Devosia: Community Outreach Journal of Indonesian Movement
Vol 1 No 4 October 2026, Hal 15-27
ISSN: 3163-8430 (Electronic)
Open Access: https://researchfrontiers.id/devosia/index

Developing Community Digital Safety Capacity through Participatory Cybersecurity Literacy for Micro-Entrepreneurs and Local Community Organizations

Abdul Kholik[1*], Edward Francis G. Gabor[2], Yassine HADDIOUI[3], Dilli Ram Rai[4]
[1] Universitas Negeri Jakarta, Indonesia
[2] Pamantasan ng Cabuyao, Philippines
[3] University Mohamed V in Rabat, Morocco
[4] Jana Chetana Secondary School and Pursuing, Nepal
email: abdulkholik@unj.ac.id[1]

Article Info :
Received:
26-09-2026
Revised:
27-10-2026
Accepted:
02-11-2026

Abstract

Digitalization has expanded opportunities for micro-entrepreneurs and local community organizations while simultaneously increasing their exposure to account compromise, online fraud, social engineering, privacy breaches, and other forms of cyber risk. Despite the growing emphasis on cybersecurity awareness, many community-level interventions remain centered on one-way information delivery and provide limited attention to how cybersecurity knowledge can be transformed into sustained protective practices and collective capacity. This study aims to develop and examine a participatory cybersecurity literacy approach for strengthening digital safety capacity among micro-entrepreneurs and local community organizations. The study employed an applied community-based intervention design combining contextual cybersecurity assessment, participatory learning activities, practical simulations, guided security practices, and pre- and post-intervention assessment of digital safety capabilities. The intervention addressed core domains of cybersecurity literacy, including password and account protection, phishing and social-engineering recognition, privacy and personal-data protection, secure digital transactions, device security, and incident-response practices. The results indicate that the participatory approach strengthened participants' understanding of common cyber risks while improving the translation of cybersecurity knowledge into practical protective routines and encouraging greater collective awareness of digital threats. The study contributes a community-centered framework for connecting individual cybersecurity literacy with organizational and collective digital resilience, offering a practical basis for designing more contextual, inclusive, and sustainable cybersecurity capacity-building programs for vulnerable digital communities.

Keywords: *Cybersecurity Literacy, Digital Safety, Micro-Entrepreneurs, Participatory Learning, Community Resilience*

©2026 Authors.. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.
(https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

The rapid diffusion of digital commerce, mobile financial services, cloud-based platforms, and social media has transformed the operating environment of micro-entrepreneurs and local community organizations, while simultaneously expanding their exposure to phishing, credential theft, social engineering, payment fraud, data leakage, and other forms of cyber-enabled disruption. For small businesses with limited financial, technical, and managerial resources, cybersecurity is no longer confined to the protection of sophisticated information systems but increasingly concerns the everyday practices through which owners and community members authenticate accounts, manage customer information, conduct digital transactions, and respond to suspicious online activities (Adriko, 2024; Al-Dosari & Fetais, 2023). Research on SMEs indicates that digital transformation can generate substantial opportunities for market access and operational efficiency, yet these benefits remain accompanied by cybersecurity vulnerabilities when organizational capabilities and security practices fail to evolve at a comparable pace (Benjamin et al., 2024; Yigit Ozkan & Spruit, 2023). This tension is particularly significant in community-based economic environments, where digital adoption may occur rapidly through informal learning and platform use without a corresponding development of systematic cybersecurity awareness, institutional routines, or collective mechanisms for managing digital risks.

Recent scholarship increasingly conceptualizes cybersecurity as a socio-technical capability rather than a purely technological function, emphasizing the interaction between infrastructure, organizational processes, individual behaviour, and contextual conditions. Perozzo et al. (2022) demonstrate the relevance of a socio-technical perspective for understanding SME cybersecurity readiness, while Pollini et al. (2022) emphasize that human factors constitute an integral component of cybersecurity rather than an external variable that can be addressed independently of technological systems. Evidence from awareness research similarly suggests that possessing general knowledge about information security does not automatically translate into consistent protective behaviour, making the quality, contextual relevance, and behavioural orientation of cybersecurity education particularly consequential (Baraković & Baraković Husić, 2022; Rohan et al., 2023). This body of scholarship shifts the analytical focus from whether communities possess digital technologies toward whether they possess the knowledge, routines, confidence, and collective capacity required to use those technologies safely and sustain protective practices under changing threat conditions.

The literature on cybersecurity interventions provides further evidence that training can influence security-related knowledge and behaviour, but its effectiveness appears contingent upon how closely learning activities correspond to users' actual risk environments and decision-making processes. Khan et al. (2023), for example, demonstrate the value of protection-motivation-based cybersecurity awareness training while evaluating outcomes through a structured training-assessment framework, indicating that awareness interventions should extend beyond the passive transmission of technical information. Argyridou et al. (2023) similarly frame cyber hygiene as a structured awareness methodology that connects data privacy and cybersecurity practices with organizational routines, whereas Ugbebor et al. (2024) highlight the importance of tailoring awareness programmes to SME contexts and human-error risks. These findings collectively suggest that cybersecurity literacy is more consequential when it is embedded in practical activities that allow participants to recognize threats, rehearse protective responses, and connect security principles with the digital practices that structure their economic and organizational activities.

Despite this progress, an important conceptual and empirical gap remains concerning the scale at which cybersecurity literacy should be developed among economically vulnerable micro-enterprises and community organizations. Existing SME-oriented studies frequently examine cybersecurity readiness, maturity, risk management, or technological safeguards at the organizational level, whereas community-based interventions tend to emphasize general awareness without systematically connecting individual learning outcomes to the resilience of local economic networks (Al-Dosari & Fetais, 2023; Yigit Ozkan & Spruit, 2023). The distinction matters because micro-entrepreneurs commonly operate through highly personalized digital accounts and informal business processes, meaning that a security failure involving one owner, employee, family member, or community administrator can potentially affect customers, suppliers, payment channels, and other interconnected actors. A research approach that treats cybersecurity literacy solely as an individual competency therefore risks overlooking the relational and collective dimensions through which digital vulnerabilities are produced, transmitted, recognized, and mitigated within local communities.

The Indonesian context makes this gap particularly salient because the expansion of digital economic participation among small businesses has increased both the potential benefits of connectivity and the consequences of inadequate digital protection. Research concerning Indonesian SMEs associates cybersecurity skills with business development in the digital economy, while studies of community-oriented digital education demonstrate that awareness-building can become an important mechanism for strengthening users' ability to identify and avoid online threats (Napu et al., 2024; Anan et al., 2024). However, interventions that concentrate primarily on digital adoption or transaction skills may leave a capability gap when participants begin to depend on online marketplaces, social-media accounts, digital payments, and electronic communication without understanding account security, privacy protection, social engineering, or incident-response practices. The practical challenge is consequently not simply to increase technology use but to develop a form of digital participation in which economic opportunity and security capacity evolve together, particularly among actors whose limited resources make recovery from cyber incidents more difficult.

A further limitation concerns the participatory dimension of cybersecurity capacity building, which remains comparatively underdeveloped in the literature when contrasted with the extensive attention given to formal organizational security frameworks and awareness measurement.

Cybersecurity programmes designed externally may provide standardized information efficiently, yet their relevance can be weakened when training content does not reflect the language, routines, technological constraints, and threat experiences encountered by micro-entrepreneurs and local organizations in their everyday environments. Research on human factors and cyber hygiene indicates the importance of contextualizing security behaviour, while community-based training evidence in Indonesia points to the value of direct educational engagement for strengthening public awareness (Pollini et al., 2022; Saragih et al., 2024). Participatory learning therefore offers a potentially important bridge between formal cybersecurity knowledge and locally situated practice because participants can contribute their own experiences, identify recurring vulnerabilities, test protective responses, and collectively formulate routines that are more compatible with their actual digital activities.

The unresolved issue has both scientific and practical consequences because persistent cybersecurity vulnerability can constrain the sustainability of digital entrepreneurship even when access to technology, online markets, and digital financial services continues to expand. Digital resilience research emphasizes the capacity of organizations to anticipate, withstand, respond to, and recover from disruptive events, suggesting that resilience should be understood as an ongoing capability rather than a one-time achievement produced by the installation of security technologies (Kumar et al., 2024; Tzavara & Vassiliadis, 2024). For micro-entrepreneurs and community organizations, such resilience depends not only on technical safeguards but also on whether people can recognize suspicious behaviour, protect sensitive information, make informed decisions under uncertainty, and coordinate responses when incidents occur. A community-oriented cybersecurity literacy intervention consequently addresses a practical capability problem while also extending cybersecurity scholarship toward a more socially embedded understanding of how resilience can be cultivated among resource-constrained actors.

Against this background, this study positions participatory cybersecurity literacy as a community capacity-building mechanism through which micro-entrepreneurs and local community organizations can strengthen practical digital safety competencies and develop more resilient patterns of digital participation. The study aims to examine how a participatory approach to cybersecurity education can improve participants' capacity to recognize common cyber threats, protect digital identities and business information, apply safer online practices, and respond appropriately to potential security incidents within their everyday economic and organizational activities. Its theoretical contribution lies in connecting cybersecurity literacy, human-centred security behaviour, and community digital resilience within a single capacity-building perspective rather than treating them as isolated domains. Its methodological contribution lies in translating cybersecurity education into a participatory intervention that links diagnostic assessment, contextual learning, practical simulation, collective reflection, and post-intervention evaluation, thereby providing an empirically grounded framework for strengthening digital safety capacity among micro-entrepreneurs and local community organizations.

METHODS

This study employed a quasi-experimental one-group pretest–posttest design to measure changes in cybersecurity literacy and digital safety capacity among micro-entrepreneurs and members of local community organizations following a structured cybersecurity education program. Participants were selected purposively based on their active use of digital platforms for business transactions, communication, marketing, financial activities, or community administration, with the intervention focusing on five competency domains: password and account security, phishing and social-engineering detection, personal-data protection, secure digital transactions, and basic cyber-incident response. Before the intervention, participants completed a structured baseline assessment measuring their knowledge and self-reported safety practices, followed by a standardized learning intervention consisting of short instructional sessions, practical demonstrations, threat-recognition exercises, simulated phishing scenarios, and guided security configuration tasks. The same competency instrument was administered after the intervention to identify changes in participants' cybersecurity capacity, while observation sheets were used to document participants' performance during practical exercises. This design was selected because cybersecurity awareness cannot be adequately assessed through conceptual knowledge alone; behavioral application and the ability to recognize and respond to common threats constitute important dimensions of cybersecurity readiness (Pollini et al., 2022; Rohan et al., 2023; Khan et al., 2023; Perozzo et al., 2022).

Quantitative data were analyzed by comparing pre-intervention and post-intervention scores for each cybersecurity competency, including mean scores, percentage changes, competency distributions, and normalized gain where appropriate, enabling the intervention effect to be examined at both aggregate and domain-specific levels. The analysis also distinguished between knowledge-based improvement and practical performance to determine whether increased awareness was accompanied by greater ability to apply basic protective measures in realistic digital situations. Descriptive analysis was complemented by paired statistical testing when the distributional assumptions were satisfied, while a non-parametric alternative was applied when those assumptions were not met. The interpretation of the findings was guided by the socio-technical perspective, which recognizes that cybersecurity capacity among smaller organizations is influenced by the interaction of individual awareness, organizational routines, technological practices, and resource constraints (Al-Dosari & Fetais, 2023; Adriko, 2024; Yigit Ozkan & Spruit, 2023). The resulting evidence was used to identify which dimensions of community digital safety demonstrated the greatest improvement and which remained comparatively resistant to intervention, providing an empirical basis for developing a scalable community cybersecurity literacy framework for micro-enterprises and local organizations.

RESULTS AND DISCUSSION

Baseline Digital Safety Capacity and Cybersecurity Vulnerability

The baseline assessment identified a heterogeneous level of digital safety capacity among the 48 participants, consisting of 32 micro-entrepreneurs and 16 representatives of local community organizations. The overall pre-intervention cybersecurity literacy score was 54.6 out of 100, indicating that participants possessed basic familiarity with digital technologies but had not yet developed sufficiently consistent protective practices across the different stages of digital activity. The weakest baseline dimension was basic incident response, with a mean score of 46.8, followed by phishing and social-engineering recognition at 49.7, whereas secure digital transactions recorded the highest score at 61.5. This pattern indicates that routine exposure to digital commerce does not automatically translate into systematic cybersecurity competence, supporting the argument that digital transformation among smaller organizations can create new vulnerabilities when technological adoption develops faster than organizational security capability (Perozzo et al., 2022; Adriko, 2024).

The baseline results are presented in Table 1, which differentiates the five competency domains examined in the intervention. Account and password security obtained a mean score of 55.4, suggesting that participants generally understood the importance of passwords but lacked consistent implementation of stronger practices such as unique credentials, multi-factor authentication, and systematic account recovery protection. Personal-data protection was similarly moderate at 55.2, reflecting awareness of privacy risks but less developed understanding of how business and community information can be exposed through digital platforms. The relatively higher score for transaction security should not be interpreted as evidence of comprehensive cybersecurity readiness because transaction safety represents only one component of the broader socio-technical security environment (Al-Dosari & Fetais, 2023; Yigit Ozkan & Spruit, 2023).

Table 1. Baseline Cybersecurity Literacy of Participants

Cybersecurity competency	Participants (N)	Pretest Mean	Standard Deviation	Competency classification
Account and password security	48	55.4	10.8	Moderate
Phishing and social-engineering recognition	48	49.7	11.6	Low
Personal-data protection	48	55.2	10.4	Moderate
Secure digital transactions	48	61.5	9.7	Moderate
Basic cyber-incident response	48	46.8	12.1	Low
Overall cybersecurity literacy	48	54.6	8.9	Moderate

The comparatively weak performance in phishing recognition is particularly relevant for micro-enterprises because many small businesses depend on messaging applications, social media, online marketplaces, and electronic payment systems that expose users to impersonation, fraudulent links, deceptive requests, and credential theft. Participants were able to identify conventional examples of fraudulent messages but frequently struggled when suspicious messages used familiar business contexts, urgent payment requests, apparently legitimate logos, or language resembling communications from customers and service providers. This finding is consistent with research emphasizing that social engineering remains strongly dependent on human judgment and that cybersecurity interventions must address behavioral vulnerabilities rather than concentrate exclusively on technical controls (Olaniyan & Ogunola, 2024; Pollini et al., 2022). The finding also explains why cybersecurity awareness should be framed as an operational capability embedded in everyday business decision-making rather than as an abstract technological competence.

The baseline assessment further revealed differences between micro-entrepreneurs and community-organization representatives. Micro-entrepreneurs obtained an overall mean score of 53.1, while community-organization representatives obtained 57.5, producing a 4.4-point difference before the intervention. The gap was most visible in data-protection practices and incident-response knowledge, whereas the two groups showed relatively similar performance in transaction security. This distinction suggests that the nature of digital exposure affects cybersecurity capacity: entrepreneurs encounter risks through sales, payments, customer communication, and marketing, while community organizations face additional concerns involving member databases, administrative records, shared accounts, and communication channels.

Table 2. Baseline Cybersecurity Literacy by Participant Group

Competency	Micro-entrepreneurs (n=32)	Community organizations (n=16)	Overall
Account and password security	53.8	58.6	55.4
Phishing/social engineering	48.5	52.1	49.7
Personal-data protection	53.7	58.2	55.2
Secure digital transactions	61.0	62.5	61.5
Incident response	45.8	48.8	46.8
Overall	53.1	57.5	54.6

The relatively small difference between the two participant groups is analytically important because it demonstrates that cybersecurity vulnerability cannot be reduced to the characteristics of individual entrepreneurs alone. Both groups operated within resource-constrained digital environments in which security responsibilities were frequently distributed informally, meaning that a single compromised account could affect customers, suppliers, members, or other community actors. Such conditions correspond with the socio-technical interpretation of SME cybersecurity readiness, in which security outcomes emerge from interactions among people, organizational practices, technologies, and environmental conditions (Perozzo et al., 2022). The intervention therefore treated cybersecurity as a collective capacity problem rather than simply a matter of individual knowledge acquisition.

Another important baseline finding concerned the relationship between digital activity and security practice. Participants reported frequent use of smartphones, messaging applications, social-media platforms, electronic payments, and online marketplaces, but these practices were not consistently accompanied by protective mechanisms such as multi-factor authentication, periodic password review, privacy configuration, backup routines, or formal incident-response procedures. This pattern illustrates a digitalization paradox in which greater technological participation may increase economic opportunity while simultaneously expanding the number of points through which security failures can occur. Similar tensions have been identified in research examining digital transformation, cybersecurity risks, and organizational readiness among SMEs (Benjamin et al., 2024; Ozturk et al., 2024).

The baseline condition also supports the importance of contextualized cybersecurity education. Participants generally responded more effectively to concrete examples involving their own business or organizational activities than to generalized explanations of cybersecurity terminology. This observation is consistent with evidence that awareness programs become more meaningful when they are connected to actual human behavior, organizational processes, and recognizable risk scenarios (Argyridou et al., 2023; Ugbebor et al., 2024). The result suggests that community-based cybersecurity interventions should prioritize practical recognition and response capabilities rather than rely predominantly on lecture-based information transmission.

The findings are also consistent with the broader literature on cybersecurity measurement, which emphasizes that awareness instruments encompass multiple dimensions rather than a single universal construct. Rohan et al. (2023) demonstrate the diversity of cybersecurity-awareness measurement approaches, while Baraković and Baraković Husić (2022) show that knowledge does not necessarily translate automatically into secure behavioral practices. The baseline profile observed in this study similarly indicates that participants could possess general awareness while remaining vulnerable in specific situations requiring immediate judgment. This distinction became a central consideration in evaluating the post-intervention outcomes.

Effect of the Cybersecurity Literacy Intervention

Following the intervention, the overall cybersecurity literacy score increased from 54.6 to 81.7, representing an improvement of 27.1 percentage points or approximately 49.6% relative to the baseline score. Improvements occurred across all five competency dimensions, although the magnitude varied substantially between domains. Basic incident response recorded the largest increase, from 46.8 to 79.6, while phishing and social-engineering recognition increased from 49.7 to 82.4. The results indicate that practical, scenario-based cybersecurity education can produce substantial short-term improvements when learning activities are directly connected to the risks encountered in participants' everyday digital environments (Khan et al., 2023; Saragih et al., 2024).

Table 3. Pretest–Posttest Changes in Cybersecurity Competency

Cybersecurity competency	Pretest Mean	Posttest Mean	Mean Difference	Relative Improvement
Account and password security	55.4	83.1	+27.7	50.0%
Phishing and social-engineering recognition	49.7	82.4	+32.7	65.8%
Personal-data protection	55.2	80.3	+25.1	45.5%
Secure digital transactions	61.5	83.1	+21.6	35.1%
Basic cyber-incident response	46.8	79.6	+32.8	70.1%
Overall	54.6	81.7	+27.1	49.6%

The strongest gains in incident response and phishing recognition demonstrate the value of moving beyond conceptual instruction toward simulated decision-making. Participants were required to distinguish legitimate and suspicious messages, identify common manipulation techniques, determine appropriate reporting or verification actions, and practice immediate containment responses after hypothetical account compromise. Such exercises transform cybersecurity literacy from passive recognition into procedural knowledge, which is particularly important because many incidents originate from decisions made under time pressure or uncertainty. Khan et al. (2023) similarly emphasize the importance of structured cybersecurity awareness training, while Pollini et al. (2022) highlight the need to incorporate human factors into cybersecurity interventions.

Account and password security increased by 27.7 points, reaching 83.1 after the intervention, suggesting that participants could more readily translate general awareness into concrete protective actions. The training emphasized unique passwords, password managers, multi-factor authentication, recovery mechanisms, and the risks of credential reuse, thereby linking technical controls to everyday business routines. This outcome is relevant to the SME context because smaller organizations often lack

dedicated cybersecurity personnel and consequently depend heavily on users themselves to implement basic safeguards. The result supports the argument that security maturity can be improved when controls are translated into accessible practices appropriate to the operational capacity of smaller organizations (Yigit Ozkan & Spruit, 2023; Adriko, 2024).

Personal-data protection improved from 55.2 to 80.3, indicating a 25.1-point increase, although the post-intervention score remained slightly below the highest-performing dimensions. Participants demonstrated stronger recognition of sensitive customer and organizational information, improved awareness of unnecessary data sharing, and greater attention to privacy settings and account permissions. This outcome has particular significance because micro-enterprises frequently collect customer names, telephone numbers, addresses, transaction records, and payment-related information without formal data-governance procedures. The result reinforces the relevance of privacy-oriented cybersecurity education within broader digital literacy programs and aligns with Argyridou et al. (2023) regarding the integration of cybersecurity and data-privacy awareness.

Secure digital transaction competency increased by 21.6 points, from 61.5 to 83.1, representing the smallest relative improvement among the five dimensions. The smaller gain is partly attributable to participants' relatively stronger baseline familiarity with digital payments and online purchasing, meaning that the intervention had less room to produce large proportional improvements. Nevertheless, participants demonstrated greater ability to verify payment requests, distinguish official transaction channels from suspicious alternatives, and recognize risks associated with sharing authentication information. This finding is important because trust and security are intertwined in digital commerce, and weaknesses in either dimension can undermine continued participation in electronic transactions (Handoyo, 2024).

Table 4. Pretest–Posttest Comparison of Overall Cybersecurity Literacy

Indicator	Pretest	Posttest	Mean Difference	Statistical Result	Effect Size
Overall cybersecurity literacy	54.6 ± 8.9	81.7 ± 7.1	+27.1	$t(47) = 18.42$, $p < .001$	Cohen's $d = 1.98$
Normalized gain	N/A	N/A	0.60	N/A	N/A

The paired analysis indicates a statistically significant increase in overall cybersecurity literacy following the intervention, with the posttest mean substantially exceeding the pretest mean, $t(47) = 18.42$, $p < .001$, and a large standardized effect (Cohen's $d = 1.98$). The normalized gain of 0.60 further indicates a substantial proportion of the theoretically attainable improvement was achieved during the intervention period. These statistics strengthen the interpretation that the observed changes were not merely attributable to participants becoming familiar with the questionnaire itself. At the same time, the absence of a comparison group means that the findings should be interpreted as evidence of within-group improvement rather than definitive causal proof that excludes all alternative explanations.

The intervention also generated observable changes in practical security behavior. Before the program, only 15 of the 48 participants had enabled multi-factor authentication on their principal business or organizational accounts, whereas this number increased to 41 after the intervention. Similarly, the number of participants who correctly identified at least four of five simulated phishing scenarios increased from 17 to 42, while those able to articulate an appropriate immediate response to a compromised account increased from 14 to 39. These behavioral indicators are important because cybersecurity capacity should not be evaluated solely through declarative knowledge; practical application provides stronger evidence that learning has entered routine digital behavior (Baraković & Baraković Husić, 2022; Ugbebor et al., 2024).

Table 5. Practical Security Behaviors Before and After the Intervention

Practical indicator	Pre-intervention	Post-intervention	Increase
Participants enabling multi-factor authentication	15 (31.3%)	41 (85.4%)	+54.2 pp
Participants using unique passwords for key accounts	19 (39.6%)	40 (83.3%)	+43.8 pp
Participants correctly identifying ≥4/5 phishing scenarios	17 (35.4%)	42 (87.5%)	+52.1 pp
Participants checking links/senders before responding	21 (43.8%)	44 (91.7%)	+47.9 pp
Participants applying privacy/security settings	18 (37.5%)	39 (81.3%)	+43.8 pp
Participants able to state an appropriate incident-response sequence	14 (29.2%)	39 (81.3%)	+52.1 pp
Participants maintaining a basic backup routine	16 (33.3%)	37 (77.1%)	+43.8 pp

The practical results indicate that the intervention affected both preventive and responsive dimensions of cybersecurity capacity. The strongest behavioral movement occurred in phishing recognition, multi-factor authentication, and incident-response sequencing, all of which were directly practiced during the intervention rather than merely explained. This distinction is theoretically important because digital resilience requires organizations to absorb, respond to, and recover from disruptions rather than simply avoid every possible threat (Kumar et al., 2024; Tzavara & Vassiliadis, 2024). The results therefore position cybersecurity literacy as one component of a broader resilience capability in which knowledge, behavior, and organizational routines reinforce one another.

The findings are also consistent with community-oriented digital-literacy interventions in Indonesia. Anan et al. (2024) demonstrate the relevance of digital-awareness education for preventing online fraud among MSMEs, while Cahyanto et al. (2024) show the value of structured digital-literacy initiatives for MSME actors. Pratiwi et al. (2025) similarly emphasize the role of literacy strengthening in enabling MSMEs to adapt to digital transactions, while Wijaya and Juardi (2026) place cybersecurity education within broader community responses to emerging digital threats. The present intervention extends this orientation by concentrating specifically on cybersecurity competencies and by measuring changes through a pretest–posttest framework rather than relying solely on participant perceptions of training usefulness.

The intervention model can also be interpreted through the socio-technical perspective because the observed improvement did not depend on sophisticated cybersecurity infrastructure. Instead, the learning process connected relatively simple technical controls with human decision-making, organizational routines, and contextual risk recognition. This is consistent with Kumar et al. (2024), who conceptualize digital resilience as dependent on multiple organizational enablers, and with Perozzo et al. (2022), who argue that SME cybersecurity readiness requires integration between technical and social dimensions. The finding has practical significance for resource-constrained communities because meaningful improvements in digital safety do not necessarily require large investments in specialized cybersecurity systems when foundational practices remain underdeveloped.

From Individual Awareness to Community Digital Safety Capacity

The post-intervention results suggest that cybersecurity literacy can become a collective capability when individual learning is linked to shared routines and organizational practices. The intervention did not restrict learning to personal device protection but encouraged participants to consider how insecure practices could propagate across customers, family members, business partners, community members, and organizational networks. This perspective changes the analytical unit from the isolated digital user toward a local digital ecosystem in which vulnerabilities can move between interconnected actors. Such an interpretation corresponds with the broader conceptualization of cyber resilience as an organizational and systemic capability rather than a purely technical property (Tzavara & Vassiliadis, 2024).

One of the clearest changes was the emergence of shared security routines among participants. Following the intervention, 37 participants reported establishing a routine for periodic password review or credential-security checking, 39 reported adopting more systematic backup practices, and 40 reported

introducing verification procedures before responding to unusual payment or account requests. These changes demonstrate that training can stimulate organizational routines when participants perceive cybersecurity as directly relevant to operational continuity. The finding complements research suggesting that human behavior and organizational context are central determinants of cybersecurity outcomes, particularly in smaller organizations where formal security departments are absent (Pollini et al., 2022; Ugbebor et al., 2024).

Table 6. Community-Level Adoption of Digital Safety Practices

Community safety practice	Participants adopting practice after intervention	Adoption rate
Periodic account-security checking	37	77.1%
Regular backup of important digital information	39	81.3%
Verification of unusual payment/account requests	40	83.3%
Shared protocol for suspicious messages	36	75.0%
Designated person/contact for reporting incidents	34	70.8%
Privacy review for organizational/business accounts	38	79.2%
Periodic cybersecurity knowledge sharing	35	72.9%

The establishment of a shared suspicious-message protocol is particularly relevant because phishing and social engineering frequently exploit uncertainty regarding who should verify an unusual request. Before the intervention, participants tended to resolve suspicious messages individually, creating inconsistent responses and increasing the possibility that one user could inadvertently validate a malicious communication for others. After the intervention, 36 participants reported using a shared verification approach, indicating movement from individual judgment toward collective risk management. Such a shift is compatible with the socio-technical framing of cybersecurity and with the emphasis placed by Al-Dosari and Fetais (2023) on integrated risk-management systems for smaller organizations.

The creation of designated incident-reporting contacts also represents a meaningful organizational development. Thirty-four participants reported establishing a person or contact point responsible for receiving reports of suspicious digital activity, providing an elementary governance mechanism where previously responsibility had been diffuse. This practice is particularly useful for community organizations and micro-enterprises because the absence of formal IT personnel can cause uncertainty during the early stages of an incident. Research on SME cyber risk emphasizes that organizational readiness includes not only preventive technologies but also decision structures for recognizing and managing risk (Sukumar, 2023; Adriko, 2024).

The intervention further demonstrated that cybersecurity education can generate spillover effects beyond the direct participants. Participants reported sharing selected practices with employees, family members, fellow entrepreneurs, and community colleagues, creating an informal diffusion mechanism through which security knowledge could move beyond the training setting. Such diffusion is important because micro-enterprises and community organizations rarely operate as isolated entities; their digital activities are embedded in networks of customers, suppliers, relatives, payment providers, marketplaces, and local institutions. The community-level orientation therefore expands the potential impact of cybersecurity literacy from individual competence to network resilience.

Table 7. Participant-Reported Knowledge Diffusion After the Intervention

Dissemination activity	Participants	Percentage
Shared cybersecurity practices with family members	31	64.6%
Shared practices with business colleagues/employees	28	58.3%
Shared phishing examples with community members	34	70.8%
Helped another person activate MFA/security settings	26	54.2%
Shared incident-response procedures	24	50.0%
Participated in subsequent cybersecurity discussions	35	72.9%

The diffusion pattern provides a useful complement to the individual-level pretest–posttest findings because it demonstrates how educational effects may extend through social relationships. Community learning becomes more sustainable when participants can reproduce and communicate practices rather than depending continuously on external trainers. This is compatible with the human-factor perspective of Pollini et al. (2022) and the emphasis on contextualized cybersecurity training in SME environments reported by Ugbebor et al. (2024). It also indicates that community organizations can function as intermediary institutions for cybersecurity knowledge diffusion when they are equipped with simple, transferable procedures.

The results have implications for the conceptualization of digital resilience. Digital resilience should not be reduced to the ability to withstand a cyberattack through technological controls, because the findings demonstrate that preparedness, recognition, communication, and recovery procedures can be strengthened through relatively low-cost educational mechanisms. Kumar et al. (2024) identify multiple organizational enablers of digital resilience, while Tzavara and Vassiliadis (2024) emphasize the conceptual evolution of resilience toward adaptive capacity rather than simple resistance. The present findings support this broader interpretation by showing that resilience-building can begin with routine practices that improve the capacity of local actors to recognize disruption and coordinate an appropriate response.

At the same time, the results expose an important boundary between awareness and institutionalization. Although most participants adopted several protective behaviors, fewer than three quarters established formalized community procedures, suggesting that knowledge acquisition does not automatically produce durable governance structures. This distinction matters because cybersecurity practices can deteriorate when they are not embedded in organizational routines, periodically reviewed, or reinforced through continued learning. Similar concerns appear in research on SME cybersecurity maturity and sustainable digital transformation, where organizational readiness and resource constraints influence the persistence of newly adopted practices (Yigit Ozkan & Spruit, 2023; Benjamin et al., 2024; Ye, 2026).

The Indonesian context adds another dimension to this interpretation because digital safety is increasingly intertwined with the economic sustainability of micro-enterprises. Cybersecurity failures can interrupt transactions, compromise customer trust, expose sensitive information, and impose recovery costs that are disproportionately difficult for small businesses to absorb. Tetteh and Otioma (2025) demonstrate the relationship between cyberattacks, mitigation capabilities, and firm productivity, while Napu et al. (2024) connect cybersecurity and digital skills with the development of Indonesian SMEs. The present intervention therefore contributes to the practical literature by treating cybersecurity capacity as part of economic continuity rather than as a narrowly technical concern.

Finally, the findings indicate that participatory delivery remains useful even within a quasi-experimental design because participation can improve the contextual relevance of standardized cybersecurity content without changing the underlying evaluation structure. Participants were not merely exposed to generic security information; they worked through scenarios derived from digital activities encountered in micro-business and community settings, enabling the intervention to connect standardized competencies with local practices. This contextualization is consistent with evidence that effective awareness programs should reflect the actual risk environment and characteristics of their target populations (Khan et al., 2023; Argyridou et al., 2023). The resulting model can therefore be understood as a measurable cybersecurity-literacy intervention with community-oriented

implementation, combining quantitative evidence of competency change with practical mechanisms for embedding digital safety within local economic and organizational routines.

CONCLUSION

This study establishes community digital safety as a collective capacity rather than a narrowly technical capability located within individual users or organizations. The central contribution lies in demonstrating how participatory cybersecurity literacy can connect individual awareness, everyday protective practices, and community-level coordination into a more coherent foundation for digital resilience among micro-entrepreneurs and local community organizations. The study indicates that cybersecurity capacity becomes more meaningful when learning is embedded in participants' actual digital routines, including account management, transaction security, privacy protection, social-engineering recognition, and responses to suspicious digital activity. This perspective extends existing cybersecurity awareness approaches by positioning community participation, contextual learning, and shared responsibility as interconnected mechanisms through which vulnerable digital actors can strengthen their capacity to anticipate, recognize, and respond to cyber risks.

The findings carry implications for both cybersecurity scholarship and community-oriented digital development. Theoretically, the study supports a socio-technical understanding of cybersecurity in which human behavior, organizational routines, technological practices, and community relationships jointly shape digital safety capacity rather than operating as isolated determinants. Methodologically, the study demonstrates the value of participatory learning and practice-oriented assessment for examining cybersecurity interventions in settings where standardized technical indicators alone may not adequately capture changes in everyday digital behavior. For practitioners and policymakers, the study suggests that community cybersecurity programs should move beyond one-off awareness campaigns toward continuous, locally contextualized capacity-building that incorporates micro-enterprise needs, organizational realities, accessible learning materials, and mechanisms for peer support.

The interpretation of these contributions remains bounded by the community-based setting, the characteristics of participating micro-entrepreneurs and local organizations, and the duration and scope of the intervention. The study primarily captures cybersecurity capacity within the behavioral and community dimensions of digital safety and therefore does not constitute a comprehensive assessment of technical security infrastructure, advanced cyber-defense capabilities, or long-term organizational cybersecurity maturity. The findings should also be interpreted in relation to the contextual conditions under which the intervention was implemented, because differences in digital infrastructure, economic conditions, institutional support, prior digital experience, and exposure to cyber threats may shape the transferability of the approach to other communities.

Subsequent research can extend this contribution through longitudinal designs that examine whether participatory cybersecurity literacy produces sustained behavioral change and whether strengthened community capacity translates into measurable reductions in security incidents and economic disruption. Comparative research across different regions, sectors, and levels of digital maturity could further clarify which elements of participatory cybersecurity education are context-dependent and which constitute more generalizable mechanisms of community digital resilience, while mixed-method and quasi-experimental designs could strengthen causal assessment of intervention effectiveness. For the wider public, the study contributes a practical understanding that digital safety is not solely an individual responsibility or a matter of sophisticated technology, but can be developed through accessible knowledge, repeated practice, collective vigilance, and locally organized support. The broader significance of the research therefore rests in framing cybersecurity literacy as a form of community capacity that can help vulnerable economic actors participate more safely and sustainably in increasingly digital social and commercial environments.

REFERENCES

Adriko, R. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. *Information and Computer Security, 32*(5), 691–710. http://doi.org/10.1108/ICS-01-2024-0025.

Al-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. *Electronics, 12*(17), 3629. http://doi.org/10.3390/electronics12173629.

Angraen Napu, I., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis peran keamanan siber dan keterampilan digital dalam pertumbuhan usaha kecil menengah di era ekonomi digital di Indonesia. *Sanskara Ekonomi dan Kewirausahaan, 2*(3), 156–167. http://doi.org/10.58812/sek.v2i03.411.

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: Concept study. *Journal of Medical Internet Research, 25*, e41294. http://doi.org/10.2196/41294

Baraković, S., & Baraković Husić, J. (2022). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective, 32*(5), 347–370. http://doi.org/10.1080/19393555.2022.2088428

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances, 19*(2), 134–153. http://doi.org/10.30574/gjeta.2024.19.2.0084

Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon, 10*(8), e29714. http://doi.org/10.1016/j.heliyon.2024.e29714

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model. *Computers & Security, 125*, 103049. http://doi.org/10.1016/j.cose.2022.103049

Klitis, C., Makris, I., Bouzinis, P., Asimopoulos, D. C., Mallouli, W., Kioskli, K., Seralidou, E., Douligeris, C., & Christofi, L. (2024). NERO: Advanced cybersecurity awareness ecosystem for SMEs. *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–9. http://doi.org/10.1145/3664476.3670447

Kumar, V., Sindhwani, R., Behl, A., Kaur, A., & Pereira, V. (2024). Modelling and analysing the enablers of digital resilience for small and medium enterprises. *Journal of Enterprise Information Management, 37*(5), 1677–1700. http://doi.org/10.1108/JEIM-01-2023-0002

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis peran keamanan siber dan keterampilan digital dalam pertumbuhan usaha kecil menengah di era ekonomi digital di Indonesia. *Sanskara Ekonomi dan Kewirausahaan, 2*(3), 156–167. http://doi.org/10.58812/sek.v2i03.411

Olaniyan, J., & Ogunola, A. A. (2024). Protecting small businesses from social engineering attacks in the digital era. *World Journal of Advanced Research and Reviews, 24*(3), 834–853. http://doi.org/10.30574/wjarr.2024.24.3.3745

Perozzo, H., Zaghloul, F., & Ravarini, A. (2022). CyberSecurity readiness: A model for SMEs based on the socio-technical perspective. *Complex Systems Informatics and Modeling Quarterly, 33*, 53–66. http://doi.org/10.7250/csimq.2022-33.04

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*, 371–390. http://doi.org/10.1007/s10111-021-00683-y

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3), e14234. http://doi.org/10.1016/j.heliyon.2023.e14234

Saragih, S. P., Svinarky, I., & Ukas. (2024). Pelatihan cyber security awareness kepada masyarakat menghadapi perkembangan kejahatan siber. *PUAN INDONESIA, 6*(2). http://doi.org/10.37296/jpi.v6i2.340

Sukumar, A. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*. http://doi.org/10.1111/risa.14092

Tetteh, G. K., & Otioma, C. (2025). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics, 64*, 1493–1514. http://doi.org/10.1007/s11187-024-00946-8

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security, 23*, 1695–1719. http://doi.org/10.1007/s10207-023-00811-x

Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents. *Journal of Knowledge Learning and Science Technology, 3*(3), 382–409. http://doi.org/10.60087/jklst.vol3.n3.p382-409

Wijayanto, A., Abdillah, M. F., Maulidah, A. A., Maynardian, A., Madina, G. N., Wijaya, A., Gerungan, R. A. C., Najha, N., Ahsani, A. Z., & Ramadhan, S. M. (2025). Peningkatan kesadaran keamanan siber siswa SMK melalui pelatihan dan simulasi serangan dalam lingkungan virtual. http://doi.org/10.30822/hj4rr981

Yigit Ozkan, B., & Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems, 63*(4), 965–987. http://doi.org/10.1080/08874417.2022.2119442

Ye, W. (2026). Strengthening cybersecurity in small and medium-sized enterprises: Balancing technology, costs, compliance, and employee awareness. *SAGE Open*. http://doi.org/10.1177/21582440251414951

Zhen, J., Dong, K., Xie, Z., & Chen, L. (2022). Factors influencing employees' information security awareness in the telework environment. *Electronics, 11*(21), 3458. http://doi.org/10.3390/electronics11213458

Wijaya, R., & Juardi, D. (2026). Edukasi masyarakat tentang keamanan siber dalam tantangan dan solusi di era digital. *Jurnal Informatika dan Teknik Elektro Terapan, 14*(1). http://doi.org/10.23960/jitet.v14i1.8336

Anan, M., Rahmah, S. A., & Risuhendri, R. (2024). Meningkatkan kesadaran digital dalam pencegahan penipuan online untuk kelompok UMKM Desa Tanjung Haratan. *ABDI DALEM: Jurnal Pengabdian Kepada Masyarakat, 1*(2), 56–63. http://doi.org/10.70585/abdidalem.v1i2.29

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum, 6*(1), 132–134. http://doi.org/10.38043/jah.v6i1.4484

Cahyanto, R. P., Agustini, V. D., Khotimah, W. Q., & Wardana, A. K. (2024). Education & community PaDi UMKM program as a digital literacy effort for MSME players. *ELS Journal on Interdisciplinary Studies in Humanities, 7*(4), 607–616. http://doi.org/10.34050/els-jish.v7i4.42302

Pratiwi, E., Saidah, M., & Rahmawati, I. (2025). Penguatan literasi digital dalam adaptasi teknologi transaksi jual beli bagi UMKM Desa Kanekes Baduy. *Abdi: Jurnal Pengabdian dan Pemberdayaan Masyarakat, 7*(3). http://doi.org/10.24036/abdi.v7i3.1336

Wicaksana, P. B., Randikaparsa, I., Fatchan, I. N., Pramurindra, R., & Kusuma, H. R. (2026). Pelatihan pemanfaatan ChatGPT untuk meningkatkan literasi digital UMKM ibu-ibu PKK di Kecamatan Rakit, Kabupaten Banjarnegara. *Jurnal Pelayanan Masyarakat, 2*(4). http://doi.org/10.62951/jpm.v2i4.2702.