



Empowering Rural Communities through Digital Literacy: An Empirical Study of Former Women Migrant Workers in Panjer Village, Kebumen - Indonesia

Donny Budi Utoyo
Institut Pertanian Bogor
Bogor, Indonesia
donnyutoyo@apps.ipb.ac.id

Abstract. People from many backgrounds should be digitally literate since the digital age is fast changing, and rural areas must overcome several challenges. This study examines how efforts toward digital literacy affect former migrant workers and rural women in Panjer Village in Kebumen District, Indonesia. Using participant observation and focus group discussions in addition to pre- and post-training evaluations provided by Migrant Care and ISOC Foundation, this study assesses ICT Watch Indonesia's digital literacy effort qualitatively and descriptively. Emphasising security and economic growth through small and micro-enterprises, the program seeks to increase participants' technical skills while improving their critical knowledge of digital hazards. Key obstacles, according to the study results, are restricted access to digital resources as well as socioeconomic factors and general saturation of privacy. This paper shows the urgent necessity of a digital literacy framework aiming to close the digital divide and consider local socioeconomic factors together with their influence. According to current research, digital literacy programs in rural communities should integrate technical education with the development of critical thinking abilities to generate digital competency and boost the local economy. This study supports current projects aiming at creating inclusive digital literacy systems with sustainability concepts in order to close urban and rural differences.

Keywords: Digital Literacy, Women Empowerment, Rural Digitalisation, Digital Security, Capacity Building, Former Migrant Worker

1 Introduction

In the increasingly digital era, digital literacy has become an important aspect that involves technical skills in using devices and includes a critical understanding of the risks and opportunities posed by technology. Digital literacy is a set of competencies that enable individuals to use digital technology safely, effectively, and responsibly [Pangrazio et al., 2020]. In this sense, digital literacy emphasises technical skills and knowledge of relevant security and privacy issues. This is especially true in rural areas, which often face particular challenges in using modern technologies. This study used a descriptive qualitative methodology to explore community knowledge, particularly among former migrant women in Panjer Village, Kebumen.

Their digital literacy is key to ensuring their financial stability and economic

sustainability. Many of these women return home after years of working abroad with savings, usually stored in digital bank accounts or e-wallets. Lack of proper digital literacy makes people more vulnerable to identity theft, financial fraud, and cyberattacks, which put their hard-earned assets at risk. Moreover, digital literacy enables them to set up online businesses, conduct e-commerce transactions, and safely interact with financial institutions, thus protecting their financial independence from losses. Improving digital literacy can help former migrant workers maximise the benefits and minimise the drawbacks of digital financial services.

The purpose of this study was to determine the implementation of the digital literacy training program entitled "Made in Indonesia (Safe Migration and Inclusive Economy in Indonesia)", organised by ICT Watch Indonesia on November 28-29, 2023, for two days and May 15, 2024, for focus groups using participatory observation methods, focus group discussions (FGD), pre-test and post-test (initial test). The training program supported by Migrant Care and ISOC Foundation involved 30 adult women and former migrant workers who work as housewives or small and micro business owners. Rural communities, especially in developing countries, often experience limited access to digital infrastructure and adequate technical knowledge.

Due to a lack of access to internet services and modern digital devices, as well as a lack of technical support, rural communities are slow to adopt important digital security measures. In addition, low digital literacy makes rural areas more vulnerable to online fraud, privacy violations, and other cybercrimes. Literature studies have shown that low digital literacy levels are closely associated with increased cybersecurity risks, especially among groups of people who are less exposed to technology [Greene et al., 2014; Reddy et al., 2023]. Social, economic, and cultural factors contribute to this view, where people feel that their digital activities are not significant enough to be targeted by cybercrimes. This condition is often exacerbated by a lack of understanding of the risks posed by unsafe digital technologies, such as online fraud, identity theft, and privacy violations [Elueze & Quan-Haase, 2018].

In addition, there is an interesting phenomenon related to "privacy fatigue", which influences the reluctance of rural communities to adopt digital security practices. Privacy fatigue refers to a condition when individuals feel overwhelmed by the obligation to maintain the privacy and security of their data across various digital platforms. Therefore, they ignore the risks involved [Neumann et al., 2017]. These findings indicate an urgent need to develop more inclusive and sustainable digital literacy models that are tailored to the local context and specific needs of rural communities

Digital literacy should include understanding everyday situations, especially social and economic ones so that people not only know how to use digital devices but also understand the risks associated with using these technologies [Pangrazio et al., 2020]. Literature research has shown that digital literacy is not only about skills in using digital devices but also about aspects of critical thinking, including awareness and understanding of potential cyber risks. Critical thinking skills are essential for digital literacy because they enable people to manage information more safely and effectively

[Green et al., 2014]. It is important to have a digital literacy model that can reduce the digital skills gap between those with access to the latest technology and those without access. Rural communities often face fundamental challenges, such as limited Internet access and minimal technical support, which can slow down digital security adoption [Reddy et al., 2023].

The results of this study offer practical contributions to efforts to improve digital literacy in Indonesia. This study underlines the importance of a holistic digital literacy programme approach, which teaches technical skills and strengthens the community's critical awareness of the ever-evolving digital risks. Designing a digital literacy training programme is also expected to be gender-sensitive so that it can reach a wider group of women according to their conditions and abilities to be more effective and efficient in the use of resources. No less important is that digital literacy education in rural areas needs to be linked to efforts to develop the economic potential of rural families through small and micro businesses so that it has strong relevance and can be carried out sustainably.

2 Methodology

This study aims to analyse the level of digital literacy in the context of security among rural communities in Kebumen, Indonesia. This study uses a descriptive qualitative approach, which focuses on understanding subjective aspects such as the understanding of rural community members in securing the digital technology they use and the challenges of its use. This approach was chosen because it allows for the initial exploration of community attitudes and behaviours towards digital technology and the adoption of digital security measures. The data collection methods used include participatory observation, focus group discussion (*FGD*), and simple surveys in the form of pre-tests and post-tests, the main target being digital literacy training participants in the area. The activity that was observed participatory and conducted *a pre-test* and *post-test* was a digital literacy training entitled “*Made in Indonesia*” (Safe Migrants and Indonesia's Inclusive Economy) served by ICT Watch Indonesia (ictwatch.id), and supported by Migrant Care and ISOC Foundation, for 2 (two) days, namely on November 28-29, 2023, in Panjer Village, Kebumen, Central Java. The activity was attended by 30 adult women, primarily former migrant workers who worked as housewives or small and micro business owners upon returning to their hometowns. Several key local persons and stakeholders' representatives also participated in the training.

The pre-test was given on the first day of the opening session before the training started, while the post-test was given in the closing session on the second day after all training material was delivered. The pre-test and post-test questions were the same, in the form of multiple choice with only 1 (one) correct answer, to quickly find out the increase in participants' understanding of several essential digital security matters between before and after attending the training. The number of questions in this study was 10 (ten) of the most relevant. Then, the answers to these questions were assessed based on the answers from the training participants. The percentage of correct answers was calculated by identifying the number of participants who chose the correct one for each

question, dividing it by the total respondents, and then multiplying it by 100 to get the percentage. The enhancement figure (in percentage) is an additional or increase in value calculated by subtracting the percentage of correct answers in the post-test from the percentage of correct answers in the pre-test. Conversely, if there is a decrease, the number will be negative, indicating areas that require further attention. This method provides a modest method to picture the effectiveness of training in improving participants' understanding of various aspects of security and the use of digital technology.

Researchers were also involved in training participants in this activity, observing and recording interactions, providing direct responses, and studying the challenges faced by participants in understanding and implementing digital security measures. These observations include observing participants' responses to training materials on password management, privacy settings, and basic steps to protect devices. Then, on May 15, 2024, an FGD discussion was held with ten women representing training participants to find out their experiences related to digital technology after 6 (six) months of attending the training. The FGD was conducted by the ICT Watch team and was documented for later analysis by researchers, focusing on participants' personal experiences related to digital risks, their understanding of the importance of data security, and their views on the security measures they had adopted or avoided. Interview questions were structured semi-structured so that respondents could freely express their views. Overall, this study contributes to the digital literacy literature by providing an enriched understanding of several things that can influence the adoption of digital security in rural communities and women in particular, who, in this case, are represented by former migrant workers. In addition, this study provides recommendations for designing effective digital literacy programmes, which not only focus on technical skills but also strengthen the community's critical awareness of risks and protection in the digital era.

3 Results and Discussion

The increase in participants' understanding of digital security principles after this training shows a positive impact in forming awareness and essential skills needed to deal with digital threats. A linear navigation social network model was effective in enhancing digital literacy skills for elderly participants, promoting a sense of control and usefulness in ICT engagement [Castilla et al., 2018]. In questions related to digital security principles, an additional 20% (6 people) of 30 participants answered correctly from the pre-test to the post-test, reflecting the success of the training in emphasising the concept that digital security is never completely guaranteed.

Table 1. Pre-Test/Post-Test Results

Table of Pre-Test/Post-Test Results	Pre-	Post-Test Enhancement	
	Test %	%	%
1. The statement that best describes the meaning of the internet:	36.67	80.00	43.33
2. The following can be seen from our digital footprint on Google except:	60.00	70.00	10.00
3. Important things to consider when using Public WiFi:	76.67	96.67	20.00
4. If you receive a link from an unknown person via email or WhatsApp, this is what you can do:	80.00	86.67	6.67
5. We need to check our security status on Google to know:	66.67	70.00	3.33
6. Enabling Two-Factor Authentication (2FA) is beneficial for:	90.00	96.67	6.67
7. A good password is a password that:	80.00	96.67	16.67
8. One of the general principles of digital security is:	63.33	83.33	20.00
9. Important things to consider when installing applications on the phone except:	33.33	26.67	-6.67
10. What needs to be done to maintain our digital security, except:	46.67	70.00	23.33

This concept is the basis for developing a critical and vigilant mindset in the digital world, where participants are expected to be able to apply the principle of caution consistently in all their digital activities. This principle is fundamental to instil, especially because perfect security is challenging to achieve, so users must always be prepared for potential risks. Understanding the characteristics of a strong password is one of the critical points successfully improved through this training. With an increase of 16.67% (5 people) after the training, this result shows that participants know the importance of using a complex combination of characters, including uppercase letters, lowercase letters, numbers, and symbols. It is quite an important preventive move, particularly in the face of growing data theft and account hack cases. Not only does a deeper understanding of solid passwords protect them from unauthorised access, but it also gives participants the knowledge to help keep themselves and their privacy and personal data secure.

And, of course, Two-Factor Authentication (2FA) is another critical aspect of the digital security arsenal that more and more participants are coming to terms with. While, as retrospectively noted, the increase in % knowledge from pre-test to post-test (6.67% increase on average 60/90 individual points = 6%) is quite low, this suggests that participants started out with high knowledge of positive aspects of 2FA, even before the program started. In digital security, 2FA acts as a secondary security layer, which is based on a second authentication factor; it essentially minimises the chances of unauthorised access/gain in case the user's password is hacked successfully. This increase in 2FA-related comprehension suggests that participants have taken on the principle of defence in depth, making them more ready to counter ever more advanced cyber tactics.

Understanding the right action to take when receiving an unknown link increased significantly from 80.00% to 86.67%. This 6.67% moderate increase highlights the

moderate success of the training in educating participants on how to identify risky links and avoid phishing or malware threats. This awareness is especially critical in today's digital era, where social engineering threats are becoming increasingly sophisticated. Attackers can easily disguise themselves as trusted parties, making it more challenging for individuals to identify and avoid such risks.

Therefore, this training is vital in equipping participants to assess links received via email or messaging apps critically. However, a big challenge is understanding security when installing applications on mobile phones (question number #9). Data shows that only 33.33% of participants answered correctly in the pre-test, which decreased to 26.67% in the post-test. This decrease of 6.67% indicates that participants still have difficulty understanding the risks of installing applications, including access permissions that are often unnecessary. Another possible reason for this decline is that participants may not have fully understood the question's meaning or the given answer choices, even after attending the training. This suggests that the language used might have been too technical for them, or they may have already experienced *privacy fatigue*, a phenomenon that will be explained later.

This phenomenon highlights the need for further emphasis on mobile security, which is increasingly essential amidst high smartphone penetration and potential threats from third-party applications. This decrease also suggests that the content or delivery methods used in this aspect may require further improvement to ensure the message is conveyed more clearly, effectively, and in a way that resonates better with participants' understanding and needs.

Overall, the training effectively increased participants' understanding of most aspects of digital security, although there were some areas for improvement. Assessing online credibility could strengthen arguments on digital literacy's critical thinking aspect. Integrating this can emphasise the need for practical skills in evaluating information online, especially in contexts with limited access to diverse information sources. Some improvements in the fundamental understanding of digital security, password quality, and suspicious link management indicated that the training achieved most of its objectives. However, the importance of managing mobile applications highlighted the need for a more in-depth and interactive approach to the training so that participants could better understand the risks and precautions that need to be implemented. These results provide insight into the current training programme's effectiveness and opportunities for developing materials more responsive to participants' needs in the future.

Divide or lack of understanding of potential digital security risks will make users vulnerable to online fraud and privacy violations. The extent and the nature of this divide depend on the kind of access defined, revealing differential access in terms of skills and usage likely to increase [Van Dijk & Hacker, 2003]. As stated by *respondent #1* in the FGD, he almost became a victim of fraud when making online transactions. This also confirms that people less exposed to technology tend to be more vulnerable to digital fraud, especially *phishing* and *e-commerce fraud* [Choi et al., 2018]. Another thing is the inadequate adoption of essential security measures, such as password

management. Based on direct observation during the training activities, several participants could not remember the passwords installed on their digital devices or their e-mail or social media accounts. Some even had to ask their relatives (spouses or children) at home. This is because the digital accounts on their devices were not installed or registered by themselves. When they were introduced to the password manager application, many of them were still hesitant to use it because they were afraid that they would forget their master password later, *which* would make them completely unable to access their accounts. This behaviour regarding password management is increasingly depicted as unique and complicated when *respondent #2* in the FGD stated that her husband at home refused to change the password on his gadget or application, which was considered unsafe, even though he had been warned about the risks. This indicates resistance to the evolving habits related to efforts to anticipate potential security risks using digital technology.

For those with limited access to the latest technology, it will have an impact on strengthening the view that digital security measures are not or are not yet necessary [Elueze & Quan-Haase, 2018]. This makes their vulnerability to the risk of hacking even greater. This aligns with the findings during the training activities in Kebumen, when several respondents still use digital devices with relatively old production types and technical limitations. These limitations make it challenging to practice essential security features such as antivirus, two-factor authentication (2FA), or more technical ones related to *virtual private networks (VPNs)*. These devices' limitations are definitely risks to the digital security of their users.

On the contrary, the second interesting finding is the phenomenon of privacy fatigue, which contributes to the low usage of digital security measures by the participants. This is an unconcerned attitude towards privacy due to the pressure of addressing privacy [Choi et al., 2018]. In Kebumen, the training, which was not delivered in a hurry and thorough step-by-step on how to install antivirus or 2FA on various digital platforms, such as social media (Facebook, Instagram, TikTok and Twitter) and WhatsApp instant messenger, they feel if the steps to install this feature is not practical or not urgently needed.

This is a sign of *privacy fatigue*, with little emphasis on the need for privacy protection in daily technology usage. Inadequate understanding of security risks can also contribute to this attitude. When individuals do not understand how their data can be exploited, they tend not to care about the security of their personal information [Neumann et al., 2017]. They argue that they do not feel involved in “important” digital activities or risk being hacked.

Another thing that also emerged in the training session and FGD was related to online loan sharks. The lack of understanding of the participants about the risks when trapped by online loan sharks can have negative impacts, both economically and socially. Respondent #3 told us about some of his relatives who were victims of high-interest “*pinjol ilegal*” or online loan sharking. This also suggests that digital literacy education must include understanding financial risks in the digital world, including traps that can arise from easy access to online loans [Pangrazio et al., 2020]. Online loans are often

promoted as a quick and easy solution, but people who do not understand this scheme often get trapped in debt with very high interest rates. Respondent #4 told how his neighbour got trapped in an online loan cycle that damaged his financial stability and social relationships. People with low levels of digital financial literacy are more vulnerable to cyber financial traps, especially in developing countries [Reddy et al., 2023].

The digital literacy programme in Kebumen also revealed the importance of digital technology for Small and Micro Enterprises, especially in rural areas. The training participants, who are generally also small or micro business managers, have only basic knowledge of digital technology and are generally more comfortable using easy-to-understand and familiar platforms. In Kebumen, most participants still rely on simple platforms such as *WhatsApp Business* to sell online, and many of them are reluctant to use *e-commerce platforms* such as *Shopee* or *Lazada*. The reason is that although these platforms have relatively more complete features, they are considered more complex and not as simple as just using WhatsApp Business. This confirms that although digital technology offers significant economic potential, especially in rural areas, people will have difficulty taking advantage of this opportunity without adequate digital skills support. [HAJI, 2021]. But we also are aware that even though digital literacy has promoted income growth among rural residents, it also widens income disparities, particularly benefiting those with higher initial digital competencies [Liu & Zhou, 2023].

Due to limited expertise, many SMEs use digital technology only for marketing activities, not for more complex transactions such as stock management or online transactions [Kabanda & Brown, 2017]. As also happened in the Kebumen training, participants found managing more advanced *e-commerce platform features*, such as shipping or digital payments, difficult. However, after further examination in the FGD, their reluctance to use a more complete e-commerce platform was also related to digital infrastructure, especially Internet access. Although most villages in Kebumen already have Internet access, the quality and speed are often inadequate to support more complex e-commerce transactions. It should be noted that adequate Internet in rural areas will accelerate the adoption of technology among SMEs [AlBar & Hoque, 2019]. Conversely, inadequate Internet quality will result in SMEs in rural areas lagging in utilising digital technology [Harahap et al., 2024].

In the FGD, participants also stated that the main challenges they face are limited technical knowledge and the inability to adapt to technological changes quickly. Social factors, especially gender roles, also influence the success of digital technology adoption by digital literacy training participants in Kebumen. Indeed, unequal gender roles are often an obstacle to empowering women through digital technology because domestic responsibilities often prevent women from being involved in training and developing new skills [Chan et al., 2019]. Most of the training participants were married women who must shoulder the responsibility of large household domestic affairs, so they stated that they had limited time to learn and practice new digital technology skills.

4 Conclusion

Digital literacy can be understood as a “range of skills” that includes competencies across media literacy and information literacy, both integral for navigating a digital society [Leaning, 2019]. The capability approach emphasises digital literacy as a bridge from resources to functions, enhancing individual and community capabilities. [McDougall et al., 2018]. Implementing digital literacy training for former women migrant workers in Panjer Village, Kebumen, has provided a positive foundation in raising participants' initial awareness of digital security risks and introducing the essential use of digital technology. The training was an important first step for participants to acquire basic digital skills and learn about safe digital practices.

These trends raise the need for a more contextual and holistic approach to developing digital literacy programs during implementation. Educational interventions should be tailored to the needs and local realities of participants to ensure the information is understandable, useful, and relevant. In Panjer, a rural part of the country, there are structural barriers at every step preventing efficient adoption of digital technologies. The major challenge is that participants have limited access to the internet and digital devices, reducing their use of online resources and devices. However, there is an infrastructure gap, which results in unequal access to the service, worsening the digital divide between urban and rural areas.

Sociocultural factors present an additional challenge to women, particularly from a gender perspective. Women face systemic societal pressures that largely favour their position about the family at the expense of their own freedom and time to attend educational programmes. These demands are a major deterrent for women to spend time and energy upskilling / reskilling or learning new digital skills. Another major challenge is participants' understanding and awareness of digital security. Although education begins to increase awareness of digital risks, progress is often hampered by a phenomenon known as *privacy fatigue*. Among participants, the responsiveness and quality of digital security steps, like protecting devices, updating devices and managing passwords, felt overwhelming as these efforts were perceived as complex, repetitive, and burdensome. These challenges show that the best practices for the guarantees of power training in producing digital security are being implemented in reality.

Nonetheless, digital security remains vital to empowering women and bolstering their families' economic strength in rural areas. Implementing secure digital practices is crucial for safeguarding sensitive financial information, establishing trust with customers, and ensuring the longevity of business for women involved in small and micro enterprises. Through listening to and applying technology, these women will be able to grow their businesses, reach new customers, and broaden their journey from survival to thriving.

We will then offer policy recommendations based on our findings that various digital literacy programs can yield meaningful, inclusive, and sustainable impacts. These programs should address rural areas' unique challenges and support efforts to empower women and sustainably build capacity.

First, the design and implementation of digital literacy programmes need to take

a holistic approach. They can't just be about enhancing technical know-how, like how to use various digital tools and a grasp of fundamental technologies; they should also focus on ensuring that participants develop a critical consciousness. Critical thinking helps individuals be able to analyse digital content, assess information critically and see the timeline and challenges the digital world brings. Training participants not only as participants in technology but also as users through this holistic training ensures that the participants are not just consumers of technology but also helps them to use it in a smarter and responsible manner.

Second, digital literacy training must incorporate a gender-sensitive perspective to ensure inclusivity and maximise its effectiveness. Women, particularly those in underserved or marginalised communities, often face unique barriers to accessing and utilising digital resources. Programmes should address these barriers by considering women's diverse conditions, needs, and abilities. Digital literacy programmes can orient better towards engaging women by at least meeting some of their realities, such as availability of time, cultural considerations and different levels of prior knowledge, while content and method of delivery can be optimised to aid such engagement. That gender-sensitive approach makes sure women do not get behind during the digital transformation process and instead become empowered actors in the technology-driven society today.

Third, in rural areas, the design and execution of digital literacy programmes should be closely aligned with efforts to develop the economic potential of villages. Digital literacy initiatives must go beyond general training and link directly to supporting micro and small businesses in rural communities. By linking digital skills with economic activities and helping businesses to improve their marketing, access e-commerce platforms, or use digital tools to manage their finances, these programmes can also foster concrete, sustainable benefits. This also fosters the relevance of digital literacy training and ensures its longevity as the community can see tangible economic benefits tied back to their digital capabilities.

By implementing these strategies, future digital literacy programmes can become more inclusive, sustainable, and meaningful, whether aimed at rural communities, women's empowerment, or broader societal needs. A well-designed programme will empower individuals to thrive in the digital era and protect communities from the potential risks and adverse effects of today's evolving digital technologies.

References

- [1] AlBar, A. M., & Hoque, M. R. (2019). Factors affecting the adoption of information and communication technology in small and medium enterprises: a perspective from rural Saudi Arabia. *Information Technology for Development*, 25(4), 715–738. <https://doi.org/10.1080/02681102.2017.1390437>
- [2] Castilla, D., Botella, C., Miralles, I., Bretón-López, J., Dragomir-Davis, A. M., Zaragoza, I., & Garcia-Palacios, A. (2018). Teaching digital literacy skills to the elderly using a social network with linear navigation: A case study in a rural area. *International Journal of Human Computer Studies*, 118, 24–37. <https://doi.org/10.1016/j.ijhcs.2018.05.009>
- [3] Chan, C. M. L., Teoh, S. Y., Yeow, A., & Pan, G. (2019). Agility in responding to disruptive

- digital innovation: Case study of an SME. *Information Systems Journal*, 29(2), 436–455. <https://doi.org/10.1111/isj.12215>
- [4] Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51. <https://doi.org/10.1016/j.chb.2017.12.001>
- [5] Elueze, I., & Quan-Haase, A. (2018). Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited. *American Behavioral Scientist*, 62(10), 1372–1391. <https://doi.org/10.1177/0002764218787026>
- [6] Greene, J. A., Yu, S. B., & Copeland, D. Z. (2014). Measuring critical components of digital literacy and their relationships with learning. *Computers and Education*, 76, 55–69. <https://doi.org/10.1016/j.compedu.2014.03.008>
- [7] HAJI, K. (2021). E-commerce development in rural and remote areas of BRICS countries. In *Journal of Integrative Agriculture* (Vol. 20, Issue 4, pp. 979–997). Editorial Department of Scientia Agricultura Sinica. [https://doi.org/10.1016/S2095-3119\(20\)63451-7](https://doi.org/10.1016/S2095-3119(20)63451-7)
- [8] Harahap, V., Kamp, L. M., & Ubacht, J. (2024). A decision support scheme for solving the mobile coverage gap in rural areas in developing countries – Demonstrated with a case in Indonesia. *Technological Forecasting and Social Change*, 207. <https://doi.org/10.1016/j.techfore.2024.123600>
- [9] Kabanda, S., & Brown, I. (2017). A structuration analysis of Small and Medium Enterprise (SME) adoption of E-Commerce: The case of Tanzania. *Telematics and Informatics*, 34(4), 118–132. <https://doi.org/10.1016/j.tele.2017.01.002>
- [10] Leaning, M. (2019). An approach to digital literacy through the integration of media and information literacy. *Media and Communication*, 7(2 Critical Perspectives), 4–13. <https://doi.org/10.17645/mac.v7i2.1931>
- [11] Liu, B., & Zhou, J. (2023). Digital Literacy, Farmers' Income Increase and Rural Internal Income Gap. *Sustainability (Switzerland)*, 15(14). <https://doi.org/10.3390/su151411422>
- [12] McDougall, J., Readman, M., & Wilkinson, P. (2018). The uses of (digital) literacy. *Learning, Media and Technology*, 43(3), 263–279. <https://doi.org/10.1080/17439884.2018.1462206>
- [13] Neumann, M. M., Finger, G., & Neumann, D. L. (2017). A Conceptual Framework for Emergent Digital Literacy. *Early Childhood Education Journal*, 45(4), 471–479. <https://doi.org/10.1007/s10643-016-0792-z>
- [14] Pangrazio, L., Godhe, A. L., & Ledesma, A. G. L. (2020). What is digital literacy? A comparative review of publications across three language contexts. *E-Learning and Digital Media*, 17(6), 442–459. <https://doi.org/10.1177/2042753020946291>
- [15] [Reddy, P., Chaudhary, K., & Hussein, S. (2023). A digital literacy model to narrow the digital literacy skills gap. *Heliyon*, 9(4). <https://doi.org/10.1016/j.heliyon.2023.e14878>
- [16] Van Dijk, J., & Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. In *Information Society* (Vol. 19, Issue 4, pp. 315–326). <https://doi.org/10.1080/01972240309487>

Table of Pre-Test/Post-Test Multiple Choice Questions

Question	a	b	c	d
The statement that best describes the meaning of the Internet	A device that can search for information	Social media platforms like Instagram, Facebook, TikTok, and others	✓ A network of computers connected to each other worldwide	Smartphones, computers, or other devices that can run various applications
The following can be seen from our digital footprint on Google, except	Videos we watch on YouTube	Our search history on Google	Locations we have visited	✓ Phone calls we have made
Important things to consider when using Public WiFi	Make sure the WiFi is free to feel more comfortable	Use any available WiFi	Avoid using social media	✓ Do not use m-banking or perform sensitive transactions
If you receive a link from an unknown person via email or WhatsApp, this is what you can do	Open it to see what it contains	✓ Ignore and delete it	Share it with others	None of the above
We need to check our security status on Google to know	✓ On which devices we are logged in with our Google account	Whether our phone contacts have changed	How many hours per day we watch YouTube	Who we are connected with on Google
Enabling Two-Factor Authentication (2FA) is beneficial for	Making it easier to log into accounts	✓ Enhancing digital account security to prevent hacking	Making our social media more popular	Replacing passwords
A good password is a password that	Contains personal data such as a child's name or date of birth	Is easy to guess	Is the same for all accounts, such as email and social media	✓ Contains a combination of uppercase, lowercase letters, numbers, and symbols
One of the general principles of digital security is	✓ Nothing is 100% safe in the digital world	The more applications people use, the fewer security threats exist	Digital literacy related to security is only necessary for Gen-Z	All of the above
Important things to consider when installing applications on a phone, except	Make sure to install from official sources such as Play Store (Android) or App Store (iPhone)	Check the permissions requested by the application	✓ Only use applications that require an internet connection while in use	Check the storage space required by the application to ensure it does not slow down the phone
What needs to be done to maintain our digital security, except	Use strong and unique passwords for each account	Enable Two-Factor Authentication (2FA)	✓ Engage in oversharing or sharing personal data on social media	Think critically and avoid clicking on suspicious links

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

