid, H. (n.d.). *Edukasi Keamanan Siber Di Komunitas Young Ozer Indonesia Sebagai Upaya Mengurangi Risiko Tindak Kejahatan Siber*.

Lubis, S. N., Irwan, M., & Nasution, P. (2023). Analisis Penyalahgunaan Data Pribadi Dalam Menggunakan Media Sosial. *JoSES: Journal of Sharia Economics Scholar, 2*(2), 75–78. https://doi.org/10.5281/zenodo.12527836

Qolbi, N., & Kabetta, H. (2024). PLATFORM EDUKASI KEAMANAN SIBER BERBASIS WEB BERDASARKAN KERANGKA GLOBAL LITERASI DIGITAL UNESCO. *Jurnal INTEKNA*, *24*(2). http://ejurnal.poliban.ac.id/index.php/intekna/issue/archive

Rifqy, M., Arham, H., & Risal, M. C. (2023). PERLINDUNGAN DATA PRIBADI BAGI PENGGUNA MEDIA SOSIAL. *Jurnal Al Tasyri'iyyah*, *3*(2).

Satria, D., & Chandra, F. (2024). Sosialisasi Penggunaan Media Sosial Secara Bijak Berdasarkan Undang-Undang Ite di Desa Sungai Ulak. *Vox Populi: Jurnal Umum Pengabdian Kepada Masyarakat*, *1*(2), 87-96. https://doi.org/10.70308/voxpopuli.v1i2.72

Satria, D. (2024). Penyuluhan Komunikasi dalam Antisipasi Efek Negatif Pemaparan Pornografi di Media Online dan Pengaruhnya Terhadap Perilaku Generasi Milenial Desa Sungai Ulak. *Vox Populi: Jurnal Umum Pengabdian Kepada Masyarakat*, *1*(1), 29-49. https://doi.org/10.70308/voxpopuli.v1i1.22

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

Suryati, S., Sardana, L., Disurya, R., & Putra, Y. S. (2024). Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law). *Wajah Hukum*, *8*(1), 84. https://doi.org/10.33087/wjh.v8i1.1447

Utomo, F. W., Rorin, D., Insana, M., & Mayndarto, E. C. (2024). Mekanisme penipuan digital pada masyarakat era 5.0 (studi kasus penipuan online berbasis lowongan kerja paruh waktu yang merebak di masyarakat). *Jurnal Ilmiah WUNY*, *6*(1). https://doi.org/10.21831/jwuny.v6i1