

Strengthening Digital Legal Literacy for Cybercrime Prevention in Ngadiluwih Village

Basri Basri^{1*}, Achmad Irmawan², Herman Septianto³, Tsuroyyaamaitasaa'Jaudah⁴

Universitas Muhammadiyah Magelang, Jawa Tengah, Indonesia^{1,2,3,4}

basri@unimma.ac.id^{1*}, ipm.achmadirmawan@gmail.com², hermanseptianto66@gmail.com³, tsuroyyaamaitasaa@unimma.ac.id⁴



Article History

Received on 07 May 2026

1st Revision on 15 May 2026

2nd Revision on 27 May 2026

3rd Revision on 02 June 2026

Accepted on 13 June 2026

Abstract

Purpose: This community service program aimed to strengthen digital legal literacy as a preventive approach to cybercrime in Ngadiluwih Village, Magelang Regency, Indonesia.

Research Methodology: The program involved 30 community participants and used a participatory community-based educational approach through legal counselling, interactive discussion, contextual problem analysis, and collective reflection. The program focuses on legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness.

Results: The implementation demonstrated that participatory legal education provides a practical mechanism for connecting legal knowledge with participants' everyday digital experiences and cyber-related risks. Based on the implementation process and reflection, the study proposes the Community-Based Digital Legal Literacy (CBDLL) Model, which integrates community digital risks, community-based legal education, five dimensions of digital legal literacy, preventive capacity, and community resilience to cybercrime.

Conclusions: Community-based digital legal education can serve as an important component of cybercrime prevention in rural communities by strengthening individuals' capacity to recognize and respond to digital risks in the future.

Limitations: The program relied primarily on qualitative observations and did not employ standardized pre- and post-test instruments. It involved only 30 participants from one rural community, and the CBDLL Model has not yet been evaluated through longitudinal or comparative implementation.

Contributions: This study contributes a practice-based conceptual framework for integrating legal education and digital literacy into community-level cybercrime prevention and provides a practical reference for stakeholders developing sustainable digital legal literacy programs in rural communities.

Keywords: *Community Empowerment, Cybercrime Prevention, Digital Legal Literacy, Digital Literacy, Rural Communities*

How to Cite: Basri, B., Irmawan, A., Septianto, H., & Tsuroyyaamaitasaa'Jaudah. (2026). Strengthening Digital Legal Literacy for Cybercrime Prevention in Ngadiluwih Village. *Jurnal Nusantara Mengabdi*, 5(3), 41-53.

1. Introduction

The rapid expansion of digital technology has transformed the way people communicate, obtain information, conduct transactions, and participate in social lives ([Chayko, 2020](#)). Digital platforms provide substantial benefits to communities, including easier access to information, communication, and economic opportunities ([Baderan et al., 2025](#)). However, these developments have created new vulnerabilities. Cyber-related risks, such as online fraud, phishing, misinformation, misuse of personal data, and harmful online communication, increasingly form part of everyday digital experiences ([Nath, 2024](#)). Therefore, cybercrime prevention requires not only technological and law enforcement responses but also the development of individual and community capacity to recognize, understand, and respond to digital risks ([Cross, 2020](#); [Ichsan et al., 2026](#)).

The challenges associated with digital environments are particularly important in communities where access to digital technology has expanded faster than the development of the knowledge and capabilities required for its safe and responsible use ([Van Deursen, 2019](#)). Digital inequality is no longer limited to whether individuals have physical access to digital devices and the Internet. It also involves differences in the material conditions, skills, and capacities required to benefit from digital technology ([Helsper, 2021](#)). Similarly, differences in digital resources and capabilities can affect how individuals communicate and access information ([Nguyen, 2021](#)). These conditions suggest that strengthening digital capacity should involve not only technical skills but also the ability to understand risks, evaluate information, and make informed decisions in digital environments ([Martínez-Bravo, 2022](#)).

One of the most important challenges is the increasing circulation of misinformation and misleading online content. The rapid dissemination of false information makes it difficult for users to distinguish reliable information from fraudulent or manipulated content ([Guess, 2019](#)). Research has shown that false news can spread rapidly through online networks, and individual users may contribute to its dissemination under particular social and informational conditions ([Vosoughi, 2018](#)). Therefore, media and information literacy is an important component of responsible digital participation because individuals need the capacity to access, evaluate, verify, and use information critically ([Longinus, 2024](#)). Digital literacy indicators similarly include the ability to evaluate information and use digital technologies appropriately and responsibly ([M. Claire Buchan 2024](#)).

However, digital literacy cannot be separated from legal awareness. Individuals may possess technical skills for accessing social media, conducting online transactions, or communicating through digital platforms while lacking a sufficient understanding of the legal consequences of their actions ([Martínez-Bravo & Serrano-Puche, 2022](#)). Legal literacy is important because it enables individuals to understand their rights, responsibilities, risks, and possible legal consequences associated with their behavior ([Tymoshenko, 2025](#); [Dwijaya et al., 2026](#)). In the context of digital environments, this connection becomes increasingly significant because online activities may involve issues related to fraud, privacy, personal data, harmful communication, and other forms of unlawful conduct. The integration of legal awareness with digital literacy can provide a stronger foundation for responsible digital behavior ([Reddy, 2020](#)).

The concept of digital citizenship further emphasizes that responsible participation in digital environments involves ethical behavior, awareness of rights and responsibilities, and appropriate interactions with others ([Huschle, 2024](#)). Digital citizenship skills have also been associated with efforts to prevent cybercrime, particularly through the development of knowledge, beliefs, and responsible digital practices ([Althibyani, 2023](#)). Thus, cybercrime prevention at the community level should not be understood exclusively as a matter of identifying offenders and enforcing the criminal law. It should also involve empowering community members to recognize risks, verify information, protect personal data, communicate responsibly, and understand the legal implications of their digital activities ([Asimakopoulou, 2025](#)).

This perspective is particularly relevant to rural communities, where community-based approaches can provide accessible mechanisms for translating legal and digital knowledge into everyday practice. Community education can create opportunities for participants to discuss problems they encounter and connect formal legal knowledge with their experiences. Recent community-based initiatives have

highlighted the potential of digital legal literacy education to strengthen users' understanding of legal issues associated with social media and digital environments ([Cahyani et al. 2026](#)). Similarly, community awareness has been identified as an important basis for developing community-based approaches to high-tech crime prevention in the context of digital transformation ([Trung 2026](#)).

From this perspective, universities and other knowledge-based institutions play an important role in translating legal and digital knowledge into forms that can be understood and applied by community members ([Mudashir Adeola Olaitan & Sennuga, 2025](#)). Legal education delivered through participatory methods can move beyond the one-way transmission of legal information by incorporating discussions, contextual cases, problem analyses, and reflections. This approach is consistent with the broader understanding that access to law should involve not only the formal availability of legal institutions but also the capacity of individuals to understand and effectively use legal knowledge to address problems affecting their lives ([Sandefur, 2019](#)).

The need for such an approach provides the background for the community service program conducted in Ngadiluwih Village, Salam District, and Magelang Regency. The program was designed to strengthen community capacity to respond to digital risks through legal counseling, interactive discussions, contextual problem analyses, and collective reflections. Rather than treating digital legal literacy as a single form of knowledge, the program approached it as an interconnected set of capacities involving legal awareness, digital literacy, information verification, digital ethics, and cybersecurity.

Based on the implementation process and reflection on the issues discussed during the program, this article proposes the Community-Based Digital Legal Literacy (CBDLL) Model as a practice-based conceptual framework for cybercrime prevention in rural communities. The model connects the identification of community digital risks with participatory legal education and the development of interconnected digital-legal literacy capacities. This study aims to provide a practical framework for strengthening preventive capacity and supporting community resilience against cybercrime. Accordingly, this study addresses the following question: How can community-based digital legal literacy education contribute to strengthening preventive capacity for cybercrime in rural communities? This study contributes to the discussion by linking legal education, digital literacy, information verification, digital ethics, and cybersecurity awareness within a community-based preventive framework while recognizing the need for further empirical evaluation of the proposed model.

2. Research Methodology

2.1 Research Design and Approach

This study employed a participatory community-based educational approach to strengthen digital legal literacy for cybercrime prevention in rural communities. This approach was implemented through a community service program in Ngadiluwih Village, Salam District, Magelang Regency, Indonesia. Rather than employing an experimental or survey-based design, the program emphasized participatory legal education, in which community members were encouraged to identify, discuss, and reflect upon the digital risks encountered in their everyday activities. The methodological approach was designed to connect legal knowledge with practical digital experience. The program integrated legal counseling, interactive discussions, contextual problem analysis, and collective reflection ([Syafiih et al., 2024](#); [Nurhayati et al., 2021](#)). These activities were used to explore community concerns regarding digital risks and strengthen five interconnected dimensions of digital legal literacy: legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness.

2.2 Study Location and Participants

The program was conducted in Ngadiluwih Village, Salam District, Magelang Regency, Central Java, Indonesia. The participants consisted of 30 members of the local community, representing different elements of the village community. The participants were involved in educational activities and discussions concerning digital risks, responsible digital behavior, and the legal implications of activities conducted through digital platforms. The selection of the community as the program setting was based on the importance of strengthening preventive capacity at the local level of the

community. The village environment provides a relevant context for examining how legal and digital knowledge can be translated into practical awareness and preventive behavior in everyday community life.

2.3 Educational Materials and Learning Activities

Educational materials were developed around digital risks relevant to community members. The principal issues addressed during the program included online fraud, misinformation, online gambling, cyberbullying, personal data misuse, and harmful or irresponsible forms of digital communication. The educational process consisted of four interconnected activities. The first involved legal counseling to introduce participants to relevant legal rights, responsibilities, risks, and potential consequences associated with digital activities. The second activity was conducted through interactive discussions that encouraged participants to share their experiences, concerns, and questions regarding digital risk. The third activity involved contextual problem analysis by discussing examples of digital problems that may occur in everyday community life, enabling participants to connect legal concepts to practical situations. The final activity consisted of a collective reflection to consolidate the participants' understanding and encourage consideration of appropriate preventive responses to digital risks. The learning process focused on five dimensions of digital legal literacy: legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness.

2.4 Data Collection and Evaluation

The program did not employ a standardized survey instrument, questionnaire, or experimental pre- and post-test design. Instead, the evaluation was based primarily on qualitative observations of participant engagement, questions, responses, interactions, and discussions during the educational activities. Particular attention was given to the participants' ability to identify digital risks, relate digital problems to legal responsibilities and consequences, evaluate the reliability of information, recognize responsible digital behavior, and discuss basic measures for protecting personal information and digital accounts. The observations and reflections generated during the activities were used to identify the principal issues that emerged from the community-based educational process. These observations did not constitute statistical measurements of changes in knowledge or behavior; rather, they provided qualitative evidence regarding the implementation process and participants' engagement with the subject matter.

The qualitative evaluation was intended to provide a context-sensitive understanding of how participants interpreted and responded to the educational material. Qualitative observation is particularly appropriate for identifying processes, meanings, and participant reactions that cannot always be adequately represented through standardized numerical indicators ([Creswell & Poth, 2018](#); [Patton, 2015](#)). Accordingly, the observational material was reviewed to identify recurring issues and patterns related to digital-risk awareness, legal understanding, information verification, responsible online conduct, and personal data protection. The interpretation focused on the substance and context of participants' contributions rather than merely counting the frequency of their responses.

To strengthen the credibility of the evaluation, interpretations were grounded in observable participant responses and concrete interactions occurring during the activities. Attention was also given to responses that differed from the dominant pattern to avoid presenting participants' experiences as entirely uniform. This approach is consistent with qualitative research principles that emphasize transparency, contextual richness, reflexivity, and the close connection between interpretations and empirical evidence ([Braun & Clarke, 2021](#); [Tracy, 2010](#)). Nevertheless, because the program did not use baseline measurements, standardized indicators, or follow-up assessments, the findings should be interpreted as evidence of participation and emerging understanding rather than proof of measurable or sustained changes in participants' knowledge and digital behavior.

2.5 Data Analysis and Development of the CBDLL Model

The analysis followed a qualitative, descriptive, and reflective process. The issues identified during the educational activities were organized according to the major components of digital legal literacy addressed in this program. Participant interactions, questions, discussions, and reflections were examined to identify recurring themes related to digital risks, legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness. The findings from this process

were conceptually integrated into the Community-Based Digital Legal Literacy (CBDLL) Model. The model was developed as a practice-based conceptual framework rather than a statistically validated predictive model. Its development follows a sequential logic: identification of community digital risks, implementation of community-based legal education, strengthening of interconnected digital legal literacy capacities, development of preventive capacity, and enhancement of community resilience against cybercrime.

The analysis followed a qualitative, descriptive, and reflective process. The issues identified during the educational activities were organized according to the major components of digital legal literacy addressed in the program. Participant interactions, questions, discussions, and reflections were examined to identify recurring patterns related to digital risks, legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness. This flexible thematic approach enabled the analysis to remain responsive to the participants' contextual experiences while maintaining consistency with the program's educational objectives ([Braun & Clarke, 2021](#)). The analytical process combined concept-driven categories derived from the program framework with patterns emerging from participant engagement, reflecting a hybrid integration of deductive and inductive interpretation ([Xu & Zammit, 2020](#)). Themes were reviewed according to their conceptual coherence, relevance to the educational activities, and ability to represent meaningful patterns within the qualitative observations. Such conceptual and methodological alignment is important for maintaining coherence between the research objectives, analytical procedures, and interpretation of themes ([Braun & Clarke, 2022](#)).

The findings generated through this process were conceptually integrated into the Community-Based Digital Legal Literacy (CBDLL) Model. The model was developed as a practice-based conceptual framework rather than a statistically validated predictive model. Its construction involved synthesizing the identified themes and explaining the relationships among the principal components of community digital legal literacy. This approach is consistent with contemporary conceptual-model development, which requires a transparent research design, clear specification of the concepts included, and logical explanation of the relationships connecting those concepts ([Jaakkola, 2020](#)). The CBDLL Model follows a sequential logic comprising the identification of community digital risks, implementation of community-based legal education, strengthening of interconnected digital legal literacy capacities, development of preventive capacity, and enhancement of community resilience against cybercrime. Accordingly, the model represents an interpretive synthesis of program implementation and observed participant engagement and requires further empirical examination before it can be treated as a validated explanatory or predictive model.

2.6 Research Conditions and Methodological Boundaries

The program was conducted as a community-based educational activity involving 30 participants from a single rural community. The methodological approach assumes that participatory legal education can provide a mechanism for connecting formal legal knowledge with community members' everyday digital experiences. The approach also assumes that the integration of legal awareness and digital literacy is relevant for strengthening preventive capacity against cybercrime. Because the program did not employ standardized quantitative instruments or longitudinal observations, the results cannot be interpreted as statistical evidence of changes in participants' knowledge, attitudes, or behavior. Similarly, the CBDLL Model should be understood as a practice-based conceptual framework emerging from the implementation and reflection process. Further empirical testing in different communities and through more systematic evaluation designs is required to assess the effectiveness and generalizability of this approach.

3. Results and Discussion

3.1 Community Digital Risks Identified During the Program

The community service program identified several digital risks relevant to everyday activities in Ngadiluwih Village. The principal issues addressed during legal counseling and interactive discussions included online fraud, misinformation, online gambling, cyberbullying, personal data misuse, and harmful or irresponsible digital communication. These issues indicate that the risks

associated with digital technology are not limited to technically sophisticated cybercrimes but are also connected to routine communication, information consumption, online transactions, and personal data management.

Online fraud and phishing are particularly relevant because cybercrime may exploit ordinary patterns of digital interaction and users' vulnerabilities. Routine activity perspectives suggest that victimization can occur when motivated offenders encounter suitable targets in the absence of adequate protective measures (Taufik, Mulyapradana, Prayetno, & Hasim, 2026). Demonstrates the relevance of routine activity theory to phishing victimization (Leukfeldt, 2014), while emphasizing the broader relationship between online safety, security, and everyday digital activities (Cross, 2022). These perspectives support the importance of strengthening preventive capacity at the level of ordinary digital users rather than relying exclusively on responses after victimization.

Misinformation was another important issue addressed in the program. Participants were encouraged to consider the credibility of the information before sharing or acting on it. This issue is significant because false information can spread rapidly through online networks, and users may contribute to its dissemination without fully recognizing its accuracy or reliability (Vosoughi, Roy, & Aral, 2018). Guess, Nagler, and Tucker (2019) further indicated that the dissemination of fake news is associated with particular patterns of social media use and individual characteristics. These findings reinforce the importance of information verification in digital legal literacy.

The discussion of online gambling, cyberbullying, personal data misuse, and harmful digital communication further demonstrates that digital risks have both legal and social dimensions. These risks require community members to understand not only how digital technologies operate, but also the responsibilities and consequences associated with their use. Accordingly, the program approached digital risks as interconnected issues requiring legal awareness, digital literacy, ethical awareness, and basic cyber security knowledge. The implementation of the community-based digital legal literacy program involved legal counseling and the delivery of educational materials on various digital risks and their legal implications for children. The activity was designed to provide participants with practical knowledge relevant to their everyday use of digital technology, as shown in Figure 1.



Figure 1. Implementation of the community-based digital legal literacy program in Ngadiluwih Village

3.2 Community Engagement in Participatory Digital Legal Education

The program involved 30 community participants who engaged in legal counseling, interactive discussions, contextual problem analysis, and collective reflection. Participant questions, responses, and discussions provided opportunities to connect formal legal concepts with situations encountered in everyday digital activity. The participatory nature of the activities was important because digital legal literacy cannot be developed solely through passive transmission of legal information. Community members need opportunities to relate legal concepts to their experiences and discuss practical responses to digital problems. This approach is consistent with the broader understanding that meaningful access to the law involves the ability of individuals to understand and use legal knowledge to address problems affecting their lives (Sandefur, 2019).

The community-based approach is also supported by recent initiatives that emphasize digital legal literacy through community education. For example, it highlights the importance of community education in strengthening digital legal literacy among social media users ([Cahyani, 2026](#)). [Similarly, Trung_ \(2026\)](#), emphasizes community awareness as a basis for developing community-based approaches to high-tech crime prevention in the context of digital transformation.

Therefore, the engagement observed during the program should be understood as an important process-related finding rather than as statistical evidence of increased knowledge ([Zainuddin et al., 2025](#)). Because no standardized pre- and post-test instruments were employed, the program could not establish the magnitude of changes in participants' knowledge or behavior. Nevertheless, the discussions and reflections provided qualitative evidence that participatory education created opportunities for participants to examine digital risks from legal and preventive perspectives. Following the delivery of the educational materials, the participants actively engaged in interactive discussions and contextual analyses of digital problems. The discussion provided an opportunity for community members to share their experiences, raise questions, and reflect on appropriate preventive responses to digital risks, as illustrated in Figure 2.



Figure 2. Community Participation in Legal Counseling and Interactive Discussion on Digital Risks

3.3 Strengthening the Five Dimensions of Digital Legal Literacy

The implementation process identified five interconnected dimensions that constitute an important foundation for community-based digital legal literacy: legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness. Rather than functioning as isolated competencies, these dimensions form a mutually reinforcing framework through which community members can understand, evaluate, and respond to legal and security risks in digital environments. Legal awareness represents the normative foundation of this framework, encompassing participants' understanding of their rights, responsibilities, applicable legal provisions, potential legal risks, and the consequences associated with digital activities. Such awareness is essential for preventive behavior because individuals are more likely to exercise caution when they understand not only what constitutes risky or unlawful digital conduct but also why such conduct may produce legal, social, or economic consequences. However, legal knowledge alone may have limited preventive value if individuals lack the practical digital competencies required to identify and respond to risks encountered in everyday online activities.

Digital literacy therefore represents a complementary dimension that enables individuals to navigate digital environments critically, effectively, and responsibly. It extends beyond basic operational skills and includes the capacity to access, evaluate, interpret, and use digital technologies in ways that support personal and collective well-being. Research on digital inequality demonstrates that disparities in digital participation are not limited to physical access to devices or internet connectivity but also involve differences in material resources, skills, and individual capabilities ([Van Deursen, 2019](#)). These inequalities may influence an individual's capacity to recognize online threats, protect personal information, evaluate digital content, and make informed decisions. Similarly, digital inequality has broader social causes and consequences that can shape how individuals benefit from or

become vulnerable to digital technologies ([Helsper, 2021](#)). Consequently, effective cybercrime prevention cannot rely solely on increasing access to digital technology; it must also strengthen the competencies that allow community members to engage with digital environments safely, critically, and meaningfully.

Within this framework, information verification functions as a critical analytical capability that connects digital literacy with legal and preventive awareness. It involves the ability to assess the credibility, accuracy, origin, and intent of digital information while recognizing misleading, fraudulent, manipulated, or deliberately deceptive content. This capability is increasingly important because digital platforms enable information to circulate rapidly across social networks, messaging applications, and online communities, often without adequate verification. In the context of cybercrime prevention, weak verification practices may increase individuals' exposure to phishing, online fraud, impersonation, misinformation, and other forms of digital deception. Information verification therefore should not be understood merely as a media-literacy skill but as a preventive mechanism that enables individuals to interrupt potentially harmful interactions before they develop into legal, financial, or security-related problems. By encouraging users to question sources, cross-check information, and identify suspicious patterns, this dimension strengthens the practical application of both legal awareness and digital literacy.

Digital ethics constitutes another essential dimension because responsible participation in digital environments requires individuals to consider not only whether an action is technically possible or legally permissible but also whether it is socially and ethically appropriate. Digital ethics encompasses responsible communication, respect for others, protection of privacy, awareness of the consequences of online behavior, and avoidance of harmful practices such as cyberbullying, harassment, unauthorized distribution of information, and misuse of digital content. The concept of digital citizenship emphasizes responsible participation, ethical conduct, rights, and responsibilities within digital environments ([Ribble, 2015](#)). From a cybercrime-prevention perspective, ethical awareness can contribute to reducing harmful online behavior by encouraging individuals to recognize that digital actions can affect other people, communities, and institutions even when physical interaction is absent. Digital citizenship skills are therefore relevant not only to appropriate online participation but also to broader efforts to prevent digital misconduct and cyber-related harm ([Althibyani, 2023](#)). Integrating digital ethics into digital legal literacy consequently broadens the preventive approach from compliance with formal rules toward the development of responsible digital behavior.

Cybersecurity awareness provides the practical protection dimension of the framework by equipping community members with the knowledge and vigilance necessary to recognize common digital threats and implement basic protective measures. This includes identifying suspicious messages and communications, detecting fraudulent or malicious links, maintaining secure passwords and accounts, protecting personal and financial information, and exercising caution when sharing data through digital platforms. Cybersecurity awareness is particularly important because many cyber incidents exploit human behavior rather than solely technical vulnerabilities. Individuals who possess legal and ethical knowledge but lack awareness of common attack methods may still become victims of fraud, account compromise, identity theft, or unauthorized data disclosure. Conversely, basic technical awareness can be strengthened when individuals understand the legal and social consequences associated with careless digital practices. Cybersecurity awareness therefore complements the normative dimensions of legal awareness and digital ethics by translating knowledge and values into concrete protective behaviors.

Taken together, these five dimensions form an integrated system of preventive digital competence. Legal awareness establishes an understanding of rights, obligations, and consequences; digital literacy provides the capacity to navigate digital environments; information verification enables individuals to evaluate the credibility and risks of digital content; digital ethics guides responsible and socially conscious behavior; and cybersecurity awareness provides practical strategies for protecting individuals, accounts, and personal information. The interaction among these dimensions is particularly important because weaknesses in one dimension may undermine the effectiveness of the others. Legal awareness without sufficient digital literacy, for example, may leave individuals unable to identify the risks encountered in complex digital environments. Similarly, strong technical skills

without legal and ethical awareness may enable individuals to use technology effectively while remaining insufficiently aware of the consequences of their actions. Information verification strengthens decision-making by helping individuals distinguish legitimate opportunities from deceptive or malicious content, while cybersecurity awareness provides the practical safeguards necessary to act on that judgment. Thus, community-based digital legal literacy should be conceptualized not simply as the transfer of legal information but as a multidimensional capacity-building process that integrates knowledge, critical evaluation, ethical judgment, and protective behavior. Such an integrated approach can strengthen communities' resilience against cybercrime while simultaneously promoting safer, more responsible, and legally informed participation in the digital environment.

3.4 Development of the Community-Based Digital Legal Literacy (CBDLL) Model

The integration of the findings from the implementation process led to the development of the Community-Based Digital Legal Literacy (CBDLL) Model as a practice-based conceptual framework for cybercrime prevention in rural communities. The model begins with the identification of digital risks in the community. These risks provide a substantive basis for community-based legal education. Through legal counseling, interactive discussions, contextual case analyses, and collective reflections, the participants were encouraged to connect their digital experiences with legal, ethical, informational, and security considerations. The educational process strengthens five interconnected dimensions of digital legal literacy: legal awareness, digital literacy, information verification, digital ethics, and cybersecurity awareness. Their integration is expected to contribute to preventive capacity, understood in this study as the community's ability to recognize digital risks, assess potential consequences, make informed decisions, and take appropriate preventive measures.

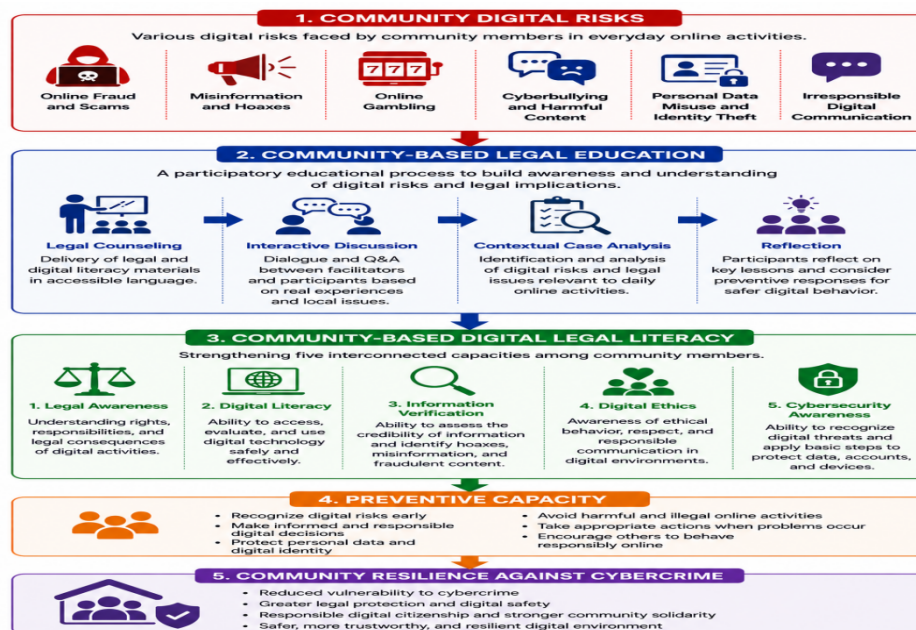


Figure 3. Community-Based Digital Legal Literacy (CBDLL) Model for Cybercrime Prevention in Rural Communities

Figure 3. Community-Based Digital Legal Literacy (CBDLL) Model for Cybercrime Prevention in Rural Communities

Figure 3 illustrates the logical relationship between community digital risks, community-based legal education, digital legal literacy, preventive capacity, and community resilience. The model does not claim a statistically validated causal relationship between the variables. Rather, it represents a practice-based conceptual framework derived from the implementation process and reflections on the issues addressed during the community service program. The model is consistent with the broader argument that cybercrime prevention should involve community capacity rather than depend exclusively on reactive law enforcement agencies. Digital literacy, information verification, responsible digital behavior, and cybersecurity awareness provide practical mechanisms through which legal awareness can be translated into preventive actions. Therefore, the model positions the community as an active participant in cybercrime prevention rather than merely as a potential victim.

3.5 Implications for Community Empowerment and Cybercrime Prevention

These findings have several implications for community empowerment. First, cybercrime prevention can begin before an offence or victimization occurs by strengthening individuals' capacity to identify risks and make informed decisions. This preventive orientation complements, rather than replaces, formal law enforcement. Second, community members can actively identify and address digital risks. Participatory education enables communities to discuss problems arising from their digital experiences and develop a shared understanding of appropriate preventive responses.

Third, the integration of legal awareness and digital literacy is important because digital competence and legal knowledge address different but complementary dimensions of prevention training. Digital literacy helps individuals navigate digital environments, and legal awareness provides an understanding of rights, responsibilities, and consequences. Information verification, digital ethics, and cybersecurity awareness further translate these capacities into practical preventive behaviors. Finally, this approach has implications for the role of local institutions. Village governments, universities, community organizations, legal aid institutions, and other relevant stakeholders should collaborate to develop continuous digital legal literacy programs. Such collaboration is particularly important because a single educational intervention cannot establish long-term community resilience.

Overall, the results indicate that community-based digital legal education offers a promising, practice-based approach to cybercrime prevention. However, the findings should be interpreted within the methodological limitations of the program. The observed engagement and discussions provide qualitative evidence of the educational process but do not constitute statistical evidence of behavioral changes. Further implementation using systematic pre-test and post-test assessments, follow-up observations, and comparative community settings is therefore necessary to evaluate the effectiveness and adaptability of the CBDLL Model.

4. Conclusion

4.1 Conclusion

This community service program demonstrates the importance of strengthening digital legal literacy as a preventive measure against cybercrime in rural communities. Conducted in Ngadiluwih Village with 30 community participants, the program connected legal counselling, interactive discussion, contextual problem analysis, and collective reflection with everyday digital risks encountered by community members. The implementation process identified several relevant digital risks, including online fraud, misinformation, online gambling, cyberbullying, personal data misuse and harmful or irresponsible digital communication. The program further highlighted the importance of integrating five interconnected dimensions of digital legal literacy: legal awareness, digital literacy, information verification, digital ethics, and cybersecurity. These dimensions provide complementary capacities that can support individuals in recognizing digital risks, understanding potential consequences, making informed decisions, and taking preventive measures against cyberbullying.

Based on the implementation process and reflection, this article proposes the Community-Based Digital Legal Literacy (CBDLL) Model as a practice-based conceptual framework for cybercrime prevention in rural communities. The model connects community digital risks with participatory legal education, the five dimensions of digital legal literacy, preventive capacity, and community resilience against cybercrime. The contribution of this study lies in positioning digital legal literacy as an integrated community-based preventive approach, rather than treating legal education, digital literacy, and cybersecurity awareness as separate interventions. The CBDLL Model provides a practical conceptual reference for universities, village governments, community organizations, legal aid institutions, and other stakeholders seeking to strengthen community capacity to respond to digital risks.

4.2 Research Limitations

This study had several limitations. First, the evaluation relied primarily on qualitative observations of participant engagement, questions, responses, discussions and reflections during the program. The activity did not employ standardized pre- and post-test instruments or other quantitative measures. Consequently, this study could not statistically establish changes in participants' knowledge, attitudes, or preventive behavior. Second, the program involved 30 participants from a single rural

community in Ngadiluwih Village. Therefore, the findings reflect the specific context of the community service program and should not be generalized to other communities without further investigation.

Third, the CBDLL Model is a practice-based conceptual framework developed from the implementation process and reflective analysis. However, it has not yet been tested through longitudinal, comparative, or experimental research. Therefore, the relationships proposed in the model should not be interpreted as statistically validated causal relationships. These limitations indicate the need for a more systematic evaluation and broader implementation before the effectiveness and generalizability of the CBDLL Model can be firmly established.

4.3 Suggestions and Directions for Future Research

Future community service programs should incorporate systematic evaluation instruments, including pre- and post-test assessments, follow-up surveys, interviews, or behavioral observations, to measure changes in participants' digital legal literacy and preventive capacity. Such instruments would provide stronger empirical evidence regarding the educational outcomes of community-based digital legal literacy programs. The CBDLL Model should also be implemented in different rural and semi-urban communities to examine its adaptability across different social, demographic, and digital contexts. Comparative studies involving different communities could help identify the contextual factors that influence the effectiveness of digital legal literacy interventions.

Future research should further examine the relationship between the five dimensions of digital legal literacy and specific preventive outcomes, such as the ability to identify online fraud, verify information, protect personal data, recognize cybercrime risks, and practice responsible digital communication. Longitudinal research would also be valuable for determining whether knowledge and awareness developed through community-based education are maintained and translated into sustained preventive behaviors. Finally, future programs should encourage stronger collaboration among universities, village governments, community organizations, legal aid institutions, community leaders, youth organizations, women's groups, and relevant government or law enforcement agencies. Such collaboration may support the development of continuous digital legal literacy programs rather than isolated educational activities and contribute to stronger and more sustainable community resilience against cybercrime.

Acknowledgements

The authors would like to express their sincere gratitude to the Government of Ngadiluwih Village, Salam District, Magelang Regency for its support and cooperation in facilitating the implementation of this community service program. The authors also extend their appreciation to the community participants, village officials, community leaders, youth representatives, and women's community members who actively participated in digital legal literacy activities and discussions.

References

- Althibyani, H. A., & Al-Zahrani, A.M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. *Sustainability*, 15(15), 11512. <https://doi.org/10.3390/su151511512>
- Baderan, U. S., Lantowa, F. D., Makur, D. S., & Idji, A. (2025). Manajemen administrasi dan keuangan di Desa Bajo, Kecamatan Tilamuta, Kabupaten Boalemo. *Jurnal Pemberdayaan Ekonomi*, 4(2), 69-75. <https://doi.org/10.35912/jpe.v4i1.4828>
- Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, 18(3), 328–352. <https://doi.org/10.1080/14780887.2020.1769238>
- Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, 9(1), 3-26. <https://doi.org/10.1037/qup0000196>
- Cahyani, I., Raharjo, S., Saputro, N. D., Oktarina, K., & Hidayati, P. I. (2026). Strengthening digital legal literacy among social media users through international online community education. *Teumulong: Journal of Community Service*, 4(3), 204-216. <https://doi.org/10.62568/jocs.v4i3.817>
- Chayko, M. (2020). *Supperconnected: The internet, digital media, and techno-social life*.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches (4th ed.)*.
- Cross, C. (2020). *Crime, security and online safety in Australia: Concepts and issues*.
- Cross, C. (2022). Meeting the Challenges of Fraud in a Digital World.
- Dwijaya, P. A. ., Marlissa, E. R. ., & Hafizrianda, Y. (2026). Regional financial independence and audit opinion quality effects on capital expenditure in Papua: Studi Ekonomi Dan Kebijakan Publik, 4(2), 51–69. <https://doi.org/10.35912/sekp.v4i2.7113>
- Guess, A. M., Nagler, J., & Tucker, J. A. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1).
- Helsper, E. J. (2021). *The digital disconnect: The social causes and consequences of digital inequalities*.
- Ichsan, O. A. N., Santoso, B., Pranata, B., Nurmaseli, T., Yanuriati, A., & Hermanto, H. (2026). Strengthening community economic capacity in Sei Selincah through Gambier Jelly Candy Innovation. *Jurnal Nusantara Mengabdi*, 5(2), 15-24. <https://doi.org/10.35912/jnm.v5i2.6140>
- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1–2), 18–26. <https://doi.org/10.1007/s13162-020-00161-0>
- Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551-555. <https://doi.org/10.1089/cyber.2014.0008>
- Longinus, E. C. (2024). Emerging Technologies and Cyber-Crime: Strategies for Mitigating Cyber-Crime and Misinformation on Social Media and Cyber Systems. *International Journal of Business Ecosystem & Strategy*. Retrieved from <https://www.bussecon.com/ojs/index.php/ijbes>
- Lucy Huschle, M. K., and Hermann J. Abs. (2024). Personal responsibility and beyond: Developing a comprehensive conceptualization of digital citizenship competences. *Weizenbaum Journal of the Digital Society*, 4(4), 1-25. <https://doi.org/10.34669/wi.wjds/4.4.5>
- M. Claire Buchan , J. B. a. T. R. K. (2024). Navigating the digital world: Development of an evidence-based digital literacy program and assessment tool for youth. <https://doi.org/10.1186/s40561-024-00293-x>
- Martínez-Bravo, M. C., Sádaba Chalezquer, C., & Serrano-Puche, J. (2022). Dimensions of digital literacy in the 21st century competency frameworks. *Sustainability*, 14(3), 1867. <https://doi.org/10.3390/su14031867>
- Nath, M. A. I. M. a. R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, 190(1).
- Nguyen, M. H., Gruber, J., Fuchs, J., Marler, W., Hargittai, E., & Hargittai, E. (2021). Digital inequality in communication during a time of physical distancing. <https://doi.org/10.1016/j.socsci-med.2021.114293>

- Nurhayati, S., Musa, S., Boriboon, G., Nuraeni, R., & Putri, S. (2021). Community learning center efforts to improve information literacy in the community for cyber crime prevention during a pandemic. *Journal of Nonformal Education*, 7(1), 32-38. <https://doi.org/10.15294/jne.v7i1.26883>
- Olaitan, M. A., Oshioriamhe, I. O., Oyotomhe, J. B., & Sennuga, R. M. (2025). Community-based natural resource management as a catalyst for sustainable rural development: A critical review. *Scholastic Agriculture*, 1(3).
- Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.).
- Pritika Reddy, B. S., and Kaylash Chaudhary. (2020). Digital Literacy: A Review of Literature. *International Journal of Technoethics (IJT)*, 11(12), 30. <https://doi.org/10.4018/IJT.20200701.oa1>
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.).
- Sandefur, R. L. (2019). Access to what? *Daedalus*, 148 (1), 49-55. https://doi.org/10.1162/DAED_a_00534
- simakopoulos, G., Giotopoulos, K., & Halkiopoulos, C. (2025). Impact of information and communication technologies on democratic processes and citizen participation. *Societies*, 15(2), 40. <https://doi.org/10.3390/soc15020040>
- Syafiih, M., Khairi, M., Furqan, M., & Yusman, B. (2024). Pendampingan literasi digital untuk mengurangi risiko kejahatan siber membentuk masyarakat yang lebih aman. *Jurnal Ilmiah Pengabdian dan Inovasi*, 2(4), 1027-1036. <https://doi.org/10.57248/jilpi.v2i4.456>
- Taufik Mastiyar, Mulyapradana, A. ., Prayetno, P. H. ., & Hasim, M. (2026). Integrasi literasi digital dan karakter islami berbasis artificial intelligence. *Jurnal Pemberdayaan Umat*, 5(1), 9-20. <https://doi.org/10.35912/jpu.v5i1.5725>
- Tracy, S. J. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative Inquiry*, 16(10), 837-851. <https://doi.org/10.1177/1077800410383121>
- Trung, P. N. (2026). Community awareness of high-tech crime prevention in the digital transformation context in Ho Chi Minh City: A basis for community-based solutions and policy implications. *Journal of Community Service and Society Empowerment*, 4(2), 155-168. <https://doi.org/10.59653/jcsse.v4i02.2341>
- Tymoshenko, V. (2025). The role of the concept of “Legal Awareness” in the study of delinquent behaviour. *Law Journal of the National Academy of Internal Affairs*, 15(1), 18-26. <https://doi.org/10.63341/naia-chasopis/1>
- Van Deursen, A. J. A. M., & Van Dijk, J. A. G. M. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New Media & Society*, 21(2), 354-375. <https://doi.org/10.1177/1461444818797082>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151. <https://doi.org/10.1126/science.aap9559>
- Xu, W., & Zammit, K. (2020). Applying thematic analysis to education: A hybrid approach to interpreting data in practitioner research. *International Journal of Qualitative Methods*, 19, 1–9. <https://doi.org/10.1177/1609406920918810>
- Zainuddin, Z., Tohiroh, T., Putra, A. L., & Kultsum, U. (2025). Penguatan manajemen pangan berkelanjutan melalui branding dan teknologi digital nelayan Lere Palu. *Jurnal Nusantara Mengabdi*, 5(1), 11-20. <https://doi.org/10.35912/jnm.v5i1.5750>