

## Digital Ethics for Safe Online Shopping (Digital Literacy and Secure Online Transaction Education for the Tunggilis Village Community, Kalipucang)

**Elia Setiana, Budiman, Muhammad Rozan Aqila**

Informatics, Universitas Informatika dan Bisnis Indonesia

Email: elia.setiana@unibi.ac.id; budiman@unibi.ac.id; muhammadrozanaqila23@student.unibi.ac.id.

|                            |                                            |                              |
|----------------------------|--------------------------------------------|------------------------------|
| Accepted:<br>3 August 2026 | Accepted After Revision:<br>14 August 2026 | Published:<br>31 August 2026 |
|----------------------------|--------------------------------------------|------------------------------|

### Abstract

This community service program aimed to strengthen digital ethics and safe online-shopping practices among residents of Tunggilis Village, Kalipucang District, Pangandaran Regency. A preliminary interview with 30 residents indicated a practical literacy gap: 72% used the internet daily, 85% did not understand privacy settings, 63% had received suspicious messages or links, and only 22% knew how to report them. The program was conducted on 21-23 July 2025 through a participatory approach combining contextual presentations, interactive discussions, case studies, demonstrations, and simulations. The learning content covered responsible digital communication, personal-data protection, strong passwords, phishing and hoax recognition, online-store verification, secure payment practices, and complaint or reporting channels. Qualitative evaluation through facilitator observation, question-and-answer sessions, participant reflections, and simulation performance indicated that participants developed a more structured way of recognizing suspicious offers, protecting credentials, checking seller information, and selecting safer responses before completing online transactions. The activity also encouraged participants to use digital platforms more confidently, responsibly, and productively for everyday communication and commerce. The participatory, problem-based format was particularly suitable for rural community learning because it connected digital-safety principles with situations residents commonly encounter. Continuous mentoring, periodic refresher sessions, and a village digital-information corner are recommended to sustain these practices.

**Keywords:** digital ethics, digital literacy, online shopping, personal data protection, online fraud

## 1 INTRODUCTION

Digital transformation has expanded the ways in which people communicate, access information, and meet their daily needs. Activities that were previously conducted face-to-face are increasingly shifting to digital platforms, including product searches, price comparisons, payments, and communication with sellers. At the beginning of 2025, Indonesia was estimated to have approximately 212 million internet users, representing a penetration rate of 74.6% [1]. This substantial user base demonstrates that the internet has become an integral component of social and economic life, not only in urban areas but also in villages that are increasingly connected through smartphones and mobile networks.

Expanded access has not always been accompanied by the ability to use technology safely, critically, and responsibly. Indonesia's digital literacy framework identifies digital skills, digital ethics, digital

safety, and digital culture as four interrelated pillars [2]. In the context of online shopping, the ability to operate an application is insufficient. Users must also understand the consequences of sharing personal data, recognize manipulative communication, assess store credibility, read transaction terms, select secure payment methods, and retain transaction evidence. Without these competencies, digital convenience may become a source of financial loss, identity misuse, communication disputes, and the dissemination of inaccurate information.

The threats encountered by users are not limited to technical attacks. Digital fraud frequently exploits urgency, fear, the desire to obtain exceptionally low prices, or trust in identities that appear official. National cybersecurity reports and guidance continue to identify phishing, data breaches, account takeover, malware, and social-engineering-based fraud as risks that the public must understand [3]. The urgency of education is also



Publishing services by BPPM UNIBI

This is an open access article under the CC-BY-SA license (<https://creativecommons.org/licenses/by-sa/4.0/>)

reflected in the operation of the Indonesia Anti-Scam Centre. As of 23 March 2025, the centre had received 74,243 reports, with reported losses amounting to approximately IDR 1.4 trillion [4]. These figures indicate that transaction fraud is not merely an individual problem, but a public-protection challenge that requires preventive action at the family and community levels. At the community level, large losses can begin with everyday actions that appear minor, such as trusting an urgent link, disclosing an OTP, or transferring funds before independently verifying the recipient. Village-based education therefore functions as grassroots prevention by interrupting risky decisions before they develop into account compromise or financial loss.

Personal data protection is central to safe online shopping because digital transactions invariably involve user information. Law Number 27 of 2022 establishes the legal framework for personal data protection and the rights of data subjects [5]. Nevertheless, regulation alone does not automatically transform user behaviour. Communities still require concrete examples of information that must not be shared indiscriminately, such as one-time password (OTP) codes, personal identification numbers (PINs), passwords, identity photographs without a clear purpose, card numbers, and other authentication information. Users must also understand that fraudsters may impersonate couriers, bank officers, marketplace administrators, customer-service representatives, or officials of particular institutions.

Tunggilis Village is located in Kalipucang District, Pangandaran Regency, West Java. The village is connected to the principal Pangandaran-Cilacap route and supports economic activities in agriculture, plantations, livestock, trade, and home-based industries. Road access and widespread smartphone use create opportunities for online marketing and purchasing. However, preliminary interviews with 30 residents revealed a gap between the intensity of internet use and preparedness for digital security. Of the respondents, 72% used the internet every day, 85% did not understand privacy settings, 63% had received suspicious messages or links, and only 22% knew how to report them. These findings indicate that residents were active users, but had not yet developed adequate self-protection practices.

This community service program was developed in response to these needs under the theme "Digital Ethics for Safe Online Shopping." Digital ethics was understood not merely as politeness in written communication, but as an awareness of the need to respect others, refrain from disseminating hoaxes or engaging in bullying, avoid misusing data, and take responsibility for one's digital footprint. Safe online shopping, meanwhile, was directed toward the ability to make informed decisions before, during, and after a transaction. These two dimensions must be taught in an

integrated manner because secure users must also behave ethically, while ethical users still require technical skills to protect their accounts and transactions. The purpose was not to discourage residents from using digital services, but to equip them to communicate, shop, and participate in online economic activities more safely, confidently, and productively.

Media and information literacy emphasizes critical thinking, information verification, privacy protection, awareness of internet risks, and responsible decision-making [6]. In digital commerce environments, users are also exposed to interface designs and promotional strategies that may encourage hasty decisions. The OECD describes digital commercial patterns that may mislead, coerce, or manipulate consumer choices [7]. Educational materials should therefore extend beyond a list of permitted and prohibited actions and train participants to pause, examine evidence, compare information, and confidently cancel a transaction when suspicious indicators are identified.

Previous community service activities have demonstrated that participatory methods, hands-on practice, and cases closely related to participants' experiences can support improvements in digital literacy. A digital literacy and artificial intelligence education program in Tunggilis Village employed workshops, discussions, and simulations to connect technological concepts with community needs [8]. Another activity addressing online fraud prevention emphasized the importance of recognizing fraudulent methods, verifying information, and providing community-based assistance [9]. Digital skills training has also shown that project-based activities and interactive evaluation can strengthen participant engagement [10]. These findings informed the selection of communicative and contextual educational strategies for the present program.

The program aimed to enhance community understanding of digital ethics, build awareness of hoaxes and online fraud, provide practical skills for protecting accounts and personal data, and cultivate the habit of verifying seller credibility before completing transactions. Evaluation was intentionally formative and qualitative, drawing on participant activity during simulations, oral question-and-answer sessions, facilitator observation, and participant reflection. These sources were used to describe how participants recognized and responded to digital risks rather than to claim statistical effects. For future community service cycles, this formative approach can be strengthened with a brief structured pre-test/post-test instrument, a simulation rubric, and a follow-up checklist so that learning outcomes and behavioural adoption can be documented more systematically.

Table 1. Initial needs profile of the Tunggilis Village community.

| Indicator                                       | Finding                              |
|-------------------------------------------------|--------------------------------------|
| Daily internet use                              | 72% of the 30 residents interviewed. |
| Limited understanding of privacy settings       | 85% of respondents.                  |
| Received suspicious messages or links           | 63% of respondents.                  |
| Knew how to report suspicious messages or links | 22% of respondents.                  |

Source: preliminary interviews conducted by the implementation team with 30 residents, as documented in the activity report.

## 2 METHODS

### 2.1 Participatory Approach and Participants

The activity employed a participatory community service approach that positioned residents as active participants. Rather than delivering exclusively one-way presentations, the team invited residents to recount their experiences, assess sample messages, examine online store interfaces, and practise security measures. This approach was selected because digital ethics and security are strongly influenced by everyday habits. Knowledge is more likely to be applied when participants understand the relationship between the concepts presented and situations they have personally encountered.

The program was implemented in Tunggilis Village, Kalipucang District, Pangandaran Regency, from 21 to 23 July 2025. The preliminary needs assessment involved 30 residents. The training targeted community members who used smartphones, social media, messaging applications, banking services, or online marketplaces, and was designed for a general community audience rather than a specialized technical group. The available activity documentation recorded the 30-person figure for the preliminary interview but did not provide a separate verified total for training attendance; therefore, the manuscript does not equate the needs-assessment sample with the final attendance count. The implementation team consisted of Elia Setiana as team leader, Budiman as a faculty member, and Muhammad Rozan Aqila as a student member. The student's involvement focused on preparing materials, documenting activities, assisting participants, and strengthening communication between the team and the community.

### 2.2 Preparation and Learning Materials

The preparation stage began with coordination with the partner to agree on the theme, schedule, venue, participant characteristics, and learning needs. The team then reviewed the preliminary findings, developed case

examples, prepared presentation materials, and identified practices that participants could perform using their own smartphones. The materials were written in accessible language and avoided unnecessary technical terminology. Each security concept was translated into a concrete action, such as "do not share an OTP," "check the website address," "use different passwords," and "retain transaction evidence."

The educational content was organized into three clusters. The first addressed ethical digital communication, including courtesy, verification before sharing information, responsibility for comments, and respect for privacy. The second addressed account and data protection, including passwords, OTPs, two-factor authentication, privacy settings, and vigilance toward impersonation. The third addressed transaction security, including store verification, reviews, payment methods, links, additional fees, transaction evidence, complaints, and reporting procedures.

To facilitate understanding, the team introduced the "pause-check-decide" principle. Pause means refraining from immediately clicking a link or transferring funds when a message provokes an emotional response. Check means verifying the sender's identity, website address, store reputation, price, reviews, and payment method. Decide means proceeding, postponing, cancelling, or reporting the transaction on the basis of the verification results. This principle served as a simple reminder that residents could continue to use after the activity.

### 2.3 Implementation Procedure

The implementation stage combined concise presentations, question-and-answer sessions, experiential discussions, simulations, and case studies. Presentations provided the conceptual foundation. Discussions explored residents' experiences with prize links, parcel messages, transfer requests, and implausibly priced promotions. Simulations trained participants to distinguish legitimate from suspicious messages, assess store credibility, and formulate safe responses. Case studies demonstrated that decisions should not be based solely on logos, profile photographs, or language that appears official.

### 2.4 Qualitative Evaluation

Evaluation was conducted descriptively using four sources of information. First, facilitators observed participant involvement when assessing cases. Second, oral questions were posed at the end of each learning segment to examine understanding. Third, participants were asked to restate safe practices in their own words. Fourth, facilitators observed performance during simulations, including the ability to identify suspicious indicators, select appropriate actions, and name

information that must not be disclosed. This approach was suitable for formative evaluation in a community setting, but was not intended to generate statistical inference.

Qualitative indicators of success included participants' ability to: (1) explain the meaning of digital ethics; (2) identify the risks of sharing personal data; (3) recognize elements of phishing or scam messages; (4) distinguish reasonable promotions from offers that are too good to be true; (5) examine seller reputation and reviews; (6) use stronger passwords; (7) understand the function of two-factor authentication; and (8) identify the initial actions to take after experiencing fraud. These indicators guided observation and discussion rather than serving as a quantitative measurement scale.

Table 2. Stages of program implementation.

| Stage                | Principal activity                                                                                                  |
|----------------------|---------------------------------------------------------------------------------------------------------------------|
| Preparation          | Coordination with the partner, needs assessment, and identification of target participants.                         |
| Material development | Preparation of materials on digital ethics, privacy, fraud prevention, and secure transactions.                     |
| Implementation       | Presentations, discussions, case studies, demonstrations, and simulations.                                          |
| Formative evaluation | Observation, oral questions, reflection, and assessment of simulation performance.                                  |
| Follow-up            | Recommendations for mentoring, refresher materials, and the development of community digital literacy facilitators. |

### 3 RESULTS AND DISCUSSION

#### 3.1 Initial Conditions and Program Relevance

The initial conditions indicated that the internet was used routinely, but security practices had not yet become habitual. The high proportion of daily users demonstrated that the community already possessed access and basic experience. However, the finding that 85% of respondents did not understand privacy settings showed that operational ability was not aligned with the ability to control personal information. This issue is important because many applications request access by default to cameras, locations, contacts, microphones, or device storage. Without adequate understanding, users may approve every request or share data without considering its purpose and associated risks.

The finding that 63% of respondents had received suspicious messages or links demonstrated that digital threats were not remote possibilities, but experiences already present in residents' communication environments. Such messages may involve prize notifications, withheld parcels, threatened account suspension, invitations, employment offers, loans, social assistance, or requests to update personal data. The fact that only 22% knew how to report suspicious content

revealed a response gap. Some users may recognize that a message is suspicious but remain uncertain whether they should block or delete it, contact an official service, preserve evidence, or report it to the relevant platform or institution.

This gap reinforced the relevance of integrating ethics and security within a single program. Digital ethics helps residents understand that security is not limited to self-protection. Users also have a responsibility not to forward unverified links, upload other people's identity documents, shame fraud victims, or disseminate personal data in group conversations. Digital ethics therefore contributes to a culture of mutual protection, while security skills provide concrete measures through which such a culture can be implemented.

The village context also influenced the educational design. Close social relationships can be an advantage because information can circulate through families, community groups, and village authorities. However, social proximity may also create risk when messages are forwarded without verification simply because they were received from a known person. Participants were therefore reminded that "sent by someone familiar" does not necessarily mean "the information is accurate." A friend's account may have been compromised, a telephone number may have been taken over, or the sender may have forwarded information without checking its source.

#### 3.2 Implementation of Participatory Education

The activity was conducted in an interactive environment. Participants did not merely listen, but actively asked questions and shared experiences concerning promotions, links, prize messages, marketplace transactions, and communication with sellers. This engagement was valuable because participants' experiences provided authentic cases that were easier to understand than overly general examples. Facilitators subsequently connected each experience to relevant safety principles, such as checking official channels, avoiding payments outside the platform, and never disclosing OTPs.

One interactive moment occurred when facilitators presented prize-style and urgent account messages during the simulation. Several participants initially focused mainly on whether the sender used an unknown number, consistent with the pattern observed at the beginning of the session. Guided questioning then prompted them to identify additional warning signs, including requests for confidential data, time pressure, inconsistent website addresses, and payment outside official channels. This exchange illustrated a shift from single-cue judgments toward a more layered verification process.

Presentations were kept concise so that more time could be devoted to discussion and practice. During the digital ethics session, participants assessed several communication examples: abusive comments directed at sellers, dissemination of screenshots containing telephone numbers, forwarding news without a source, and posting complaints that exposed personal data. The discussion demonstrated that several actions considered routine could harm others or increase risk. Participants were encouraged to present complaints factually, conceal sensitive data, and use complaint channels before disseminating information publicly.

During the account security session, participants examined examples of weak and strong password characteristics. The team emphasized long passphrases that were unique to each service and did not contain easily guessed information. Participants were also introduced to two-factor authentication. The explanation focused not on technical terminology, but on its function: even when a password becomes known to another person, an additional authentication layer may help prevent unauthorized access. Participants were reminded that an OTP is a temporary key and must never be disclosed to anyone, including a person claiming to be an authorized officer.

During the online shopping session, participants practised assessing stores according to account age, number of transactions, review patterns, image consistency, product descriptions, prices, location, and return policies. They were asked to distinguish informative reviews from repetitive or excessively uniform reviews. Facilitators also explained that a high star rating alone is insufficient; users should read the review content, examine customer photographs, consider dates, and compare similar products.

The link and payment session emphasized checking website addresses, refraining from entering credentials through randomly distributed links, and avoiding transactions that require payment outside marketplace systems. Participants were shown messages designed to create urgency, such as "your account will be closed in five minutes" or "your prize expires today." They were trained to recognize time pressure as a manipulation technique. The recommended response was to close the message, independently open the official application, and contact an official service through the application's menu or the legitimate website.

The documentation in Figure 1 shows a presentation and dialogue session with residents. Visual examples helped participants identify the characteristics of suspicious offers and relate them to everyday experiences. The facilitator's close proximity to participants also supported two-way communication, enabling questions to be addressed immediately without creating an excessively formal classroom atmosphere.



Figure 1. Presentation and discussion of digital ethics with residents of Tunggilis Village.

### 3.3 Strengthening Digital Ethics

The discussion indicated that participants began to understand digital ethics as a set of considerations applied before communicating and sharing information. The principal criteria emphasized were accuracy, necessity, safety, and courtesy. Information should be verified for accuracy; sharing should be assessed for its usefulness; data should be protected; and language should preserve the dignity of others. This simple framework helped participants evaluate actions that had previously been performed spontaneously.

In online shopping, ethics also applies to the relationship between consumers and sellers. Consumers have the right to submit complaints, but should describe the problem accurately, provide an opportunity for resolution, and avoid threats or insults. Conversely, sellers are obligated to provide honest information and refrain from manipulating consumers. This understanding is important because transaction security depends not only on technology, but also on human behaviour on both sides of the exchange.

Participants were also encouraged to understand the persistence of digital footprints. Screenshots, comments, photographs, and transaction data may remain accessible for long periods and can be copied by others. When uploading evidence to support a complaint, telephone numbers, addresses, order numbers, payment codes, and identity photographs should be concealed. This practice is consistent with the principles of personal data protection [5] and media and information literacy competencies that emphasize privacy, security, and user responsibility [6].

The discussion of hoaxes focused on developing the habit of pausing before forwarding information. Participants were asked to examine the original source, date, context, provocative headlines, and consistency between the headline and content. They were also reminded that photographs or videos may be reused in a different context. Critical engagement therefore does not mean rejecting all information, but withholding trust until sufficient evidence is available.

Strengthening digital ethics can generate broader social benefits by encouraging participants to remind and assist one another. Residents who understand digital risks can support older family members or novice users. This role is particularly important in village communities, where informal learning frequently occurs through everyday conversation. To prevent such assistance from becoming victim blaming, participants were encouraged to respond empathetically and focus on recovery, reporting, and prevention.

### 3.4 Safe Online Shopping Skills

The skills practised covered three stages of a transaction: before purchase, during payment, and after purchase. Before purchasing, users should assess their needs, compare prices, examine store reputation, read product descriptions, evaluate reviews, and understand return policies. This stage helps prevent impulsive decisions caused by discounts, countdown timers, artificial scarcity, or unverifiable testimonials. The OECD report on dark commercial patterns explains that digital design may steer or manipulate consumer choices [7]. The ability to recognize pressure and postpone a decision is therefore an essential component of self-protection.

During payment, participants were encouraged to use official mechanisms that provide transaction records and consumer protection. Requests to move to private communication channels or make direct transfers should be treated as risk indicators, particularly when the stated reason is to avoid platform fees or obtain a lower price. Participants were also reminded to verify the recipient's name, transaction amount, additional fees, and payment purpose before confirming the transaction.

After making a purchase, users should retain payment evidence, conversations, order numbers, and delivery information. Such documentation is necessary when disputes arise. If the delivered product is unsuitable or inconsistent with the description, participants were advised to use the platform's complaint feature and upload evidence without exposing sensitive data. When financial fraud is suspected, initial actions include contacting the financial service provider, blocking the relevant account or card when necessary, changing passwords, preserving evidence, and reporting the incident through official channels.

The simulations enabled participants to recognize that a single message may contain several risk indicators simultaneously. Examples included an exceptionally low price, a very short deadline, a website address differing by one letter, a request for an OTP, and a threat that an account would be blocked. Participants who initially focused on only one indicator were guided to conduct a layered assessment. The greater the number of warning

signs identified, the stronger the justification for terminating the transaction.

To keep the guidance concise and actionable, the transaction material was summarized into a practical sequence: confirm the need and reasonableness of the price; verify store identity, reviews, and return policies; keep communication and payment within official channels; check links and recipient details; retain transaction evidence; and respond promptly through official services if an incident occurs. This operational summary reinforces the "pause-check-decide" principle introduced during the training without requiring participants to memorize a long list of rules.

Figure 2 presents a mentoring session that combined visual explanations with demonstrations using participants' devices and supporting documentation. This format enabled participants to follow each step sequentially. Hands-on learning also allowed them to ask about different settings on their respective smartphones, enabling facilitators to explain general principles without depending on a particular brand or application.



Figure 2. Guided practice in account security and secure digital transactions.

Table 3. Core learning materials and practices provided to participants.

| Dimension            | Core practice                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------|
| Communication ethics | Use courteous language, verify information, and conceal sensitive data.                           |
| Account security     | Use unique passphrases, enable two-factor authentication, and keep OTPs confidential.             |
| Store verification   | Examine store identity, transaction history, review content, prices, and return policies.         |
| Payment security     | Use official channels, verify the recipient and amount, and avoid transfers outside the platform. |
| Incident response    | Preserve evidence, contact official services, secure accounts, and submit a report.               |

### 3.5 Qualitative Outcomes and Participant Responses

Based on facilitator observations, oral questions, and discussions, participants demonstrated a more structured understanding of digital threats. At the beginning of the session, several participants identified

fraud primarily on the basis of an "unknown number." Following the simulations, they began to apply more comprehensive indicators, including requests for confidential data, time pressure, inconsistent website addresses, unreasonable prices, and payment outside the platform. This change in the way participants explained risk suggests development in their analytical framework, although it was not measured through quantitative scores.

Participants were also able to identify information that must remain confidential, particularly passwords, PINs, and OTPs. The discussion showed that the term OTP was familiar, but not all participants understood that the code must not be disclosed even to a person claiming to be an official. After the explanation and case studies, participants were able to associate an OTP with access to transactions. Understanding its function is more important than memorizing a definition because it supports decision-making when users receive urgent calls or messages.

During store-verification practice, participants became more critical of discounts and reviews. They began to compare multiple sources of information rather than relying exclusively on star ratings. Participants also understood the importance of reading negative reviews to identify recurring problems, such as products that did not match their descriptions, fictitious deliveries, or services requesting additional payments. This skill supports more rational consumer decisions and reduces dependence on visual promotions.

Community responses to the activity were positive. Enthusiasm was reflected in the number of questions, willingness to share experiences, and active involvement in the simulations. Near-fraud experiences generated productive discussion because participants recognized that digital risks were also experienced by people within their immediate social environment. Throughout this process, facilitators ensured that personal experiences were not used to shame victims. Attention was directed toward warning signs, alternative decisions, and recovery measures.

The outcomes are consistent with previous digital literacy community service activities that emphasized the importance of contextual and participatory approaches [8], [9]. A distinctive feature of the present program was its treatment of digital ethics and online shopping security as an integrated domain. This integration is important because safe decisions require both technical competence and responsible attitudes. Participants were trained not only to protect their accounts, but also to avoid disseminating information that could harm others.

The qualitative evaluation was intentionally formative. Across facilitator observation, oral responses, participant reflection, and simulation performance, participants increasingly articulated safer reasoning

steps and participated actively in verification practice. These findings are presented as activity-based evidence of learning and engagement, while the measurement improvements recommended for future programs are concentrated in the dedicated limitations and development section.

Table 4. Summary of the program's qualitative outcomes.

| Outcome indicator            | Qualitative finding                                                                                             |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Awareness of digital threats | Participants identified a broader range of phishing, scam, and impersonation indicators.                        |
| Personal data protection     | Participants understood the importance of keeping passwords, PINs, and OTPs confidential.                       |
| Online store assessment      | Participants used reviews, transaction history, prices, and policies as verification criteria.                  |
| Payment security             | Participants understood the risks of transfers outside the platform and the importance of verifying recipients. |
| Ethics and reporting         | Participants understood the need for verification, courteous language, data concealment, and official channels. |

### 3.6 Program Sustainability

Sustainability is important because fraudulent methods and application features continue to evolve. A single activity can establish a foundation, but the development of consistent habits requires reinforcement. Village authorities can reuse presentation materials, leaflets, or short messages as periodic reminders. Information should focus on actions that are easy to implement and should be updated in response to developments, such as changes in reporting channels or emerging impersonation methods.

Establishing community digital literacy facilitators may provide a low-cost sustainability strategy. These facilitators do not need to be technical experts, but should be able to communicate basic principles, help residents access official channels, and direct cases to the appropriate institutions. They may also collaborate with Family Welfare Empowerment (PKK) groups, youth organizations, schools, micro, small, and medium enterprises (MSMEs), and village authorities so that security messages reach different age groups.

A further recommendation is the establishment of a village digital information corner. This initiative may take the form of a physical space or a communication channel containing concise guidance, official service numbers, examples of fraudulent methods, and consultation schedules. To remain secure, the channel must be managed through clear rules and must never ask residents to submit passwords, OTPs, or sensitive

documents. Its primary function should be education and referral rather than replacing formal complaint procedures.

For MSME operators, security literacy can be expanded to include business-account protection, the use of official payment mechanisms, customer data management, and ethical promotion. The benefits of the program would therefore extend beyond reducing consumer risk to supporting the use of technology for local economic activities. Future programs could integrate digital security with marketing, customer service, and transaction record management.

Collaboration between higher education institutions and villages should be organized as a cycle of needs assessment, education, evaluation, and mentoring. Higher education institutions can update materials and provide facilitators, while village authorities can mobilize participants and contribute knowledge of the local context. This model supports community service that extends beyond ceremonial activities and gradually develops community capacity.

### 3.7 Limitations and Implications for Further Development

The preliminary needs profile was based on interviews with 30 residents and was used to tailor the learning content to local conditions rather than to represent the entire village population. Future programs can strengthen this stage by documenting participant characteristics more systematically and, where appropriate, differentiating needs according to age, digital experience, occupation, and commonly used applications.

For future development, the qualitative evaluation should be complemented by a brief structured instrument that remains practical for community settings. A short pre-test/post-test can assess recognition of phishing, confidential data, risky stores, and secure payment practices; simulation performance can be scored with a simple rubric; and a one- to three-month follow-up can document whether participants apply practices such as stronger passwords, two-factor authentication, store verification, evidence retention, and official reporting. Evaluation should remain accessible and must never request passwords, OTPs, PINs, account numbers, or other sensitive data.

Medium-term reinforcement is also important because immediate understanding may weaken when it is not practised. Reminder messages, refresher sessions, community digital-literacy facilitators, and the proposed village digital information corner can be used to sustain the "pause-check-decide" habit and provide residents with safe referral points when new fraud patterns emerge.

An implication for community service practice is the need for a cycle that connects education, practice, evaluation, and post-activity support. Fraudulent methods may change, but the underlying principles remain relatively stable: verify identity, protect credentials, use official channels, retain evidence, and report incidents. Emphasizing these principles helps residents respond to new fraud patterns without having to memorize every emerging method.

For community service research, a context-sensitive evaluation model can integrate brief knowledge measures, simulation performance, behavioural follow-up, and sustainability indicators. Such evidence would help higher education institutions identify the most effective materials and determine which community groups require more intensive mentoring.

At the institutional level, the activity also demonstrated the importance of sustained partnerships between higher education institutions and village governments. Higher education institutions provide updated knowledge and evaluation methods, while villages contribute context, social networks, and information dissemination mechanisms. This collaboration could be expanded to include financial institutions, law-enforcement agencies, literacy communities, and platform providers to strengthen referral mechanisms and incident responses.

## 4 CONCLUSION

The "Digital Ethics for Safe Online Shopping" program addressed the gap between routine internet use and the need for safer, more responsible digital practices among residents of Tunggilis Village. Through contextual presentations, participatory discussions, case studies, demonstrations, and simulations, participants practised ethical communication, personal-data protection, account security, store verification, secure payment, and incident response. Qualitative observations indicated a more structured approach to identifying suspicious messages, protecting credentials, assessing seller credibility, and making cautious transaction decisions. The program also positioned digital safety as an enabler of productive online participation rather than merely a defensive response to fraud. For future development, the program is recommended to add a brief structured pre-test/post-test instrument, a simulation rubric, and medium-term follow-up while continuing periodic mentoring, community digital-literacy facilitation, and a village digital information corner. Participatory digital-literacy education can therefore become an important foundation for protecting rural communities from cybercrime threats while enabling more confident, responsible, and productive use of digital technology.

## REFERENCES

- [1] DataReportal, "Digital 2025: Indonesia," 2025.
- [2] Ministry of Communication and Informatics of the Republic of Indonesia and Katadata Insight Center, Digital Literacy Status in Indonesia 2022. Jakarta, Indonesia, 2022.
- [3] National Cyber and Crypto Agency of the Republic of Indonesia, Indonesia Cybersecurity Landscape 2024. Depok, Indonesia: BSSN, 2025.
- [4] Financial Services Authority and the PASTI Task Force, "Beware of Fraudulent Websites Impersonating the Indonesia Anti-Scam Centre (IASC)," Press Release SP 3/STPASTI/III/2025, Mar. 2025.
- [5] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, 2022.
- [6] A. Grizzle et al., Media and Information Literate Citizens: Think Critically, Click Wisely! Media and Information Literacy Curriculum for Educators and Learners. Paris, France: UNESCO, 2021.
- [7] OECD, "Dark Commercial Patterns," OECD Digital Economy Papers, no. 336, 2022, doi: 10.1787/44f5e846-en.
- [8] B. Budiman, E. Setiana, and D. I. Pirdaus, "Enhancing Digital Literacy and the Use of Artificial Intelligence: Innovative Educational Strategies for Communities," *Jurnal Bhakti Karya dan Inovatif*, vol. 6, no. 1, pp. 7-12, 2026, doi: 10.37278/bhaktikaryadaninovatif.v6i1.1360.
- [9] E. Rosliani, D. Rahayu, Y. Nugraha, Yusep, and M. Fauzan, "Enhancing Digital Competence to Empower the Sirnajaya Village Community: Staying Safe in the Digital World by Recognizing and Preventing Online Fraud," *Jurnal Bhakti Karya dan Inovatif*, vol. 5, no. 2, pp. 140-149, 2025.
- [10] R. W. Arifin, A. N. Alfian, Sumardiono, and R. R. Awiliyanto, "Developing Digital Skills among Vocational High School Students through the Use of Generative AI," *Jurnal Bhakti Karya dan Inovatif*, vol. 5, no. 1, pp. 63-72, 2025.