Optimizing Digital Communication in Dealing with Cybercrime for the Visually Impaired

Nani Nurani Muksin[1], Siska Yuningsih[2], Fitria Rosmi[3], Khalid Pirmansyah[4]
[1,2,4]Ilmu Komunikasi, FISIP, Universitas Muhammadiyah Jakarta,[3]PGSD, Fakultas Ilmu Pendidikan,
Universitas Muhammadiyah Jakarta
E-mail: naninuranimuksin@umj.ac.id

Abstract

The advancement of digital technology in the cyber era has opened up wide access to information, communication, and digital services. However, this progress has also given rise to challenges in the form of increasing cybercrime targeting vulnerable groups, including people with visual sensory disabilities. Limitations in receiving visual information make this group more vulnerable to threats such as phishing, theft of personal data, and digital fraud. In response to this, a community service activity entitled "Optimizing Digital Communication in Dealing with Cybercrime for People with Visual Sensory Disabilities" was held at the Raudhatul Makfufin Foundation, South Tangerang on June 15, 2025. This activity was attended by 37 blind participants aged 17-60 years, most of whom were active users of screen reader-based digital technology. The training method was carried out in a participatory manner through the delivery of materials, discussions, and simulations. The results of the training showed an increase in participants' understanding of various forms of cybercrime as well as the ability to recognize and anticipate digital crime modes. The training also equipped participants with secure digital communication skills, including the use of two-factor authentication and security applications. It is hoped that this activity can increase inclusive digital literacy and strengthen cyber resilience for the blind sensory disability community.

Keywords: Optimization, Digital communication, Countering cybercrime

INTRODUCTION

Digital transformation has become a major marker of today's rapidly developing cyber era. Advances in communication and information technology have opened up wide access to information sources, social networks, and public services that were previously difficult for some people to reach (Mokobombang et al., 2023). In this context, people with disabilities, especially those with visual sensory disabilities, benefit significantly from the increasingly inclusive advancement of digital technology. Technologies such as screen readers (screen reader), text-to-speech converters, and accessibility features on mobile devices allow them to access information, communicate, and participate in socio-economic life more independently. However, this progress also brings new consequences, namely increased vulnerability to increasingly complex and organized cybercrime (Iskandar et al., 2023).

Cyber crime or cybercrime covers various forms of legal violations committed through digital media, ranging from online fraud, identity theft, hacking of personal data, to the spread of false information (hoax) and content manipulation on social media (Saramuke et al., 2025). This phenomenon continues to grow along with the increasing number of internet users worldwide. Quoted from Cybercrime Magazine, the report Cybersecurity Ventures Estimates that global losses from cybercrime will reach USD 10.5 trillion per year by 2025. The group of blind sensory disabilities is included in the category of internet users who are at high risk of digital crime, especially because of their limitations in recognizing visual warning signs which are one of the main protection mechanisms in digital security systems, such as suspicious URLs, security icons, or inauthentic site designs (Wosah et al., 2024).

In addition to visual impairments, studies have shown that low digital literacy and a lack of inclusive cybersecurity training make people with disabilities more vulnerable to digital threats (Furnell et al., 2021; Sharevski, 2024). Most cybersecurity education campaigns and programs are aimed at general users without considering the specific needs of groups with sensory impairments. As a result, many people with visual impairments are unaware of the potential digital risks they face in everyday activities, such as shopping online, receiving messages from unknown numbers, or accessing websites without secure encryption.

In the context of Indonesia, where awareness of digital security is still relatively low among the general public, people with disabilities face greater challenges. A study by the Katadata Insight Center in Romadhianti et al. (2021) showed that only around 23% of respondents with disabilities admitted to having received digital literacy training, including on the threat of cybercrime. In fact, digital communication is not only related to the technical ability to use devices, but also involves aspects of security, ethics, and social responsibility. Therefore, efforts to strengthen digital communication for people with disabilities cannot be postponed any longer and need to be supported by contextual, participatory, and real-needs-based training.

Responding to these challenges, community service activities entitled"Optimizing Digital Communication in Dealing with Cybercrime for People with Visual Sensory Disabilities"was held as a form of scientific and social contribution in increasing awareness and safe and inclusive digital skills. This activity was held on Sunday, June 15, 2025 at the Raudhatul Makfufin Foundation, Serpong District, South Tangerang City, which is an educational and empowerment institution for the blind. The Raudhatul Makfufin Foundation is an institution for the blind that applies more to the religious field. This foundation aims to become a forum for the blind in the religious field and strives to create welfare among Muslim blind people. This training activity was attended by 37 participants with an age range of 17-60 years, most of whom are active users of digital technology through screen reader-based mobile devices.

The training was designed to equip participants with soft skills and practical skills in dealing with cybercrime, including recognizing forms of digital fraud, understanding how safe social media works, managing personal data, and using security features such as two-factor authentication and data protection applications. The main material was delivered by lecturers of Communication Science at the University of Muhammadiyah Jakarta, with an experience-based approach and real case simulations. The results of this activity showed that participants experienced a significant increase in their understanding of cyber risks and preventive strategies that can be carried out independently. In addition, interactive discussions in the training also encouraged participants to be more active in sharing their experiences in dealing with everyday digital communication challenges.

Thus, this activity is not only a learning medium, but also a forum for empowering the disabled community in facing digital challenges more critically and adaptively. This training is expected to be a model of educational intervention that can be replicated in other regions as part of an inclusive and socially just digital development agenda. Optimizing digital communication for people with disabilities is not only about access, but also about protection, independence, and recognition of their rights as citizens in the digital space.

IMPLEMENTATION METHOD

This community service activity uses an educational-participatory approach with a pretest-posttest based training and evaluation method to measure the effectiveness of increasing participants' understanding of safe digital communication in dealing with cybercrime. This training was held in one day, precisely on Sunday, June 15, 2025, at the Raudhatul Muffin Foundation, Serpong District, South Tangerang City. This activity was attended by 37 participants with visual sensory disabilities ranging in age from 17 to 60 years, most of whom are active users of screen reader-based digital devices.

Activity Design

The activity consists of three main stages, namely:

1. The preparation stage includes preparing training materials, developing evaluation instruments, and coordinating with organizing partners.
2. The implementation stage includes interactive presentation of material and direct practice on:
   a. Ethics and security in digital communications
   b. Types of cybercrime (phishing, digital fraud, personal data theft)
   c. Strategies for recognizing and avoiding digital crime modes

d. Use of security apps, two-factor authentication, and privacy management
3. The evaluation stage, namely giving a pretest before the training begins and a posttest after the training is completed to see changes in the level of understanding of the participants.

Delivery Method

The material is delivered by lecturers from the Communication Science Study Program, Universitas Muhammadiyah Jakarta using a combination of lectures, interactive discussions, and case simulations that are tailored to the needs and abilities of the participants. All communications are delivered verbally and interactively to accommodate the visual limitations of the participants, and are supported by demonstrations of the use of technology through audio-based devices (screen readers).

Evaluation Instrument

The evaluation instrument used in the training activity "Optimizing Digital Communication in Dealing with Cybercrime for People with Visual Sensory Disabilities" is in the form of a pretest and posttest questionnaire. This instrument is designed to measure the level of understanding of participants before and after training in aspects of digital literacy and cybersecurity. The evaluation is carried out orally (oral test) to accommodate the needs of blind participants, with answers recorded by the committee.

Analysis Techniques

The pretest and posttest data were analyzed descriptively quantitatively by calculating the average understanding score before and after the training. The increase in the posttest score compared to the pretest was used as an indicator of the success of the training in improving participants' digital communication literacy.

RESULTS AND DISCUSSION

The training entitled "Optimizing Digital Communication in Dealing with Cybercrime for People with Visual Sensory Disabilities" is part of a community service program that aims to improve safe digital communication literacy for groups of people with disabilities, especially the blind. This activity was held on June 15, 2025 at the Raudhatul Muffin Foundation, Serpong District, South Tangerang City. The participants of the activity numbered 37 people with an age range of 17 to 60 years, consisting of individuals who are mostly accustomed to using mobile devices with screen reader support such as NVDA and TalkBack, and are active in utilizing online communication applications such as WhatsApp and Facebook.

Although participants showed a fairly high level of technology use, most of them did not have an adequate understanding of the security aspects of digital communication. This creates vulnerability to various forms of cybercrime, such as phishing, personal data theft, information manipulation, and privacy violations. In this context, the training was designed not only to introduce basic concepts of digital security, but also to equip participants with preventive skills that can be directly applied in their daily digital lives.

Figure 1. Paparan Materi dari Dr. Nani Nurani Muksin, M.Si (Photo Pribadi)

To measure the effectiveness of the training, an evaluation instrument was used in the form of a pretest and posttest consisting of 10 questions. The evaluation material covers topics such as introduction to phishing, the function of a Virtual Private Network (VPN), the benefits of two-factor authentication (2FA), characteristics of encrypted applications, principles of digital ethics, and appropriate actions in dealing with potential cyber attacks. The entire evaluation process was carried out verbally to accommodate the sensory needs of the participants, and was assisted by a facilitator who accompanied them throughout the process.

The purpose of this evaluation is to see changes in the level of understanding of participants before and after training. The approach used is participatory and

communicative, where participants not only answer questions, but are also invited to discuss their experiences related to the use of technology and the potential digital risks they have experienced. Thus, the evaluation results not only describe the cognitive dimensions of participants, but also reflect a humanistic, empathetic, and context-based learning process.

Table 1. Descriptive Statistics of Pretest and Posttest Results

Statistics	Pretest	Posttest
Number of participants	37 people	37 people
The highest score	8	10
Lowest Value	2	6
Rate-rate	5,1	8,2
Standard Deviation	1,6	1,1
Participants with a score of ≥ 7	9 people	34 people
Participants with a score <7	28 people	3 people

The results of the quantitative evaluation of the training showed a significant increase in participants' understanding of secure digital communication. Based on data analysis, before the training was conducted, only 24% of participants scored ≥ 7 out of a total of 10 questions given. This shows that most participants still have limitations in recognizing forms of cybercrime and prevention strategies. However, after participating in the training, there was a drastic increase, where 92% of participants managed to achieve a score of ≥ 7, with only three people below the threshold. This increase indicates the success of the training in significantly improving participants' digital literacy.

The improvement was also seen from the average score of the participants, which was previously at 5.1, increasing to 8.2 in the posttest. This means that there was a 60.8% increase in mastery of the material, which reflects the success of the training strategy designed according to the characteristics of blind participants, namely with an audio-based, participatory, and practical approach. This finding is in line with the results of research by Sidiq, Latif dan Nurfaidah (2022), which emphasizes that an inclusive and accessibility-oriented learning approach can increase the effectiveness of learning for groups of people with disabilities.

The most prominent thematic improvement in participant scores was in understanding the concept of phishing, the benefits of two-factor authentication (2FA), and safe digital communication practices, including the use of encrypted applications and the principles of maintaining online privacy. Participants demonstrated improved ability to identify potential cyber threats and respond to them with appropriate actions. A study by Sulistyan & Afrianto (2024) supports these findings, where a training approach based on hands-on practice and real-world experiences was shown to be effective in building digital security awareness among vulnerable groups, including people with sensory disabilities.

In addition to the increase in the average score, another indicator that strengthens the success of the training is the decrease in the standard deviation from 1.6 to 1.1, which shows that the increase in participants' understanding occurred evenly, not only limited to individuals with a strong initial knowledge background. This indicates that the training not only succeeded in increasing general understanding but also in reducing the gap between individuals in mastering the material. These results strengthen the findings of Faliza dkk. (2025), which explain that learning strategies that adopt the principles of Universal Design for Learning (UDL) tend to produce equal learning outcomes through flexibility of approach and delivery.

More than just access to technology, digital literacy plays a crucial role in protecting groups of people with disabilities. Fatmawati (2020) emphasized that the affordability of technology must be accompanied by the ability to use it safely, ethically, and responsibly. Within this framework, the training held in this activity not only functions as a means of education, but also provides a transformative and protective

impact on participants. In line with this, Almasyhari dkk (2022) emphasized that strengthening digital literacy for marginalized groups is an integral part of efforts to build social inclusion, as well as an important strategy in strengthening community resilience to various risks in the digital era.

Thus, the results of the pretest and posttest evaluations of this training show that an inclusive and adaptive educational approach has great potential in improving the ability of people with visual sensory disabilities to understand, recognize, and deal with various forms of cybercrime. The significant improvements achieved collectively are also evidence that appropriately designed digital literacy education is able to answer the challenges of inequality of access and digital risks in the cyber era.

Visualization of Comparison of Pretest and Posttest Scores

To quantitatively describe the changes in participants' level of understanding before and after the training, a two-color bar graph was created that represents the distribution of pretest and posttest scores from all 37 participants. This graph is based on the number of participants who achieved a certain score in the range of 2 to 10, which reflects the number of questions answered correctly from a total of 10 evaluation items.
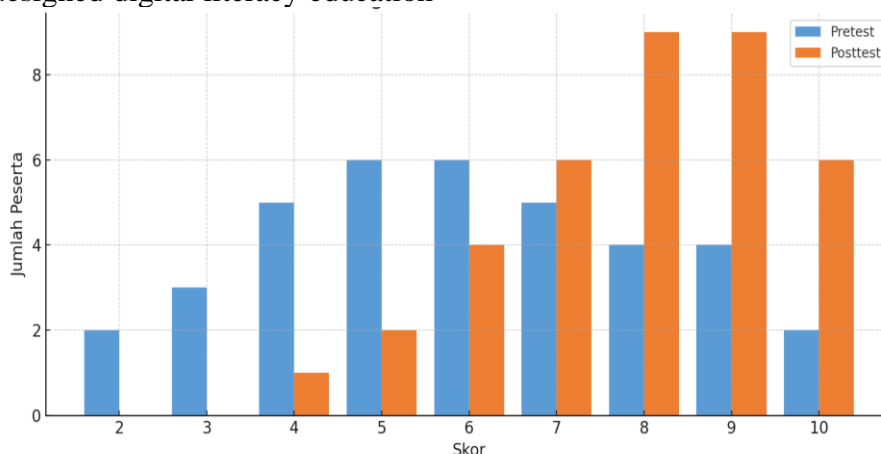

Figure 1. Comparison of Pretest and Posttest Scores

As shown in Figure 1, the blue color indicates the number of participants for each score at the pretest, while the orange color indicates the number of participants for the same score at the posttest. Visually, there is a quite striking shift in the distribution of scores. At the pretest, most participants were concentrated in the low to medium score category (scores 2–6), indicating a limited initial level of understanding of the topic of secure digital communication. In contrast, at the posttest, there was a significant increase in the high score category (scores 8–10), indicating that most participants experienced a substantial increase in understanding after participating in the training.

Figure 2. Foto Bersama dengan peserta pelatihan dan tim pengabdian kepada masyarakat (Photo Pribadi)

This distribution pattern shows the positive impact of the training provided, especially in the context of an oral, participatory, and contextual learning approach, which is tailored to the needs of participants with visual sensory disabilities. These results reinforce the findings of previous numerical evaluations, and at the same time serve as a visual indicator that

the training method used is able to accommodate the diversity of participant backgrounds and is effective in improving safe and inclusive digital literacy.

Effectiveness and Optimization of Activities

The effectiveness of this activity can be seen from the increase in the number of participants with a score of ≥7 from 9 people to 34 people. In addition, the use of an auditory-verbal approach, real case simulations, and facilitators who understand an empathetic approach to participants with special needs are the keys to the success of the activity. This principle is in line with UNESCO's (2020) Almasyhari dkk (2022) guidelines on inclusive digital literacy as part of fulfilling human rights in a digital society.

For future program optimization, several things are suggested, including the preparation of advanced modules with the topic of digital transaction security, strengthening practical assistance through direct applications, and implementing long-term impact evaluations. This activity also has the potential to be replicated in other areas that have similar disability communities, with local adaptations according to the needs of the participants.

CONCLUSION

This training proves that people with visual impairments can actively and effectively learn about digital communication security, if given materials and approaches that suit their needs. Pretest and posttest-based evaluations confirmed an increase in participants' understanding of digital literacy aspects, as well as fostering awareness and independence in facing cyber challenges in the digital era.

SUGGESTIONS

This activity can be a best practice model for inclusive training in the field of digital security, while also contributing to the national agenda of digital literacy and protection of vulnerable groups in cyberspace.

ACKNOWLEDGEMENTS

REFERENCES

Almasyhari, A. K., Sari, Y. P., & Sukesti, F. (2022). Edukasi literasi digital: Peningkatan kesadaran masyarakat dalam perlindungan data pribadi dan kaitannya terhadap financial technology. *Jurnal Abdimas PHB Vol*, *5*(3). https://doi.org/https://doi.org/10.30591/japhb.v5i3.3849

Faliza, N., Khan, R. B. F., & Fauzi, M. N. (2025). *The Future of Human Capital: Adaptasi dan Pertumbuhan di Era AI*. Takaza Innovatix Labs.

Fatmawati, E. (2020). Kebebasan informasi kalangan milenial dalam bermedia sosial. *Jurnal Perpustakaan Universitas Airlangga*, *10*(2), 94–103.

Furnell, S., Helkala, K., & Woods, N. (2021). Disadvantaged by disability: examining the accessibility of cyber security. *International Conference on Human-Computer Interaction*, 197–212.

Iskandar, A., Winata, W., Kurdi, M. S., Sitompul, P. H. S., Kurdi, M. S., Nurhayati, S., Hasanah, M., Arisa, M. F., & Haluti, F. (2023). *Peran teknologi dalam dunia pendidikan*. Yayasan Cendekiawan Inovasi Digital Indonesia.

Mokobombang, W., Syafaruddin, S., Syafaruddin, A. R. A., Khaeriyah, K., & Natsir, N. (2023). Dampak Perubahan Layanan Publik Yang Disebabkan Oleh Teknologi Dan Media Sosial. *Journal of Business, Finance, and Economics (JBFE)*, *4*(1), 348–359.

Romadhianti, R., Wulandari, Y., & Kartika Sari, R. D. (2021). Acceleration of Strengthening Digital Literacy in the Era of Society 5.0. *Jurnal Pendidikan Dan Pengajaran*, *54*(2), 297.

Saramuke, S. S., Putri, V. A., & Sormin, A. M. (2025). *Ancaman Keamanan Siber dan*

Peran Aktor Non-Negara di Dunia Digital. *6*(02), 141–152.

Sharevski, F. (2024). Inclusive Involvement of At-Risk Users in Cybersecurity Research. *IEEE Security & Privacy*.

Sidiq, Z., Latif, A., & Nurfaidah, N. (2022). Pendidikan Inklusif: Suatu Strategi Menuju Pendidikan untuk Semua. *Journal of Dissability Studies and Research (JDSR)*, *1*(2), 101–115.

Sulistyan, R. B., & Afrianto, E. (2024). Sosialisasi penguatan organisasi melalui teknologi digital pada generasi muda. *Capacitarea: Jurnal Pengabdian Kepada Masyarakat*, *4*(2), 43–49.

Wosah, P. N., Ali Mirza, Q., & Sayers, W. (2024). Analysing the email data using stylometric method and deep learning to mitigate phishing attack. *International Journal of Information Technology*, 1–12.