Bulletin of Social Science and Community Development

ISSN: 3025-6798 | Journal's DOI: 10.61436/bsscd

Homepage: https://imrecsjournal.com/journals/index.php/bsscd

Institutional Perspectives on Youth Digital Vulnerability in Lampung, Indonesia: Problematic Information, Cyber Financial Fraud, and a Community-Based Resilience Model

Apria Mamudza Permana*, Fauzia Gustarina Cempaka Timur, Alif Asy'ari, & Oktaheroe Ramsi

Asymmetric Warfare Department, Republic of Indonesia Defense University, Indonesia

ARTICLE INFO

Article History:

Received: 25 August 2026

Accepted: 11 October 2026

Published: 14 November 2026

Keywords:

Youth digital vulnerability;
Problematic information;
Cyber financial fraud;
Community-based prevention;
Lampung

Corresponding Author:

apria.permana@sp.idu.ac.id

ABSTRACT

This study examines institutional perspectives on youth digital vulnerability in Lampung Province, Indonesia, focusing on problematic information, cyber financial fraud, and community-based prevention. Using a qualitative descriptive approach, data were collected through face-to-face, semi-structured interviews with purposively selected representatives from 13 organizational units across provincial and municipal government, police, territorial defense, social resilience, and digital-governance institutions. Documented interview records were analyzed thematically and contextualized using policy and connectivity documents, alongside provincial cyber-governance evaluations covering 2022–2025. The analysis generated four themes: youth vulnerability within an unequal digital environment; problematic information and cyber financial fraud as converging risks; a layered institutional response and its implementation constraints; and a proposed community-based youth digital resilience model. Institutional informants linked youth digital vulnerability to unequal connectivity, uneven information-verification capacity, and limited digital-safety awareness. Problematic information and cyber financial fraud were described as distinct but related risks that may exploit trust, emotion, urgency, and limited verification. Institutional accounts identified complementary functions in public communication, education, policing, territorial outreach, and referral. Provincial evaluations documented constraints in personnel, training, resources, and coordination. The asymmetric-warfare lens highlights how digital deception may exploit societal trust and everyday vulnerabilities. The findings support an integrated preventive approach combining critical literacy and digital safety with trusted community actors, community forums, educational spaces, youth networks, and government support. The proposed model requires direct testing with young people and community stakeholders before wider implementation.

To cite this article:

Permana, A. M., Timur, F. G. C., Asy'ari, A., & Ramsi, O. (2026). Institutional Perspectives on Youth Digital Vulnerability in Lampung, Indonesia: Problematic Information, Cyber Financial Fraud, and a Community-Based Resilience Model. *Bulletin of Social Studies and Community Development*, *5*(4), 632-651 doi: https://doi.org/10.61436/bsscd/v5i4.pp632-651

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

■ INTRODUCTION

Young people actively participate in digital environments for learning, social connection, self-expression, and civic engagement. Kligler-Vilenchik and Literat (2020) argue that digital participation expands access to information, supports learning opportunities, facilitates social networks, and contributes to identity development. In Lampung Province, this population is also demographically significant. In 2026, the province had approximately 738.9 thousand residents aged 15–19 and 724.5 thousand aged 20–24, amounting to about 1.463 million people aged 15–24, representing approximately 15.2% of the provincial population (BPS Provinsi Lampung, 2026). The size of this age group makes young people important to understanding both the opportunities and potential risks associated with digital participation in Lampung.

Digital participation may provide learning, social, and civic benefits, yet it can also expose young people to privacy risks, psychological pressure, harmful content, information manipulation, and unsafe online interactions (Kolotouchkina et al., 2023). These risks are not experienced uniformly. They depend on how young people participate, their critical skills, their access to credible information and social support, and the wider digital environment (Balakrishnan et al., 2025). In a survey of Indonesian youth, Luthfia et al. (2021) found that digital literacy was

associated with online opportunities, whereas more intensive online engagement may also increase exposure to online risks. Technical ability alone is therefore insufficient for safe participation. Writing on Indonesian youth and electoral disinformation, Jati (2024) argues that critical judgment and the capacity to interrogate information sources matter more than device fluency.

One area of concern is the circulation of false, misleading, or harmful information through networked digital environments. Wardle and Derakhshan (2017) distinguish misinformation, disinformation, and malinformation by the information's falsity and the intent to cause harm. Emotionally charged messages, persuasive visual material, and circulation through trusted social networks may facilitate the acceptance and recirculation of misleading content (van der Meer & Hameleers, 2024). Analyzing a decade of verified stories on social media, Vosoughi et al. (2018) found that false information diffused faster and more broadly than true information, largely because of human sharing decisions rather than automated accounts. Experimental evidence also suggests that false information presented in video form can, in some circumstances, be processed more superficially and perceived as more credible than equivalent audio or text messages (Sundar et al., 2021). Information-related threats may also overlap with cyber financial fraud, including phishing, fraudulent investment offers, illegal online lending, and relational fraud. Although these phenomena are analytically distinct, both may involve social engineering tactics that exploit trust, emotion, perceived urgency, and limited verification capacity.

These risks also carry a security dimension. Arreguín-Toft (2001) describes asymmetric conflict as a contest in which a weaker actor avoids a stronger opponent's strengths and targets its vulnerabilities instead. Digital deception follows a similar logic. Disinformation and fraud networks need few resources and seldom confront state institutions directly. Many fraud operations in the region are run by transnational syndicates that combine scam compounds, illegal online gambling platforms, and underground banking (United Nations Office on Drugs and Crime, 2024). What they exploit are gaps in public trust, verification habits, and financial capability. Wither (2016) observes that hybrid threats blur the boundary between war and peace and rely heavily on non-military instruments, including information operations. Rid (2012) makes a related point about cyberspace: most hostile activity there takes the form of sabotage, espionage, or subversion rather than war. Subversion, which seeks to erode trust in established authority, is the form closest to disinformation. Maschmeyer (2021) develops this point: subversion appeals because it is cheap and deniable, yet its effects arrive slowly and are hard to steer once set in motion, so this kind of activity accumulates as persistent pressure rather than a decisive blow. Indonesian law reflects this broader view. Law No. 23 of 2019 on the Management of National Resources for National Defense frames national defense as a total system that draws on national resources. Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management likewise provides a national framework for protecting national interests from cyber threats, including their social and economic consequences. This study does not treat every hoax or scam as an act of war. It uses the asymmetric lens to show how low-cost digital threats target society rather than military capacity, and why community-level resilience becomes part of national defense.

Digital vulnerability cannot be understood solely as a lack of access or basic technical skill. Heeks (2022) argues that digital inequality may persist even where individuals are incorporated into digital systems, because such incorporation can involve unequal exposure to exploitation, dependency, and risk. Digital resilience therefore offers a useful lens for understanding how individuals and groups recognize, manage, and recover from adverse online experiences. Sharma et al. (2021) describe digital resilience as involving learning, recovery, and adaptation following adverse online experiences, while Hammond et al. (2024) emphasize its dynamic nature across individual, home, community, and societal contexts. These perspectives highlight capacities such as information verification, privacy protection, safe online practice, reporting, and social support (Putra et al., 2024). In this study, digital resilience serves as an interpretive framework rather than a measured outcome. The study therefore analyses youth digital vulnerability as institutions perceive it, and uses digital resilience to frame the preventive model it proposes.

The study also draws on community resilience, which focuses on collective capacities for responding to shared adversity. F. H. Norris et al. (2008) identify social capital, information and communication, community competence, and economic development as four interconnected capacities of community resilience; the last of these directs attention to

resource equity and livelihood conditions that shape exposure to economic exploitation. In the context of digital risks, this perspective highlights the potential relevance of trusted communication, local social support, community learning, and collective problem-solving. Aldrich and Meyer (2015) similarly argue that bonding and bridging social ties operate as practical infrastructures of warning, mutual assistance, and recovery. Together, these arguments provide a basis for examining how educational institutions, community forums, trusted local actors, youth networks, and government institutions may contribute to a broader environment of support for safer digital participation.

Lampung provides a relevant structural and policy context for this study. The province recorded a composite score of 50.36 on the 2025 Indonesian Digital Society Index (Indeks Masyarakat Digital Indonesia, IMDI) (Kemkomdigi RI, 2025), while provincial connectivity mapping conducted in August 2025 identified 659 blank-spot locations (Diskominfotik Provinsi Lampung, 2025d). The Lampung Provincial Medium-Term Development Plan (Rencana Pembangunan Jangka Menengah Daerah, RPJMD) for 2025–2029 identifies digital transformation, broadband expansion, youth capacity development, and information security as regional priorities (Bappeda Provinsi Lampung, 2025). Together, these conditions provide an appropriate setting for examining institutional perspectives on youth digital vulnerability and community-based prevention.

Previous studies have examined youth digital literacy, online opportunities and risks, misinformation, cyber financial fraud, information security, and digital governance. However, these issues are frequently examined separately. Less attention has been given to how institutional actors at the provincial and municipal levels understand the intersection of youth vulnerability, digital inequality, information-related threats, cyber financial fraud, and community-based prevention in Indonesia. In particular, few studies bring together perspectives from digital governance, social resilience, public security, territorial defense, and municipal government institutions.

This study examines institutional stakeholder perspectives on youth digital vulnerability in Lampung Province, Indonesia, with particular attention to problematic information and cyber financial fraud, and develops a proposed community-based youth digital resilience model. The study addresses three research questions: (1) How do institutional informants perceive youth digital vulnerability in Lampung Province in relation to problematic information and cyber financial fraud? (2) What preventive and responsive functions do institutional informants describe, and what constraints do they identify in implementing them? (3) How can local values, community forums, and youth networks be integrated into a proposed community-based youth digital resilience model from institutional perspectives?.

■ METHOD

Informants/Research Subjects

Institutional representatives were selected through purposive sampling. The interviews covered 13 organizational units across six institutional categories, with each unit interviewed in a separate session. Informants were selected because their structural or functional responsibilities related to digital governance, public communication, social resilience, public security, territorial defense, local government coordination, and preventing or mitigating digital threats. Purposive sampling was used to obtain information-rich institutional perspectives rather than statistical representation of a wider population, consistent with Patton's (2015) argument that qualitative sampling logic rests on each case's informational yield.

The informants represented six institutional categories: provincial government, provincial police, regional military command, Bandar Lampung city government, military resort command, and Metro city government. These categories encompassed institutional responsibilities related to social resilience, digital governance, public security, intelligence, territorial communication, local coordination, and community protection. To protect confidentiality, Table 1 reports the aggregated institutional coverage and interview sessions rather than individual profiles. Names, precise job titles, internal units, service numbers, contact details, and other direct or indirect identifiers were excluded from the analysis and reporting. All participants were adult professionals.

Table 1 summarises the organizational units represented, the number of separate interview sessions, and their broad functional coverage. These figures describe data-collection coverage, not the number of individual participants or evidence of data saturation. Interview durations were not systematically recorded during fieldwork, and reliable session-level durations could not be established. Duration figures are therefore not reported.

Table 1. Institutional coverage and interview sessions

Institutional Category	Number of Organizational Units Represented	Number of Interview Sessions	Broad Functional Category
Provincial government	2	2	Social resilience and digital governance
Provincial police	2	2	Security, intelligence, and community protection
Regional military command	3	3	Operational, territorial, and intelligence functions
Bandar Lampung city government	1	1	Municipal digital governance
Military resort command	3	3	Territorial, operational, and intelligence functions
Metro city government	2	2	Municipal digital governance and social resilience
Total	13	13	

Source: Authors' fieldwork data, 18–20 May 2026.
Note: Organizational units refer to the agencies or functional units represented in the interviews, not the number of individual participants. Each unit was interviewed in one separate session; unit and session counts therefore coincide.

Research Design and Approach

This study employed a qualitative descriptive design to examine institutional perspectives on youth digital vulnerability and community-based prevention in Lampung Province. Qualitative description was selected because the study sought to provide a contextual account that remained close to institutional informants' expressed assessments, institutional experiences, and prevention approaches, rather than testing causal relationships or generating a formal theory (Sandelowski, 2000).

The study examined institutional perspectives on youth digital vulnerability in relation to problematic information and cyber financial fraud, as well as the potential integration of local values, community forums, and youth networks into a proposed community-based youth digital resilience model. The study did not directly investigate young people's lived experiences, online behaviors, victimization, levels of digital literacy, or digital resilience.

Fieldwork was conducted in Lampung Province from 18 to 20 May 2026. Provincial-level interviews were conducted on 18 and 19 May 2026, while interviews with Metro City institutions were conducted on 20 May 2026. The study included provincial institutions and municipal governments in Bandar Lampung and Metro to obtain perspectives from public security, territorial defense, social resilience, digital governance, and local government actors. Reporting follows the Standards for Reporting Qualitative Research (O'Brien et al., 2014), developed in the health sciences but applied here as a generic reporting checklist covering design, participant selection, data collection, analysis, and interpretive boundaries.

Data Collection

Primary data were collected through face-to-face semi-structured interviews with institutional representatives, held at their offices or other institutional locations, with each organizational unit interviewed in a separate session. Following Kallio et al. (2016), the interview guide was developed from the research questions and relevant literature, and the semi-structured format ensured coverage of comparable topics while allowing follow-up questions based on each participant's institutional mandate and professional role. The interview guide addressed perceived digital threats to social stability; youth and community vulnerability; disinformation and cyber financial fraud; information verification practices; institutional responses; interagency coordination; local values; community forums; youth networks; and implementation constraints.

Interview information was recorded in structured interview records and consolidated in post-fieldwork summaries. Full audio recordings and verbatim transcripts were not produced. The analysis therefore relied on documented substantive accounts rather than full conversational transcripts. Findings are presented through thematic synthesis and role-based attribution to institutional categories.

Any illustrative statements are paraphrased from documented interview records and are not presented as verbatim quotations. Original records were kept in Indonesian; the paraphrased accounts reported here were translated by the authors. Unless a published or official documentary source is cited, the institutional accounts discussed in the following sections come from these records, compiled during fieldwork conducted from 18 to 20 May 2026.

Because full verbatim transcripts were not available, this study reports a thematic synthesis of documented substantive accounts rather than a discourse, narrative, or conversation-analytic account. The authors did not reconstruct participants' wording retrospectively, and no paraphrased material is presented as direct quotation. Audio recording was not used, given the institutionally sensitive character of several interview settings and the practical conditions of fieldwork. Before finalizing thematic attribution and English translation, the authors reviewed the institutional accounts against the available structured interview records. The links between documented accounts, initial codes, subthemes, and themes were recorded as the analysis proceeded. This procedure was intended to preserve the substantive meaning of the accounts while avoiding unverifiable quotation.

The interview analysis was contextualized with relevant official and public documents. These comprised the 2025 IMDI report, the provincial RPJMD for 2025–2029, the August 2025 provincial connectivity mapping, and four evaluations of the provincial cyber incident response team covering 2022, 2023, 2024, and 2025, together with internal reports of two provincial financial-crime coordination meetings convened by the Financial Services Authority (Otoritas Jasa Keuangan, OJK) in February 2025. Documentary materials provided structural and policy context and were used to examine the consistency of selected institutional accounts. They did not replace the interview evidence and were not treated as direct evidence of young people's experiences or behaviors.

Data Analysis and Trustworthiness

The structured interview records were analyzed using thematic analysis, combining deductive and inductive coding. Deductive coding followed the research questions and the study's conceptual focus on youth digital vulnerability, problematic information, cyber financial fraud, and community-based prevention. Inductive coding allowed additional patterns to emerge from participants' documented accounts, including concerns related to uneven outreach, local legitimacy, reporting practices, resource constraints, operational continuity, and cross-sector coordination. Analysis was conducted primarily at the semantic level, focusing on the explicit meanings conveyed in the interview records.

The analysis followed the six phases of thematic analysis proposed by Braun and Clarke (2006): familiarisation with the interview records, generating initial codes, developing candidate themes, reviewing themes, defining and naming themes, and analytical writing. The coding process resulted in four interrelated themes that structured the subsequent analysis. Coding was carried out manually rather than with qualitative data analysis software. The documented capability indicators were then read alongside institutional accounts of prevention needs, producing a qualitative assessment of capability constraints and their implications for complementary prevention.

Trustworthiness was addressed through the criteria of credibility, dependability, confirmability, and transferability set out by Lincoln and Guba (1985), operationalized for thematic analysis as recommended by Nowell et al. (2017). Credibility was supported by triangulation. Accounts from provincial and municipal government, police, territorial defense, social resilience, and digital governance informants were compared to identify convergent assessments, differences in institutional emphasis, and perceived implementation constraints. Official documents on digital development, connectivity, policy priorities, and cybersecurity governance were then used to contextualize and examine the consistency of selected institutional accounts. They were not treated as substitutes for interview evidence. Dependability and confirmability were supported by an audit trail of coding decisions, thematic development, and interpretive links between interview data, contextual documents, and the proposed model. Transferability was supported by the contextual description of the research setting provided in this article. The analysis prioritized substantive accounts that recurred across the interview records and across institutional categories.

Member checking with participants after the interviews was not undertaken because the original fieldwork design relied on a single period of institutionally authorized access and did not include a post-interview participant-validation stage. Credibility therefore rests on the authors' review of the reported institutional accounts against the available structured interview records, comparison of accounts

across the six institutional categories, and triangulation with official documents. These measures do not substitute for participant validation or verbatim transcripts; rather, they were used to strengthen the accuracy and traceability of the thematic synthesis within the limits of the available material. The absence of participant verification is acknowledged as a limitation of the study.

Fieldwork was conducted under administrative authorization provided through a Letter of Assignment issued by the Rector of the Republic of Indonesia Defense University (No. SPRIN/2020/V/2026). Formal review by a research ethics committee was not obtained. The study relied on this institutional authorization together with the informed-consent procedure described below. It involved adult professional participants speaking to their institutional mandates and did not involve minors, interventions, experimental procedures, clinical data, or the collection of sensitive personal data. Before each interview, institutional informants were informed of the study purpose, the intended use of the information, the voluntary nature of participation, and confidentiality procedures, and provided informed consent before the interviews were conducted. Names, contact details, internal units, and operationally sensitive information were excluded from the materials used for analysis and reporting.

■ RESULT AND DISCUSSION

The thematic analysis generated four interrelated themes: youth vulnerability within an unequal digital environment; problematic information and cyber financial fraud as converging risks; a layered institutional response and its implementation constraints; and a proposed community-based youth digital resilience model. The findings present institutional perspectives gathered from representatives of 13 organizational units across provincial government, provincial police, regional military, and municipal institutions, situated through contextual documents on policy, connectivity, digital development, and cybersecurity governance. Unless otherwise indicated by a citation to a published or official documentary source, the institutional accounts discussed below are paraphrased from structured interview records and attributed by institutional category to protect confidentiality. Table 2. summarises the codes, subthemes, and themes, together with their institutional sources and contextual documents

Table 2. Summary of coding and thematic structure

Initial Codes	Institutional Sources Represented in the Subtheme	Documents Used for Contextual Interpretation	Subtheme	Main Theme
High platform exposure, harmful content, cyberbullying, risky online challenges, and uneven risk awareness	Provincial government, provincial police, regional military command, Metro city government	IMDI 2025	Youth exposure and uneven protective capacity	Youth vulnerability within an unequal digital environment
Connectivity inequality, blank-spot locations, access without verification capacity, and unequal preventive outreach	Provincial police, regional military command, Bandar Lampung city government; military resort command; Metro city government	Provincial connectivity mapping; RPJMD 2025–2029; IMDI 2025	Structural and geographic inequality	Youth vulnerability within an unequal digital environment
Hoaxes, provocative narratives, hate-related content, identity-related issues, manipulation of public opinion, and unverified information	Provincial government, provincial police, regional military command, military resort command, Metro city government	IMDI 2025 (information-verification indicators)	Problematic information	Problematic information and cyber financial fraud as converging risks

Phishing, illegal online lending, fraudulent investment offers, love scamming, impersonation, and misuse of digital identities; online gambling as a related financial harm	Provincial government, provincial police, regional military command, Bandar Lampung city government, military resort command, Metro city government	IMDI 2025 (phishing indicators); Satgas PASTI and TPAKD meeting reports	Cyber financial fraud and related financial harms	Problematic information and cyber financial fraud as converging risks
Monitoring, detection, verification, clarification, counter-narratives, public education, reporting channels, and interagency coordination	Provincial government, provincial police, regional military command, Bandar Lampung city government, military resort command, Metro city government	CSIRT/TTIS evaluations 2022–2025	Formal institutional response	A layered institutional response and its implementation constraints
Reactive responses, uneven outreach, limited personnel, resource constraints, operational continuity, coordination gaps, and legal-authority limitations	Provincial government, provincial police, regional military command, Bandar Lampung city government, Metro city government	CSIRT/TTIS evaluations 2022–2025	Implementation constraints	A layered institutional response and its implementation constraints
Local values, customary and religious figures, FKDM (community early warning forum), community organizations, community policing, territorial communication, and early referral	Provincial government, provincial police, regional military command, Bandar Lampung city government, military resort command, Metro city government	Interview records only	Trusted community actors and local legitimacy	Proposed community-based youth digital resilience model
Schools, universities, youth groups, creative content, facilitated learning, community education, digital safety, and reporting referral	Provincial government, provincial police, regional military command, Bandar Lampung city government, military resort command, Metro city government	RPJMD 2025–2029	Educational spaces and youth networks	Proposed community-based youth digital resilience model

Source: Authors' thematic synthesis of structured institutional interview records and contextual documents (2026). Note: Institutional sources are identified at the subtheme level and do not imply that every participant or organizational unit addressed every code.

Whereas Table 2 traces the codes and themes, Figure 1 maps the institutional functions and community-facing relationships described in the interview records. It is read in three layers: young people at the base, the community-facing actors and channels enclosed by the dashed boundary, and above them the institutions that hold formal mandates, linked across the top by interagency coordination. Movement runs in both directions, with preventive education and official clarification traveling downward while reporting, referral, and local information travel upward. Hence, the map describes circulation rather than a chain of command. Community-facing actors and channels are represented

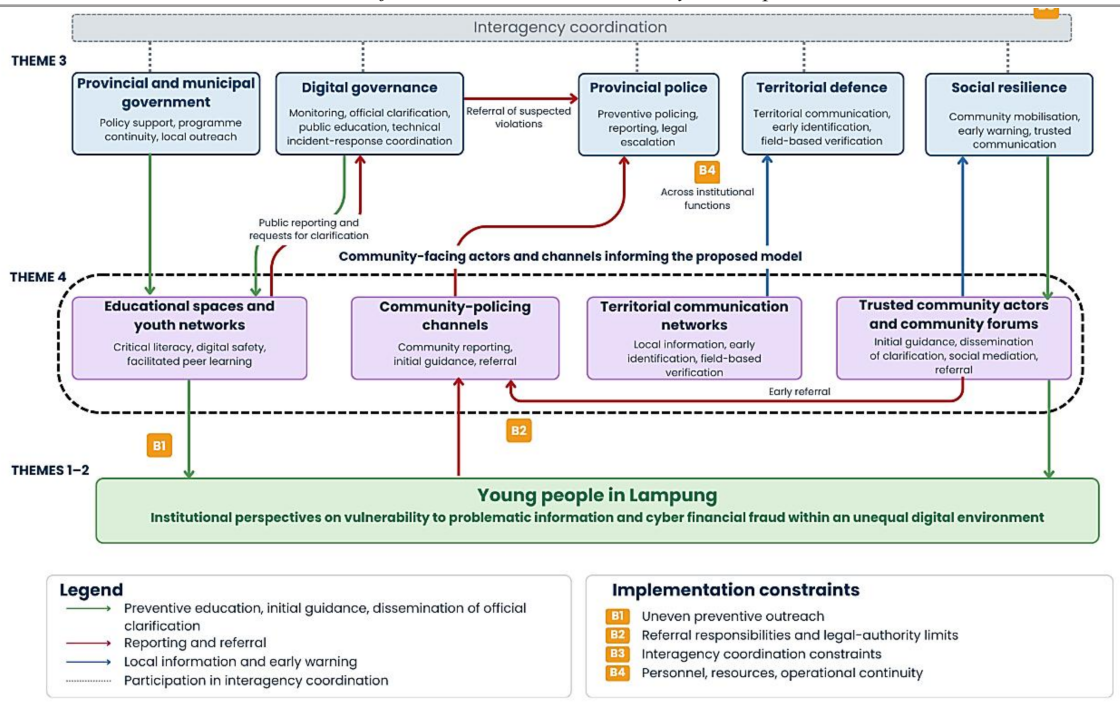


Figure 1. Thematic network map of institutional and community roles in youth digital vulnerability and prevention. Source: Authors' thematic synthesis of documented institutional interview records and contextual documents (2026)

through institutional accounts rather than direct data collection wi those actors. Implementation constraints are marked at the points in the network where informants located them.

Youth Vulnerability within an Unequal Digital Environment

Provincial government and municipal informants identified adolescents, students, and young social-media users as groups requiring preventive attention. They associated this concern with limited awareness of online risks, uneven information-verification practices, exposure to harmful content, cyberbullying, and potentially harmful online challenges. A municipal digital-governance informant emphasized that familiarity with devices should not be equated with readiness to assess complex and rapidly circulating information. Provincial police and territorial informants similarly described limited capacity to verify sources, interpret context, and recognize problematic information as factors that may intensify vulnerability, particularly where access to education and preventive outreach is uneven.

These institutional readings correspond closely to survey evidence on Indonesian youth. Luthfia et al. (2021) found that digital literacy was positively associated with online opportunities, while more intensive digital activity could also increase exposure to risks such as misinformation, harmful content, and unsafe online interactions. High levels of platform exposure and use, therefore, do not automatically translate into stronger digital resilience. Afrina et al. (2024) reach a comparable conclusion from an analysis of Indonesian online media content, identifying infrastructure limitations, insufficient emphasis on critical thinking in education, and limited awareness of ethical social-media use as factors associated with low digital literacy. The gap between device fluency and critical judgment described by informants is also discussed in studies from other Indonesian settings.

Contextual documents provide structural context for these institutional perspectives. The provincial IMDI profile for 2025 varies across its four pillars: Infrastructure and Ecosystem (57.42), Digital Literacy (53.29), Empowerment (47.02), and Employment (41.90) (Kemkomdigi RI, 2025). Provincial planning documents identify equitable network expansion as a continuing development challenge (Bappeda Provinsi Lampung, 2025), while the August 2025 connectivity mapping recorded 54 health facilities with unreliable connections and two without service (Diskominfotik Provinsi Lampung, 2025d). These conditions do not demonstrate that rural youth are automatically more vulnerable than

urban youth. Rather, they indicate uneven conditions that may shape access to reliable information, digital learning opportunities, prevention programs, and relevant protection services. The IMDI and the connectivity mapping measure neither youth digital vulnerability nor exposure to online harm, and are used here only as contextual indicators of an unevenly distributed digital environment.

The pattern matters theoretically because it is not simply a matter of exclusion. Heeks (2022) argues that inclusion in digital systems can itself produce inequality when people are incorporated without protective capacity. He calls this adverse digital incorporation. The combination informants described, high participation alongside weak verification and safety practices, fits this description better than the idea of disconnection. It also explains why prevention cannot rest on individual skill alone. Hammond et al. (2024) treat digital resilience as a socio-ecological process spread across the individual, the home, the community, and wider institutions, which points ahead to the layered response examined in the third theme. In asymmetric terms, this is the terrain where low-cost threats operate most easily: they do not need to exclude anyone, only reach connected but unprotected users.

Problematic Information and Cyber Financial Fraud as Converging Risks

Institutional informants across all six categories described problematic information and cyber financial fraud as analytically distinct but related elements of the regional digital-risk environment. Problematic information included hoaxes, provocative narratives, hate-related content, identity-related issues, manipulation of public opinion, and unverified material. Cyber financial fraud included phishing, illegal online lending, fraudulent investment offers, love scamming, impersonation, misuse of digital identities, and other deceptive practices. Online gambling was also raised by several institutional informants as a related digital financial and social concern. However, it is not treated in this study as synonymous with cyber financial fraud. These institutional perspectives suggest that the two categories may converge when deceptive content circulates through digital platforms and exploits trust, emotion, perceived urgency, and limited verification practices. Regional evidence points the same way. Studying scam-related fraud in Vietnam and the compounds across the border that service it, Luong and Ngo (2024) trace how fabricated job offers circulated on social media open operations that end in investment schemes, online gambling, and the conscription of victims as operators. Deceptive content is not adjacent to financial fraud; it is a pathway into it.

Following Wardle and Derakhshan (2017), the information disorder framework distinguishes misinformation, disinformation, and malinformation according to the falsity of information and the intention to cause harm. The documented interview records do not establish the intent of every content creator or distributor. This study therefore uses the term problematic information to refer to false, misleading, provocative, or unverified material identified by institutional informants. Provincial police, regional military, military-resort, and municipal perspectives associated problematic information with potential community anxiety, identity-related sensitivities, and possible disruption of social relations, whereas provincial government and municipal digital-governance perspectives emphasized source verification, public clarification, digital literacy, and accessible communication channels.

Institutional informants also described a perceived shift in which digital issues could move beyond online discussion and become relevant to public order, social stability, or community relations. Provincial police and territorial perspectives particularly emphasized the potential importance of early identification, local communication networks, and field verification when online narratives concerned sensitive local conditions, infrastructure, public institutions, or identity-related issues. This escalation path makes the threat's asymmetric character visible. Cheap online content turns into offline pressure on public order, a pattern that Wither (2016) associates with hybrid activity below the threshold of armed conflict. Comparative research also suggests that this kind of susceptibility is patterned rather than accidental. Humprecht et al. (2020) show that resilience to online disinformation varies with structural conditions such as media trust, polarisation, and the strength of public information institutions. The local verification capacity described by informants is therefore better understood as a structural resource than as an individual attribute.

National survey data indicate how uneven verification capacity is. The 2025 IMDI report indicates that 30.3% of respondents were unable to independently check information sources and credibility, while 16.5% could do so only with assistance; by contrast, 40.9% reported being able to perform this task independently, and 12.3% reported being able to check sources, assist others, and solve related problems (Kemkomdigi RI, 2025).

These figures do not measure the verification capacity of young people or residents of Lampung specifically. The same survey reports a comparable gap in security awareness: 36.3% of respondents did not recognize the signs of phishing at all, and only 11.2% could identify, address, and prevent it (Kemkomdigi RI, 2025). Taken together, these distributions indicate gaps in information verification and phishing recognition at the national level. This provides context for the shared verification needs described in the institutional accounts, but does not establish that the two weaknesses occur among the same respondents.

Format compounds the problem. Experimental research from India found that false news presented in video form was more likely to be processed superficially, perceived as realistic, believed, and shared than equivalent audio or text formats (Sundar et al., 2021), and the diffusion advantage of false content over true content documented by Vosoughi et al. (2018) was driven primarily by ordinary users rather than automated accounts. This evidence does not establish identical responses among people in Lampung. It nevertheless supports preventive literacy that addresses visual cues, perceived realism, emotional appeal, and the need to pause before sharing. In a study of rural Indonesian communities, Reindrawati et al. (2023) likewise found that technical social-media use did not correspond with critical media literacy or routine verification practices.

Turning to the financial side of this convergence, cyber financial fraud was described across institutional perspectives as involving deceptive messages, suspicious links, false identities, promises of financial gain, fabricated urgency, and other forms of digitally mediated persuasion. Some regional military perspectives also identified manipulated images, false profiles, and artificial-intelligence-enabled impersonation as emerging concerns. These mechanisms are consistent with research on social engineering and internet fraud. In a systematic review, G. Norris et al. (2019) identify trust, social influence, perceived rewards, and scarcity or urgency as factors that can increase susceptibility to fraudulent communications. Studying Malaysian adults, Balakrishnan et al. (2025) found that overconfidence and social influence significantly predicted online fraud victimization. Neither study establishes predictors of fraud victimization among young people in Lampung. However, both support the analytical relevance of trust, urgency, social influence, and critical verification in understanding cyber financial fraud.

These are not only analytical categories in the provincial setting. In February 2025, the provincial Task Force for the Eradication of Illegal Financial Activities (Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal, Satgas PASTI) met to coordinate its annual program. Its membership includes the regional police, the military resort command, the prosecutor's office, and the provincial digital-governance agency. The task force listed the fraud types it handles through the Indonesia Anti Scam Center (IASC), including illegal investment, illegal online lending, impersonation calls, job-offer fraud, social-media fraud, phishing, love scams, and malicious application files distributed through messaging services (Diskominfotik Provinsi Lampung, 2025c). This official typology overlaps closely with the practices informants described, which indicates that the convergence reported in this theme is already recognized in provincial coordination practice.

Table 3 places the two risk categories side by side on the dimensions that recur in the institutional accounts and the literature reviewed above. It makes explicit where they differ and where the shared vulnerability mechanism lies.

Table 3. Institutional perspectives on the convergence of problematic information and cyber financial fraud

Analytical Dimension	Problematic Information	Cyber Financial Fraud	Shared Vulnerability Mechanism
Illustrative forms	Hoaxes, misleading narratives, provocative content, identity-related issues, and unverified information	Phishing, illegal online lending, fraudulent investment offers, love scamming, impersonation, and misuse of digital identities	Exposure to persuasive, deceptive, or unverified digital content
Primary concern	Distrust, polarisation, reputational harm, and potential social tension	Financial loss, debt-related pressure, economic exploitation, and privacy	Manipulation of emotion, trust, perceived urgency, and limited verification

		or identity compromise	capacity
Common circulation or delivery channels	Social media platforms and messaging applications	Messaging applications, SMS, social-media advertisements, suspicious links, fraudulent websites, and impersonation profiles	Rapid circulation through peer, family, and community networks
Protective capacities needed	Source evaluation, fact-checking, contextual interpretation, and responsible sharing	Fraud recognition, privacy protection, secure account practices, financial caution, and reporting	Critical literacy, digital-safety awareness, and access to trusted information and support

Source: Authors' thematic analysis of documented interview records and contextual documents, informed by Wardle and Derakhshan (2017) and G. Norris et al. (2019). Note: Online gambling, raised by several informants, is treated as a related financial harm rather than as cyber financial fraud and is therefore not listed.

These findings do not establish the prevalence of cyber financial fraud, nor do they present young people as its sole targets. Young people may encounter deceptive content as users, recipients, interpreters, or potential re-sharers within peer and family networks. Herrero-Diz et al. (2020) found that adolescents who forwarded false content on WhatsApp usually did so to inform the people around them, and were markedly less skeptical when the material came from someone they trusted. Sharing of this kind looks less like carelessness than a misdirected social act. Preventive support should therefore connect source evaluation, fraud awareness, privacy protection, digital-safety practices, and accessible reporting or referral pathways.

A Layered Institutional Response and Its Implementation Constraints

Institutional informants described a multi-layered response to digital risks rather than a single provincial-government mechanism. Across the institutional perspectives, preventive and responsive functions were distributed among digital-governance institutions, social-resilience institutions, police, territorial institutions, municipal governments, and community-facing educational spaces. These functions overlapped in some areas, particularly public education, early identification, clarification, reporting, and coordination, but each institutional category emphasized different mandates and operational capacities.

Provincial digital-governance institutions were associated with monitoring digital issues, verified clarification, public communication, digital-literacy education, reporting channels, and coordination of technical cybersecurity arrangements, and informants there described a working sequence of detection, verification, action, and public education. Provincial social-resilience institutions emphasized community mobilization, early recognition of social dynamics, the involvement of the Community Early Warning Forum (Forum Kewaspadaan Dini Masyarakat, FKDM) and other community organizations, and communication through socially trusted actors. Provincial police informants described preventive policing, community-based reporting, cyber monitoring, clarification, and legal escalation when suspected violations met the relevant threshold. Regional military and military-resort informants emphasized territorial communication, local networks, early identification of emerging concerns, and field-based verification through community-facing structures. Municipal government informants highlighted local outreach, public education, service-related reporting channels, and the use of community and educational forums to reach different population groups. These are reported institutional arrangements and perceived functions; the study did not evaluate whether the mechanisms described operate effectively in practice.

The institutional perspectives also showed points of functional intersection. Informants across categories described monitoring or early identification as requiring both digital observation and local information. Formal clarification was associated primarily with authorized government communication channels, while community-facing actors were described as supporting initial guidance, dissemination of clarification, social mediation, and referral. Reporting functions were viewed as connecting citizens and communities with formal agencies, whereas legal investigation, technical incident response, and formal content-removal requests remained within the mandates of authorized institutions. This distribution of roles indicates that community-based prevention was perceived as complementary to, rather than a substitute for, institutional authority. It also aligns with what F. H. Norris et al. (2008) describe as community competence: a collective capacity

for problem-solving exercised through linked organizations rather than concentrated in a single agency.

The formal digital-governance infrastructure provides important context for these institutional accounts. The provincial cyber incident response team, LampungProv-CSIRT, was established on 11 April 2022 through Governor Decree No. G/270/V.14/HK/2022 and documented as providing cybersecurity warnings, incident-handling coordination, containment and recovery support, security assessment, and cybersecurity education (Diskominfotik Provinsi Lampung, 2022). Its mandate was subsequently updated through Governor Decree No. G/798/V.14/HK/2025, and the 2024 evaluation reframed its work in line with the national reclassification of cyber incident response teams (Tim Tanggap Insiden Siber, TTIS), categorizing its services as reactive incident response, proactive security measures, and security-quality management (Diskominfotik Provinsi Lampung, 2024).

Within the national framework introduced earlier, Regulation No. 5 of 2025 of the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) sets out a roadmap for protecting vital information infrastructure in the public administration sector during 2025–2029. Its scope provides context for provincial technical governance, not a benchmark for the effectiveness of community-based prevention.

Institutional informants identified constraints that correspond to this picture. These included uneven preventive outreach across geographically diverse areas, limited specialized personnel, resource and operational-budget constraints, dependence on short-term or activity-based programs, fragmented or case-responsive coordination, and the difficulty of responding at the speed of digital circulation. Provincial and municipal government informants emphasized resource, staffing, program-continuity, and service-outreach limitations. In contrast, police and territorial informants highlighted geographic reach, the need for local communication networks, and the challenge of combining early identification with timely field verification.

Table 4 relates these reported prevention needs to the constraints documented in provincial evaluations and planning materials.

Table 4. Documented capability constraints and implications for prevention

Capability Domain	Documented Evidence	Identified Constraint	Implication For Complementary Prevention
Incident handling and recovery	TMPI was reported as 1.4 in the 2022 and 2025 evaluations. Separately, the 2025 cybersecurity assessment recorded a response and recovery domain score of 1.74. The team also reported an inability to handle ransomware incidents (Diskominfotik Provinsi Lampung, 2022, 2025a).	Reported limitations in specialized incident handling and recovery.	Early recognition and referral may help concerns reach authorized response teams; containment and recovery still require specialized technical capacity.
Personnel and capacity development	The 2025 evaluation recorded no internal or external capacity-building activities, limited technical personnel, and dependence on particular staff members (Diskominfotik Provinsi Lampung, 2025a).	Limited staffing and discontinuous capacity development.	Preventive education delivered through local institutions requires supported facilitators, reliable materials, and access to authoritative guidance.
Resources and geographic outreach	The 2025 evaluation reported an annual cybersecurity budget of IDR 10–100 million. Institutional accounts described operational-resource and outreach constraints, while planning and connectivity documents identified uneven infrastructure and local capacity (Bappeda Provinsi Lampung, 2025; Diskominfotik Provinsi Lampung, 2025a, 2025d).	Resource constraints and uneven conditions for preventive outreach.	Locally accessible education and reporting guidance may extend outreach, but require resources and continuity rather than reliance on unpaid or temporary participation alone.
Coordination and referral	The 2025 evaluation recorded no cooperation with other response teams or cybersecurity communities and no	Limited documented inter-team	Clear contact points, referral responsibilities, and feedback arrangements are needed

	incidents escalated to sector or national response teams. Provincial planning documents reported response teams in six of fifteen districts and cities (Bappeda Provinsi Lampung, 2025; Diskominfotik Provinsi Lampung, 2025a).	cooperation and uneven local response-team coverage.	between community-facing actors, municipal institutions, police, and CSIRT/TTIS.

Source: Authors' synthesis of provincial evaluation and planning documents, connectivity mapping, and documented institutional interview accounts (2026). Note: TMPI and the response and recovery domain score belong to different assessments and are not treated as interchangeable measures. The table presents an indicator-informed qualitative assessment, not a quantified comparison of technical and community prevention capacity.

The TMPI values of 1.4 were reported in 2022 and 2025, while the intervening evaluations did not supply comparable updated scores (Diskominfotik Provinsi Lampung, 2023, 2024). These observations do not establish an unchanged trend throughout the period. Similarly, the absence of recorded cooperation or escalation identifies a limit in documented coordination activity; it does not establish that referral procedures were unavailable or ineffective. Read alongside the response-team coverage reported in provincial planning documents, these findings suggest a need to strengthen technical coordination across administrative levels. They do not indicate an absence of institutional commitment.

The practical gap lies between the prevention tasks described by institutional representatives and the resources available to sustain them. Public education, local reporting guidance, and timely clarification require staff time, accessible communication channels, and continuing support. Staffing limits and reliance on short-term programs may disrupt preventive work. Uneven geographic outreach also makes local communication channels relevant, suggesting that prevention should not be organized solely around a provincial technical team. The budget range alone does not establish underfunding, since the records do not provide a comparable estimate of expenditure needs.

Community-facing institutions may help expand prevention reach, but they cannot remedy shortages in specialized incident response. Police-linked community channels can assist with reporting and referral; municipal and territorial networks may help circulate guidance and identify concerns requiring follow-up. In the institutional accounts, territorial organizations contributed local knowledge, community communication, and field verification rather than assuming responsibility for the overall response. These are potential contributions inferred from institutional accounts, not measured reductions in workload or demonstrated improvements in response performance. The available material contains no comparable data on report volumes, staff workload, response times, or community-network effectiveness.

This supporting role fits within the broader total-defense (semesta) orientation of Indonesia's defense system discussed earlier in relation to Law No. 23 of 2019. The connection concerns the contribution of different social and institutional resources; it does not imply that every digital offense constitutes a defense threat or that community actors acquire technical or law-enforcement authority. A comparable argument runs through the hybrid-threat literature. Wigell (2021) argues that interference below the threshold of armed conflict is dissuaded less by military response than by denying it the social conditions it depends on, bringing civic institutions, trusted communication, and public confidence into deterrence. Community-facing prevention, on that reading, sits alongside security work rather than beneath it. Figure 1 shows these contributions entering the network at different points rather than substituting for one another. The constraints marked there concern reach, coordination, and continuity, not demonstrated failure of any particular relationship.

The capability-gap analysis therefore supports a division of preventive responsibilities rather than a claim that community capacity is stronger than technical capacity. It shows why technical capability development and community-facing prevention need to proceed together: one addresses specialized incident handling, while the other may extend education, initial guidance, and access to reporting. The following subchapter develops the proposed model from these needs and institutional perspectives.

Proposed Community-Based Youth Digital Resilience Model

The proposed community-based youth digital resilience model is a conceptual synthesis, not an empirically tested intervention. It draws on institutional perspectives, contextual documents, and relevant scholarship on digital and community resilience, and it responds to the gap between

formal institutional mechanisms and the need for preventive support in young people's everyday digital environments. It should therefore be understood as a basis for future pilot testing and direct evaluation with young people, educators, community organizations, and local government actors, rather than as evidence of effectiveness. The roles it assigns to youth networks and educational spaces rest on institutional assessments and on the resilience literature, not on accounts from young people themselves.

The model distributes preventive functions across actors with different institutional mandates, drawing on the institutional and community-facing relationships summarised in Figure 1 and set out in the five components below. This arrangement does not transfer state authority to communities. Rather, it treats community-based prevention as complementary to formal institutional responsibilities.

The first component is critical literacy and digital safety capacity. Institutional informants across all six categories associated vulnerability with limited source verification, unsafe digital practices, and limited awareness of harmful content or deceptive online activity. Provincial and municipal digital-governance perspectives particularly emphasized source evaluation, fact-checking, privacy protection, fraud recognition, secure account practices, and awareness of online risks, while police and territorial perspectives also linked prevention to the capacity to recognize manipulation, assess context, and avoid emotionally driven sharing. Experimental work on psychological inoculation supports this emphasis. Roozenbeek and van der Linden (2019) show that exposing people in advance to weakened forms of manipulation techniques improves their later recognition of misleading content. Literacy components are likely to work better when they rehearse deception techniques than when they only transmit warnings. This component therefore focuses on capacities that may help young people assess information, protect personal data, recognize cyber financial fraud, and make safer online decisions. It does not replace formal cybersecurity, investigative, or law-enforcement functions.

The second component is local ethical framing and trusted social actors. Institutional informants identified religious leaders, customary leaders, parents, community figures, and local cultural approaches as potentially trusted channels for communicating digital literacy, responsible sharing, online ethics, tolerance, and social cohesion. Provincial social-resilience perspectives emphasized the legitimacy of community and religious figures. In contrast, police, territorial, and municipal perspectives described trusted local actors as relevant to community communication, early guidance, social mediation, and reducing the circulation of harmful information. Aldrich and Meyer (2015) argue that such ties function as an operational infrastructure for warning and mutual assistance, which is how they are treated here. The proposed model does not assume that cultural authority automatically changes behavior. Parental mediation, in particular, requires support rather than assumption: reporting on a communicative-parenting workshop in Lampung, Nurhaida et al. (2025) found that parents needed structured guidance to accompany children’s digital activity, indicating that family-level actors in this component are themselves targets of capacity building.

The third component is community forums as clarification and referral nodes. Institutional perspectives identified FKDM, community organizations, neighborhood forums, religious groups, community-policing mechanisms, territorial communication networks, and local information communities as potential spaces for preventive education, initial clarification, social mediation, early warning, and referral. Provincial social-resilience perspectives highlighted community forums and local figures as channels for recognizing emerging social dynamics, and provincial police perspectives emphasized community-policing arrangements and participatory problem-solving forums such as the neighborhood security belt (Sabuk Kamtibmas) and village deliberation meetings (Rembuk Pekon). Regional military and military-resort perspectives highlighted communication networks and trusted local relationships for early identification and field-based clarification. In contrast, municipal perspectives identified local forums, religious institutions, information communities, and digital-volunteer networks as community-facing routes for education and referral. These actors are not assigned responsibility for formal verification, investigation, content removal, technical incident response, or law enforcement. Their function in the model is closest to what F. H. Norris et al. (2008) term trusted information and communication: a community's capacity to circulate credible information and know where to find authoritative answers.

The fourth component is educational spaces and youth networks. Institutional informants identified schools, universities, student organizations, youth groups,

community-learning spaces, and local education programs as strategic settings for preventive support. Provincial and municipal digital-governance perspectives emphasized literacy education, creative public communication, online-safety awareness, and accessible reporting pathways. In contrast, police and territorial perspectives identified schools, campuses, and youth-oriented activities as spaces for prevention, civic education, and direct engagement. Municipal social-resilience perspectives linked educational institutions and youth organizations with character education, tolerance, responsible participation, and resilience-supporting social networks. The proposed model positions youth networks as sites for facilitated peer learning and responsible information sharing, not as autonomous fact-checking, monitoring, or enforcement bodies. Karami and Keshavarz (2024) show that online social capital can support coping and collective resilience, but their findings also indicate that such networks operate through existing trust relationships rather than spontaneously; participation therefore requires structured materials, trained facilitators, supervision, and clear referral guidance.

The fifth component is enabling government support. Government institutions retain responsibility for formal verification, technical response, investigation, content-removal requests, program continuity, and legal action, as described in the preceding theme. The provincial arrangements described earlier already provide two concrete anchors for this component: the reporting and referral pathway of the Indonesia Anti Scam Center promoted through Satgas PASTI, and the public-education role assigned to the provincial digital-governance agency within that task force (Diskominfotik Provinsi Lampung, 2025c).

Read through the lens of community resilience theory, the model addresses the four capacities identified by F. H. Norris et al. (2008), including the economic dimension that studies of digital literacy rarely incorporate. Social capital runs through the second, third, and fourth components. Aldrich and Meyer (2015) distinguish bonding ties within families and close groups, bridging ties across groups, and linking ties to formal institutions, and the model draws on all three. Bonding ties give parents, peers, and trusted local figures a chance to question suspicious offers or messages before anyone acts. Bridging ties carry warnings across communities through forums such as FKDM and neighborhood security networks. Linking ties connect those forums to official clarification and reporting channels. The circulation patterns documented in Table 3 also suggest that the same peer and family networks through which deceptive content spreads can carry verified warnings. Economic development enters the model in two ways. First, the province's weakest IMDI pillar concerns employment and economically productive digital use (Kemkomdigi RI, 2025). This provides context for the economic dimension of prevention, but it does not directly measure young people's economic opportunities or their relationship to digital vulnerability. Second, provincial practice already treats financial capability as preventive infrastructure. The Regional Financial Access Acceleration Team (Tim Percepatan Akses Keuangan Daerah, TPAKD) framed its 2025 village financial-literacy and inclusion program as a way to keep rural residents who lack relevant knowledge and skills out of online gambling and illegal online lending. It assigned the provincial digital-governance agency a publication and education role within that program (Diskominfotik Provinsi Lampung, 2025b). The model therefore includes financial literacy, financial inclusion, and referral to the illegal-finance task force as proposed fraud-prevention measures. Asymmetric, this narrows one of the vulnerabilities low-cost fraud networks exploit most readily.

Table 5 summarises the five components, and the final column makes explicit which community-resilience capacity each component is intended to strengthen and where the boundary of the community role lies.

Table 5. Proposed community-based youth digital resilience model

Model Component	Main Actors or Spaces	Proposed Function	Community-Resilience Capacity Addressed	Boundary of the Role
Critical literacy and digital	Schools, universities, youth learning spaces, and facilitated	Source evaluation, fact-checking, privacy protection, fraud	Community competence	Does not replace formal cybersecurity, fraud

safety	community education	recognition, secure account practices, and safe decision-making		investigation, or law-enforcement functions
Local ethical framing and trusted social actors	Customary leaders, religious leaders, parents, community figures, and local cultural actors	Culturally meaningful communication of responsible sharing, digital ethics, safe online conduct, and early referral	Social capital	Does not assume that social legitimacy or cultural authority automatically produces behavioral change
Community forums as clarification and referral nodes	FKDM, community organizations, neighborhood forums, religious groups, community-policing networks, territorial communication networks, and local information communities	Preventive education, initial clarification, social mediation, early warning, and referral to official channels	Information and communication	Does not independently verify all content, investigate offenses, remove content, conduct technical incident response, or undertake formal enforcement
Educational spaces and youth networks	Students, universities, schools, youth groups, student organizations, community-learning spaces, and digital-volunteer networks	Facilitated peer learning, positive and creative content, responsible sharing, digital-safety awareness, and early reporting	Community competence and social capital	Requires structured materials, trained facilitators, supervision, and clear referral guidance; youth are not assumed to be automatic educators or fact-checkers.
Enabling government support	Diskominfotik (provincial digital-governance agency), Kesbangpol (national and political unity agency), municipal governments, police, territorial institutions, CSIRT/TTIS, Satgas PASTI and TPAKD, and other authorized agencies	Standardized materials, verified clarification, reporting pathways, coordination, technical response, program monitoring, financial-literacy and inclusion programs, and legal escalation.	Economic development and information and communication	Formal verification, technical incident response, investigation, content-removal requests, and legal action remain with the respective authorized institutions, according to their mandates

Source: Authors' conceptual synthesis from thematic findings, contextual documents, Hammond et al. (2024), and F. H. Norris et al. (2008).

■ CONCLUSION

This study presents institutional perspectives on youth digital vulnerability in Lampung as a layered condition associated with unequal connectivity, uneven information-verification capacity, limited digital-safety awareness, and exposure to problematic information and cyber financial fraud. Institutional informants described problematic information and cyber financial fraud as analytically distinct but converging risks because both may exploit trust, emotion, perceived urgency, and limited capacity to evaluate digital content. They also identified complementary institutional functions in monitoring, public clarification, reporting, education, community communication, and coordination, while noting constraints related to specialized capacity, operational continuity, geographic reach, and reactive response patterns. Provincial cyber-governance evaluations provide documentary support for selected staffing, training, resource, and coordination constraints.

The study contributes a cross-institutional account of how digital-governance, social-resilience, public-safety, territorial, and municipal institutions may contribute to prevention. It develops a proposed community-based youth digital resilience model that

distributes preventive functions across educational spaces, trusted community actors, community forums, youth networks, and government institutions, and that incorporates the social-capital and economic-development capacities of community resilience alongside information and communication and community competence. The proposed model positions communities as partners in preventive education, initial clarification, social mediation, and referral, while authorized institutions remain responsible for formal verification, technical incident response, investigation, content-removal requests, and legal action. For the study of asymmetric warfare, the findings suggest that responding to low-cost digital threats requires specialized technical capacity and community-facing prevention. Verification habits, trusted communication, financial awareness, and accessible referral may each contribute, but their contributions still need direct evaluation.

The evidence has clear limits. It comes from documented interview records covering 13 organizational units and from contextual documents, not from young people themselves. Without verbatim transcripts, the analysis cannot capture wording, emphasis, or interactional detail. Interview durations were not recorded systematically, which limits how fully the data-collection process can be described. Post-interview member checking was not undertaken, so participants did not verify the authors' thematic interpretations. The findings should therefore be read as a thematic synthesis of institutional assessments rather than as a transcript-based account of individual voices. Several contextual documents are internal or working materials, and their indicator values were used as recorded rather than independently audited. Future research should directly examine young people's perspectives and pilot the proposed community-based youth digital resilience model with youth, educators, community organizations, and local government actors across diverse urban, rural, coastal, and connectivity-constrained settings in Lampung.

■ DECLARATION OF GENERATIVE AI USAGE IN THE WRITING PROCESS

During the preparation of this manuscript, the authors used ChatGPT (OpenAI) and Perplexity to support background literature searching. Information and references identified with these tools were verified against the sources. Following the use of these tools, the authors reviewed and revised the content as necessary and accept full responsibility for the final content of the article.

■ DATA AVAILABILITY

Publicly available sources are identified in the reference list. The remaining documents were issued by provincial government institutions for internal use and were never put into circulation. The authors can pass them on to researchers who ask, with the permission of the issuing agency. The structured interview records are a different matter. Informants spoke on the understanding that their accounts would appear only in aggregated form, so these can be obtained from the authors in an anonymized version that identifies informants by institutional category rather than by post.

■ REFERENCES

Afrina, C., Zulaikha, S. R., & Jumila. (2024). The Low Level of Digital Literacy in Indonesia: An Analysis of Online Media Content. Record and Library Journal, 10(2), 374–387. https://doi.org/10.20473/rlj.V10-I2.2024.374-387

Aldrich, D. P., & Meyer, M. A. (2015). Social Capital and Community Resilience. American Behavioral Scientist, 59(2), 254–269. https://doi.org/10.1177/0002764214550299

Arreguín-Toft, I. (2001). How the Weak Win Wars: A Theory of Asymmetric Conflict. International Security, 26(1), 93–128. https://doi.org/10.1162/016228801753212868

Balakrishnan, V., Ahmed, U., & Basheer, F. (2025). Personal, environmental, and behavioral predictors associated with online fraud victimization among adults. PloS One, 20(1), e0317232. https://doi.org/10.1371/journal.pone.0317232

Bappeda Provinsi Lampung. (2025). Rencana Pembangunan Jangka Menengah Daerah (RPJMD) Provinsi Lampung Tahun 2025-2029. Pemerintah Provinsi Lampung. https://bappeda.lampungprov.go.id/berkas/uploads/e3eRmPmRYaEpnjfPQ5OoMQoHhY25KMSo0SbYDbJB.pdf

BPS Provinsi Lampung. (2026). Provinsi Lampung Dalam Angka 2026. Badan Pusat Statistik Provinsi Lampung. https://lampung.bps.go.id/id/publication/2026/02/27/71de40a96c9fb7130aae19e3/provinsi-lampung-dalam-angka-2026.html

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Diskominfotik Provinsi Lampung. (2022). Laporan Evaluasi Penyelenggaraan TTIS/

CSIRT Provinsi Lampung Tahun Anggaran 2022 [Unpublished institutional evaluation report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Diskominfotik Provinsi Lampung. (2023). Laporan Evaluasi Penyelenggaraan TTIS/ CSIRT Provinsi Lampung Tahun Anggaran 2023 [Unpublished institutional evaluation report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Diskominfotik Provinsi Lampung. (2024). Laporan Evaluasi Penyelenggaraan TTIS/ CSIRT Provinsi Lampung Tahun Anggaran 2024 [Unpublished institutional evaluation report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Diskominfotik Provinsi Lampung. (2025a). Evaluasi Penyelenggaraan CSIRT/TTIS Pemerintah Daerah Tahun 2025 (Survey ID 981649) [Unpublished institutional evaluation report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Diskominfotik Provinsi Lampung. (2025b). Laporan Hasil Rapat Rencana Kegiatan Program Kerja Tim Percepatan Akses Keuangan Daerah (TPAKD) dan Edukasi Tahun 2025 (Nota Dinas No. 900.1.12/0652/IV.14-6/2025) [Unpublished internal meeting report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Diskominfotik Provinsi Lampung. (2025c). Laporan Kegiatan Rapat Koordinasi Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI) Provinsi Lampung dan Sosialisasi Indonesia Anti Scam Center (Nota Dinas No. 000.6.3.4/0817/IV.14-6/2025) [Unpublished internal meeting report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Diskominfotik Provinsi Lampung. (2025d). Pemetaan Blankspot dan Layanan Internet dalam Mendukung Transformasi Digital di Provinsi Lampung (Versi Agustus 2025) [Unpublished institutional mapping report]. Dinas Komunikasi, Informatika, dan Statistik Provinsi Lampung.

Hammond, S. P., Polizzi, G., Duddy, C., Bennett-Grant, Y., & Bartholomew, K. J. (2024). Children's, parents', and educators' understandings and experiences of digital resilience: A systematic review and meta-ethnography. New Media & Society, 26(5), 3018–3042. https://doi.org/10.1177/14614448241232065

Heeks, R. (2022). Digital inequality beyond the digital divide: conceptualizing adverse digital incorporation in the global South. Information Technology for Development, 28(4), 688–704. https://doi.org/10.1080/02681102.2022.2068492

Herrero-Diz, P., Conde-Jiménez, J., & de Cózar, S. R. (2020). Teens' Motivations to Spread Fake News on WhatsApp. Social Media + Society, 6(3). https://doi.org/10.1177/2056305120942879

Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. Journal of Press/Politics, 25(3), 493–516. https://doi.org/10.1177/1940161219900126

Jati, W. R. (2024). From Millennial to Generation Z: The State of Digital Literacy among Youths Dealing with Disinformation During Elections. Jurnal Komunikasi Indonesia, 13(1), 129–143. https://doi.org/10.7454/jkmi.v13i1.1228

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of Advanced Nursing, 72(12), 2954–2965. https://doi.org/10.1111/jan.13031

Karami, R., & Keshavarz, M. (2024). The emergence of online social capital during the COVID-19 outbreak and its impact on individual coping and community resilience in rural areas. Current Psychology, 43(19), 17787–17800. https://doi.org/10.1007/s12144-023-05167-y

Kemkomdigi RI. (2025). Indeks Masyarakat Digital Indonesia 2025. Badan Pengembangan Sumber Daya Manusia Komunikasi dan Digital, Kementerian Komunikasi dan Digital RI. https://bpsdm.komdigi.go.id/satker/pusbangesdmk/publikasi-indeks-masyarakat-digital-indonesia-2025-17-6

Kligler-Vilenchik, N., & Literat, I. (2020). Youth Digital Participation: Now More than Ever. Media and Communication, 8(2), 171–174. https://doi.org/10.17645/mac.v8i2.3180

Kolotouchkina, O., Rangel, C., & Gómez, P. N. (2023). Digital Media and Younger Audiences. Media and Communication, 11(4), 124–128. https://doi.org/10.17645/mac.v11i4.7647

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. SAGE Publications.

https://doi.org/10.1016/0147-1767(85)90062-8

Luong, H. T., & Ngo, H. M. (2024). Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective. Laws, 13(6), 70. https://doi.org/10.3390/laws13060070

Luthfia, A., Wibowo, D., Widyakusumastuti, M. A., & Angeline, M. (2021). The Role of Digital Literacy on Online Opportunity and Online Risk in Indonesian Youth. Asian Journal for Public Opinion Research, 9(2), 142–160. https://doi.org/10.15206/ajpor.2021.9.2.142

Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. International Security, 46(2), 51–90. https://doi.org/10.1162/isec_a_00418

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. American Journal of Community Psychology, 41(1–2), 127–150. https://doi.org/10.1007/s10464-007-9156-6

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. Journal of Police and Criminal Psychology, 34(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. International Journal of Qualitative Methods, 16(1), 1–13. https://doi.org/10.1177/1609406917733847

Nurhaida, I., Sugiyanto, P. S., Windah, A., Oktiani, H., & Sugiyanta. (2025). Communicative Parenting Workshop in the Digital Era : Reducing Challenges and Finding Solutions for Parents and Early Childhood Children. Bulletin of Social Studies and Community Development, 4(1), 14–23. https://doi.org/10.61436/bsscd/v4i1.pp14-23

O'Brien, B. C., Harris, I. B., Beckman, T. J., Reed, D. A., & Cook, D. A. (2014). Standards for Reporting Qualitative Research: A Synthesis of Recommendations. Academic Medicine, 89(9), 1245–1251. https://doi.org/10.1097/ACM.0000000000000388

Patton, M. Q. (2015). Qualitative Research & Evaluation Methods (4th ed.). SAGE Publications.

Putra, F. A., Samad, M. Y., & Mulyadi. (2024). Optimising "Lambe Hoaks" Digital Literacy to Strengthen National Resilience Against Hoaxes. Jurnal Lemhannas RI, 12(2), 203–214. https://doi.org/10.55960/jlri.v12i2.599

Reindrawati, D. Y., Setiawan, F., Satrianto, M. D., & Nata, J. H. (2023). The Use of Social Media in Improving Literacy in Rural Village. The International Journal of Applied Business (TIJAB), 7(1), 50–58. https://doi.org/10.20473/tijab.v7.I1.2023.43259

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Roozenbeek, J., & van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. Palgrave Communications, 5, Article 65. https://doi.org/10.1057/s41599-019-0279-9

Sandelowski, M. (2000). Whatever happened to qualitative description? Res. Nurs. Health, 23, 334–340. https://doi.org/10.1002/1098-240X(200008)23:4<334::AID-NUR9>3.0.CO;2-G

Sharma, M. K., Anand, N., Roopesh, B. N., & Sunil, S. (2021). Digital resilience mediates healthy use of technology. Medico-Legal Journal, 90(4), 211–215. https://doi.org/10.1177/00258172211018337

Sundar, S. S., Molina, M. D., & Cho, E. (2021). Seeing Is Believing: Is Video Modality More Powerful in Spreading Fake News via Online Messaging Apps? Journal of Computer-Mediated Communication, 26(6), 301–319. https://doi.org/10.1093/jcmc/zmab010

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. Retrieved October 11, 2026, from https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

van der Meer, T. G. L. A., & Hameleers, M. (2024). Misinformation perceived as a bigger informational threat than negativity: A cross-country survey on challenges of the news environment. Harvard Kennedy School (HKS) Misinformation Review. https://doi.org/10.37016/mr-2020-142

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

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. Retrieved October 11, 2026, from https://rm.coe.int/information-disorder-report-november-2017/1680764666

Wigell, M. (2021). Democratic Deterrence: How to Dissuade Hybrid Interference. The Washington Quarterly, 44(1), 49–67. https://doi.org/10.1080/0163660X.2021.1893027

Wither, J. K. (2016). Making Sense of Hybrid Warfare. Connections: The Quarterly Journal, 15(2), 73–87. https://doi.org/10.11610/Connections.15.2.06