

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

Khalida Utami^{1*}, Lita Darmayuni², Tri Astuti³, Bayu Retno⁴, Ateniyanti⁵, M. Ardiansyah Syam⁶, Syamsul Bahri⁷, Salma Atikah⁸, Arditha Zakiyah Azahroh⁹, Fajar Kurniawan¹⁰

^{1,2,4,5,6,7,8,9,10} Universitas Pancasila

³Bintang Nusantara Learning Center

ABSTRACT: This community service program aims to equip Indonesian Migrant Workers (PMI) in Hong Kong with digital literacy as a preventive measure against the rising prevalence of online scams. The primary issue faced by PMI is a high vulnerability to social engineering techniques, phishing, fraudulent investments, and the threat of Human Trafficking (TPPO) due to low awareness of digital security. The program was conducted online via the Zoom platform on February 15, 2026, involving 44 PMI participants from the Bintang Nusantara Hong Kong community. Training materials included the definition of digital literacy, identification of various scam modes (such as phishing, illegal online loans, and fake job advertisements), recognition of linguistic markers used in scams, and practical verification steps through official government channels. Evaluation was carried out using pre-tests and post-tests to measure the improvement in participants' understanding. The results indicated a significant increase in the participants' ability to recognize cyber threats and their awareness of personal data protection. This initiative proved effective in building PMI's digital resilience and is recommended to be implemented periodically to protect their income and personal safety from evolving cybercrimes.

KEYWORDS: Indonesian Migrant Workers, Digital Literacy, Online Scam, Cyber Security, Hong Kong

I. INTRODUCTION

The rapid pace of digital transformation over the past few decades has revolutionized various aspects of human life, ranging from business communication and social interaction to the education sector (Fithriyah et al., 2023; Silmina et al., 2025). Information and communication technology (ICT) has become an indispensable component of daily activities, where the use of email, social media, and knowledge management systems has significantly enhanced productivity and cross-sector collaboration. Easy access to digital technologies enables individuals to conduct instant financial transactions, access unlimited information regardless of geographical boundaries, and organize travel through web-based applications. In the era of Industry 4.0 and Society 5.0, proficiency in information technology has become an essential competency for individuals seeking to adapt and remain competitive in an increasingly information-driven society. This unprecedented level of global connectivity has fundamentally transformed the way people communicate, work, and interact.

Despite these considerable benefits, technological advancement has also generated significant concerns, particularly regarding the increasing prevalence of online fraud (Riani et al., 2024). The anonymity and extensive reach of the digital environment have been exploited by cybercriminals to develop increasingly sophisticated, innovative, and organized fraudulent schemes. As digital technology becomes more widespread across all segments of society, evidence suggests that many users still lack sufficient knowledge of its appropriate and responsible use. Consequently, improper utilization often results in adverse consequences for both individuals and society. Digital literacy has therefore emerged as a crucial safeguard, enabling individuals to critically evaluate online information and mitigate the negative impacts associated with the misuse of digital technologies.

Contemporary cybercrime extends beyond purely technical attacks and increasingly relies on social engineering techniques that exploit human psychological vulnerabilities (Pitchan et al., 2025). Rather than directly hacking computer systems, cybercriminals manipulate victims' emotions by exploiting trust, fear, or the expectation of financial gain. Various forms of cyber fraud—including phishing, smishing, investment scams, and digital identity theft—continue to evolve rapidly in both complexity and scale. Furthermore, advances in generative artificial intelligence (AI) have equipped fraudsters with new capabilities to

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

automate cyberattack infrastructures and generate highly convincing fraudulent content, making deception considerably more difficult for ordinary users to detect. This trend is further exacerbated by the widespread dissemination of misinformation (hoaxes) and personal data breaches, which are frequently exploited by transnational criminal syndicates (Putrazta, 2025).

One of the most vulnerable populations to these cyber threats is Indonesian Migrant Workers (PMI), who are often recognized as "foreign exchange heroes" while simultaneously facing numerous challenges abroad (Fadillah et al., 2023). Many migrant workers are attracted by fraudulent job advertisements circulated through social media that promise high salaries. In reality, however, they are frequently recruited through irregular channels and subsequently become victims of Human Trafficking (TPPO) (Afifah, 2025; Saksornchai, 2025). Across Southeast Asia, a growing humanitarian crisis has involved thousands of Indonesian citizens trapped in scam centers or so-called "virtual slavery," where they are coerced under physical and psychological pressure to conduct fraudulent investment and illegal gambling schemes targeting unsuspecting victims (Rozalena et al., 2024). A key factor contributing to the high incidence of victimization is the inadequate level of digital literacy and cybersecurity awareness among migrant workers, many of whom depart for overseas employment without receiving adequate digital security training.

In the context of Hong Kong, one of the primary destination countries for Indonesian migrant workers, digital crime has shown an alarming upward trend. The Consulate General of the Republic of Indonesia (KJRI) in Hong Kong has reported an increasing number of cases involving the misuse of migrant workers' personal data for illegal online lending activities and other forms of transnational crime (KP2MI, 2025). Most Indonesian migrant workers in Hong Kong possess a secondary educational background (58% are senior high school graduates and 30% completed junior secondary education). Although they actively use smartphones in their daily lives, they remain highly susceptible to social engineering techniques employing persuasive language and artificial urgency (Riani et al., 2024). Moreover, psychological factors such as overconfidence in limited financial knowledge often make them more vulnerable to fraudulent schemes than individuals who exercise greater caution (Chen et al., n.d.). These circumstances underscore the urgent need for educational interventions aimed at protecting both the financial well-being and personal safety of Indonesian migrant workers in Hong Kong.

Previous studies have highlighted the importance of digital literacy among various community groups, including training programs for micro, small, and medium-sized enterprises (MSMEs) and organic vegetable farmers to improve digital marketing capabilities and promote positive social media engagement. In Malaysia, a similar community service initiative conducted within the PERMAI community successfully enhanced participants' digital security awareness and practical skills for protecting personal information. Structured digital literacy training has been shown to increase participants' confidence in recognizing online threats by as much as 90% (Rahayu et al., 2024). Furthermore, the integration of animated educational videos and interactive simulations has been found to accelerate participants' understanding of technical cybersecurity concepts, such as two-factor authentication (2FA), particularly among individuals with limited technological experience.

As a practical contribution, this community engagement program seeks to strengthen the digital resilience of Indonesian migrant workers in Hong Kong through individual capacity building. By equipping participants with practical skills to protect their digital identities and financial assets, the program supports the Indonesian government's efforts to ensure that migrant workers' earnings remain secure and continue benefiting their families in Indonesia, thereby contributing positively to the national economy. Enhanced digital literacy is expected to foster greater critical thinking, vigilance, and resilience against misinformation and cyber fraud. Moreover, these competencies will serve as valuable assets when migrant workers return to Indonesia, enabling them to adapt more effectively to an increasingly digitalized industrial and business environment.

Accordingly, the primary objective of this community service article is to describe the process of enhancing Indonesian migrant workers' awareness and understanding of various online fraud schemes through a participatory digital literacy training program. The program focuses on introducing common cyber threats, including phishing attacks, fraudulent investment schemes, and the linguistic cues commonly employed by fraudsters to manipulate victims' emotions. In addition, the training provides participants with practical competencies in implementing fundamental cybersecurity practices, such as creating strong passwords and enabling two-factor authentication (2FA). Through this comprehensive approach, Indonesian migrant workers are expected to utilize digital technologies safely, responsibly, critically, strategically, and in compliance with legal and ethical standards, thereby contributing to the development of a secure, resilient, and productive digital ecosystem for Indonesian migrant communities abroad.

II. METHOD

The major equipment and specialized tools used in this community engagement program consisted of both hardware and software to support the implementation of online training activities. The hardware included laptop computers equipped with integrated webcams to facilitate real-time visual interaction between facilitators and participants. Supporting infrastructure also included wireless internet modems providing stable broadband connectivity with a minimum speed of 20 Mbps to ensure uninterrupted data transmission throughout the virtual sessions.

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

The primary software platform utilized was Zoom Cloud Meetings under a professional license, enabling extended virtual meetings without time limitations. Training materials consisted of a digital literacy handbook distributed electronically to all participants. In addition, animated educational videos were prepared to facilitate participants' visual understanding of various online fraud schemes. The evaluation instruments comprised electronic questionnaires developed using Google Forms, containing ten multiple-choice questions administered as both pre-tests and post-tests to assess participants' knowledge before and after the training.

This community engagement program adopted a community education approach implemented through interactive online training designed to strengthen participants' digital resilience. The implementation process was systematically organized into the following stages:

A. Preparation Stage

The preparation stage began with a needs assessment conducted through a preliminary survey and situational analysis to identify the specific digital challenges encountered by Indonesian Migrant Workers (PMI) in their destination country. Based on the findings, the project team developed relevant training materials and a structured curriculum covering personal data protection, cybersecurity awareness, and information regarding legal migration pathways. Technical coordination was subsequently carried out with migrant community organizations to facilitate participant recruitment and ensure the smooth implementation of the program.

B. Implementation Stage: Session I

The first training session focused on raising participants' awareness of digital security issues. The session commenced with the administration of a pre-test through an online questionnaire to measure participants' baseline knowledge. Subsequently, the facilitator delivered the core training materials, including the concept of digital literacy and an explanation of various online fraud schemes such as phishing attacks, fraudulent investment scams, and fake job advertisements. Animated educational videos were incorporated to enhance participants' understanding of these cyber threats.

C. Implementation Stage: Session II

The second session consisted of a Focus Group Discussion (FGD) in which participants were encouraged to share their personal experiences regarding cyber threats and online fraud they had encountered. This interactive discussion was followed by hands-on practical training on smartphone and account security, including the creation of strong passwords and the direct activation of Two-Factor Authentication (2FA) on each participant's personal accounts.

D. Evaluation and Follow-up Stage

The final stage involved administering a post-test at the conclusion of the training to quantitatively evaluate improvements in participants' knowledge and understanding. To ensure the sustainability of the program, the community engagement team established a mentoring group through WhatsApp, which serves as an ongoing platform for consultation, experience sharing, and the dissemination of updated information regarding emerging cyber threats affecting Indonesian Migrant Workers.

III. RESULTS AND DISCUSSION

This community engagement program was conducted as an online training workshop for Indonesian Migrant Workers (PMI) residing in Hong Kong. The activity, entitled "Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes," was held on 15 February 2026, from 11:30 a.m. to 2:00 p.m. (Western Indonesian Time) or 12:30 p.m. to 3:00 p.m. (Hong Kong Time) via the Zoom platform. A total of 44 Indonesian Migrant Workers participated in the training.

The program commenced with an opening ceremony, the singing of the Indonesian national anthem (Indonesia Raya), followed by welcoming remarks from the community partner and representatives of the Faculty of Economics and Business, Universitas Pancasila. The training materials were carefully designed to be practical, interactive, and communicative in order to maximize participants' engagement throughout the program. The training modules delivered during the activity are presented in Table I.

Table I. Digital Literacy Training Modules for Indonesian Migrant Workers

Session	Main Topic	Focus of Discussion
I	Definition of Digital Literacy	Cognitive competencies for using digital technologies in a safe, responsible, intelligent, prudent, and legally compliant manner.
II	Understanding Online Fraud Schemes	Identification of phishing, smishing, investment scams, and illegal online lending practices.
III	Scam Center Crisis	Risks associated with "virtual slavery" and human trafficking in Southeast Asia.

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

IV	Psychology of Fraud	Social engineering techniques and the phenomenon of overconfidence.
V	Digital Defense Protocols	Verification procedures using the Siskop2MI system and the principle of "Think Before You Share."

During the training sessions, the facilitator utilized animated educational videos to simplify complex cybersecurity concepts, including Two-Factor Authentication (2FA) and digital footprint management. Participants actively engaged in the Focus Group Discussion (FGD), sharing their personal experiences regarding fraudulent government financial assistance messages and parcel delivery scams targeting their families in Indonesia.

This community engagement program was designed to enhance Indonesian Migrant Workers' awareness and understanding of online fraud schemes through practical digital literacy training. The instructional materials were developed based on participants' practical needs and focused on competencies that could be directly applied in their daily lives. The training was facilitated by Khalida Utami, S.E., M.Sc., CIBA, Faculty of Economics and Business, Universitas Pancasila, using a participatory, communicative, and contextual learning approach. The presentation emphasized the growing importance of digital literacy amid rapid technological transformation and the increasing sophistication of cybercrime.

During the core presentation, the facilitator emphasized that digital literacy extends beyond technical proficiency in operating smartphones or digital applications. Rather, it encompasses the cognitive ability to utilize digital media, communication technologies, and online networks in a healthy, responsible, critical, prudent, accurate, and legally compliant manner. Technology was described as a double-edged sword: while it provides greater efficiency in financial transactions and cross-border communication, it simultaneously exposes users to increasingly complex cyber threats, including identity theft, personal data breaches, and various forms of online fraud. Consequently, digital literacy serves as a critical filter that enables Indonesian Migrant Workers to distinguish credible information from misinformation and to avoid becoming victims of fraudulent schemes.

The facilitator provided a comprehensive explanation of the online fraud schemes most frequently targeting Indonesian Migrant Workers. The first category consisted of phishing and smishing, in which fraudsters distribute malicious links or deceptive text messages designed to impersonate legitimate institutions and steal victims' banking credentials or personal identities. In addition, investment scams and illegal online lending platforms were identified as major threats to migrant workers' financial security. Fraudsters commonly exploit financial vulnerability by offering unsecured loans or promising exceptionally high investment returns within a short period, ultimately trapping victims in cycles of financial loss and debt.

Another major concern highlighted during the training was the misuse of personal data. The facilitator explained that the careless sharing of sensitive information on social media—such as passport photographs, national identity cards, or other official documents—creates opportunities for criminals to apply for illegal online loans or engage in other forms of transnational crime using victims' identities. Furthermore, fraudulent overseas job advertisements were discussed as one of the primary gateways to Human Trafficking (TPPO). Perpetrators frequently use persuasive language to promote high-paying employment opportunities in countries such as Cambodia, Thailand, and Myanmar, despite the fact that Indonesia does not maintain official labor placement agreements for non-professional migrant workers in these destinations.

A particularly important section of the training focused on the scam center crisis currently affecting several Southeast Asian countries. The facilitator explained that many Indonesian citizens who pursue irregular migration pathways ultimately become victims of "virtual slavery," where they are forced to participate in romance scams, online gambling operations, or other cyber fraud schemes under conditions involving physical and psychological abuse. Participants were reminded that traveling abroad through unauthorized migration channels or relying solely on tourist visas poses severe risks to personal safety. To date, the Indonesian government has facilitated the repatriation of hundreds of migrant workers who had been detained or exploited within these scam centers.

The facilitator also examined the psychological mechanisms underlying successful cyber fraud through social engineering techniques. Rather than attacking computer systems directly, fraudsters manipulate human emotions, including trust, fear, and the expectation of financial gain. Participants learned to recognize common linguistic indicators of fraud, such as emotionally charged language and the deliberate creation of urgency intended to pressure victims into making impulsive decisions without proper verification. The facilitator further discussed the phenomenon of overconfidence, explaining that individuals who perceive themselves as financially knowledgeable may actually become more vulnerable to fraud because excessive confidence often reduces their level of vigilance.

As a preventive strategy, participants were introduced to the principle of "Think Before You Share." Indonesian Migrant Workers were advised never to disclose personal identification documents, including national identity cards or family registration

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

documents, to unauthorized individuals through unofficial online channels. Participants were also introduced to several essential verification procedures before accepting employment opportunities or making financial decisions:

1. **Verify Legitimacy:** Ensure that recruitment agencies or placement companies are officially registered with the Ministry of Manpower or BP2MI through the Siskop2MI platform.
2. **Avoid Transfers to Personal Bank Accounts:** Official administrative fees should only be transferred to authorized corporate or designated bank accounts rather than personal accounts.
3. **Be Skeptical of Unrealistic Offers:** Employment opportunities promising exceptionally high salaries with rapid processing and no training requirements should be treated as strong indicators of fraud.
4. **Conduct Direct Verification:** Contact the nearest Indonesian Consulate General (KJRI), Indonesian Embassy (KBRI), BP3MI, or KP2MI office before making important employment or investment decisions.

The effectiveness of the community engagement program was assessed by comparing participants' knowledge before and after the educational intervention. Analysis of the evaluation instruments revealed a substantial improvement in participants' understanding of online fraud prevention. A summary of the evaluation results is presented in Table II.

Table II. Summary of Participant Evaluation Results (Pre-test and Post-test)

Indicator	Mean Score	Pre-test	Mean Score	Post-test	Improvement (%)
Understanding of Online Fraud Schemes	87,11		95,78		9,95%
Ability to Identify Cyber Threats	70,00		90,00		28,57%
Awareness of Data Security (Passwords & 2FA)	40,00		80,00		100,00%

The increase in the average score from 87.11 to 95.78 demonstrates that the training materials were well understood by participants. This improvement can be attributed to the contextual learning approach employed during the program, in which digital literacy concepts were directly linked to real-world cases of Human Trafficking (TPPO) and cyber-enabled crimes currently occurring in border areas of Thailand, Myanmar, and Cambodia. Participants who initially displayed a high degree of confidence in their financial knowledge (overconfidence) came to recognize that, without adequate digital vigilance, they remained highly susceptible to psychological manipulation and social engineering attacks.

One immediate impact observed following the training was a positive change in participants' attitudes toward protecting their personal information. Participants demonstrated a greater awareness that carelessly sharing identity documents, such as national identity cards or passports, on social media may enable criminals to obtain illegal online loans or commit other forms of identity-related crime. Furthermore, participants acquired practical skills for verifying the legitimacy of overseas recruitment agencies through official government platforms such as Siskop2MI before making employment-related decisions.

Compared with previous community engagement initiatives, this program demonstrated a similarly positive trend while placing greater emphasis on digital security. A digital literacy training program for Indonesian migrant workers in Malaysia conducted by Fithriyah et al. (2023) also reported a 100% participant attendance rate and significant improvements in participants' competencies in using digital media productively. However, the present program differs by focusing specifically on cybersecurity awareness in response to the increasingly sophisticated cyber threats emerging across Southeast Asia.

Similarly, Rahayu et al. (2024) reported that, within the PERMAL community in Malaysia, the proportion of participants using strong passwords increased from 40% before training to 80% after receiving technical assistance. These findings are consistent with the outcomes of the present program, suggesting that practical, hands-on instruction has a more substantial impact than theoretical explanations alone. Moreover, communication barriers encountered in previous community engagement programs—particularly concerning technical concepts such as encryption and Two-Factor Authentication (2FA)—were effectively mitigated in this training through the use of simple analogies, contextual examples, and animated educational videos, thereby improving participants' comprehension of essential cybersecurity practices.

CONCLUSIONS

Based on the implementation of this community engagement program, it can be concluded that the digital literacy training made a meaningful contribution to strengthening the resilience of Indonesian Migrant Workers (PMI) in Hong Kong against increasingly sophisticated cyber threats. The program enhanced participants' understanding that digital literacy extends beyond technical competence to encompass the ability to use digital technologies in a safe, responsible, critical, and legally compliant manner, thereby reducing their vulnerability to online fraud schemes such as phishing, investment scams, and illegal online lending.

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

Through the discussion of social engineering techniques, participants became more aware of the emotional manipulation and linguistic cues commonly employed by fraudsters to create a false sense of urgency. Furthermore, increased awareness of the risks associated with fraudulent overseas job advertisements—particularly those promoting employment opportunities in countries without official labor migration agreements with Indonesia, such as Cambodia, Thailand, and Myanmar—represents an important preventive measure against recruitment into scam centers and Human Trafficking (TPPO) networks. Overall, the program successfully improved participants' confidence in recognizing cyber threats while strengthening their commitment to protecting personal information as a means of safeguarding both their financial security and personal safety.

To maximize its long-term impact, digital literacy education for Indonesian Migrant Workers should be implemented on a continuous and sustainable basis rather than as a one-time intervention, ensuring that participants remain informed about the rapidly evolving nature of online fraud and cybercrime. Stronger collaboration among higher education institutions, training providers such as Bintang Nusantara Learning Center, and government agencies, including BP2MI and the Consulate General of the Republic of Indonesia (KJRI), is essential for establishing a comprehensive protection system for Indonesian migrant workers overseas. In addition, continuous mentoring through digital platforms or online discussion groups is recommended to provide timely consultation and practical assistance for migrant workers encountering cybersecurity challenges in their daily lives. Future community engagement initiatives may further strengthen the program by incorporating more advanced topics on device security, cybersecurity best practices, and the integration of digital literacy with personal financial management. Such enhancements would better equip Indonesian Migrant Workers with the digital and financial competencies necessary to achieve greater economic independence and facilitate their successful socioeconomic reintegration upon returning to Indonesia.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude and appreciation to all individuals and institutions that contributed to the successful implementation of this community engagement program. Special appreciation is extended to the Faculty of Economics and Business, Universitas Pancasila, for its institutional support; Bintang Nusantara Learning Center (BNLC), Hong Kong, for its valuable collaboration in organizing and facilitating the training activities; and all Indonesian Migrant Workers (PMI) in Hong Kong who enthusiastically participated in the program. Their active engagement, cooperation, and commitment were instrumental in the successful implementation of this community service initiative.

REFERENCES

- 1) Afifah, S. N. (2025, November 11). Marak PMI Terjerat Online Scam Akibat Minimnya Literasi Digital. Voice Indonesia. <http://voiceindonesia.co/ketenagakerjaan/pekerja-migran-indonesia/11/11/2025/64174/marak-pmi-terjerat-online-scam-akibat-minimnya-literasi-digital/>
- 2) Chen, H., Guo, Y., & Wang, K. (n.d.). Investigating Migrant Workers' Information-Seeking Behaviors on Scams: The Impact of Scam Prevention Communication and Victimization Experiences. *Journalism & Mass Communication Quarterly*. <https://doi.org/10.1177/10776990251336383>
- 3) Fadillah, A., Nopitasari, D., Bilda, W., Yanti, R., Sulistyo, D. R., & Aini, I. D. N. (2023). Pelatihan Literasi Digital Pekerja Migran Indonesia (PMI) di Hongkong. *Jurnal Anugerah*, 5(1), 33–40. <https://doi.org/10.31629/anugerah.v5i1.4867>
- 4) Fithriyah, N. N., Diana, N., Mutia, C. I., Hasan, K., & Surya, A. (2023). Digital Literacy Training For Indonesian Migrant Workers (PMI) In Malaysia. 1(02).
- 5) KP2MI. (2025, April 18). KemenP2MI Susun Strategi Berantas Kasus Penipuan Modus Gaji Besar Kerja Ilegal di Kamboja, Myanmar, dan Thailand. Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia.
- 6) Pitchan, M. A., Salman, A., & Arip, N. M. (2025). A Systematic Literature Review on Online Scams: Insights into Digital Literacy, Technological Innovations, and Victimology. *Jurnal Komunikasi: Malaysian Journal of Communication*, 41(1), 107–124. <https://doi.org/10.17576/JKMJC-2025-4101-07>
- 7) Putrazta, S. A. (2025). Perlindungan Hukum Korban Tindak Pidana Perdagangan Orang Lintas Negara Berkedok Lowongan Kerja Digital di Myanmar. *Majelis: Jurnal Hukum Indonesia*, 2(4), 89–103. <https://doi.org/10.62383/majelis.v2i4.1204>
- 8) Rahayu, P., Asnati, S. D., Cahyaningsih, E., & Durunavis, D. A. (2024). Enhancing Digital Safety Knowledge Indonesian Migrant Worker In Malaysia. *ICCD*, 6(1), 383–388. <https://doi.org/10.33068/iccd.v6i1.699>
- 9) Riani, L. P., Mustofa, M., Fikri, A. A. H. S., Sholeh, M., & Supriyanto, S. (2024). Edukasi dan Pendampingan Literasi Keuangan dan Digital pada Mantan Pekerja Migran Indonesia. *Jurnal ABDINUS : Jurnal Pengabdian Nusantara*, 8(1), 151–162. <https://doi.org/10.29407/ja.v8i1.21201>

Enhancing Indonesian Migrant Workers' Awareness and Understanding of Online Fraud Schemes

- 10) Rozalena, A., Thaherudin, M., & Tri, N. (2024). Improving Digital Media Literacy Knowledge for Indonesian Migrant Workers in Malaysia. *International Journal of Community Care of Humanity (IJCCH)*, 2(5).
- 11) Saksornchai, J. (2025, February 28). 84 Indonesians freed from scam centers in Myanmar are set to go home. *The Associated Press*. <https://apnews.com/article/myanmar-scam-centers-indonesia-thailand-57d644b606335eecbd5d3a27a1053e3b>
- 12) Silmina, E. P., Sarmin, S., Umar, R., & Herman, H. (2025). Meningkatkan Literasi Digital: Perlindungan Data Pribadi dan Pencegahan Penipuan Online di Lingkungan PRA Ngadisuryan. *Jurnal Pengabdian UntukMu Negeri*, 9(2), 322–330. <https://doi.org/10.37859/jpumri.v9i2.9860>



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.