Transformatif: Jurnal Pengabdian Masyarakat
Vol.7, No.2, July-December 2026, pp. 120-150
https://doi.org/10.22515/tranformatif.v7i2.15590
ISSN: 2745-3847 (P) ISSN: 2745-3855 (E)

Inclusive Cybersecurity Literacy in Cybercrime Prevention Among MSME Operators in Lhokseumawe

Safwan[1*], Nur Sari Dewi[2], Nora Maulana[3], Friyal Dara Azkia[4] , Nur Zahra Azira[5]

Universitas Islam Negeri Sultanah Nahrasiyah, Lhokseumawe, Indonesia[1,2,3,4,5]
*Corresponding author's email: safwan@uinsuna.ac.id

Keywords:
cybersecurity literacy; MSMEs; participatory action research; digital transformation; community engagement; digital resilience

Abstract

The rapid digitalization of Micro, Small, and Medium Enterprises (MSMEs) has increased exposure to cyber threats, while limited cybersecurity literacy remains a major challenge for business sustainability. This community service program developed and evaluated a contextual cybersecurity mentoring model designed to strengthen digital security awareness and practices among MSME *owners* in Lhokseumawe, Indonesia. Using a Participatory Action Research (PAR) approach, the program integrated needs assessment, cybersecurity education, hands-on training, and continuous mentoring tailored to the actual cyber risks faced by MSMEs. Sixty MSME operators under the Rumah BUMN Lhokseumawe participated in the program. Effectiveness was assessed using pre- and post-test instruments and analyzed through paired-sample *t*-tests and normalized gain (N-Gain). The results demonstrated a significant improvement in participants' cybersecurity literacy, with mean scores increasing from 41.45 before the intervention to 93.25 afterward ($p < 0.001$). The N-Gain score of 0.876 indicated a high level of learning effectiveness. Participants also showed substantial improvements in cybersecurity knowledge, digital security practices, and risk awareness, enhancing their capacity to prevent cyber threats and strengthen business resilience. The findings demonstrate that an adaptive, participatory, and locally contextualized mentoring model is an effective strategy for improving cybersecurity literacy among MSMEs. This model provides a scalable framework for supporting secure digital transformation and can be replicated in MSME empowerment initiatives across other regions.

Submitted: May 13, 2025 | Accepted: July 17, 2026 | Published: July 19, 2026

Introduction

Advances in information and communication technology have significantly transformed the way society operates, including in the economic and entrepreneurial sectors. Digitalization opens up significant opportunities for Micro, Small, and Medium Enterprises (MSMEs) to grow through digital marketing, online transactions, and integration with the national digital economy ecosystem. In Indonesia, MSMEs have become the backbone of the economy. Data for 2025 indicates that the MSME sector contributes 60% or 8,573 trillion to the Gross Domestic Product (GDP), employs approximately 117 million workers or 97% of the total workforce and accounts for 15.7% of total national exports, while attracting 60.4% of total investment. To date, the number of SMEs in Indonesia has reached 64 million business units (Coordinating Ministry for Economic Affairs, 2025) .

In line with national trends, the strategic strength of SMEs is also clearly evident in regions such as the city of Lhokseumawe, one of the developing cities in Aceh Province that is showing positive dynamics in SME growth as it begins to adapt significantly to digital transformation. According to data from the Lhokseumawe City Department of Trade, Industry, Cooperatives, and SMEs, there are currently 6,848 active SMEs operating in Lhokseumawe City. Of this total, approximately 6,438 are classified as micro enterprises, while 439 fall into the small enterprise category, and 60 are medium-sized enterprises. These SMEs are spread across various key economic sectors in such as trade, agriculture, food processing, fisheries, transportation, and livestock farming which collectively support local economic growth. It is known that a number of MSME operators in Lhokseumawe City have begun adopting digital platforms in their business activities, ranging from digital business transactions and online marketing to digital payment systems for integrated customer data storage (Lhokseumawe Portal, 2024) .

The increasing use of digital technology is not always accompanied by the ability of MSME operators to manage cybersecurity risks. Low cybersecurity literacy leaves business operators vulnerable to various threats, such as phishing, account hijacking, data theft, malware, ransomware, and digital transaction fraud. These threats not only result in financial losses but also disrupt business operations, erode customer trust, and even threaten business sustainability (Raisah, 2025). This situation is becoming evident in the city of Lhokseumawe,

with an increase in reports of digital fraud that exploit digital banking services, e-wallets, and ordering apps as vehicles for cybercrime (Arroji et al., 2025). This phenomenon indicates that the success of SMEs' digital transformation is determined not only by their ability to adopt technology but also by their capacity to protect digital assets and manage cybersecurity risks sustainably.

Cybersecurity literacy is an individual's ability to understand, recognize, and apply digital security practices to protect data, accounts, and information assets from various cyber threats. In the context of SMEs, this literacy includes the ability to recognize phishing attempts, use strong passwords, enable two-factor authentication, and secure transactions and customer data. Therefore, cybersecurity literacy is not only focused on increasing knowledge but also on fostering safe digital behaviors (Pangrazio et al., 2020) . Improving cybersecurity literacy serves as the foundation for building digital resilience the ability of business operators to anticipate, respond to, and recover from cyber threats without disrupting business continuity. SMEs with strong cybersecurity literacy tend to be better able to maintain business operations, protect customer data, minimize losses from cyberattacks, and maintain consumer trust. Statistical evidence shows that 43% of SMEs that experience cyberattacks are unable to fully recover, and the majority go out of business within 6 months of the incident (Palatty, 2025). However, cybersecurity training for SMEs still faces various obstacles, primarily due to differences in educational levels, digital experience, and business characteristics. Most training programs still use a general and technical approach, making them ill-suited to the needs of SME operators. Therefore, an inclusive educational approach is essential so that the material is presented in simple language, based on real-world experiences, and supported by hands-on guidance, making it easier to understand and apply in daily business activities.

A number of previous empirical reviews, such as Safar et al., (2025); Aji et al., (2025); Sari et al., (2025); Anan et al., (2024); Yusnanto et al., (2023); Falch et al., (2023) and Junior et al., (2023) show that cybersecurity literacy programs can increase public knowledge about digital threats and the importance of data protection. However, the majority of studies still focus on general awareness campaigns or training, thus emphasizing knowledge enhancement over changes in digital security behavior. Furthermore, the approaches used generally do not account for the diverse characteristics of MSME operators and do not integrate ongoing mentoring tailored to participants' actual needs. Based on this synthesis, several research gaps exist. First, there are still few programs that develop

inclusive and context-specific cybersecurity literacy models for MSMEs. Second, previous research has not extensively linked cybersecurity literacy to the development of digital resilience as part of a strategy to ensure business sustainability. Third, program effectiveness evaluations are generally descriptive in nature and thus do not provide empirical evidence regarding changes in participants' capabilities following the mentoring.

To address these gaps, this study aims to develop an inclusive, participatory, and locally- -based cybersecurity literacy mentoring model for SMEs under the guidance of Rumah BUMN in Lhokseumawe. This model integrates participant needs assessment, conceptual education, practical digital security mentoring, and evaluation using pre-tests, post-tests, paired-sample t-tests, and N-Gain. Consequently, this research not only enhances cybersecurity literacy but also strengthens the digital resilience of SME operators to support business sustainability in the era of digital transformation. The mentoring model developed also has the potential to be replicated in SME empowerment programs in other regions with similar characteristics.

Method

Research Design

This community service program employs a Participatory Action Research (PAR) approach, as it positions SME operators as active partners in collaboratively identifying problems, designing solutions, implementing actions, and evaluating program outcomes (Oliveira, 2023). This approach was chosen because it aligns with the characteristics of SME operators, who have varying levels of digital literacy, experience, and needs, thus requiring an adaptive, contextual, and participatory learning model. The implementation of PAR follows five stages: diagnosis, planning, action, observation, and reflection. During the diagnosis stage, the community service team, in collaboration with Rumah BUMN in Lhokseumawe, conducted discussions, interviews, and needs assessments to identify participants' levels of cybersecurity literacy and the most common digital threats they face. These findings served as the foundation for developing training materials, mentoring methods, and cybersecurity practices tailored to the real-world needs of MSME operators.

The participatory element of PAR was realized through the active involvement of participants in every stage of the program. Participant feedback regarding difficulties in understanding technical material, experiences with digital

fraud, and the need to secure business accounts was used to refine training materials, expand local case studies, hands-on exercises, and consultation sessions. Thus, participants served not only as training recipients but also as partners in program development. Through this approach, the program aims not only to increase knowledge about cybersecurity but also to build the skills, digital security behaviors, and digital resilience of MSME stakeholders so that cybersecurity practices can be applied sustainably in their daily business activities.

Participants and Sampling

Program participants consisted of 60 MSME operators under the guidance of Rumah BUMN in Lhokseumawe, selected using purposive sampling. This technique was used because participants were selected based on characteristics aligned with the program's objectives namely, MSME operators who have utilized digital technology in their business activities and are at risk of facing cybersecurity threats. The inclusion criteria for participants were as follows: (1) active MSME owners registered as partners of Rumah BUMN in Lhokseumawe; (2) those who have used digital platforms such as social media, online marketplaces, or digital payment systems in their business operations; (3) those willing to participate in the entire series of mentoring activities; and (4) those who provided consent to participate in the program evaluation process. Meanwhile, participants who do not complete all mentoring stages or fail to complete the pre-test and post-test will not be included in the final analysis.

The number of participants was determined based on coordination with Rumah BUMN in Lhokseumawe, taking into account mentoring capacity, the effectiveness of participatory learning, and the representation of various types of businesses managed by the participants. Given these characteristics, the sample was deemed capable of providing relevant information to evaluate the effectiveness of the developed cybersecurity literacy mentoring model.

Instrument Development and Validation

The research instrument was developed based on a literature review on cybersecurity literacy and adapted to the characteristics of MSME actors and the digital business activities carried out by the participants. The instrument consists of four main indicators, namely: (1) knowledge of cybersecurity threats and practices, (2) skills in implementing security measures for accounts and digital transactions, (3) attitudes toward the importance of data protection and information security, and (4) behaviors in applying cybersecurity practices in daily business activities. Each indicator is measured using a five-point Likert-scale

questionnaire, ranging from 1 (strongly disagree) to 5 (strongly agree). Before use, the instrument first underwent a content validity test, with each statement item yielding a Sig. value < 0.05 and a $_{\text{calculated}}r$ value > $_{\text{the table}}r$ value. The results of the review were used to improve the clarity of the language, the appropriateness of the indicators, and the relevance of each statement item to the research objectives (Sugiyono, 2022).

Next, the instrument was tested on a number of respondents with characteristics similar to those of the study participants to determine its reliability. The test results showed that the instrument had a Cronbach's Alpha value > 0.70, indicating a good level of internal consistency and making it suitable for use as a data collection tool. The instrument, having met the criteria for validity and reliability, was then used in the pre-test and post-test to measure changes in participants' cybersecurity literacy following the mentoring program.

Program Implementation

The mentoring program was implemented through five stages: (1) needs assessment, (2) cybersecurity literacy training, (3) practice and simulation, (4) implementation mentoring, and (5) evaluation and reflection. All stages were designed in accordance with the principles of Participatory Action Research (PAR), which emphasizes the active involvement of participants in every learning process. During the needs assessment stage, the community service team conducted discussions, interviews, and pre-tests to map participants' levels of cybersecurity literacy and identify the problems they most frequently faced. The results of the needs assessment showed that the most common threats experienced were phishing, misuse of business social media accounts, and digital transaction security. These findings then served as the basis for determining training materials, developing case studies, and designing practical exercises tailored to the participants' needs.

During the mentoring process, participants not only received training materials but also engaged in discussions, simulations, case studies, and shared their experiences regarding the digital security challenges they faced. Participant feedback was collected through observations, group discussions, and consultations during each session. The results of this formative evaluation were used to adjust delivery methods, clarify material that was still difficult to understand, and add case examples more relevant to participants' business activities. The mentoring and evaluation phases played a strategic role in linking the knowledge gained during training to its implementation in daily practice (Dianastiti et al., 2023) . The final stage was conducted through a joint reflection

process using a post-test, evaluative discussions, and feedback from participants and partners at Rumah BUMN in Lhokseumawe. This reflection process was used to assess the program's effectiveness while formulating recommendations for improvement and strategies for continued mentoring to support the sustainable implementation of cybersecurity practices.

SWOT Analysis

The Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis was used as a framework to identify internal and external conditions affecting the implementation of cybersecurity literacy among MSMEs under the guidance of Rumah BUMN in Lhokseumawe. This analysis aimed to develop mentoring strategies aligned with participants' needs and the conditions of the digital business environment. SWOT data was collected through field observations, semi-structured interviews with Rumah BUMN managers and SME operators, focus group discussions, and the results of needs assessments conducted during the program's initial phase. All data was then qualitatively analyzed by categorizing the findings into strengths, weaknesses, opportunities, and threats related to the SMEs' digital readiness and cybersecurity. The results of the SWOT analysis were used as the basis for developing training materials, determining mentoring priorities, and designing more adaptive implementation strategies. Thus, the program not only focused on enhancing participants' knowledge but was also tailored to the characteristics of SMEs' their level of digital readiness, and the potential cyber threats they face in their day-to-day business operations.

Evaluation and Data Analysis

Program evaluations are conducted both formatively and summatively to measure the effectiveness of cybersecurity literacy mentoring. Formative evaluations are carried out during the mentoring process through observation, discussions, consultations, and participant feedback to monitor participants' level of understanding and the challenges they face. The findings of this evaluation are used to adjust delivery methods, clarify material that has not been understood, and add case studies that are more relevant to participants' needs in subsequent sessions. Summative evaluation is conducted at the end of the program using pre-tests and post-tests to measure changes in cybersecurity literacy based on four indicators: knowledge, skills, attitudes, and digital security behaviors. The data obtained is analyzed using descriptive statistics to describe the characteristics of the measurement results.

Furthermore, a paired-sample t-test was used to test the difference between pre-test and post-test scores to determine the significance of the increase in participants' competencies after completing the program. The effectiveness of the mentoring was also analyzed using N-Gain to measure the magnitude of the improvement in learning outcomes. The combination of these two analyses provides insight into both the statistical significance and the program's effectiveness in improving the cybersecurity literacy of MSME operators.

Research Bias and Study Limitations

This study has several potential biases that need to be considered. First, the use of pre-test and post-test questionnaires allows for the possibility of social desirability bias—that is, the tendency for participants to provide answers they believe align with the researchers' expectations. To minimize this bias, participants completed the questionnaires independently, respondent identities were kept confidential, and participants were informed that all responses would be used solely for research and program evaluation purposes.

The study's limitations also lie in the fact that the evaluation was conducted over a short period, making it impossible to assess the sustainability of participants' cybersecurity behavior changes after the program ended. Additionally, this study only involved MSMEs under the guidance of Rumah BUMN in Lhokseumawe, so the results cannot be widely generalized. Nevertheless, the use of the Participatory Action Research (PAR) approach, formative and summative evaluations, and statistical analysis helped enhance the credibility of the study's findings. Future research is recommended to conduct longitudinal evaluations and involve participants from various regions to test the sustainability and replicability of the mentoring model developed.

Results and Discussion

The implementation of this community service program had a measurable positive impact, particularly in improving cybersecurity literacy among 60 SME operators under the guidance of Rumah BUMN in Lhokseumawe. The results and discussion of the activities are outlined as follows:

Forms of Cybercrime Threats Faced by MSMEs Mentored by Rumah BUMN Lhokseumawe

Findings from field observations, interviews, and participatory discussions with the 60 SME operators under the guidance of Rumah BUMN in Lhokseumawe indicate that digital transformation has improved operational efficiency and

expanded market access; however, it has simultaneously increased exposure to various cybersecurity threats. These findings reinforce the concept **of** cybersecurity literacy, which views the ability to recognize, understand, and respond to cyber threats as an essential competency in ensuring the sustainability of digital business activities. Low cybersecurity literacy prevents SME operators from identifying risks or implementing appropriate mitigation measures, making them a relatively vulnerable group to cybercrime.

The threats most frequently experienced by participants include phishing, digital transaction fraud, and the spread of malware through malicious links or apps. Based on the results of the mentoring program, phishing attacks are the most prevalent form of threat. Most participants reported having received messages purporting to be from marketplaces, banks, or delivery service companies in an attempt to obtain account data or verification codes. This situation indicates that SME owners remain more susceptible to social engineering techniques, particularly when business activities are conducted via personal smartphones that are used simultaneously to manage marketplaces, social media, and digital banking services.

In addition, digital transaction fraud is also a common threat, particularly through fake payment receipts, manipulation of QRIS codes, and transactions outside the platform's official mechanisms. These findings indicate that cybersecurity vulnerabilities among SMEs stem not only from technological limitations but also from a lack of ability to verify transactions and consistently implement digital security procedures. Another identified threat is the spread of malware through malicious links in messaging apps, which can potentially lead to data theft, system disruptions, and even the loss of access to business accounts.

Theoretically, these findings reinforce the view that cybersecurity literacy is a key foundation for building the digital resilience of SMEs. Digital resilience is determined not only by the availability of security devices or technology but also by business owners' ability to recognize threats, make the right decisions, and restore business operations in the event of a cyber incident. Therefore, low cybersecurity literacy is not merely a matter of a lack of knowledge but a strategic factor that affects operational sustainability, customer trust, and the competitiveness of SMEs in the digital economy era.

These findings are also consistent with the research by Akbar & Wijaya (2024) , which states that low cybersecurity literacy makes MSME operators more vulnerable to phishing attacks, account theft, and digital transaction fraud due to limited knowledge of basic digital security practices. The results of this study also

reinforce the findings of Arroji et al.'s research which indicate that low awareness of data protection and information security remains a major challenge in the digital transformation of SMEs. Furthermore, the study by Falch et al. (2023) explains that human factors are the dominant cause of cybersecurity incidents in small-scale organizations; therefore, improving cybersecurity literacy is a more effective preventive strategy than relying solely on security technology.

Nevertheless, the findings of this study differ from those of previous studies. Akbar & Wijaya (2024) and Arroji et al., (2025) focus more on identifying the level of cybersecurity literacy and the factors causing SME vulnerabilities, whereas this study not only maps the types of cyber threats faced by MSME operators but also integrates these findings into a cybersecurity literacy mentoring model based on Participatory Action Research (PAR) that is inclusive, contextual, and adaptive to the characteristics of the MSMEs under the guidance of Rumah BUMN in Lhokseumawe. Thus, the contribution of this study goes beyond simply mapping the problems; it produces an intervention model that can be applied to strengthen the digital resilience of MSMEs in a sustainable manner.

The Impact of Cyber Threats on the Sustainability of MSMEs Under the Guidance of Rumah BUMN in Lhokseumawe

The impact of cyber threats on the sustainability of MSMEs under the guidance of Rumah BUMN in Lhokseumawe extends beyond immediate financial losses to broader operational and long-term business consequences. Direct financial losses reported by participants generally ranged from IDR 200,000 to IDR 2,000,000 per incident, although several cases involving marketplace account hijacking resulted in substantially higher losses. Cyber incidents also disrupted business operations, as owners were required to spend considerable time recovering compromised accounts, contacting banks or digital platform providers, addressing customer concerns, and managing canceled or delayed orders. In addition, MSMEs incurred recovery and mitigation costs, including expenses for technical support, device replacement, software updates, antivirus subscriptions, and other basic cybersecurity measures. More importantly, repeated cyber incidents undermined customer trust, reduced business owners' confidence in conducting digital transactions, and discouraged the adoption of online sales channels. For micro-scale enterprises with limited financial reserves, these cumulative impacts significantly increased the risk of business closure, particularly when cyberattacks occurred repeatedly or on a systemic scale.

Findings from observations and interviews indicate that the impact of cybersecurity threats experienced by MSMEs under the guidance of Rumah

BUMN in Lhokseumawe extends beyond mere short-term financial losses; it also affects the overall operational sustainability of their businesses. These findings demonstrate that cybersecurity has evolved from a purely technical issue into a strategic factor that determines business sustainability in the digital economy era. Based on the results of the mentoring program, the impacts most frequently reported by participants include financial losses due to digital transaction fraud, hijacking of business marketplace and social media accounts, disruptions to customer service processes, and increased costs for system and device recovery. Some SME owners also reported having to temporarily halt sales activities due to losing access to their business accounts or waiting for recovery processes from digital service providers. These conditions resulted in disrupted business cash flow, delays in fulfilling customer orders, and decreased business productivity.

These findings demonstrate that cybersecurity threats have a cascading effect on SME operations. Losing access to digital accounts not only hinders transactions but also disrupts communication with customers, product distribution, business data management, and digital marketing processes. For SMEs, whose business activities largely depend on digital platforms, such disruptions can halt business processes entirely, even if triggered by a single cybersecurity incident.

From the perspective of digital resilience theory, a business's capability is measured not only by its capacity to prevent cyberattacks but also by its ability to maintain operations, adapt, and recover quickly after a security incident. The results of this study indicate that most participants do not yet have adequate *recovery plans*, data *backup* procedures, or digital security operational standards. This situation causes the impact of a cyber incident to be greater than the actual financial loss, as business owners require a relatively long time to restore their business activities.

Figure 1. Cybersecurity Literacy Assistance for MSME Owners

These findings are consistent with the research by Palatty (2025), which shows that low cybersecurity readiness is one of the main factors causing MSMEs to struggle to maintain business continuity after experiencing a cyberattack. The results of this study also reinforce the findings of Arroji et al., (2025), who state that weak awareness of data protection and information security increases the vulnerability of MSMEs to operational disruptions and reduces customer trust. Thus, the losses suffered by MSMEs are not only economic in nature but also include damage to business reputation, which takes longer to recover from.

This study offers a distinct contribution compared to previous research. Most prior studies have only examined the impacts of cybersecurity from the perspective of economic losses or the level of SME vulnerability, whereas this study demonstrates that these impacts are interrelated and form a risk cycle that affects business sustainability. Through field observations and mentoring processes, it was found that a single cybersecurity incident can trigger operational disruptions, erode customer trust, increase recovery costs, hinder digital market expansion, and ultimately reduce a business's competitiveness. These findings indicate that enhancing cybersecurity literacy serves not only as a risk mitigation strategy but also as a strategic investment to strengthen digital resilience and the business sustainability of SMEs**.**

In practical terms, the results of this study show that improving cybersecurity literacy provides broader benefits than simply increasing

participants' knowledge. The ability of SME operators to recognize threats, verify digital transactions, securely manage business accounts, and protect customer data directly contributes to operational efficiency, increased consumer trust, and business sustainability. Therefore, cybersecurity literacy must be positioned as an integral part of SME empowerment strategies not merely as information technology training, but as an effort to build resilient, adaptive, and sustainable business capacity in the face of the dynamics of the digital economy.

An Inclusive Approach-Based Cybersecurity Literacy Mentoring Model to Build Digital Resilience in MSMEs

Based on the results of the needs assessment, the cybersecurity literacy mentoring program in this study was not designed as one-way technical training but was developed through a Participatory Action Research (PAR) approach that positions SME actors as the primary subjects in the learning process . This approach allows the content, methods, and format of the mentoring to be tailored to the participants' actual needs, as identified through observation, interviews, participatory discussions, and pre-test results. Thus, the program is not only oriented toward knowledge transfer but also toward behavioral change and the sustained strengthening of participants' capacity to address cybersecurity risks.

Conceptually, the effectiveness of this mentoring model can be explained through digital literacy theory, which states that the ability to use technology safely is not solely supported by mastery of digital devices but also by the ability to think critically, evaluate information, identify risks, and make appropriate decisions when facing threats in the digital space. In the context of this study, improvements in cybersecurity literacy are reflected in participants' ability to recognize the characteristics of phishing, verify digital transactions, manage business accounts more securely, and implement data protection practices in their daily business activities. These changes indicate that participants not only acquired new knowledge but also developed the ability to apply that knowledge in real-world situations.

In addition to being supported by the concept of digital literacy, the program's success can also be explained through cybersecurity awareness theory, which emphasizes that cybersecurity awareness is formed through a repetitive, contextual, and experience-based learning process. Therefore, the mentoring activities were not limited to the delivery of course material but were enriched with phishing attack simulations, case study analyses, demonstrations of account security practices, group discussions, and individual consultations. This strategy provides participants with the opportunity to understand the relationship

between cybersecurity concepts and the risks they face in their daily business operations. Observations during the mentoring sessions showed that participants found it easier to understand the material when the examples used were drawn from their own experiences rather than from purely theoretical explanations.

The findings of this study are consistent with Akbar & Wijaya (2024) , which state that improving cybersecurity literacy among MSMEs requires a learning approach that is simple, contextual, and easy to implement. The results of this study also reinforce the findings of , which show that ongoing mentoring is more effective than one-time training because it enhances the consistency of digital security practices. Furthermore, the study by Falch et al. (2023) emphasizes that human factors are a key component in cybersecurity management; therefore, changing user behavior is a critical prerequisite for building an organization's digital resilience.

Figure 2. Cybersecurity Literacy Mentoring for MSME Actors

Nevertheless, this study offers a distinct contribution compared to previous research. Most prior community service programs were primarily focused on delivering digital literacy content or technical training on cybersecurity. In contrast, this study developed an inclusive cybersecurity literacy mentoring model that integrates participant needs assessment, participatory learning, practical simulations, implementation support, formative evaluation, and shared

reflection within a single cycle of Participatory Action Research (PAR**)**. This approach allows the material to be tailored to participants' digital literacy levels, business characteristics, and experiences, making the learning process more adaptive and easier to implement.

Furthermore, the research findings indicate that the program's success is not solely due to the quality of the training materials, but rather to a combination of a participatory approach, ongoing mentoring, and active participant engagement throughout all stages of the activities. This demonstrates that improving cybersecurity literacy is a process of behavioral transformation that requires interaction, reflection, hands-on practice, and continuous reinforcement. Therefore, the mentoring model developed in this study not only enhances individual competencies but also builds digital resilience as the foundation for the sustainability of MSMEs in facing cybersecurity risks in the digital economy era.

The practical implication of these findings is that SME empowerment programs should no longer treat cybersecurity as supplementary training material but rather as an integral part of business capacity-building strategies. The mentoring model developed in this study has the potential to be replicated among MSMEs in other regions because it is flexible, based on local needs, and emphasizes active participant engagement throughout the entire learning process. Thus, this model not only yields short-term competency improvements but also supports the formation of a sustainable digital security culture within the MSME ecosystem.

The Effectiveness of the Mentoring Model in Improving Cybersecurity Literacy and Digital Resilience Among MSMEs

The effectiveness of this program was evaluated by measuring the capabilities of SME operators before and after the mentoring using a pre-test and post-test design, with instruments assessing knowledge, skills, behaviors, and attitudes related to cybersecurity. Statistical analysis of the effectiveness of this community service program was conducted using a paired-sample t-test and an N-Gain test. The paired-sample t-test was used to determine whether there was **a** significant difference between the pre-test and post-test scores, thereby allowing us to conclude whether the mentoring program was statistically effective. Meanwhile, the N-Gain test was used to measure the level of effectiveness in improving capabilities, taking into account the maximum score that could be achieved. The following are the descriptive statistics of the paired-sample t-test results obtained from the data:

Table 1. Descriptive Statistics for the Paired-Sample t-Test

Paired Samples Statistics

		Mean	N	Std. Deviation	Standard Error of the Mean
Pair 1	PRE-TEST	41.4500	60	10.85564	1.40146
	POST-TEST	93.2500	60	5.10774	.65941

Source: Processed data, 2025.

The highly significant difference between the pre-test and post-test scores was then statistically tested using a paired-sample t-test. The results of the paired-sample t-test are as follows:

Table 2. Results of the Paired-Samples t-Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Standard Deviation	Standard Error of the Mean	95% Confidence Interval for the Difference Lower	Upper			
Pair 1	PRE-TEST - POST-TEST	-51.80000	12.83243	1.65666	-55.11497	-48.48503	-31.268	59	,000

Source: Processed data, 2025.

The effectiveness and sustainability of this community service program were further confirmed based on the results of the N-Gain test, which yielded the following results:

Table 3. N-Gain Test Results

Descriptive Statistics

	N	Minimum	Maximum	Mean	Standard Deviation
NGain	60	.51	1.00	.8760	.10920
Valid N (listwise)	60				

Source: Processed data, 2025.

Based on the statistical output of the N-Gain test, the average N-Gain value was 0.876, the minimum value was 0.51, and the maximum value was 1.00, with a standard deviation of 0.109. Referring to the N-Gain effectiveness criteria, namely:

Table 4. Effectiveness of N-Gain Values

N-Gain Value	Category
< 0.3	Low
0.3 – 0.7	Medium
> 0.7	High

Source: Melzer in Syafitri, 2008.

The results of the statistical analysis indicate that the cybersecurity literacy mentoring program had a highly significant impact on improving the capacity of MSME participants mentored by Rumah BUMN in Lhokseumawe. The average pre-test score of 41.45 increased to 93.25 on the post-test, with a difference of 51.80 points. The results of the paired t-test yielded a significance value of 0.000 ($p < 0.05$), indicating that this increase did not occur by chance but was a direct consequence of the intervention provided through the mentoring program. These findings are further reinforced by an N-Gain value of 0.876, which falls into the "high" category, indicating that the majority of the participants' potential for competency improvement was successfully achieved through the implemented mentoring model.

However, the significance of this study's findings lies not only in the increase in statistical scores but also in the changes in competencies observed in the participants' day-to-day business operations. Based on observations during the mentoring period, most MSME owners began to be able to identify the characteristics of phishing messages, distinguish between safe and malicious links, implement *two-factor* authentication, use stronger passwords, and verify digital transactions before making payments. These behavioral changes indicate that the increase in scores not only reflects an expansion of cognitive knowledge but also illustrates shifts in attitudes and skills that can be directly applied in daily business activities.

From the perspective of digital literacy theory, this improvement indicates that participants have experienced a more comprehensive development of digital competencies. Digital literacy is not merely defined as the ability to use technology, but also as the ability to understand risks, critically evaluate digital information, and make safe decisions in a digital environment. Therefore, the 51.80-point increase in the score indicates that participants not only understand

the concepts of cybersecurity in theory but are also beginning to integrate digital security practices into the management of their MSMEs.

The success of this program can also be explained through cybersecurity awareness theory, which emphasizes that cybersecurity awareness is formed through a combination of knowledge, hands-on experience, repeated practice, and habit formation. In this program, the learning process does not stop at the delivery of material but is reinforced through cyberattack simulations, account security exercises, discussions of real-life cases experienced by participants, and guidance on implementation within their respective business environments. This approach enables participants to understand the real-world consequences of each cyber threat, resulting in behavioral changes that are more permanent than those achieved through lecture-based learning alone.

The findings of this study are consistent with the research by which concluded that the effectiveness of cybersecurity education is greatly influenced by the use of contextual learning methods that are easily understood by MSME operators. The results of this study also reinforce the findings of the study , which show that ongoing mentoring programs can lead to a more stable improvement in digital competencies compared to one-time training sessions. Furthermore, the study by Falch et al. (2023) emphasizes that raising user awareness is the most effective strategy in to reduce cybersecurity risks, as the majority of security incidents stem from human error rather than technological weaknesses.

Nevertheless, this study offers a distinct contribution compared to previous research. Most prior studies merely measured changes in participants' knowledge levels or perceptions following cybersecurity training. This study not only evaluates knowledge gains through statistical analysis but also integrates field observations, participant reflections, mentoring practices, and implementation evaluations to explain how these competency changes are applied in daily business activities. Thus, the program's effectiveness is demonstrated not only through statistical significance but also through tangible changes in the digital behavior of MSME operators.

Observations during the mentoring process showed that participants became more cautious about accepting links or digital documents, more disciplined in verifying customer identities before transactions, and began implementing simple procedures to protect customer data and business accounts. Some participants also reported that they had begun regularly backing *up* their business data and restricting access to business accounts to authorized personnel only. These changes indicate that the mentoring process successfully fostered a

culture of digital security an aspect that had not previously been a primary focus in business management.

The practical implications of these findings are crucial for the sustainability of MSMEs. Improved cybersecurity literacy enables business owners to reduce the risk of financial losses due to digital fraud, minimize operational disruptions caused by account hijacking or data loss, maintain customer trust through more secure information management, and enhance preparedness to face various forms of cyber threats in the future. Thus, cybersecurity literacy is no longer viewed as an additional competency but as an integral part of a strategy to strengthen digital resilience, contributing to the sustainability, competitiveness, and adaptability of MSMEs within the digital economy ecosystem.

Overall, the results of this study indicate that the Participatory Action Research (PAR)-based mentoring model developed is not only effective in enhancing participants' individual capabilities but also succeeds in building a foundation for digital resilience at the business organizational level. This model demonstrates that the integration of participatory learning, hands-on practice, continuous evaluation, and contextual mentoring is capable of producing more sustainable behavioral changes compared to conventional training approaches, making it worthy of consideration as a model for empowering SMEs in various regions facing similar cybersecurity challenges.

SWOT Analysis as the Basis for Formulating Strategies to Strengthen SME Digital Resilience

To formulate a strategy for strengthening sustainable cybersecurity literacy, this study complements quantitative analysis with a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis**.** Unlike conceptual SWOT analyses, the analysis in this study is based on empirical evidence obtained through observations during the mentoring process, interview results, focus group discussions, participant reflections, and program implementation evaluations. This approach allows for the identification of the real conditions faced by MSME actors, ensuring that the resulting strategic recommendations are more contextual and practical.

Strengths

The observation results show that the majority of participants are highly motivated to improve their digital security capabilities because they recognize that business activities have become dependent on electronic transactions, social

media, and online marketplaces. Of the 60 participants, all use smartphones as their primary tool for running their businesses and have incorporated digital payments and social media-based marketing into their daily operations. During the reflection session, several participants noted that they had only recently come to understand that cybersecurity is a critical component of business sustainability—not merely an information technology issue. One participant stated,

> *"Up until now, we've focused on finding customers, but after participating in the mentoring program,* we *realized that safeguarding our accounts is just as important as maintaining product quality."*

These findings indicate that the program successfully fostered a new awareness of the importance of digital security as an integral part of business management.

Analysis results show that the participants' main strengths lie in their high motivation to utilize digital technology as a means of business development, as well as the institutional support from Rumah BUMN, which facilitated the learning and mentoring process. Throughout the program, the majority of participants showed great enthusiasm for engaging in digital security practices, discussing their experiences with online scams, and sharing solutions to the challenges they faced. These interactions served as vital social capital in collectively building a culture of digital security.

Weaknesses

Although participant motivation was quite high, initial observations and pre-test results indicated that basic cybersecurity skills remained relatively low. Most participants had not yet implemented *two-factor* authentication, were still using the same password for multiple business accounts, and had not yet developed the habit of regularly backing up their business data. Group discussions also revealed that some participants still struggle to distinguish between genuine messages and phishing messages, particularly when attackers impersonate banking institutions or marketplace platforms. As one participant noted,

> *"Up until now, I assumed that any message featuring a bank's logo was legitimate. It wasn't until after the training that I realized there are many fake messages that look almost identical to the real ones."*

These findings indicate that the primary weakness lies not only in limited technical knowledge but also in low awareness of the importance of digital risk management as part of daily business operations. This situation explains why a personalized and context-specific mentoring approach is essential. Furthermore, there are significant differences in digital literacy levels among participants, so the learning process requires a more personalized and adaptive approach.

Opportunities

This program has great potential to be developed into a sustainable empowerment model because it is supported by Rumah BUMN, an institution that assists MSMEs and already has a network for providing regular guidance. In addition, the increasing digital transformation in the MSME sector is driving the need for more systematic cybersecurity training. Participants' feedback indicates that they want the mentoring program to extend beyond a single session, continuing through periodic consultations and updates to the training materials in line with evolving cyber threats. One participant remarked,

> *"Training like this should be conducted regularly because fraud schemes are constantly changing. If it's only a one-time event, we're worried we'll forget or won't know how to deal with new scams."*

This statement highlights a real need for a cybersecurity learning community that serves as a platform for sharing experiences, technical consultations, and updates on digital threats. This situation presents an opportunity for local governments, universities, and Rumah BUMN to develop a sustainable mentoring model.

Challenges

On the other hand, the rapid evolution of cybercrime tactics poses a major challenge to maintaining the program's effectiveness. Based on interview results, some participants admitted to having received fake links, account verification messages, or payment requests purporting to be from specific customers or institutions. These threats continue to evolve alongside the increasing use of artificial intelligence, social engineering, and digital identity fraud. This situation indicates that improving cybersecurity literacy cannot be achieved through a one-time training session but requires a continuous learning process to ensure participants' skills keep pace with evolving digital threats. One participant remarked:

"Nowadays, these scams are becoming harder to spot. Sometimes the messages look so convincing that we almost gave away the OTP code."

These findings indicate that threats to SMEs are dynamic and continue to evolve alongside the increasing use of digital technologies, including social engineering, artificial intelligence, and digital identity fraud. Therefore, improving cybersecurity literacy cannot be achieved through one-time training but requires a continuous learning mechanism so that SME operators can adapt to the ever-changing landscape of cyber threats.

The findings of the SWOT analysis are strongly correlated with the results of the quantitative evaluation. The increase in scores from the pre-test to the post-test**,** the significant t-test value, and the high N-Gain category indicate that the mentoring program successfully mitigated most of the internal weaknesses previously identified through the SWOT analysis. For example, low ability to recognize phishing, weak digital account management, and a lack of awareness regarding data protection showed tangible improvements after participants underwent the practice-based mentoring process. Thus, the statistical results do not stand alone but confirm the changes previously observed through the process of observation and reflection during program implementation.

Based on the integration of SWOT analysis results and statistical evaluations, this study offers several strategic recommendations. First, cybersecurity literacy programs for SMEs need to be implemented on an ongoing basis through a mentoring mechanism, rather than as one-time training sessions. Second, training materials must be tailored to participants' digital literacy levels and business characteristics so they are easier to understand and apply. Third, a cybersecurity learning community should be established within the Rumah BUMN environment as a forum for sharing experiences, consultations, and updates on the latest cyber threats. Fourth, local governments, universities, and SME support institutions need to strengthen collaboration in formulating empowerment policies that integrate cybersecurity aspects as part of the SME digital transformation strategy.

These findings indicate that SWOT analysis serves not only as a tool for mapping initial conditions but also as a foundation for developing more targeted intervention strategies. The integration of SWOT analysis, the Participatory Action Research (PAR) approach, and quantitative evaluation yields a mentoring model that is not only effective in improving cybersecurity literacy but also strengthens the digital resilience and sustainability of SMEs. Therefore, the model developed

in this study has the potential to be replicated in SME empowerment programs in other regions with similar characteristics. Overall, this empirically grounded SWOT analysis demonstrates that program success is influenced not only by participants' increased knowledge but also by institutional support, collaboration among stakeholders, and the sustainability of the mentoring process. Consequently, strengthening cybersecurity literacy must be positioned as part of a strategy to build SMEs' digital resilience so that business owners can anticipate, respond to, and adapt to the ever-evolving dynamics of cyber threats.

Synthesis of Findings, Theoretical Contributions, and Practical Implications of the Mentoring Program

Overall, the research results indicate that improving cybersecurity literacy among SME operators cannot be achieved solely through the dissemination of information or short-term technical training. These findings demonstrate that changes in digital competencies occur when the learning process is designed to be participatory, contextual, and oriented toward solving real-world problems faced by participants. Thus, the program's effectiveness is not solely determined by the quality of the materials provided but by the integration of participant needs assessment, ongoing mentoring, hands-on practice, shared reflection, and systematic evaluation.

From a theoretical perspective, these findings reinforce the concept of digital literacy, which views digital literacy as a combination of knowledge, skills, attitudes, and the ability to make critical decisions regarding the use of digital technology. The increase in scores from the pre-test to the post-test, accompanied by changes in participants' behavior, indicates that cybersecurity literacy is not limited to cognitive aspects but also encompasses the ability to consistently apply digital security practices in business activities. These results also support the theory of cybersecurity awareness, which explains that cybersecurity awareness develops through repeated, contextual, and practice-based learning experiences, thereby fostering more sustainable behavioral changes compared to purely informative learning approaches.

The findings of this study also expand our understanding of the concept of digital resilience among MSMEs. Until now, digital resilience has often been understood as an organization's ability to leverage digital technology to ensure business continuity. However, the research results show that digital resilience is also significantly influenced by business owners' ability to recognize, anticipate, respond to, and recover from various cybersecurity threats. In other words, cybersecurity literacy is the cornerstone of building digital resilience, enabling

SMEs to continue operating safely, adaptively, and sustainably amid rising risks of cybercrime.

Compared to previous studies, this study offers a distinct contribution. The study by(2024) , places greater emphasis on the importance of improving cybersecurity literacy as a means of reducing the vulnerability of MSMEs to digital threats, whereas the study by Arroji et al.,(2025) , focuses on the low level of awareness among business owners regarding data protection as a key factor in the increasing risk of cybercrime. The study (2023) also indicates that mentoring yields better results than conventional training; however, it has not yet developed a mentoring model that integrates needs assessment, simulations, formative evaluation, participatory reflection, and SWOT analysis into a single empowerment cycle. Therefore, the novelty of this study lies in the development of a Participatory Action Research (PAR)-based cybersecurity literacy mentoring model that combines participatory approaches, adult learning, local needs analysis, quantitative evaluation, and qualitative reflection to build the sustainable digital resilience of MSMEs.

The scientific contribution of this research not only strengthens the relationship between cybersecurity literacy and digital resilience but also demonstrates that the effectiveness of an empowerment program is significantly influenced by the level of participant engagement throughout all stages of the activities. Through the Participatory Action Research (PAR) approach, MSME actors are no longer positioned as objects of training but as partners who actively participate in identifying problems, formulating solutions, implementing digital security practices, and evaluating the results of the mentoring. This approach results in a more adaptive learning process, increases a sense of ownership of the program, and encourages the sustainable adoption of digital security practices after the program is completed.

From a practical standpoint, the findings of this study have important implications for local governments, universities, Rumah BUMN, and SME support institutions. Digital transformation programs—which have traditionally focused more on enhancing marketing capabilities, the use of digital platforms, and the digitization of transactions need to be integrated with programs aimed at strengthening cybersecurity literacy. Improving digital capabilities without balancing them with the ability to manage cybersecurity risks actually has the potential to increase SMEs' vulnerability to various forms of digital crime. Therefore, cybersecurity must be positioned as a key component in every policy aimed at empowering and digitally transforming SMEs.

Furthermore, the mentoring model developed in this study has high potential for replication in various regions with similar SME characteristics. The flexibility of the approach, the use of simple language, experience-based learning, hands-on practice, and ongoing mentoring allow this model to be applied across various business sectors without requiring complex technological infrastructure. By adapting to the social characteristics, levels of digital literacy, and local needs of each region, this model has the potential to become one of the alternative national strategies for strengthening the digital resilience of SMEs in Indonesia.

Nevertheless, this study still has several limitations. The mentoring program involved only 60 SME participants under the guidance of Rumah BUMN in Lhokseumawe, so generalizing the research results must be done with caution. Additionally, the evaluation of the program's effectiveness remains focused on short-term changes in participants' capabilities through pre-test and post-test measurements, and thus cannot yet illustrate the sustainability of behavioral changes over a longer period. Future research is recommended to conduct a longitudinal evaluation to measure the consistency of cybersecurity practice implementation, develop more comprehensive digital resilience indicators, and test the effectiveness of this mentoring model across a wider range of regions, business sectors, and MSME characteristics, thereby yielding an empowerment model that is increasingly adaptive and possesses stronger external validity.

Strategic Implications for the Development of Cybersecurity Literacy Programs for SME Stakeholders

The findings of this study indicate that strengthening cybersecurity literacy must be viewed as an integral part of SME digital transformation strategies, not merely as additional training on technology use. Digital transformation that is not balanced with enhanced cybersecurity capabilities has the potential to create new vulnerabilities that could threaten business sustainability. Therefore, the success of SME digitalization is not only measured by the level of digital technology adoption but also by business owners' ability to manage risks, protect digital assets, maintain customer trust, and ensure operational continuity when facing cyber threats.

Research findings show that a mentoring model based on Participatory Action Research (PAR) can bring about changes that are not only cognitive in nature but also address behavioral and cultural aspects of digital security. These

changes are reflected in participants' increased awareness of the need to independently implement digital security practices, such as using two-factor authentication, managing passwords more securely, verifying digital transactions, regularly backing up business data, and exercising caution when responding to suspicious messages or links. These behavioral changes are a key indicator that the mentoring process has successfully established the foundation of a cybersecurity culture a crucial element in strengthening the digital resilience of MSMEs.

Unlike most previous community service programs, which focused on improving general digital literacy or provided technical cybersecurity training, this study offers a more comprehensive approach by integrating participant needs analysis, participatory learning, real-world case-based practice, implementation mentoring, quantitative evaluation, qualitative reflection, and SWOT analysis into a single, sustainable empowerment model. This integration allows the learning process to adapt to participants' characteristics, resulting in more sustainable behavioral changes than conventional training approaches.

From a policy perspective, the findings of this study recommend that MSME empowerment programs organized by local governments, Rumah BUMN, universities, or supporting institutions should incorporate cybersecurity literacy as a key indicator in digital transformation programs. To date, most policies have focused on enhancing digital marketing capabilities, the use of marketplaces, and the digitization of payments. However, without the ability to manage cybersecurity risks, increased use of digital technology can actually heighten the likelihood of fraud, data breaches, or operational disruptions that directly impact business sustainability.

In addition to its policy implications, the mentoring model developed in this study also has high replication potential. The program structure—comprising needs assessment, contextual training, practical simulations, implementation mentoring, ongoing evaluation, and participatory reflection—can be applied to various SME groups with different characteristics by adapting to the social conditions, digital literacy levels, and local needs of each region. This flexibility makes the model not only relevant for MSMEs under the guidance of Rumah BUMN " " in Lhokseumawe but also potentially adaptable as a national model for cybersecurity capacity-building programs for MSMEs.

Academically, this study contributes to the development of research on the relationship between cybersecurity literacy**,** digital resilience, and the business sustainability of MSMEs**.** The results show that improving cybersecurity literacy not only enhances individual competencies but also strengthens the capacity of

business organizations to anticipate, respond to, and recover from various digital threats. Thus, cybersecurity literacy can be positioned as a key determinant in building sustainable digital resilience for MSMEs.

Based on the overall research findings, it can be affirmed that the effectiveness of the mentoring program is demonstrated not only through improvements in pre-test and post-test scores, paired t-tests, and N-Gain, but also through behavioral changes, increased preparedness for cyber threats, and the establishment of digital security practices that are beginning to be implemented in participants' business operations. The integration of quantitative evidence and qualitative findings demonstrates that the developed mentoring model offers both practical value and scientific contribution in supporting the strengthening of MSMEs' digital resilience. Therefore, this study not only provides evidence regarding the effectiveness of a community service program but also produces an intervention model that is innovative, adaptive, and has the potential to serve as a reference in the development of cybersecurity literacy programs for MSMEs in various regions.

Implementation Challenges, Program Lessons Learned, and Sustainability Strategies

Although the mentoring program demonstrated a very high level of effectiveness based on both quantitative evaluation results and field observations, the implementation process was not without various challenges that affected the dynamics of activity execution. Identifying these challenges is crucial because it provides a more comprehensive understanding of the factors influencing the program's success and serves as a foundation for refining the mentoring model in future implementations.

The main challenge identified was the heterogeneity in participants' digital literacy levels. MSME owners have highly diverse educational backgrounds, experiences with technology, business types, and levels of digital platform usage. Some participants are accustomed to using marketplaces, digital payment apps, and business social media, while others still use digital technology only to a limited extent. These differences led to varying speeds of comprehension, requiring the mentoring process to adapt its delivery methods, the intensity of guidance, and communication approaches for each group of participants.

Furthermore, during the mentoring process, it was found that some participants initially still viewed cybersecurity as a technical issue that was solely the responsibility of digital platform providers or banking institutions. This

perception resulted in a relatively low level of vigilance against cyber threats, particularly regarding password practices, identity verification, customer data protection, and business account security. These conditions indicate that the greatest challenge is not limited to a lack of knowledge but also involves a shift in mindset regarding the importance of cybersecurity as part of business risk management.

The Participatory Action Research (PAR) approach allowed for an adaptive response to these various challenges throughout the program. Participant feedback gathered through group discussions, individual consultations, field observations, and reflections during each session—served as the basis for adjusting the course material, delivery methods, and simulation formats to better align with participants' needs. For example, when some participants were still having difficulty recognizing the characteristics of phishing, the facilitation team added simulations based on real-life cases the participants had experienced and increased the number of exercises to identify links and digital messages that might contain fraudulent elements. These adjustments were one of the factors contributing to a gradual improvement in participants' learning outcomes.

The results of the joint reflection also showed that the program's success was influenced not only by the quality of the training materials but also by the continuity of the mentoring process after the training activities concluded. Most participants reported that the opportunity to consult directly when facing digital security issues gave them greater confidence compared to simply receiving material through lectures. This finding demonstrates that experiential learning and ongoing mentoring play a crucial role in fostering more consistent digital security behaviors.

Another key lesson is that strengthening cybersecurity literacy requires multi-stakeholder collaboration. Higher education institutions serve as providers of expertise and innovation; Rumah BUMN acts as an empowerment facilitator; local governments formulate policies and provide regulatory support; while MSME actors play a central role in implementing digital security practices. This collaboration creates a more adaptive learning ecosystem, ensuring that capacity-building efforts do not end with a single community service program but evolve into a continuous learning process.

Based on the experience of this implementation, this study recommends several strategies for program sustainability. First, cybersecurity literacy mentoring should be conducted periodically so that participants receive updates on the ever-changing landscape of cybercrime. Second, a cybersecurity learning

community should be established within the Rumah BUMN environment as a platform for sharing experiences, consultations, and the dissemination of *best practices*. Third, the development of learning modules based on local case studies needs to be continuously updated to ensure the material remains relevant to the challenges faced by MSME operators. Fourth, program success should not be evaluated solely through short-term measurements but also through longitudinal evaluations to assess the consistency of changes in digital security behavior over the long term.

Taking into account the various challenges, adaptation processes, and lessons learned during implementation, this study demonstrates that the effectiveness of a mentoring program is determined not only by a well-designed intervention but also by the program's ability to dynamically adapt to participants' needs. Therefore, the mentoring model developed in this study not only improves cybersecurity literacy competencies but also establishes an adaptive and sustainable learning mechanism as a foundation for strengthening the digital resilience of MSMEs in the era of digital transformation.

Conclusion

This community service initiative demonstrates that participatory cybersecurity literacy mentoring is an effective strategy for strengthening the digital resilience of SMEs facing increasingly complex cyber threats. The findings confirm that a Participatory Action Research (PAR)-based approach significantly improves not only participants' cybersecurity knowledge but also their practical skills, awareness, and security-oriented behaviors. These outcomes highlight that contextual, participatory, and practice-oriented mentoring is more effective in promoting sustainable behavioral change than conventional knowledge-transfer approaches. The study contributes both theoretically and practically by positioning cybersecurity literacy as a fundamental component of SME competitiveness and business sustainability in the digital economy. Rather than being viewed solely as a technical issue, cybersecurity should be integrated into SME empowerment policies as an essential capability for protecting digital assets, maintaining customer trust, and supporting long-term organizational resilience. The cybersecurity literacy mentoring model developed in this study offers a replicable framework that combines needs assessment, participatory learning, real-case simulations, implementation assistance, quantitative and qualitative evaluation, and strategic sustainability planning. This model provides practical guidance for governments, higher education institutions, business support

organizations, and digital ecosystem stakeholders seeking to strengthen cybersecurity capacity among SMEs.

Despite these contributions, several limitations should be acknowledged. The study was conducted with a relatively limited sample of SMEs affiliated with Rumah BUMN in Lhokseumawe, which may constrain the generalizability of the findings to broader SME populations. Furthermore, the effectiveness of the program was assessed only through short-term measurements, preventing an evaluation of the long-term sustainability of behavioral changes. In addition, the study did not examine whether improved cybersecurity literacy translates into measurable business outcomes, such as productivity, financial performance, customer trust, or digital competitiveness. Future studies should employ longitudinal designs involving more diverse SME populations across different regions to evaluate the persistence of cybersecurity practices over time. Further research should also investigate the relationship between cybersecurity literacy, digital resilience, and organizational performance while exploring collaborative governance models that integrate government agencies, universities, business support institutions, financial organizations, and digital service providers. Such evidence would provide a stronger empirical foundation for developing sustainable and inclusive digital transformation policies that enhance the resilience and competitiveness of SMEs.

References

Aji, M. P., Subakdi, & Yuliandri, P. (2025). Sosialisasi Birokrasi Digital dan Keamanan Siber di Era Masyarakat Digital 5 . 0 Bagi Warga di Kelurahan Pangkalan Jati, Kota Depok. *BERNAS: Jurnal Pengabdian Kepada Masyarakat*, *6*(1), 654–661. https://doi.org/10.31949/jb.v6i1.12608

Akbar, M., & Wijaya, G. (2024). Digital Literacy of Rural Areas in Indonesia: Challenges and Opportunities. *RUSET*, *1*. https://doi.org/10.4108/eai.1-11-2023.2344347

Anan, M., Rahmah, S. A., & Risuhendri. (2024). Meningkatkan Kesadaran Digital Dalam Pencegahan Penipuan Online Untuk Kelompok UMKM Desa Tanjung Haratan. *Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 56–63. https://doi.org/10.70585/abdidalem.v1i2.29

Arroji, M. B., Rauf, A. A., Talia, L. D., Servanda, Y., & Insan, P. P. (2025). *Analisis Risiko Keamanan Siber pada Infrastruktur Digital UMKM di Balikpapan dan Strategi Mitigasi Berbasis Kerangka Kerja Keamanan Siber Nasional*. *8*(11), 1–9. https://doi.org/10.8734/Kohesi.v1i2.36 5

Dianastiti, Y., Putra, R. A., & Allamsyah, M. N. S. (2023). Pelatihan dan Pendampingan Analisis Data Penelitian Bidang Pendidikan Dengan SPSS Untuk Sivitas Akademika PVTO Universitas Bhinneka PGRI. *Madiun Spoor: Jurnal Pengabdian Masyarakat*, *3*(2), 41–46. https://doi.org/10.37367/jpm.v3i2.315

Falch, M., Olesen, H., Skouby, K. E., Tadayoni, R., & Williams, I. (2023). Cybersecurity Strategies for SMEs in the Nordic Baltic Region. *Journal OfCyber Security and Mobility*, *11*(6), 727–754. https://doi.org/10.13052/jcsm2245-1439.1161

Indonesia, K. K. B. P. R. (2025). *Pemerintah Dorong UMKM Naik Kelas, Tingkatkan Kontribusi terhadap Ekspor Indonesia*. Ekon.Go.Id. https://www.ekon.go.id/publikasi/detail/6152/pemerintah-dorong-umkm-naik-kelas-tingkatkan-kontribusi-terhadap-ekspor-indonesia

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *Computer Science: Cryptography and Security*, *1*(1), 1–32. https://doi.org/10.48550/arXiv.2309.17186

Lhokseumawe, P. P. K. (2024). *Pj Walikota Lhokseumawe Dorong Anak Muda Menjadi Pengusaha Melalui Roadshow BSI Aceh Muslimpreaneur 2024*. Lhokseumawekota.Go.Id. https://www.lhokseumawekota.go.id/berita-XWgp

Oliveira, B. De. (2023). Participatory Action Research as a Research Approach: Advantages, Limitations and Criticisms. *Qualitative Research Journal*, *23*(3), 287–297. https://doi.org/10.1108/QRJ-08-2022-0101

Palatty, N. J. (2025). *51 Small Business Cyber Attack Statistics 2025 (And What You Can Do About Them)*. Astra. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/#:~:text=Statistik Serangan Siber pada Usaha Kecil 2021,perhatian media atau penegak hukum.

Pangrazio, L., Godhe, A. L., & Ledesma, A. G. L. (2020). What is Digital Literacy? A Comparative Review of Publications Across Three Language Contexts. *E-Learning and Digital Media*, *17*(6), 442–459. https://doi.org/10.1177/2042753020946291

Raisah, E. (2025). *Ancaman Siber Mengintai UMKM Pentingnya Perlindungan Data Digital*. Datacomm. https://www.datacomm.co.id/release/ancaman-siber-mengintai-umkm-pentingnya-perlindungan-data-digital/

Safar, L., Pekarcik, M., Morawiec, P., Rutecka, P., & Wieczorek-Kosmala, M. (2025).

Mapping Cybersecurity in SMEs: The Role of Ownership and Firm Characteristics in the Silesian Region of Poland. *Information*, *16*(590), 1–16. https://doi.org/10.3390/ info16070590

Sari, P. K., Candiwan, Trianasari, N., & Prasetio, A. (2025). Peningkatan Kesadaran Keamanan Siber Melalui Pelatihan Kepada Pelaku UMKM Binaan Yayasan Purba Danarta Semarang. *Jurnal Pengabdian Kolaborasidan Inovasi IPTEKS*, *3*(4), 849–856. https://doi.org/10.59407/jpki2.v3i4.2574

Sugiyono. (2022). *Metode Penelitian Kuantitatif (Edisi ke-3)* (3rd ed.). CV Alfabeta.

Yusnanto, T., Fatkhurrochman, Muin, M. A., & Waluyo, S. (2023). Pelatihan Dasar Kemanan Digital Untuk Mengurangi Pencurian Data Yang Berdampak Pada UMKM. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(9), 2022–2029. https://doi.org/10.59837/jpmba.v1i9.458