Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

PUBLIC DIGITAL LITERACY AND INSTITUTIONAL CYBERSECURITY READINESS FOR AI-ASSISTED SOCIAL ENGINEERING IN BATAM'S FREE TRADE ZONE

Arvito Fernaldy Putra Hartono[1a*], Riska Sri Handayani[2], Jarot Prianggono[3]

[123]Magister Kajian Ilmu Kepolisian, Sekolah Pascasarjana Pembangunan Berkelanjutan, Universitas Indonesia, Indonesia

[a]*E-mail: arvito.fernaldy@ui.ac.id*

(*) Corresponding Author
arvito.fernaldy@ui.ac.id

ARTICLE HISTORY
Received : 29-08-2026
Revised : 12-10-2026
Accepted : 25-10-2026

KEYWORDS
Artificial Intelligence; Cybercrime; Digital Literacy; Free Trade Zone; Social Engineering

ABSTRACT

Batam's Free Trade Zone (FTZ) status and cross-border connectivity present cybersecurity challenges associated with organized digital fraud and emerging artificial intelligence (AI)-assisted social engineering. This study examines public digital-security literacy and policing strategies for addressing these threats. A mixed-methods explanatory sequential design combined a survey of 94 residents aged 25–29 in Sambau Subdistrict, using 53 indicators adapted from six NIST Cybersecurity Framework functions, with qualitative evidence from Polda Kepri, Diskominfo, BP Batam, and BSSN. Community-level quantitative findings were interpreted alongside institutional interview evidence. Item–total correlations ranged from 0.221 to 0.553, with Cronbach's Alpha reaching 0.888, providing preliminary evidence of item consistency and overall reliability. The surveyed population achieved a digital-literacy index of 83.00, classified as "Very Good," although the Identification dimension showed comparatively weaker performance in recognizing AI-generated content and understanding personal-data storage. Institutional findings revealed fragmented responsibilities, predominantly reactive detection, and delayed inter-agency responses. Reported criminal operations primarily involved conventional digital fraud, while AI-assisted methods remained insufficiently verified in individual cases. These findings identify institutional coordination and detection capacity as priority areas for strengthening cybersecurity governance in Batam.

This is an open access article under the CC–BY-SA license.

INTRODUCTION

The development of artificial intelligence (AI) has transformed social, economic, and institutional activities through automation, data-driven decision-making, and increasingly sophisticated digital communication (Constantin et al., 2024). Its expanding application also raises concerns regarding privacy, regulatory capacity, and social vulnerability, particularly in areas where technological development is not accompanied by adequate institutional safeguards (Hagerty & Rubinov, 2019; Prieto-Gutierrez et al., 2023). One emerging concern is the misuse of generative AI for social engineering, particularly

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

through voice cloning and deepfake technologies capable of reproducing recognizable human identities. Although these technologies offer legitimate benefits, their exploitation facilitates impersonation, financial fraud, and psychological manipulation (Genelza, 2024). Research indicates that synthetic voices can challenge conventional authentication systems and human recognition, while technical detection remains difficult because of increasingly realistic speech characteristics (Firc et al., 2023; Kulangareth et al., 2024). These developments create additional challenges for policing institutions responsible for preventing, detecting, and investigating technologically assisted criminal activities.

The increasing sophistication of AI-assisted cybercrime requires policing strategies extending beyond conventional criminal investigation. Technological detection, inter-agency cooperation, regulatory coordination, and public protection constitute important components of institutional preparedness. (Lin, 2025) identifies organizational and technological limitations affecting law-enforcement responses to AI-driven crime, while (Sarzaeim et al., 2023) and (Kheira, 2024) demonstrate the potential contribution of artificial intelligence to criminal-pattern analysis and predictive policing. Nevertheless, technological applications require appropriate institutional governance and safeguards. (Khan, 2024) emphasizes the limitations of conventional policing arrangements when confronting transnational cybercrime, whereas (Dupont & Whelan, 2021) highlight the importance of cooperation among actors involved in cybersecurity. (Mushtaq & Shah, 2024) similarly identify organizational, technical, and regulatory factors influencing effective cybercrime prevention. These considerations establish the relevance of assessing policing strategies through the relationship between crime opportunities, institutional guardianship, and coordinated preventive capabilities.

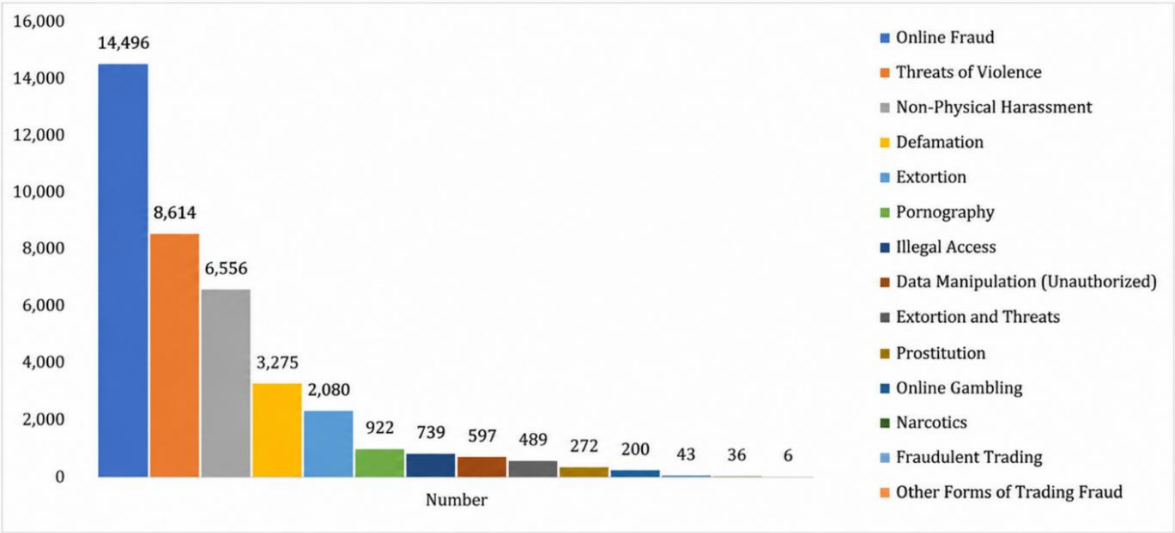


Figure 1. Cybercrime in Indonesia
Source: Bareskrim Polri, 2025.

National cybercrime statistics illustrate the broader security environment in which AI-assisted social engineering may develop. Bareskrim Polri (2025) recorded 39,482 cybercrime cases, comprising 14,496 online fraud cases (36.7%), 8,614 threats of violence (21.8%), and 6,556 defamation cases (16.6%), while unauthorized data manipulation accounted for 597 cases (1.51%) (Pusiknas Bareskrim Polri, 2025). These classifications indicate the distribution of reported offenses but do not independently establish the prevalence of AI-assisted crime. (Frensh, 2025) discusses emerging legal challenges concerning deepfake misuse, while (Ramadhanny, 2025) identifies risks associated with synthetic-voice fraud through digital communication platforms. Batam represents relevant research setting because of its strategic location near Singapore and Malaysia and its status as a Free Trade Zone (FTZ) under Government Regulation No. 41 of 2021. Although FTZ characteristics may create supervisory and jurisdictional challenges (Moiseienko et al., 2026), and the OECD/EUIPO has

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

documented criminal vulnerabilities associated with free-trade zones, available evidence does not establish that Batam experiences higher AI-related cybercrime rates than comparable regions.

Reported cases in Batam illustrate the interaction between transnational criminal activities and social engineering practices. In 2023, authorities uncovered a romance-scamming operation involving 88 Chinese nationals, with estimated financial losses reaching approximately Rp20.9 billion (Pratama, 2023). Another incident involved offenders impersonating population-administration officials to obtain personal information and verification codes under the pretext of activating Digital Population Identity services (Ridwan, 2025). These incidents demonstrate established deceptive practices but cannot automatically be classified as AI-assisted offenses without supporting technical evidence. Nevertheless, the potential integration of voice cloning into existing fraud methods raises concerns regarding the capacity of individuals and institutions to recognize manipulated identities and prevent financial losses. Batam's international economic connections and divided institutional responsibilities consequently provide a relevant setting for examining how criminal opportunities arise and how preventive policing arrangements respond to emerging technological threats.

The study adopts Situational Crime Prevention Theory and Routine Activity Theory as its principal criminological framework. Situational Crime Prevention Theory explains crime prevention through modifications to conditions facilitating offending, including increasing the effort required to commit crime, increasing detection risks, reducing anticipated rewards, reducing provocations, and removing excuses (Clarke, 2018). Routine Activity Theory explains criminal opportunities through the convergence of motivated offenders, suitable targets, and insufficient capable guardianship (Kitteringham & Fennelly, 2020). These theories are complementary: Routine Activity Theory identifies the conditions enabling AI-assisted social engineering, while Situational Crime Prevention Theory guides the formulation of interventions to restrict those opportunities. In this study, offender activities are examined through documented criminal cases and law-enforcement information; target vulnerability is assessed through public digital-literacy indicators; and guardianship is examined through the preventive, investigative, and coordination functions of Polda Kepri, Diskominfo, BP Batam, and BSSN. The resulting analysis links identified crime opportunities to appropriate preventive strategies without treating the observed relationships as statistically demonstrated causal effects.

Public digital literacy and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) provide operational support for this theoretical framework rather than functioning as additional criminological theories. Digital literacy encompasses operational, cultural, and critical competencies relevant to personal-data protection and digital threat recognition (Bulfin & McGraw, 2015; Pangrazio et al., 2020), while cybersecurity also involves human, organizational, and regulatory dimensions (Rashid et al., 2019). The NIST CSF organizes cybersecurity practices into six functions: Govern, Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2024). These functions are adapted into 53 questionnaire indicators measuring respondents' awareness, protective behavior, threat recognition, incident response, and recovery practices. The indicators are summarized through a composite-index approach informed by (OECD et al., 2008). The same six functions provide thematic categories for examining institutional governance, risk assessment, technical protection, detection capacity, inter-agency response, and post-incident evaluation. Individual survey scores and institutional findings are treated as distinct but complementary evidence, connecting public protective capacity and institutional guardianship with the criminological framework.

Previous studies have examined different aspects of AI-assisted social engineering. (Jones et al., 2020) identify persuasion mechanisms in vishing, particularly the exploitation of authority and social influence, while (Schmitt & Flechais, 2024) discuss the role of generative AI in automating and personalizing deceptive communication. (Pedersen et al., 2025) investigate deepfake-related threats and defensive measures in corporate environments, and (Madleňák & Hubočan, 2026) examine human recognition of AI-generated content. Technical research by (Lee et al., 2025) and (Triantafyllopoulos et al., 2025) addresses voice-phishing detection and the limitations of current speech-based identification approaches. From the perspective of human readiness, (Dhahir et al., 2024) demonstrate the complexity of relationships between digital literacy, deepfake exposure, and detection ability, while (Alomair et al., 2025) identify organizational and psychological influences on social engineering awareness. These findings suggest that technological detection, public awareness, and institutional preparedness constitute related but analytically distinct dimensions of cybercrime prevention.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Institutional research further identifies operational limitations in addressing technologically assisted offenses. (Lin, 2025) examines organizational challenges confronting law-enforcement agencies, while (Segara et al., 2025) document investigative difficulties associated with love-scamming offenses in Batam, including forensic limitations, financial-information access, and jurisdictional constraints. The bibliometric mapping of 200 publications presented in Figure 2 identifies research clusters associated with machine learning, web-based technologies, cybercrime, education, and society. Although these findings do not establish the complete absence of prior studies on institutional cybersecurity, they provide a descriptive basis for identifying the need for research integrating individual digital-literacy practices, situational crime opportunities, and institutional policing responses. The specific research gap addressed here concerns how public protective behavior and institutional guardianship interact in preventing AI-assisted social engineering within Batam's FTZ environment.



Figure 2. Research Gap Analysis
Source: Results of *VOSViewer* analysis, 2024.

Based on these theoretical and empirical considerations, this study addresses two research questions: (RQ1) What is the level and dimensional profile of public digital literacy among surveyed residents of Sambau Subdistrict, Nongsa, in confronting AI-assisted social engineering threats? (RQ2) How do situational crime opportunities and institutional cybersecurity capabilities shape adaptive policing strategies for preventing and countering AI-assisted social engineering crimes in Batam as a Free Trade Zone? To answer these questions, the study employs a mixed-methods explanatory sequential design, combining a quantitative assessment of 94 respondents aged 25–29 using 53 NIST CSF-based indicators with qualitative investigation of relevant cybersecurity institutions. Its contribution lies in integrating Routine Activity Theory to identify criminal opportunities, Situational Crime Prevention Theory to formulate preventive interventions, and the NIST CSF to organize individual and institutional cybersecurity evidence. This integration provides a locally grounded basis for developing adaptive policing strategies emphasizing digital-literacy improvement, coordinated risk identification, independent detection capacity, and cross-agency incident response, without assuming that the findings represent all Batam residents or establish causal relationships between FTZ status and cybercrime prevalence.

METHOD

This study employed a mixed-methods approach utilizing an explanatory sequential design to investigate public digital-security literacy and policing strategies concerning artificial intelligence (AI)-based social engineering crimes in Batam City, designated as a Free Trade Zone (FTZ). By integrating quantitative and qualitative evidence, the research framework provides a comprehensive understanding of this complex social phenomenon (Creswell & Creswell, 2018). Following this design, the quantitative assessment of digital-security literacy via a structured questionnaire preceded the qualitative interpretation of cybercrime prevention, institutional coordination, and law-enforcement capabilities, which were examined through interviews, observations, and documentary evidence (Creswell & Clark, 2017).

The research was geographically situated in *Kelurahan Sambau* and the adjacent Nongsa Digital Park (NDP), an integrated digital-economic area spanning approximately 166 hectares. The unique characteristics of Batam's FTZ, including investment facilitation and international economic connectivity, were treated strictly as contextual conditions rather than

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

predetermined causes of cybercrime. This analytical distinction aligns with scholarly perspectives emphasizing the specific institutional and regulatory environments of free-trade zones (Alansary & Al-Ansari, 2023).

The quantitative population comprised 1,602 residents of *Kelurahan Sambau* aged 25 to 29 years (Batam City Government, 2024). Employing simple random sampling and determining the sample size through Slovin's formula with a 10% precision parameter, the study yielded a final sample of 94 respondents. Consequently, the empirical findings are demographically bounded to this specific young-adult cohort and cannot be generalized to the broader Batam population, particularly as comparative victimization data across other age demographics were unavailable.

To measure digital-security literacy, the survey instrument was developed by integrating fundamental dimensions of digital literacy (Bulfin & McGraw, 2015; Pangrazio et al., 2020) with the six core functions of the NIST Cybersecurity Framework (CSF): Govern, Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2024). Furthermore, the instrument incorporated the human, organizational, and regulatory aspects of cybersecurity (Rashid et al., 2019). This multidimensional integration resulted in a context-specific adaptation designed to evaluate individual digital-security knowledge and behavior.

Data collection was administered via Google Forms, utilizing a questionnaire comprising 53 positively oriented statements. These items were evaluated on a five-point Likert scale ranging from 1 (Very Poor) to 5 (Very Good), with indicator scores subsequently standardized to a 0–100 scale to facilitate descriptive comparison and composite-index construction. The theoretical distribution of the 53 indicators across the six dimensions included Governance (7 indicators), Identification (9 indicators), Protection (11 indicators), Detection (10 indicators), Response (8 indicators), and Recovery (8 indicators).

Table 1. Dimensions of the Batam Public Digital Literacy Index

Dimension		Indicator	Indicator Type
Governance	1	Compliance_ITE_PDP_Regulations	Positive
	2	Compliance_Digital_Rights_Obligations	Positive
	3	Compliance_Safe_Digital_Behavior	Positive
	4	Compliance_Maintain_Digital_Environment	Positive
	5	Compliance_Do_Not_Misuse_AI	Positive
	6	Compliance_Understand_AI_Impacts	Positive
	7	Compliance_Platform_Rules	Positive
Identification	1	Knowledge_Account_Responsibility	Positive
	2	Knowledge_Confidential_Data	Positive
	3	Knowledge_Data_Location	Positive
	4	Knowledge_Account_Misuse	Positive
	5	Knowledge_Digital_Footprint	Positive
	6	Knowledge_Posting_Impacts	Positive
	7	Knowledge_AI_Deepfake	Positive
	8	Knowledge_AI_Content	Positive
	9	Knowledge_Others_Data_Permission	Positive
Protection	1	Protection_Strong_Password	Positive
	2	Protection_Different_Passwords	Positive
	3	Protection_Two_Step_Verification	Positive
	4	Protection_Device_Update	Positive
	5	Protection_Trusted_Applications	Positive
	6	Protection_OTP_Confidentiality	Positive
	7	Protection_Personal_Data_Limits	Positive
	8	Protection_Others_Privacy	Positive
	9	Protection_Suspicious_Links	Positive
	10	Protection_Unknown_Messages	Positive

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Dimension		Indicator	Indicator Type
	11	Protection_Unclear_Information	Positive
Detection	1	Detection_Sensational_News	Positive
	2	Detection_Unknown_Login	Positive
	3	Detection_Digital_Transactions	Positive
	4	Detection_Notification_Follow_Up	Positive
	5	Detection_Personal_Data_Request	Positive
	6	Detection_Fraud_Patterns	Positive
	7	Detection_Harmful_Content	Positive
	8	Detection_Security_Notifications	Positive
	9	Detection_Threat_Warnings	Positive
	10	Detection_Sharing_Cyber_Information	Positive
Response	1	Response_Change_Password	Positive
	2	Response_Logout_Device	Positive
	3	Response_Report_Suspicious_Account	Positive
	4	Response_Remain_Calm	Positive
	5	Response_Do_Not_Share_Information	Positive
	6	Response_Official_Guidance	Positive
	7	Response_System_Help_Feature	Positive
	8	Response_Do_Not_Spread_Hoaxes	Positive
Recovery	1	Recovery_Account_Method	Positive
	2	Recovery_Learn_From_Experience	Positive
	3	Recovery_Improve_Security	Positive
	4	Recovery_Security_Settings	Positive
	5	Recovery_Post_Attack_Vigilance	Positive
	6	Recovery_Data_Backup	Positive
	7	Recovery_Continue_Using_Technology	Positive
	8	Recovery_Evaluate_Problems	Positive

Source: Researcher's processed data, 2026.

The qualitative component used purposive sampling to identify informants with knowledge of cybercrime, cybersecurity regulation, FTZ governance, policing strategies, and public digital literacy. Informants represented the Special Criminal Investigation Unit of the Riau Islands Regional Police (Polda Kepri) and Barelang Police, the Batam City Department of Communication and Informatics (Diskominfo), the Batam Indonesia Free Zone Authority (BP Batam), the National Cyber and Crypto Agency (BSSN) in Batam, and community representatives. Informant selection was based on institutional responsibilities and relevant knowledge rather than statistical representativeness. Data collection involved interviews, observations, and documentary examination. Interviews and observations constituted primary sources of contextual evidence, while institutional records, regulatory documents, and reports of criminal cases provided secondary information. This distinction follows the principles of qualitative and mixed-methods data collection discussed by (Creswell, 2012; Creswell & Creswell, 2018; Sugiyono, 2019).

The qualitative analysis was organized using Situational Crime Prevention Theory and Routine Activity Theory as the principal criminological frameworks. Situational Crime Prevention Theory provides an analytical basis for identifying interventions intended to increase the effort required to commit crime, increase detection risks, reduce criminal rewards, reduce provocations, and remove excuses (Clarke, 2018). Routine Activity Theory explains criminal opportunities through the convergence of motivated offenders, suitable targets, and insufficient capable guardianship of Cohen & Felson, as discussed in (Kitteringham & Fennelly, 2020). These theoretical components were examined through reported criminal methods, respondents' digital-security practices, and the preventive and investigative responsibilities of relevant institutions. Crime Pattern Theory was retained as supporting contextual literature for interpreting the spatial organization of criminal

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

opportunities (Brantingham & Brantingham, 2021), while the FTZ's regulatory and economic characteristics were considered using the institutional perspective discussed by (Alansary & Al-Ansari, 2023). Social Learning Theory, including differential association and imitation, was retained as supplementary literature concerning possible offender-learning mechanisms (Akers, 2017; Onwuadiamu, 2025). Research concerning deception and psychological manipulation provided additional contextual interpretation of voice-based social engineering (Junger et al., 2023; Triantafyllopoulos et al., 2025). These supplementary perspectives were not treated as independently tested theoretical models, and recurring criminal methods alone were not interpreted as conclusive evidence of offender learning.

The explanatory connection between the quantitative and qualitative components was established by examining the institutional implications of specific survey findings. The quantitative results indicated a composite digital-literacy index of 83.00, with Governance recording the highest dimensional score (85.68) and Identification the lowest (81.65). The comparatively weak Knowledge_Data_Location (78.72) and Knowledge_AI_Content (80.00) indicators directed interpretive attention toward institutional education about personal-data risks, manipulated information, and deepfake recognition. Similarly, lower scores for Protection_Different_Passwords (77.02), Protection_Device_Update (77.23), Detection_Harmful_Content (79.15), and Detection_Unknown_Login (79.79) provided a basis for examining the adequacy of preventive cybersecurity education and threat-monitoring arrangements. Institutional evidence from Diskominfo and BP Batam was used to interpret public-awareness and protection practices, while information from Polda Kepri and BSSN was examined in relation to emerging criminal methods, AI-based threat detection, and investigative capacity. The contrast between relatively high regulatory awareness and weaker specific protective practices was also examined against evidence of fragmented institutional responsibilities and limitations in inter-agency response mechanisms.

The integration of quantitative and qualitative findings used the six NIST CSF functions as common analytical categories. Governance was examined through regulatory awareness and institutional coordination; Identification through personal-data knowledge and institutional risk assessment; Protection through individual security behavior and organizational prevention programs; Detection through public threat recognition and institutional monitoring capability; Response through individual incident-management practices and inter-agency escalation; and Recovery through personal post-incident behavior and institutional evaluation mechanisms. This approach enabled the interpretation of survey patterns alongside institutional practices without treating individual questionnaire scores and organizational capabilities as directly equivalent measurements. The integration also connected potential target vulnerability and guardianship conditions under Routine Activity Theory with preventive interventions informed by Situational Crime Prevention Theory (Clarke, 2018; Kitteringham & Fennelly, 2020).

The qualitative evidence provided contextual explanations for the survey findings, particularly concerning the difference between general digital-security awareness and practical responses to emerging technological threats. The study therefore established an explanatory relationship at the level of integrated findings, rather than through statistical causal testing. Although the original research design specifies a quantitative-first sequence, the available documentation does not independently establish whether individual interview questions were modified after the quantitative analysis. The reported integration consequently demonstrates how quantitative patterns were interpreted using institutional evidence, without claiming an undocumented procedure for developing the interview protocol.

Instrument assessment was conducted using Pearson Product Moment item–total correlations involving 53 statements and 94 respondents. At a significance level of 5%, with 92 degrees of freedom, the critical correlation coefficient was approximately 0.2028. The calculated coefficients ranged from 0.221 to 0.553, with reported significance values below 0.05, ranging from approximately 0.0326 to 2.96×10^{-8}. The strongest reported associations included Knowledge_Account_Misuse ($r = 0.553$), Detection_Security_Notifications ($r = 0.543$), and Knowledge_Account_Responsibility ($r = 0.534$). Comparatively weaker coefficients were observed for Compliance_ITE_PDP_Regulations ($r = 0.221$) and Compliance_Do_Not_Misuse_AI ($r = 0.232$). All 53 items exceeded the stated correlation threshold. These results provide preliminary evidence of item–total association but do not establish the multidimensional construct validity of the adapted instrument. Neither exploratory nor confirmatory factor analysis was reported, and evidence concerning convergent and discriminant validity remains unavailable. The instrument's validity claims are therefore limited to the statistical assessment actually conducted.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Reliability testing was performed using Cronbach's Alpha in IBM SPSS Statistics 26. All 94 cases were included, with no observations excluded. The overall coefficient reached 0.888 across 53 indicators, exceeding the 0.80 threshold associated with high internal consistency under the Sekaran/Guilford classification referenced in the original research. This result indicates strong aggregate internal consistency but does not establish the reliability of each individual dimension or confirm the instrument's proposed factor structure.

Table 2. Reliability Test

Case Processing Summary

		N	%
Cases	Valid	94	100.0
	Excluded[a]	0	.0
	Total	94	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.888	53

Source: Results processed using IBM SPSS 26, 2026.

Quantitative data were analyzed descriptively through indicator scores, dimensional comparisons, and the composite digital-literacy index. Qualitative evidence was organized thematically according to institutional responsibilities, reported cybercrime patterns, preventive activities, detection capability, inter-agency coordination, and incident-management practices. The six NIST CSF functions supported cross-source comparison, while the criminological framework provided interpretive categories for evaluating criminal opportunities and preventive interventions. This combination followed the purpose of mixed-methods integration described by (Creswell & Clark, 2017), with statistical results informing the interpretation of institutional evidence and the development of context-specific policing recommendations. The analysis did not establish causal relationships between digital-literacy scores, FTZ characteristics, and actual victimization.

Ethical Considerations, the study involved individual questionnaire responses and institutional information concerning cybersecurity and law-enforcement practices. The manuscript reports survey results in aggregated form and presents institutional findings primarily at the organizational level. However, the available research documentation does not specify formal ethics committee approval, an approval reference number, procedures for obtaining informed consent, or detailed arrangements for confidential data storage and retention.

RESULT AND DISCUSSION

Batam City occupies a unique geostrategic position within Indonesia's cybercrime landscape. Its location directly bordering Singapore and Malaysia, its status as a *Free Trade Zone*, and the high density of telecommunications infrastructure make the city vulnerable to the exploitation of digital technology for cross-border criminal purposes. The development of generative *Artificial Intelligence* in recent years has not only transformed the landscape of digital economic innovation but has also become a new instrument for cybercriminals to automate, accelerate, and enhance the precision of their attacks. AI-based cyberattacks can be understood as the use of machine-learning algorithms to automate stages of attack that previously required intensive manual intervention, ranging from *reconnaissance*, large-scale collection of victim data (*data scraping*), to the execution of psychological manipulation (*social engineering*). The principal distinguishing characteristic of AI-based attacks compared with conventional cybercrime is their ability to adapt to and learn from security-detection patterns, thereby making attacks more difficult to identify by traditional defense systems.

During the 2025–2026 period, Batam City experienced a significant escalation in organized cybercrime activities involving foreign nationals, with operational patterns indicating a shift in the bases of digital syndicates from mainland Southeast Asia to Indonesian territory.

1. Shift in the bases of transnational syndicates

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

The Riau Islands Regional Police (Polda Kepri) identified indications of a shift in the operations of *online* gambling networks and international online fraud from countries such as Cambodia, Myanmar, Laos, and Vietnam to Batam City, following increased law-enforcement pressure in those countries of origin.

2. Online gambling schemes with language-based market segmentation
   An operation uncovered in the Sukajadi area in May 2026 revealed an online gambling syndicate disguised as a lottery operation run by foreign nationals, with structured role divisions comprising hosts, operators, customer service personnel, and translators, as well as marketing strategies tailored to the language and country of origin of the target markets of each group of perpetrators.
3. Cross-jurisdictional online investment fraud and *love scamming*
   A raid on an apartment in the Baloi area secured hundreds of Chinese foreign nationals allegedly recruited for online investment-fraud and love-scamming networks targeting victims in Europe and Vietnam, with evidence comprising hundreds of computers, laptops, mobile phones, and large numbers of foreign passports.
4. Scale of operations and supporting infrastructure
   The seizure of evidence in several operations, including dozens of CPUs, hundreds of mobile phones, money-counting machines, and thousands of transaction identity cards, indicates a level of organization and infrastructure investment disproportionate to individual cybercrime and instead resembling the "scam factory" (scam compound) operational model that is known to operate in the Mekong region, Cambodia.

At the regional level, the Indonesia Anti-Scam Center recorded 7.782 fraud reports in the Riau Islands region from November 2024 to March 2026, as presented at the *Cyber Defense and Fraud Prevention* forum organized by the Riau Islands Financial Services Authority (OJK) in Batam. At the national level, the Financial Services Authority recorded more than 608 thousand *scam* cases in 2026, involving methods that utilized *money mule* accounts, digital payment systems, and crypto assets to conceal the flow of proceeds from crime. Meanwhile, the National Cyber and Crypto Agency (BSSN) reported that the majority of national cyber anomalies during the January–July 2025 period were *malware*-based, while the volume of *deepfake* content in Indonesia was reported by the Ministry of Communication and Digital Affairs to have increased rapidly over the past five years, constituting an indirect indicator of the expanding adoption of generative AI tools by criminal perpetrators.

The documented criminal operations in Batam involve online gambling, investment fraud, and *love scamming*. However, these cases cannot automatically be classified as AI-based cybercrime because the available evidence does not establish the use of artificial intelligence in each operation. Table 3 therefore distinguishes documented digital crime from unverified AI involvement.

Table 3. Distribution of Reported Cybercrime Operations in Batam City

Location	Operational Characteristics	Indicative Scale
Sukajadi Shophouses	Online gambling disguised as a lottery, Facebook live streaming	30 foreign nationals, dozens of devices
Baloi Apartment	Online investment fraud, *love scamming*	210 foreign nationals, hundreds of devices and passports
OPBC Batam Kota	Supporting operations for similar schemes	Dozens of devices
Simpang Kara	*Love scamming* by Chinese foreign nationals	Hundreds of foreign nationals

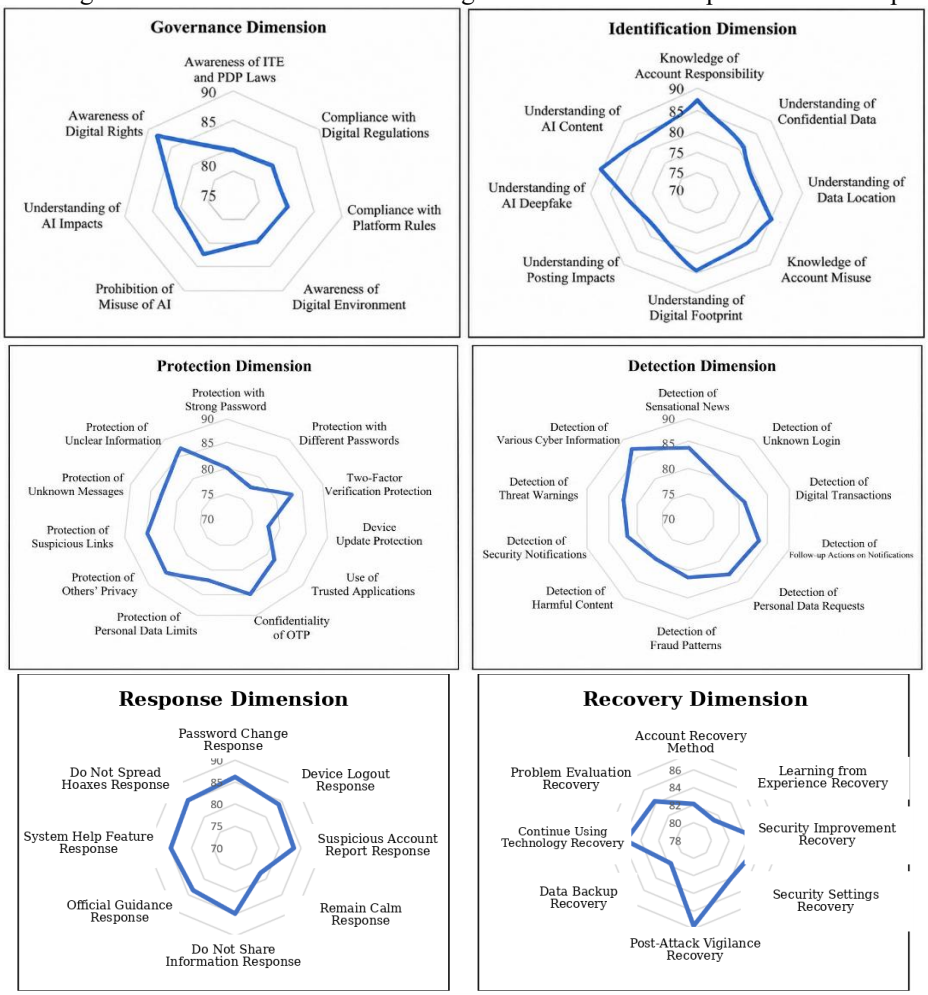
Source: Researcher's processed data, 2026.

The findings indicate that conventional digital fraud remains prevalent, while institutional interviews identified preliminary indications of voice and face cloning without establishing their involvement in the listed cases. These operations illustrate criminal opportunities and institutional guardianship challenges under Routine Activity Theory (Kitteringham & Fennelly, 2020), supporting preventive interventions based on Situational Crime Prevention Theory (Clarke, 2018).

Public digital literacy is calculated in the form of an index referring to the index-measurement approach developed by the *Organisation for Economic Co-operation and Development* (2008), which emphasizes combining a number of

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

indicators into a composite measure to describe the level of a phenomenon more comprehensively. This approach is undertaken by constructing a measurement structure consisting of dimensions that represent the concept being studied.



Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

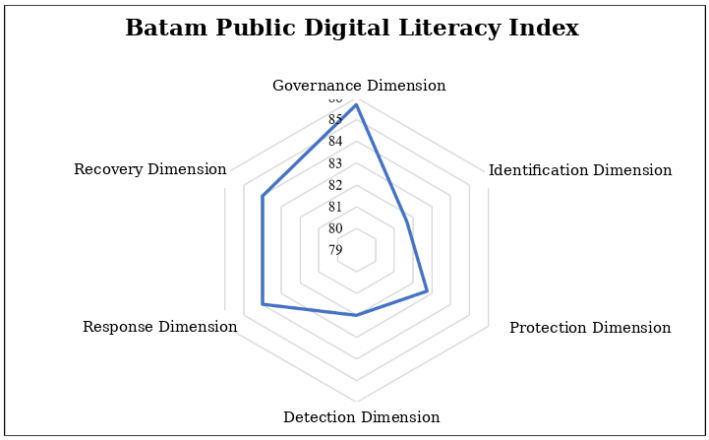


Figure 3. Measurement Results of the Dimensions of the Batam Public Digital Literacy Index
Source: Researcher's processed data, 2026.

Table 4. Measurement Results of the Batam Public Digital Literacy Index

Measurement Result	Score	Status
Governance Dimension	86	Very Good
Identification Dimension	82	Very Good
Protection Dimension	83	Very Good
Detection Dimension	82	Very Good
Response Dimension	84	Very Good
Recovery Dimension	84	Very Good
Batam Public Digital Literacy Index	83	Very Good

Description:	
1-20 : Very Poor	
21-40 : Poor	
41-60 : Adequate	
61-80 : Good	
81-100 : Very Good	

Source: Researcher's processed data, 2026.

The Batam City Public Digital Literacy Index was constructed based on six principal dimensions, namely Governance, Identification, Protection, Detection, Response, and Recovery, which were collectively measured through 53 derivative indicators using a scoring scale from 0 to 100. These six dimensions represent the complete cycle of public digital behavior, ranging from awareness of and compliance with digital regulations, understanding of risks and digital identity, implementation of security practices, the ability to detect cyber threats, to the capacity to respond and recover following digital-security incidents. Based on the measurement results, the Batam Public Digital Literacy Index reached 83.00, placing it in the "Very Good" category according to the established classification range of 81–100. This result reflects the digital literacy of the surveyed respondents in Sambau Subdistrict, Nongsa, although certain indicators, particularly within the Identification dimension, reveal areas requiring further improvement.

The Governance dimension was recorded as the dimension with the highest achievement, at 85,68, indicating that public awareness regarding compliance with digital regulations, including the Electronic Information and Transactions Law (UU ITE) and Personal Data Protection (PDP), digital-platform rules, and the responsible use of artificial intelligence, is relatively strong. This condition is supported by the Compliance with Platform Rules indicator, which achieved a score of

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

91,91, making it the highest-scoring indicator among all 53 indicators measured. Conversely, the Identification dimension became the dimension with the lowest achievement, at 81,65, reflecting that public understanding of cognitive-technical aspects, such as the location of personal-data storage and the ability to recognize artificial-intelligence-generated content, remains relatively weak compared with the level of formal compliance. This is reflected in the low scores for the Knowledge of Data Location indicator (78,72) and Knowledge of AI Content indicator (80,00), demonstrating that the public does not yet fully understand how and where their personal data are processed and is not yet accustomed to identifying content generated by artificial intelligence, including *deepfakes*.

In terms of digital-security practices, the Different Password Protection indicator was found to have the lowest overall score, namely 77,02, followed by the Device Update Protection indicator at 77,23 and the Remain Calm Response indicator at 78,09. These findings indicate a gap between the public's normative knowledge regarding digital security and its consistency in implementing everyday technical-security practices, such as using different passwords for each account, routinely updating devices, and remaining calm and acting systematically when confronting digital-security incidents. In the Detection dimension, which obtained a score of 82,00, weaknesses were also evident in the Harmful Content Detection indicator (79,15) and Unknown Login Detection indicator (79,79), indicating public vulnerability to *social engineering* and *phishing* attempts, including those that are becoming increasingly sophisticated through the use of generative artificial-intelligence technology.

On the other hand, the Response and Recovery dimensions demonstrated relatively strong achievements, each scoring 84,00, supported by the Post-Attack Vigilance Recovery indicator (87,66) and Change Password Response indicator (86,17). These findings demonstrate that although the public's composure during the initial phase of confronting an incident still requires improvement, its ability to undertake subsequent mitigation measures after an incident occurs, such as changing passwords and increasing post-attack vigilance, is relatively good. In general, these findings indicate that digital-literacy improvement programs in Batam City need to prioritize strengthening public understanding of the management and location of personal data, recognition of artificial-intelligence-based content, consistent implementation of digital-security hygiene practices, and incident-response management training in order to build the public's psychological and procedural preparedness in confronting cyber threats.

Furthermore, Batam City occupies both a strategic and vulnerable position within the national cybersecurity landscape. As a *Free Trade Zone* (FTZ) regulated through Government Regulation No. 41 of 2021, Batam experiences relatively high cross-border flows of goods, services, capital, and people, with geographical proximity to Singapore and Malaysia. The deregulatory character and export-investment orientation inherent in the FTZ, on the one hand, promote economic growth, but on the other hand create new opportunities for cross-jurisdictional cybercrime methods, including *social engineering* crimes that are now reinforced by artificial intelligence (*Artificial Intelligence/AI*).

The development of generative AI technology, particularly *voice cloning* and *deepfake* based on *Generative Adversarial Networks* (GAN), has transformed the landscape of social engineering from merely text-based *phishing* into *vishing* and voice- or face-based fraud that is far more convincing. Field data from four key actors managing cybersecurity in Batam, namely BP Batam, the Batam City Department of Communication and Informatics (Diskominfo), the Riau Islands Regional Police (Polda Kepri), and the Batam representative of the National Cyber and Crypto Agency (BSSN), indicate that this threat has already begun to emerge, although the dominant methods to date remain conventional *phishing*, *romance / love scams*, and investment fraud, with early indications of the use of *voice/face cloning*.

Historically, BP Batam has experienced cybersecurity incidents involving *phishing* and *web defacement*, although the resulting impacts were relatively limited and were fully addressed. BP Batam's institutional preparedness in confronting cyber threats is supported by several mechanisms, including the implementation of *cyber security awareness* activities for employees at least twice a year, the existence of an internal *Government Computer Security Incident Response Team* (GCR) with a tiered escalation channel to the National Cyber and Crypto Agency (BSSN), and technical infrastructure comprising a *firewall*, *Intrusion Prevention System* (IPS), and *Intrusion Detection System* (IDS), which are continuously maintained. To date, no record has been identified of artificial intelligence (AI)-based attacks directly targeting BP Batam. Nevertheless, the institution acknowledges that it does not yet have specific regulations requiring cybersecurity standards for companies

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

operating within the *Free Trade Zone* (FTZ), resulting in cybersecurity responsibility tending to remain internal-institutional and not yet comprehensively encompassing the entire area.

The Batam City Department of Communication and Informatics (Diskominfo) functions as the first point for receiving public complaints related to cyber incidents. However, its authority is limited to forwarding complaints to the aduankonten.id platform or to vertical agencies such as the Financial Services Authority (OJK) and the police, without authority to conduct blocking or direct enforcement, because such authority is centralized at the Ministry of Communication and Digital Affairs and BSSN at the national level. Digital-literacy outreach efforts conducted by Diskominfo still rely on Instagram channels, while TikTok, which empirically is more relevant to Generation Z media-consumption patterns, has not been utilized optimally, thereby revealing a gap between the educational channels used and the characteristics of the target groups. The training program entitled RabuKami was also found to reach only the internal scope of the city government, with very limited human-resource support in the field of cryptography, consisting of only three people.

Based on complaint data, the most frequently reported crime methods include: (1) *romance scams* through video calls that subsequently result in extortion; (2) *phishing* through files resembling wedding invitations on the *WhatsApp* application; (3) investment fraud exploiting Batam's image as an FTZ area; and (4) early indications of *deepfake* and *voice phishing* practices imitating the voices of parties known to the victim. The groups identified as most vulnerable to these crimes are the *boomer* generation and Generation X, which have high levels of exposure to technology but relatively low critical literacy. In addition, Batam's *hinterland* areas, comprising three island districts out of a total of twelve districts, demonstrate relatively high levels of digital crime but are minimally supported by granular and validated data.

The most significant case ever uncovered in Batam was the *scam center* network in the Kamoy Industrial Area in 2023. Interestingly, this case was first detected through a report from Chinese police authorities, rather than through independent detection by domestic authorities, a finding indicating limitations in early-detection capacity at the local level. Enforcement operations against the network involved five task forces operating on the basis of intelligence data from foreign authorities. During the enforcement process, indications were also identified of information leakage to other locations before subsequent raids were conducted, indicating gaps in inter-agency coordination.

In general, cybercrime patterns in Batam are dominated by various forms of fraud, including *mobile/internet banking* hijacking, which has again become prevalent following patterns observed in 2022, with perpetrators tending to originate from relatively similar geographical areas from year to year. Police authorities note that the fundamental modus operandi has not changed significantly; what has changed are the instruments used, including AI-based *voice cloning* and *face cloning* technologies, which perpetrators exploit to identify new opportunities in line with technological developments. From a regulatory perspective, the Electronic Information and Transactions Law (UU ITE) is generally considered to have covered most cyber offenses, while provisions in the new Criminal Code (KUHP) are viewed as more specific. Nevertheless, structural challenges remain, given that regulatory frameworks consistently lag behind the pace of technological change. In addition, there is not yet a structured development program for *hacker* communities, such as the development model commonly applied to vulnerable groups in conventional crime, and outreach to schools and university environments continues to be conducted individually and has not yet been systematically institutionalized.

BSSN in Batam performs primary functions in signal detection, *open-source intelligence* (OSINT) monitoring, and the dissemination of strategic information to leadership. The platforms predominantly monitored are TikTok and Facebook, in accordance with the media-use patterns of Batam residents. BSSN's strategy toward AI-based threats is not yet proactive or specific; such threats are only followed up reactively through OSINT reporting when indications of their use are identified. Current risk management remains focused on identifying technical assets (radio, satellite, and cellular) together with the *Standard Operating Procedures* (SOPs) governing their use, while there does not yet appear to be an explicit *risk register* specifically targeting AI-based *social engineering* threats.

From the perspective of human resources, BSSN Batam acknowledges limitations in the number of personnel compared with the workload of signal analysis that must be handled. Nevertheless, the culture of *security awareness* is relatively strong because it is based on official-service education, which is subsequently transmitted informally to non-alumni personnel. From the perspective of personal-data governance, risky operational practices have been identified, namely that certain administrative activities still use *Google Docs* and *Google Spreadsheet* that are *widely shareable*. In terms of

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

community development, BSSN facilitates the Batam IT Security community, which organizes annual activities as an initial form of collaborative approach, although this initiative has not yet been explicitly directed as a preventive-development model for potential cybercrime perpetrators.

The synthesis of field findings across the six core functions of the *NIST Cybersecurity Framework* (CSF) demonstrates that Batam City's preparedness in confronting artificial-intelligence (AI)-based *social engineering* crime still relies on the resilience of each institution separately (*institutional resilience*) and has not yet developed into collective area-wide resilience (*collective resilience*), as would ideally be required for a *Free Trade Zone* (FTZ) that is inherently at high risk of cross-jurisdictional crime.

Table 5. Batam Cybersecurity Conditions Based on the NIST Cybersecurity Framework (CSF)

CSF Function	Findings on Conditions in Batam	Principal Gap
Govern	BP Batam, Diskominfo, BSSN, and the Riau Islands Regional Police (Kepri) are known to operate within their respective lines of authority without the support of a binding cross-sector cybersecurity-governance forum; specific cybersecurity regulations for the FTZ area are also not yet available.	Fragmentation of authority and the absence of a formal inter-agency escalation *Standard Operating Procedure* (SOP) have been identified.
Identify	The available *risk registers*, for example at BSSN, were found to remain oriented toward technical signaling assets and do not yet include profiles of AI-based *social engineering* threats or maps of demographic vulnerability (elderly groups, *hinterland* areas).	There is not yet a risk mapping specifically targeting AI threats or data-based profiles of vulnerable groups.
Protect	Cybersecurity education is conducted at the institutional level (BP Batam, BSSN), while public outreach by Diskominfo remains limited to Instagram channels and has not yet reached Generation Z (which is TikTok-based) or *boomer*/Generation X groups that have low literacy but actively use digital devices.	Educational channels have not yet been segmented according to the demographic characteristics and media-consumption patterns of vulnerable victim groups.
Detect	Large-scale cases, namely the *scam* network in the Kamoy Industrial Area, were uncovered only after reports from Chinese police authorities rather than as a result of independent detection; BSSN's OSINT capacity was also identified as still being supportive rather than predictive of AI-manipulated content.	Dependence on external/foreign information and limited independent capacity to detect *deepfake* and *voice cloning* content were identified.
Respond	The handling of small-scale incidents, such as *phishing* cases at BP Batam, proceeds rapidly internally. However, inter-agency handling, such as content blocking and account freezing, is centralized at the Ministry of Communication and Digital Affairs and OJK and requires a tiered process, including prior reporting to the police.	Inter-agency response flows were identified as slow and cumbersome for handling cases requiring immediate action.
Recover	Crime patterns (*romance / love scams*, *phishing*, investment fraud) were found to recur from year to year with relatively similar modus operandi; there does not yet appear to be a structured and documented cross-agency post-incident evaluation mechanism.	A limited shared *lessons-learned* database was identified for preventing the recurrence of the same crime patterns.

Source: Researcher's data, 2026.

From the perspective of Routine Activity Theory, cybercrime opportunities in Batam emerge through the interaction of motivated offenders, suitable targets, and insufficient capable guardianship (Kitteringham & Fennelly, 2020). Organized fraud networks documented in the Kamoy Industrial Area illustrate offender capacity, while weaknesses in AI-content recognition, personal-data awareness, and protective practices increase potential target exposure. Institutional guardianship is constrained by fragmented authority among Polda Kepri, Diskominfo, BP Batam, and BSSN, particularly in threat detection

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

and incident escalation. These conditions create opportunities for fraudulent activities to continue before coordinated intervention occurs. Although interviews identified concerns involving older residents and hinterland communities, the survey findings specifically represent respondents aged 25–29. Recurring criminal methods may also involve imitation or offender learning, as discussed in Social Learning Theory (Akers, 2017; Onwuadiamu, 2025), although the available evidence does not establish these mechanisms directly.

Situational Crime Prevention Theory provides a mechanism for addressing these vulnerabilities through targeted interventions (Clarke, 2018). Increasing the effort required to commit fraud involves stronger identity verification, platform-security controls, and coordinated preventive procedures. A cross-sector cybersecurity forum connecting Polda Kepri, BP Batam, Diskominfo, BSSN, OJK, financial institutions, and digital platforms could reduce coordination barriers through standardized incident-escalation procedures aligned with the NIST CSF Govern function (National Institute of Standards and Technology, 2024). Increasing detection risks requires strengthening independent digital-forensic capabilities, particularly for suspected voice cloning and deepfake content, alongside cross-border intelligence cooperation. The Kamoy case demonstrates the operational consequences of relying on foreign investigative information. AI-assisted CCTV monitoring may provide supplementary detection capacity in selected locations, subject to technical validation, proportionality, and privacy safeguards.

Reducing criminal rewards requires faster identification and lawful freezing of accounts associated with fraudulent transactions through improved coordination among police, OJK, and financial institutions. Such measures can restrict access to illicit proceeds without disregarding procedural safeguards. Reducing provocations involves identifying manipulative communications that exploit urgency, fear, or perceived authority, supported by BSSN's proactive OSINT monitoring. These mechanisms are consistent with research on deception and persuasive communication in social engineering (Junger et al., 2023; Triantafyllopoulos et al., 2025). Removing excuses requires clearer digital-conduct standards, preventive education, and community-based engagement, including the development of the Batam IT Security community facilitated by BSSN. Economic inclusion may complement preventive efforts, although its direct relationship with cybercrime participation was not established by the present data.

Strengthening the NIST CSF Protect and Recover functions requires connecting public education with institutional incident-management capabilities. The survey's weaker Identification and Protection indicators support targeted training in recognizing AI-generated content, protecting personal information, managing passwords, and responding to suspicious communication. Diskominfo's outreach could combine TikTok-based education for younger audiences with community-based activities for older residents and hinterland areas, while recognizing that these groups were not directly represented in the quantitative sample. A shared cross-agency lessons-learned database could connect recurring phishing, romance scams, investment fraud, and emerging voice/face cloning indications with subsequent prevention and response improvements. Such integration would strengthen institutional guardianship by reducing delays between threat identification, coordinated intervention, and preventive adaptation.

CONCLUSION

Although the Batam Public Digital Literacy Index was recorded in the “Very Good” category (83.00), this achievement has not been directly correlated with regional resilience against artificial intelligence (AI)-based *social engineering* crimes. Gaps emerge specifically in the *Identify* dimension, particularly in the ability to recognize AI-generated content and understand the location of personal data storage, as well as in the consistency of everyday technical security practices (the use of different passwords and device updates). These findings indicate that the vulnerability of the Batam community is cognitive-technical and behavioral in nature, rather than merely resulting from a lack of normative awareness.

At the institutional level, the synthesis of the six functions of the *NIST Cybersecurity Framework* confirms that the preparedness of the four key actors (BP Batam, Diskominfo, Polda Kepri, and BSSN) remains institutionally partial, characterized by three principal structural gaps: *first*, fragmentation of authority without a binding cross-sector cybersecurity governance forum (the *Govern* function); *second*, dependence on reactive detection and information from foreign authorities, as demonstrated by the Kamoy Industrial Area case, which was in fact uncovered through a report from the Chinese police (the *Detect* function); and *third*, slow and tiered inter-agency response mechanisms, particularly in the processes of account

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 4 Desember 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

freezing and content *takedown* (the *Respond* function). This condition demonstrates that all three conditions for the occurrence of crime are simultaneously fulfilled in Batam, while the recurring pattern of modus operandi from year to year confirms the existence of a *differential association* process among perpetrators, as explained by *social learning theory*.

The findings suggest that Batam's principal cybersecurity challenge lies not merely in public digital literacy but in fragmented institutional coordination, limited independent detection capabilities for *deepfake* and *voice cloning*, and slow inter-agency responses. Strengthening the NIST CSF *Govern* and *Detect* functions through integrated cybersecurity governance, standardized response procedures, and digital-forensic capacity is essential to improving regional resilience and supporting situational crime prevention. Nevertheless, the survey's limited demographic coverage and the absence of verified AI involvement in several reported criminal cases restrict the generalizability of these findings. Future research should examine broader demographic groups, compare cybercrime patterns across FTZ regions and reporting periods, validate the adapted digital-literacy instrument, and evaluate the effectiveness of inter-agency coordination and AI-based crime detection using verified case evidence.

ACKNOWLEDGMENT

During the preparation of this work the authors used Artificial Intelligence (AI) in order to improve the language and readability of the manuscript. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

REFERENCES

Akers, R. (2017). Social Learning and Social Structure: A General Theory of Crime and Deviance. Routledge. https://doi.org/10.4324/9781315129587

Alansary, O. S., & Al-Ansari, T. (2023). Defining 'Free Zones': A Systematic Review of Literature. Heliyon, 9(4), e15344. https://doi.org/10.1016/j.heliyon.2023.e15344

Alomair, M., Issa, T., Zaung Nau, S., & Abu Salih, B. (2025). The Key Factors That Influence Employees' Awareness of Social Engineering: A Systematic Literature Review. Heliyon, 11(16), e44012. https://doi.org/10.1016/j.heliyon.2025.e44012

Brantingham, P., & Brantingham, P. (2021). Crime Pattern Theory. In H. N. Pontell (Ed.), Oxford Research Encyclopedia of Criminology and Criminal Justice (1st ed.). Oxford University PressNew York, NY. https://doi.org/10.1093/acrefore/9780190264079.013.8

Bulfin, S., & McGraw, K. (2015). Digital Literacy in Theory, Policy and Practice: Old Concerns, New Opportunities. In M. Henderson & G. Romeo (Eds.), Teaching and Digital Technologies (1st ed., pp. 266–281). Cambridge University Press. https://doi.org/10.1017/CBO9781316091968.026

Clarke, R. V. (2018). The Theory and Practice of Situational Crime Prevention. In H. N. Pontell (Ed.), Oxford Research Encyclopedia of Criminology and Criminal Justice (1st ed.). Oxford University PressNew York, NY. https://doi.org/10.1093/acrefore/9780190264079.013.327

Constantin, N., Nelwin, R., Christanto, A., & Irwansyah, I. (2024). Artificial Intelligence: Communication, Technology, and Society (a Systematic Literature Review). Jurnal Indonesia Sosial Teknologi, 5(10), 4514–4533. https://doi.org/10.59141/jist.v5i10.7027

Creswell, J. W. (2012). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research (4th edition). Pearson Education, Inc.

Creswell, J. W., & Clark, V. L. P. (2017). Designing and Conducting Mixed Methods Research. SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications.

Dhahir, D. F., Kenda, N., Dirgahayu, D., Syarifuddin, S., Djaffar, R., Widihastuti, R., Rustam, M., & Pala, R. (2024). The Relationship of Digital Literacy, Exposure to AI-Generated Deepfake Videos, and the Ability to Identify Deepfakes in Generation X. Jurnal Pekommas, 9(2), 357–368. https://doi.org/10.56873/jpkm.v9i2.5873

Dupont, B., & Whelan, C. (2021). Enhancing Relationships Between Criminology and Cybersecurity. Journal of Criminology, 54(1), 76–92. https://doi.org/10.1177/00048658211003925

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a Threat to a Speaker and Facial Recognition: An Overview of Tools and Attack Vectors. Heliyon, 9(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Frensh, W. (2025). Criminal Policy Toward the Crime of Defamation in Cyberspace Through the Use of Deepfake AI. JURNAL AKTA, 12(2), 472. https://doi.org/10.30659/akta.v12i2.44884

Genelza, G. G. (2024). A Systematic Literature Review on AI Voice Cloning Generator: A Game-Changer or a Threat? Journal of Emerging Technologies, 4(2), 54–61. https://doi.org/10.57040/ag587791

Hagerty, A., & Rubinov, I. (2019). Global AI Ethics: A Review of the Social Impacts and Ethical Implications of Artificial Intelligence (arXiv:1907.07892). arXiv. https://doi.org/10.48550/arXiv.1907.07892

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2020). How Social Engineers Use Persuasion Principles During Vishing Attacks. Information and Computer Security, 29(2), 314–331. https://doi.org/10.1108/ICS-07-2020-0113

Junger, M., Koning, L., Hartel, P., & Veldkamp, B. (2023). In Their Own Words: Deception Detection by Victims and Near Victims of Fraud. Frontiers in Psychology, 14, 1135369. https://doi.org/10.3389/fpsyg.2023.1135369

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. Laws, 13(4), 44. https://doi.org/10.3390/laws13040044

Kheira, B. (2024). Predictive Policing and Enhancing Security Performance through Artificial Intelligence Applications. Turkish Academic Research Review - Türk Akademik Araştırmalar Dergisi [TARR]. https://doi.org/10.30622/tarr.1464788

Kitteringham, G., & Fennelly, L. J. (2020). Environmental Crime Control. In Handbook of Loss Prevention and Crime Prevention (pp. 207–222). Elsevier. https://doi.org/10.1016/B978-0-12-817273-5.00019-3

Kulangareth, N. V., Kaufman, J., Oreskovic, J., & Fossat, Y. (2024). Investigation of Deepfake Voice Detection Using Speech Pause Patterns: Algorithm Development and Validation. JMIR Biomedical Engineering, 9, e56245. https://doi.org/10.2196/56245

Lee, C., Kim, B., & Kim, H. (2025). The Silence of the Phishers: Early-Stage Voice Phishing Detection With Runtime Permission Requests. Computers & Security, 152, 104364. https://doi.org/10.1016/j.cose.2025.104364

Lin, L. S. F. (2025). Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud. Laws, 14(4), 46. https://doi.org/10.3390/laws14040046

Madleňák, M., & Hubočan, S. (2026). Phishing 2.0: Human Ability to Detect AI-Generated Content. Transportation Research Procedia, 93, 1125–1132. https://doi.org/10.1016/j.trpro.2025.12.051

Moiseienko, A., Reid, A., & Chase, I. (2026, October 22). Improving Governance and Tackling Crime in Free-Trade Zones. Rusi.Org. https://www.rusi.orghttps://www.rusi.org

Mushtaq, S., & Shah, M. (2024). Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. Information, 15(10), 619. https://doi.org/10.3390/info15100619

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

OECD, European Union, & Joint Research Centre - European Commission. (2008). Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. https://doi.org/10.1787/9789264043466-en

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of Criminological Theories, Methods, and Concepts. Journal of Economic Criminology, 8, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

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

Pedersen, K. T., Pepke, L., Stærmose, T., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments. Journal of Cybersecurity and Privacy, 5(2), 18. https://doi.org/10.3390/jcp5020018

Pratama, I. Y. (2023, August 30). Polda Kepri: 88 tersangka "love scamming" China baru 2 bulan di Batam - Mandalika world Superbike. Antara News. https://mandalika.antaranews.com/berita/3704250/polda-kepri-88-tersangka-love-scamming-china-baru-2-bulan-di-batam

Prieto-Gutierrez, J.-J., Segado-Boj, F., & Da Silva França, F. (2023). Artificial Intelligence in Social Science: A Study Based on Bibliometrics Analysis. Human Technology, 19(2), 149–162. https://doi.org/10.14254/1795-6889.2023.19-2.1

Pusiknas Bareskrim Polri. (2025). Statistik Kejahatan Siber. https://pusiknas.polri.go.id/

Ramadhanny, F. (2025, June 21). Peringatan: Penipuan Deepfake Suara Masuk WhatsApp. detikinet. https://inet.detik.com/security/d-7975513/peringatan-penipuan-deepfake-suara-masuk-whatsapp

Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (2019). The Cyber Security Body of Knowledge. Crown Copyright, The National Cyber Security Centre.

Ridwan. (2025, September 27). Disdukcapil Batam Imbau Warga Waspada Penipuan Pengaktifan IKD. Posmetrobatam.co.id. https://posmetrobatam.co.id/disdukcapil-batam-imbau-warga-waspada-penipuan-pengaktifan-ikd/

Sarzaeim, P., Mahmoud, Q. H., Azim, A., Bauer, G., & Bowles, I. (2023). A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing. Computers, 12(12), 255. https://doi.org/10.3390/computers12120255

Schmitt, M., & Flechais, I. (2024). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. Artificial Intelligence Review, 57(12), 324. https://doi.org/10.1007/s10462-024-10973-2

Segara, I. G. B. C., Chusniyah, T., & Dharmastuti, A. (2025). Analisis Dampak Psikologis Korban Love Scam. Flourishing Journal, 5(9), 527–535. https://doi.org/10.17977/um070v5i92025p527-535

Sugiyono. (2019). Metode Penelitian Kuantitatif Kualitatif dan R&D. ALFABETA. https://scholar.google.com/scholar?cluster=14139717248943287621&hl=en&oi=scholarr

Triantafyllopoulos, A., Spiesberger, A. A., Tsangko, I., Jing, X., Distler, V., Dietz, F., Alt, F., & Schuller, B. W. (2025). Vishing: Detecting Social Engineering in Spoken Communication — a First Survey & Urgent Roadmap to Address an Emerging Societal Challenge. Computer Speech & Language, 94, 101802. https://doi.org/10.1016/j.csl.2025.101802