

# Police-led preventive cyber education and cryptocurrency scam prevention: A PRISMA-guided systematic literature review from a digital citizenship perspective

Candra Gunawan \* 

\* Sekolah Tinggi Ilmu Kepolisian, Indonesia  
[cgfigure88@gmail.com](mailto:cgfigure88@gmail.com)

Chryshnanda Dwilaksana 

Sekolah Tinggi Ilmu Kepolisian, Indonesia  
[dwilaksanachryshnanda@gmail.com](mailto:dwilaksanachryshnanda@gmail.com)

Supardi Hamid 

Sekolah Tinggi Ilmu Kepolisian, Indonesia  
[supardihamid@stik-ptik.ac.id](mailto:supardihamid@stik-ptik.ac.id)

Yopik Gani 

Sekolah Tinggi Ilmu Kepolisian, Indonesia  
[ganiyopikgani@yahoo.co.id](mailto:ganiyopikgani@yahoo.co.id)

\*Corresponding Author

## Article Info

### Article History

#### Submitted:

25 June 2026

#### Revised:

25 August 2026

#### Accepted:

31 August 2026

### Keywords

cybersecurity education;  
cryptocurrency scams; digital  
citizenship; police; protective  
behaviour; systematic  
literature review

## Abstract

Cryptocurrency participation has expanded digital economic citizenship while exposing users to fraud that combines technological complexity, social engineering, impersonation, cognitive bias, and irreversible transactions. This systematic literature review examines how police-led preventive cyber education can strengthen protective behaviour against cryptocurrency scams and how this function can be conceptualised within digital citizenship. The review followed PRISMA 2020 reporting principles and PRISMA-S search-documentation elements. A structured cross-platform search and citation-chasing process covered peer-reviewed literature published from January 2015 to 24 August 2026. Forty-seven candidate records were logged, seven duplicates were removed, 40 records were screened, 34 were assessed for full-text relevance, and 30 studies were included in the qualitative synthesis. Evidence was coded across cybersecurity education and policing, cryptocurrency fraud/literacy/risk, and digital citizenship. The synthesis identifies five persistent gaps: limited direct evidence on police-delivered education for adult crypto users, overreliance on knowledge and intention rather than observed behaviour, weak integration of crypto-specific social engineering with educational design, underdeveloped linkage between Protection Motivation Theory and digital citizenship, and an absence of directly comparable Indonesian evidence within the included corpus. The review proposes a digital civic protective capacity framework in which credible police education shapes threat and coping appraisal, interacts with actual crypto literacy and cognitive vulnerability, and produces observable protective actions and participatory reporting. The contribution is a behaviour-centred model and a set of measurable design principles for preventive policing in digital financial environments.

Article Link: <https://journal.uny.ac.id/index.php/civics/article/view/101840>

## Introduction

Digital financial participation is increasingly part of contemporary citizenship. Citizens use digital platforms not only to communicate, learn, and access public services but also to store value, invest, transact, and participate in markets that operate across institutional and



territorial boundaries. Cryptocurrency intensifies this shift because participation depends on digitally mediated decisions about platforms, wallets, credentials, information sources, and irreversible transactions. In Indonesia, the policy relevance is substantial. The Financial Services Authority reported 21.07 million crypto-asset consumer accounts by February 2026 and IDR 482.23 trillion in transaction value during 2025. The same 2026 literacy programme explicitly included a stream for law-enforcement officers, indicating that crypto literacy is now treated as both a consumer-protection and enforcement-capacity issue (Otoritas Jasa Keuangan, 2026).

The expansion of participation has been accompanied by persistent fraud risk. Cryptocurrency scams include fraudulent trading platforms, pig-butcher schemes, impersonation, phishing, fake investment communities, romance-based approaches, high-yield promises, account compromise, and manipulation through social-media or messaging channels. The threat is not reducible to a technical failure of blockchain. Bartoletti et al. (2021) and Trozze et al. (2022) show that cryptocurrency-related crime comprises diverse and changing scam types. Perdana and Jiow (2024) demonstrate that victimisation emerges at the intersection of cognitive vulnerability, social engineering, and crypto-technological characteristics. Dulisse et al. (2026) further show that impersonation and persuasion are repeated elements in verified victim narratives, with more psychologically complex scripts associated with larger losses. Prevention therefore depends on what users do at concrete decision points, not only on the security of the underlying technology.

A central problem is the knowledge-to-behaviour gap. Security awareness and literacy are necessary, but they do not guarantee protective action. Cain et al. (2018) found that cyber-hygiene knowledge and practice can diverge. The most recent meta-analysis of end-user cybersecurity training found a positive overall training effect, yet the effect on actual behaviour was considerably smaller and statistically imprecise compared with effects on knowledge, attitudes, or other behavioural predictors (Prümmer et al., 2025). This distinction matters in crypto scams because the critical outcome is not whether a user can repeat a warning. The outcome is whether the user verifies an identity, rejects abnormal returns, protects keys and authentication credentials, stops a pressured transfer, preserves evidence, and reports suspicious activity.

Police institutions occupy a distinctive preventive position. They can connect public education with complaint data, investigative knowledge, current *modus operandi*, formal reporting pathways, and the legitimacy of a public safety institution. Yet direct evidence remains thin. Within the 30-study corpus synthesised in this review, Alderman et al. (2024) is the only experimental evaluation of a police-delivered online-safety intervention. The programme improved knowledge and reporting propensity, but effects on risk perception and risky behaviour were limited. Setyawan et al. (2023) provide Indonesian qualitative evidence that police online-fraud prevention should use continuous education, multiple media, partnerships, reporting mechanisms, and victim protection, but the study is descriptive and not cryptocurrency specific. Robinson et al. (2026) shift attention to institutional capacity, finding moderate crypto literacy but weak foundational knowledge and low investigative confidence among officers with cryptocurrency experience. Together these studies suggest that police education is plausible and institutionally important, but its behavioural mechanism and crypto-specific design remain underdeveloped.

The cryptocurrency literature creates a second gap. Financial and crypto literacy can improve detection and reduce vulnerability, yet overconfidence and exposure complicate the relationship. Wei et al. (2021) found that financial literacy improves fraud-detection ability. Isaia et al. (2024) found that basic financial knowledge was protective against online financial fraud, while overconfidence increased vulnerability. Xiao et al. (2022) similarly found that financially overconfident respondents were more likely to accept abnormal investment returns as attainable. In a 2026 study of U.S. cryptocurrency investors, actual crypto literacy reduced

the odds of financial loss by about 19%, while social-media exposure increased victimisation risk and overconfidence remained common (Engle et al., 2026). These findings mean that preventive education must distinguish actual competence from perceived competence and must address the social environment in which scams are encountered.

A third gap is theoretical. Protection Motivation Theory (PMT) provides a strong explanation for why threat information may or may not generate protective action. Rogers (1975) distinguishes threat appraisal from coping appraisal, and later information-security research shows that severity, vulnerability, response efficacy, and self-efficacy can contribute to protective motivation. However, PMT does not by itself define the civic quality of the desired behaviour. Digital citizenship scholarship contributes this normative dimension. Armawi and Wahidin (2020) connect digital citizenship with literacy, commerce, and law-related competencies. Prasetyo et al. (2022) emphasise digital literacy, behavioural standards, and moral guidance. Nurjanah et al. (2024) highlight critical literacy that moves from evaluating information to concrete action. These capacities map closely onto scam prevention, yet they are rarely integrated with preventive policing and cryptocurrency-risk research.

The research gap can therefore be stated in five parts. First, there is an institutional-source gap because evidence on police-delivered cyber education is sparse, especially for adult financial users. Second, there is an outcome gap because much cybersecurity training research measures knowledge, attitudes, or intentions rather than observable protective behaviour. Third, there is a domain gap because crypto-fraud research commonly studies scam typologies, victimisation, literacy, fear, or overconfidence without examining police-originated education. Fourth, there is a mechanism-integration gap because PMT, crypto-specific cognitive vulnerability, police credibility, and digital citizenship are usually treated in separate literatures. Fifth, there is a context gap because none of the 30 included studies directly evaluates police-led preventive cyber education among adult cryptocurrency users in Indonesia. This last statement is deliberately limited to the included corpus and is not a claim that no related study exists anywhere.

This review addresses one primary research question: How can police-led preventive cyber education strengthen protective behaviour against cryptocurrency scams from a digital citizenship perspective? The review pursues three analytical objectives under that single question: to synthesise evidence on the education-to-behaviour relationship, to identify mechanisms and design conditions that make preventive education more behaviourally effective, and to develop a citizenship-oriented framework that can guide future empirical testing in the Polda Metro Jaya context.

## Method

### Review design and reporting framework

This study used a focused systematic literature review. The review followed the reporting logic of PRISMA 2020 for identification, screening, eligibility, and synthesis and used PRISMA-S principles to document search concepts and information sources (Page et al., 2021; Rethlefsen et al., 2021). The design was selected because the research question intersects criminology, policing, cybersecurity behaviour, financial and cryptocurrency literacy, risk perception, and citizenship studies. The evidence base is methodologically heterogeneous, so a qualitative thematic synthesis was more defensible than statistical pooling.

The review treated peer-reviewed studies as the evidence corpus. Foundational theory, journal-method precedents, and institutional sources were used only for conceptual or contextual support and were not counted among the 30 included studies. Rogers (1975), for example, was retained as the foundational PMT source. Otoritas Jasa Keuangan (2026) was used to establish the contemporary Indonesian crypto-literacy context. Two SLR articles previously published in *Jurnal Civics* were consulted as methodological precedents for how

systematic reviews are positioned within the target journal (Maulana & Milanti, 2023; Wicaksono & Prasetyo, 2023).

### Search strategy and information sources

The search covered January 2015 to 24 August 2026, with the exception of foundational theory cited outside the synthesis period. English- and Indonesian-language peer-reviewed journal articles were eligible. The updated retrieval used structured cross-platform scholarly searches through public publisher and index interfaces that repeatedly surfaced literature in the relevant fields, including ScienceDirect/Elsevier, SpringerLink, SAGE Journals, Emerald Insight, DOAJ and the Jurnal Civics archive. Backward and forward citation chasing was used from the dissertation seed corpus and from highly relevant reviews and meta-analyses. The approach therefore emphasised transparent reproducibility of concepts and selection decisions rather than dependence on a single proprietary bibliographic database.

Four search blocks were combined iteratively: (1) cybersecurity education terms, including ‘cybersecurity education,’ ‘cybersecurity training,’ ‘cybercrime prevention campaign,’ ‘police-delivered,’ and ‘police education,’ paired with behaviour, prevention, reporting, or risk perception; (2) cryptocurrency terms, including cryptocurrency, cryptoasset, or crypto asset, paired with fraud, scam, victimisation, literacy, overconfidence, or social engineering; (3) digital-citizenship terms, including ‘digital citizenship’ and ‘critical digital literacy,’ paired with verification, responsibility, legal awareness, or information credibility; and (4) institutional terms combining police or law enforcement with cryptocurrency or cybercrime and education, literacy, prevention, or capacity. Search wording was adjusted to the syntax and indexing behaviour of each public interface while preserving the same conceptual blocks.

**Table 1.**

#### *Search protocol and review boundaries*

| Component       | Operational decision                                                                                                                | Rationale                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Review question | Police-led preventive cyber education → protective behaviour against cryptocurrency scams, interpreted through digital citizenship. | Keeps the SLR tied to one dissertation-derived problem rather than reviewing crypto fraud in general. |
| Period          | January 2015 to 24 August 2026; foundational theory outside the window cited contextually.                                          | Captures contemporary cyber training and crypto-fraud evidence while retaining PMT foundations.       |
| Languages       | English and Indonesian.                                                                                                             | Covers the dominant international literature and Indonesian policing/citizenship evidence.            |
| Evidence type   | Peer-reviewed journal articles in the synthesis; institutional and methodological sources outside the corpus.                       | Prevents policy reports and journal guidelines from inflating the evidence count.                     |
| Search routes   | Cross-platform publisher/index search plus backward/forward citation chasing.                                                       | Reduces dependence on one database and captures multidisciplinary evidence.                           |
| Synthesis       | Thematic qualitative synthesis with an author-developed Weight of Evidence check.                                                   | Appropriate for heterogeneous experiments, surveys, qualitative studies, reviews and meta-analyses.   |

### Eligibility criteria and study selection

Studies were included when they directly contributed to at least one component of the causal or civic pathway under review: cybersecurity education/training and behaviour; police or public cybercrime-prevention interventions; financial or crypto literacy and fraud detection/victimisation; risk perception or PMT-related protective mechanisms; cryptocurrency scam techniques and social engineering; law-enforcement crypto capacity; or

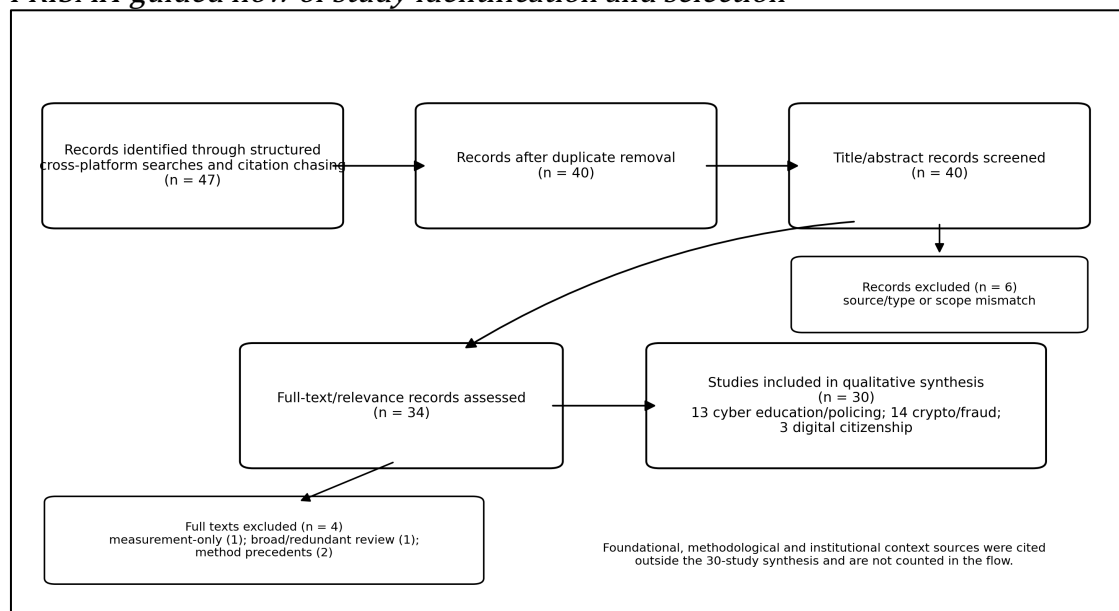
digital citizenship capacities directly relevant to verification, lawful participation, responsibility, and action. Studies had to report a sufficiently clear design, data source, method, or review procedure to permit evidence extraction.

Studies were excluded when they were purely technical blockchain-detection papers without a human-behaviour component, focused on crypto adoption or market performance without fraud-prevention outcomes, addressed regulation or money laundering without a user-protection mechanism, were non-peer-reviewed institutional reports, or discussed digital citizenship without a direct link to critical information evaluation or protective action. Measurement-only validation studies and broad reviews were excluded when they did not add unique evidence to the focused question.

The audit log contained 47 candidate records. Seven duplicate records found through more than one search route were removed. Forty unique records underwent title/abstract and document-type screening, six were excluded at that stage, and 34 proceeded to full-text or full-relevance assessment. Four were excluded after detailed assessment, leaving 30 studies in the synthesis. We logged selection decisions and then rechecked them in a second-pass consistency review against the same inclusion and exclusion rules. Figure 1 summarises the flow.

**Figure 1.**

*PRISMA-guided flow of study identification and selection*



## Data extraction and appraisal

Each included study was coded for year, context, design, sample or evidence source, focal construct, principal finding, direct relevance to the research question, and methodological limitations. The corpus was then organised into three substantive clusters: cybersecurity education/policing (13 studies), cryptocurrency fraud/literacy/risk (14 studies), and digital citizenship (3 studies). Some studies could plausibly fit more than one cluster; classification was based on their primary contribution to this review.

Because the corpus combines randomised interventions, observational surveys, qualitative studies, systematic reviews, meta-analyses, taxonomy studies, and citizenship research, a single conventional risk-of-bias instrument would not be appropriate. The review therefore used a transparent Weight of Evidence (WoE) check developed for this synthesis. Methodological strength was scored from 0 to 2, behavioural-outcome directness from 0 to 2, and topical proximity to police/crypto/fraud prevention from 0 to 2. Total scores of 5–6 were treated as High, 3–4 as Moderate, and 1–2 as Contextual. The score is an interpretive weighting

device, not a validated risk-of-bias tool, and it does not convert heterogeneous evidence into a common causal metric.

Thematic synthesis was conducted in two steps. First, findings were grouped around education effectiveness, institutional source and policing, PMT and risk appraisal, crypto-specific literacy and cognitive vulnerability, and digital citizenship. Second, we examined cross-theme relationships to identify repeated mechanisms, contradictions, boundary conditions, and missing links. The synthesis prioritised convergence across independent designs and gave greater interpretive weight to experimental, meta-analytic, representative-sample, victimisation-outcome, and directly police/crypto-relevant evidence.

Results and Discussion

Evidence profile and strength of the corpus

The 30 included studies span 2015–2026 and show a clear acceleration of scholarship after 2023. Fifteen studies were published from 2024 to 2026, reflecting the rapid maturation of both behavioural cybersecurity and cryptocurrency-fraud research. The evidence is multidisciplinary. The cybersecurity/policing cluster explains how education is designed, evaluated, and institutionally delivered. The crypto/fraud cluster explains what users must recognise and why apparently knowledgeable users remain vulnerable. The digital-citizenship cluster supplies the civic interpretation of verification, lawful participation, responsibility, and action.

The quality pattern also matters. Eleven studies received a High WoE classification because they combined stronger designs, direct behavioural/victimisation outcomes, or close topical proximity. Seventeen were Moderate, and two were Contextual. The contextual studies were retained because citizenship competence is not normally operationalised through fraud outcomes, yet they supply constructs the prevention literature lacks. The corpus therefore supports a mechanism-building synthesis rather than a claim that one homogeneous intervention has a single average effect.

Table 2.  
*Evidence profile of the 30 included studies*

| Evidence cluster                          | Studies (n) | Typical designs                                                                        | Primary contribution                                                                                            |
|-------------------------------------------|-------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Cybersecurity education and policing      | 13          | Meta-analysis, SLR, field intervention, RCT, surveys, qualitative policing study       | Education-to-behaviour evidence, source credibility, reporting, intervention design, police capacity.           |
| Cryptocurrency fraud, literacy and risk   | 14          | Representative surveys, investor surveys, scam-taxonomy/review, victim-report analysis | Crypto-specific threat scripts, objective literacy, overconfidence, social engineering, victimisation and loss. |
| Digital citizenship and critical literacy | 3           | Citizenship-education and critical-literacy studies                                    | Civic interpretation of verification, legal awareness, responsible participation and action.                    |
| WoE classification                        | 30          | High = 11; Moderate = 17; Contextual = 2                                               | Weights interpretation without forcing heterogeneous designs into one causal metric.                            |

Research gap 1: police-delivered education is institutionally plausible but empirically thin

Police are often discussed as prevention actors, but the corpus contains little direct behavioural evidence on police-delivered cyber education. Alderman et al. (2024) provide the clearest causal test. The cluster randomised trial found meaningful gains in online-safety knowledge and a stronger tendency to report incidents to police, yet changes in risk perception and risky behaviour were limited. This finding is especially important because it separates

institutional legitimacy and reporting from behavioural safety. Police can improve what citizens know and how willing they are to engage the institution, but those gains do not guarantee safer choices under pressure.

Indonesian evidence is even more preliminary. Setyawan et al. (2023) describe police strategies for building public awareness of online fraud and recommend continuity, varied media, partnerships, reporting applications, and victim protection. The study is valuable because it is embedded in Indonesian policing practice, but it does not estimate behavioural effects and is not crypto-specific. Robinson et al. (2026) add a supply-side problem: credible education depends on police capacity. Officers with cryptocurrency experience still reported uneven knowledge and limited confidence in investigative tasks. Preventive education therefore cannot be designed only as a communication problem. It also requires institutional competence, current threat intelligence, and an official information pathway that users can verify.

This institutional-source gap is the first major reason a focused SLR is needed. Existing findings support police involvement, but the evidence does not yet establish the magnitude, durability, or adult crypto-specific effect of police education. Future empirical work should therefore measure both source-related mechanisms, such as legitimacy and credibility, and user-level behavioural outcomes.

## **Research gap 2: cybersecurity education improves predictors more reliably than behaviour**

The second gap concerns outcomes. Prümmer et al. (2024) identified 142 cybersecurity-training studies and found that most reported positive effects, but designs were heterogeneous, sample sizes were often small, and many evaluations relied on knowledge, attitudes, or intentions. Their 2025 meta-analysis sharpened the concern. Across 69 eligible studies, the overall training effect was positive ( $d = 0.75$ ), while effects on behavioural predictors were larger ( $d = 1.02$ ) than effects on behaviour itself ( $d = 0.36$ , 95% CI  $[-0.09, 0.80]$ ). The confidence interval for the behavioural estimate included zero. This is not evidence that training is useless. It is evidence that training effectiveness depends on what is measured and how closely the outcome approximates real protective action.

Cain et al. (2018) reach a similar conclusion from cyber-hygiene data: knowing safe practices does not ensure consistent execution. Kemp (2023) also found that awareness of public cybersecurity schemes related to secure practices among businesses but did not clearly translate into lower victimisation. These results suggest a measurement hierarchy. Programme reach, views, attendance, or recall are outputs. Knowledge and intention are proximal outcomes. Simulated decisions, observed security behaviour, verified reporting, victimisation, and financial loss are more behaviourally consequential outcomes.

For police-led cryptocurrency education, this hierarchy should shape evaluation. A strong programme should test whether recipients can identify a fake domain, compare a claim with an official source, reject an abnormal return promise, avoid moving communication into a controlled private group, refuse requests for credentials or seed phrases, stop a transfer under pressure, preserve screenshots or transaction identifiers, and report the attempt through a legitimate channel. These measures are closer to the point at which victimisation is interrupted.

## **Research gap 3: crypto literacy is protective only when it is objective, applied and resistant to manipulation**

The crypto/fraud evidence shows that literacy matters, but the protective relationship is conditional. Wei et al. (2021) found stronger fraud-detection ability among more financially literate households. Isaia et al. (2024) found lower online financial-fraud victimisation among people with stronger basic financial knowledge, while overconfidence increased vulnerability. Ibrushi et al. (2026) similarly found that financial literacy was associated with lower fraud

victimisation and stronger scam awareness, with particular relevance for cryptocurrency investors.

The distinction between actual and perceived knowledge is especially important in digital-asset markets. Xiao et al. (2022) show that overconfident respondents are more willing to believe implausibly high investment returns. Dulisse et al. (2024) demonstrate that a strong cryptoculture of confidence, knowledge, and participation can coexist with fraud susceptibility. Engle et al. (2026) provide the clearest recent evidence: objective crypto literacy was protective against financial loss, but greater exposure to crypto-related social media increased victimisation risk and 35.5% of respondents were overconfident. Education must therefore teach not only content but calibration. Users need to know what they know, recognise what they do not know, and use independent verification when confidence is unsupported by evidence.

Crypto-specific content also matters. Bartoletti et al. (2021) and Trozze et al. (2022) show that fraud typologies are diverse. Perdana and Jiow (2024) explain why: scams combine cognitive predispositions, social engineering, and technological features. Dulisse et al. (2025) identify fraudulent trading platforms, pig-butcher, impersonation, social media, and messaging as recurring elements. Dulisse et al. (2026) show that attackers use repeatable psychological tactics rather than random persuasion. Static warnings therefore have a short shelf life. Prevention should teach transferable decision rules and scam scripts that remain useful even when brands, platforms, faces, and stories change.

#### **Research gap 4: risk perception must be separated from fear and connected to coping efficacy**

PMT provides the clearest behavioural mechanism for integrating the evidence. Threat appraisal asks whether the threat is serious and whether the individual is vulnerable. Coping appraisal asks whether a recommended response works and whether the individual can perform it. Sommestad et al. (2015) found PMT particularly useful for voluntary and self-directed information-security behaviour. Jansen and van Schaik (2019) show that theory-based phishing messages can improve relevant cognitions when threat and coping arguments are strong.

The crypto-fraud evidence indicates why threat appraisal must be carefully specified. Qu et al. (2024) found that fear and perceived risk of cyber fraud correlate differently. Vicarious victimisation, perceived seriousness, and satisfaction with police were associated with perceived risk, while fear followed a different pattern. Engle et al. (2025) likewise found that crypto literacy was not consistently associated with fear of online fraud. These studies caution against treating fear, risk perception, knowledge, and efficacy as interchangeable. A user may understand the threat but feel invulnerable. Another may fear fraud but not know what response is effective. A third may know what to do but believe the steps are too difficult.

This distinction changes the design of police messages. A threat warning should establish realistic vulnerability and consequence without creating helplessness. A coping message should immediately provide a small number of actions that are demonstrably effective and feasible. For example, a warning about impersonation should include how to verify the official account; a warning about a trading platform should include how to check regulatory status and domain legitimacy; and a warning about urgent transfer requests should include a stop-transfer rule and a reporting pathway.

#### **Research gap 5: the civic meaning of protective behaviour is underdeveloped**

Cybersecurity and fraud studies usually frame safe behaviour as individual risk management. Digital citizenship broadens the unit of analysis. Armawi and Wahidin (2020) position digital citizenship across literacy, access, commerce, and law. Prasetyo et al. (2022) emphasise behavioural standards and moral guidance. Nurjanah et al. (2024) argue that critical

literacy must culminate in concrete action. These ideas are directly relevant to crypto scams because citizens must evaluate information, understand institutional legitimacy, act responsibly in transactions, and support collective security through reporting.

The review therefore introduces the concept of digital civic protective capacity. It refers to citizens' ability to recognise and evaluate digital-financial threats, take effective protective action, use lawful and verifiable institutional pathways, and contribute information that can protect the wider community. The concept has four dimensions: critical verification, legal-institutional awareness, protective digital responsibility, and participatory reporting. The first three protect the individual. The fourth creates a civic feedback loop because reports can reveal emerging scam scripts, accounts, platforms, and contact patterns that improve subsequent warnings.

This civic framing also clarifies why police involvement is theoretically distinctive. A private platform can teach account security. A financial educator can teach investment fundamentals. Police can connect threat recognition with public safety, evidence preservation, reporting, and collective prevention. The added value is strongest when police education is credible, technically accurate, behaviourally actionable, and coordinated with regulators and licensed market actors.

**Table 3.**

*Systematic evidence matrix of the 30 included studies*

| No. | Study and design/context                                                                   | Primary focus                                      | Key finding and role in this review                                                                                                                                                       | WoE      |
|-----|--------------------------------------------------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 1   | Sommestad et al. (2015)<br>Meta-analysis; 28 information-security surveys                  | PMT and security behaviour                         | PMT explains voluntary, specific and self-directed security behaviour better than generic compliance. Supports threat/coping appraisal as a mechanism, but not police or crypto specific. | Moderate |
| 2   | Cain et al. (2018)<br>Cross-sectional survey; 268 technology users                         | Cyber-hygiene knowledge and behaviour              | Knowledge and security practice do not consistently align. Establishes the knowledge-to-behaviour gap that prevention programmes must address.                                            | Moderate |
| 3   | Jansen & van Schaik (2019)<br>Theory-based pretest-posttest intervention; 768 participants | Phishing prevention                                | Strong threat and coping arguments can improve security cognitions and behavioural intention. Shows why preventive messages need actionable efficacy, not threat information alone.       | Moderate |
| 4   | Bada & Nurse (2019)<br>Scoping review and applied SME case evidence                        | Cybersecurity education and awareness              | Programmes work better when tailored to audience needs, organisational context, and usable practices. Supports relevance, tailoring and applied guidance in police education.             | Moderate |
| 5   | Drew (2020)<br>Survey; 595 Australian adults                                               | Cybercrime victimisation and prevention strategies | Perceived prevalence and harm are associated with use of online prevention strategies. Supports risk appraisal as a bridge between awareness and protective action.                       | Moderate |
| 6   | Back & Guerette (2021)<br>Field intervention;                                              | Cyber place management and phishing                | Training can alter concrete responses to phishing threats in a managed digital environment.                                                                                               | High     |

| No. | Study and design/context                                                                  | Primary focus                                          | Key finding and role in this review                                                                                                                                                                                                            | WoE      |
|-----|-------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 7   | anti-phishing awareness training<br>Khando et al. (2021)<br>Systematic literature review  | Information-security awareness                         | Provides behavioural evidence for scenario-based prevention. Awareness interventions vary widely; organisational support, delivery design and user factors shape outcomes. Supports theory-informed, repeated and context-sensitive education. | Moderate |
| 8   | Wei et al. (2021)<br>Nationally representative household survey, China                    | Financial literacy and fraud detection                 | Higher financial literacy is associated with stronger fraud-detection ability. Shows that evaluative literacy contributes to recognising deceptive offers.                                                                                     | Moderate |
| 9   | Bartoletti et al. (2021)<br>Literature and open-source scam taxonomy                      | Cryptocurrency scams                                   | Crypto scams are heterogeneous and require consistent classification and detection. Shows why educational content must be pattern-based and regularly updated.                                                                                 | Moderate |
| 10  | Xiao et al. (2022)<br>Nationally representative survey, China                             | Financial-literacy overconfidence and investment fraud | Overconfidence increases acceptance of implausibly high returns and fraud vulnerability. Identifies a cognitive vulnerability that education must explicitly counter.                                                                          | Moderate |
| 11  | Trozze et al. (2022)<br>PRISMA-ScR scoping review plus expert consultation                | Cryptocurrency-related financial crime                 | Identified 47 crypto-related crime/fraud types and emphasised terminology and data-sharing gaps. Provides the threat taxonomy needed for targeted preventive content.                                                                          | Moderate |
| 12  | Setyawan et al. (2023)<br>Qualitative study; Cimahi Police, Indonesia                     | Police strategy for online-fraud awareness             | Continuous education, multiple media, partnerships, reporting channels and victim protection were recommended. Direct Indonesian policing evidence, but descriptive and not crypto specific.                                                   | Moderate |
| 13  | Kemp (2023)<br>Bayesian model averaging; 5,872 UK businesses                              | Public cybercrime-prevention campaigns                 | Campaign awareness is associated with security practices, but not clearly with lower victimisation. Demonstrates that exposure/output metrics cannot substitute for behavioural outcomes.                                                      | High     |
| 14  | Hadan et al. (2024)<br>Online survey; 413 investors/potential investors from 23 countries | Cryptocurrency education and gamification              | Users prefer dynamic, accessible, reliable, tailored and community-building learning. Specifies design requirements for crypto-specific prevention education.                                                                                  | Moderate |
| 15  | Alderman et al. (2024)<br>Cluster randomised controlled trial;                            | Police-delivered online-safety education               | Police delivery improved knowledge and reporting propensity; effects on risk perception and risky behaviour                                                                                                                                    | High     |

| No. | Study and design/context                                                       | Primary focus                                 | Key finding and role in this review                                                                                                                                                                             | WoE      |
|-----|--------------------------------------------------------------------------------|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|     | 1,954 participants in 100 groups                                               |                                               | were limited. Strongest direct evidence that police education can help but does not automatically change behaviour.                                                                                             |          |
| 16  | Isaia et al. (2024)<br>Representative survey; 5,009 Italian adults             | Financial literacy and online financial fraud | Basic financial knowledge is protective, while literacy overconfidence increases victimisation risk. Supports objective literacy plus debiasing, especially under high digital exposure.                        | High     |
| 17  | Perdana & Jiow (2024)<br>Analysis of 204 government-reported crypto scam cases | Crypto-cognitive exploitation                 | Scams combine cognitive vulnerability, social engineering and crypto-technological features across seven dimensions. Provides a mechanism for designing psychologically informed crypto education.              | High     |
| 18  | Qu et al. (2024)<br>Survey; 1,065 Chinese university students                  | Fear and perceived risk of cyber fraud        | Perceived risk is related to vicarious victimisation, seriousness and satisfaction with police, distinct from fear. Supports treating risk perception as a specific cognitive construct, not as fear.           | Moderate |
| 19  | Dulisse et al. (2024)<br>Survey; 919 prior cryptocurrency purchasers           | Cryptoculture, fraud and loss                 | High confidence and participation in cryptoculture can coexist with fraud susceptibility and loss. Shows why self-confidence is not a substitute for actual crypto literacy.                                    | High     |
| 20  | Prümmer et al. (2024)<br>Systematic review; 142 cybersecurity-training studies | Cybersecurity training methods                | Most studies report positive effects, but designs are heterogeneous and often rely on non-behavioural outcomes. Defines the broader evidence base and its methodological weaknesses.                            | Moderate |
| 21  | Engle et al. (2025)<br>Survey; 433 college undergraduates                      | Crypto literacy and fear of online fraud      | Crypto literacy is not consistently associated with fear across fraud domains. Confirms that knowledge, fear and risk appraisal should be measured separately.                                                  | Moderate |
| 22  | Prümmer et al. (2025)<br>Meta-analysis; 69 eligible studies                    | Effect of cybersecurity training              | Overall training effect was positive, but the behavioural effect was small and imprecise ( $d = 0.36$ , 95% CI [-0.09, 0.80]). Provides the strongest quantitative evidence for the knowledge-to-behaviour gap. | High     |
| 23  | Dulisse et al. (2025)<br>Two U.S. state                                        | Scam types, contacts and losses               | Fraudulent trading platforms and pig-butcherings were prevalent; social media,                                                                                                                                  | High     |

| No. | Study and design/context                                                                 | Primary focus                                              | Key finding and role in this review                                                                                                                                                                                      | WoE        |
|-----|------------------------------------------------------------------------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|     | crypto-scam trackers                                                                     |                                                            | messaging and impersonation were prominent contact mechanisms. Identifies concrete scripts and channels for case-based education.                                                                                        |            |
| 24  | Robinson et al. (2026)<br>Survey; 104 U.S. officers with cryptocurrency experience       | Law-enforcement crypto knowledge and capacity              | Officers show moderate overall literacy but weak foundations and low investigative confidence/readiness. Identifies institutional-capacity constraints on credible police-delivered education.                           | Moderate   |
| 25  | Engle et al. (2026)<br>Survey of U.S. cryptocurrency investors                           | Actual vs perceived crypto literacy and financial loss     | Actual crypto literacy reduced loss odds by about 19%; social-media exposure increased victimisation risk; overconfidence was common. Directly supports objective literacy, debiasing and social-media risk education.   | High       |
| 26  | Ibrushi et al. (2026)<br>2024 U.S. National Financial Capability Study                   | Financial literacy, fraud victimisation and scam awareness | Financial literacy is associated with lower fraud victimisation and higher scam awareness, with strong relevance for crypto investors. Shows literacy can support both detection and loss prevention in digital finance. | High       |
| 27  | Dulisse et al. (2026)<br>Systematic coding of 282 verified crypto-scam victim narratives | Social-engineering tactics and techniques                  | Impersonation and persuasion dominate; higher psychological complexity is associated with larger losses. Supports psychologically informed, script-based education and structured reporting.                             | High       |
| 28  | Armawi & Wahidin (2020)<br>Citizenship-education study, Indonesia                        | Digital citizenship                                        | Digital citizenship includes digital access, literacy, commerce and law-related capacities. Provides the civic frame for safe participation in digital economic life.                                                    | Contextual |
| 29  | Prasetyo et al. (2022)<br>Qualitative NVivo study with student teachers                  | Digital citizenship understanding                          | Digital literacy, behavioural standards and moral guidance are central to digital citizenship. Extends prevention from individual safety towards responsible digital conduct.                                            | Contextual |
| 30  | Nurjanah et al. (2024)<br>Critical-literacy study of young citizens                      | Critical literacy in the digital era                       | Critical literacy requires evaluating information and translating knowledge into concrete action. Supports verification and action as civic capabilities, not only knowledge.                                            | Moderate   |

## Integrated synthesis: from police communication to digital civic protective capacity

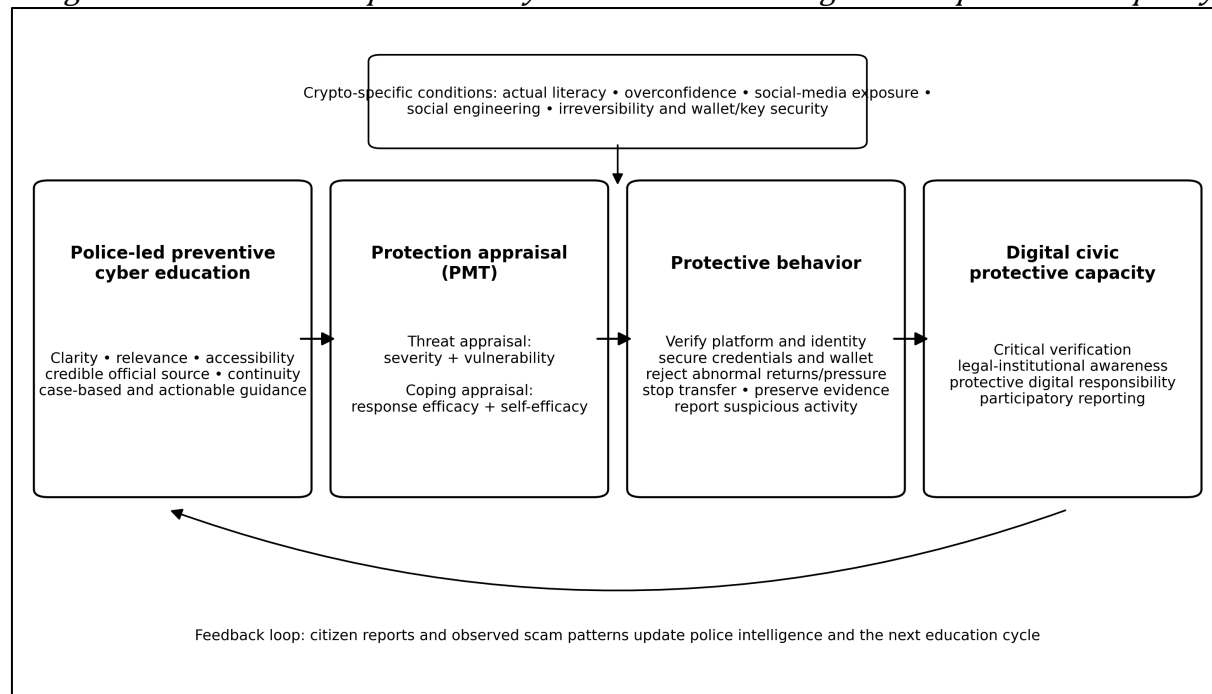
The evidence converges on a sequential but conditional mechanism. Police-led preventive cyber education provides an external informational stimulus. Its quality depends on clarity, relevance to current modus operandi, accessibility, channel appropriateness, continuity, source credibility, and practical usefulness. These features are consistent with the underlying dissertation construct and are also supported by the broader training literature, which favours tailored, repeated, active and actionable learning over undifferentiated awareness exposure.

The educational stimulus then enters a protection-appraisal process. Threat appraisal concerns whether a user recognises personal vulnerability and the seriousness of consequences. Coping appraisal concerns whether the recommended response is effective and feasible. This stage is moderated by crypto-specific conditions. Actual crypto literacy improves technical understanding. Overconfidence can weaken calibration. Social-media exposure can increase both information and victimisation opportunities. Social engineering can exploit authority, familiarity, urgency, reciprocity, FOMO, sunk-cost thinking, and trust. Transaction irreversibility and key-management requirements increase the cost of mistakes.

The immediate target is observable protective behaviour. The review identifies five behavioural families: verification, credential/wallet protection, refusal or interruption of risky transactions, evidence preservation, and reporting. These actions are then interpreted as civic capabilities. Critical verification supports informed judgement. Legal-institutional awareness helps citizens distinguish legitimate actors and official pathways. Protective digital responsibility reflects disciplined participation in digital economic life. Participatory reporting converts private threat experience into public safety information. Figure 2 summarises this integrated mechanism.

**Figure 2.**

*Integrated framework for police-led cyber education and digital civic protective capacity*



## Novelty and contribution

The first novelty is conceptual integration. Previous studies provide strong pieces of the problem but rarely connect them in one framework. Cybersecurity training research explains intervention effects and the knowledge-to-behaviour gap. PMT explains threat and coping appraisal. Crypto-fraud research explains social engineering, technological constraints, objective literacy and overconfidence. Policing research contributes institutional source,

legitimacy, reporting and capacity. Digital citizenship contributes the civic meaning of responsible, critical and lawful participation. The present review integrates these elements into a single behaviour-centred model.

The second novelty is the construct of digital civic protective capacity. The construct shifts the endpoint from passive awareness to demonstrated citizen capability. It treats verification, safe transaction behaviour, evidence preservation, and reporting as connected civic-security practices. This is particularly relevant to Jurnal Civics because the framework links media and information literacy, law awareness, civic responsibility, and civic skills to a concrete contemporary form of digital economic participation.

The third novelty is an evaluation distinction between programme outputs and protective outcomes. Social-media reach, event attendance, video views, and knowledge scores can document delivery, but they do not show whether users can interrupt victimisation. The review proposes that programme evaluation should prioritise behavioural tasks and follow-up outcomes. This distinction is supported by the meta-analytic evidence that training effects shrink when measurement moves from predictors towards actual behaviour.

The fourth novelty is a reciprocal prevention model. Most educational models are linear: institution sends message, user receives message. The civic framework adds a feedback loop. Citizens who report suspicious interactions generate data that can update police threat intelligence, which can then update the next cycle of preventive education. This transforms reporting from an after-the-fact administrative act into a component of community-based digital prevention.

**Table 4.**

*Sharpened research gap and novelty statement*

| Gap in existing literature | Evidence from the SLR                                                                                                    | Novel contribution                                                                                                      | Empirical implication                                                                                           |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Institutional-source gap   | Police-delivered experimental evidence is scarce; Indonesian evidence is descriptive; officer crypto capacity is uneven. | Positions police credibility, competence and reporting pathways as part of the intervention.                            | Measure source credibility/legitimacy and exposure to police education separately from content knowledge.       |
| Behavioural-outcome gap    | Meta-analysis shows weaker effects for behaviour than for knowledge/predictors.                                          | Distinguishes delivery outputs, proximal outcomes, and protective behaviour.                                            | Use scenario tasks, simulated verification, reporting, and follow-up measures.                                  |
| Crypto-domain gap          | Crypto studies emphasise typology, literacy, victimisation, fear, or overconfidence rather than police education.        | Embeds crypto-specific social engineering and transaction characteristics in education design.                          | Use current scam scripts, wallets/keys, platform legitimacy, irreversible transfers, and social-media pathways. |
| Mechanism-integration gap  | PMT, police legitimacy, crypto cognition and digital citizenship are largely separate literatures.                       | Digital civic protective capacity framework integrates threat/coping appraisal with civic responsibility and reporting. | Test direct and indirect pathways from education to appraisal to behaviour.                                     |

| Gap in existing literature | Evidence from the SLR                                                                          | Novel contribution                                                                                              | Empirical implication                                                               |
|----------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Indonesian-context gap     | No included study directly evaluates police-led education among adult Indonesian crypto users. | Produces a context-ready model for future Polda Metro Jaya testing without claiming evidence not yet available. | Recruit actual crypto users and distinguish behaviour from self-reported agreement. |

### Design implications for preventive policing in the Polda Metro Jaya context

The SLR does not establish the size of an educational effect in Jakarta, but it provides a defensible design architecture for empirical testing. First, educational content should be case-based and updated from current complaint and investigative patterns. The objective is to recognise transferable scam scripts, not memorise yesterday's brand names. Second, every threat cue should be coupled with an action. Users should be shown what to verify, where to verify it, when to stop, what evidence to preserve, and where to report.

Third, education should make efficacy visible. Short demonstrations can show that checking a domain, using an official application, verifying a licensed provider, enabling strong authentication, protecting private keys, and pausing under pressure are feasible behaviours. Fourth, delivery should be repeated and multi-channel because victimisation occurs across social media, messaging applications, websites, phone calls, advertisements, and interpersonal referrals. Hadan et al. (2024) suggest that dynamic, accessible and tailored learning is particularly relevant to crypto users.

Fifth, the audience should be segmented by experience and exposure. Beginners need foundational rules about custody, keys, irreversibility, provider legitimacy and common scam scripts. Experienced users may need advanced material on impersonation, transaction tracing basics, complex social engineering, deepfake-enabled authority cues, and overconfidence. Sixth, police educators themselves need continuing crypto competence. Robinson et al. (2026) show that law-enforcement capacity cannot be assumed merely because officers have encountered cryptocurrency cases.

Seventh, evaluation should be behavioural and longitudinal. Immediate post-session knowledge is insufficient. A stronger design would include baseline and post-intervention scenario tasks, a follow-up period, and measures of verified behaviour where ethically feasible. Suggested outcomes include correct identification of suspicious decision points, correct use of official verification routes, secure credential choices, refusal of pressured transfers, quality of evidence preservation, reporting intention, actual reporting where available, and later exposure or victimisation outcomes.

Finally, prevention should be collaborative without diluting institutional accountability. OJK's 2026 literacy agenda already identifies public, academic/developer, and law-enforcement literacy streams. A police-led model can connect with regulators, licensed crypto providers, universities, banks, digital platforms, and user communities while retaining a clear official source. The objective is not to promote cryptocurrency investment. It aims to strengthen citizens' capacity to participate, or choose not to participate, based on verified information and safe decision rules.

**Table 5.**

#### *Evidence-based design principles and measurable indicators*

| Design principle     | Operational content                                                                  | Target mechanism                                | Illustrative indicator                                                  |
|----------------------|--------------------------------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------|
| Case-based relevance | Current scam scripts, channels, impersonation patterns and withdrawal-fee sequences. | Threat recognition and realistic vulnerability. | Correctly identifies the first suspicious decision point in a scenario. |

| Design principle                      | Operational content                                                                                | Target mechanism                         | Illustrative indicator                                                             |
|---------------------------------------|----------------------------------------------------------------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------|
| Action coupling                       | Verification, official-source checking, account protection, stop-transfer and evidence rules.      | Response efficacy.                       | Selects the correct protective response for a given cue.                           |
| Efficacy demonstration                | Short guided practice using official verification and reporting pathways.                          | Self-efficacy and lower response cost.   | Completes a verification/reporting task without external assistance.               |
| Debiasing                             | Abnormal-return examples, overconfidence calibration, FOMO, urgency, authority and sunk-cost cues. | Reduced cognitive vulnerability.         | Rejects an implausible offer despite persuasive social proof.                      |
| Audience segmentation                 | Beginner, experienced, high-exposure, student, older-user and high-value-user variants.            | Relevance and cognitive load management. | Higher scenario accuracy within targeted risk segments.                            |
| Continuity and multi-channel delivery | Repeated official messages across social media, community events, campuses and partner channels.   | Retention and retrieval under pressure.  | Maintains knowledge and simulated behaviour at follow-up.                          |
| Participatory reporting               | Evidence preservation, reporting routes and explanation of collective prevention value.            | Civic efficacy and institutional trust.  | Reports suspicious activity with sufficient evidence through a legitimate channel. |
| Behaviour-centred evaluation          | Baseline, post-test, simulation and follow-up measures.                                            | Translation from cognition to action.    | Observed protective behaviour, not only recall or agreement.                       |

### Limitations of the review

This review has four limitations. First, retrieval used a transparent cross-platform public search rather than export-level searches from proprietary databases such as Scopus or Web of Science. The review is therefore systematic in its documented question, search blocks, eligibility rules, audit log, and synthesis, but it should not be interpreted as a claim of exhaustive global retrieval. A future update can replicate the search strings in subscription databases and compare incremental yield.

Second, the review combines heterogeneous designs and outcomes. This breadth is necessary for an interdisciplinary question, but it prevents a single pooled effect estimate. The author-developed WoE check supports interpretation but is not a validated risk-of-bias instrument. Third, selection and coding used a logged second-pass consistency review rather than independent dual human screening. Future updates should use two independent reviewers and report inter-reviewer agreement. Fourth, only three included studies directly supplied a digital-citizenship frame. This reflects the very gap the article identifies, but it means the civic synthesis is theory-building and requires empirical validation.

### Conclusion

This PRISMA-guided systematic literature review examined one question: how police-led preventive cyber education can strengthen protective behaviour against cryptocurrency scams from a digital citizenship perspective. The 30-study synthesis supports a qualified answer. Education can improve protective capacity, but knowledge acquisition is not equivalent to behavioural change. The strongest meta-analytic evidence shows that cybersecurity training has larger effects on knowledge and behavioural predictors than on behaviour itself. Police delivery adds potential value through credible threat intelligence, public authority, reporting

pathways, and community partnership, yet direct crypto-specific experimental evidence remains absent within the included corpus.

The review identifies five gaps: limited evidence on police-delivered education for adult crypto users, weak behavioural measurement, insufficient integration of crypto-specific social engineering into education, separation between PMT and digital citizenship, and lack of directly comparable Indonesian evidence. It responds by proposing digital civic protective capacity. In this framework, clear and credible police education shapes threat and coping appraisal, interacts with actual literacy and cognitive vulnerability, produces observable protective behaviour, and culminates in critical verification, legal-institutional awareness, protective digital responsibility, and participatory reporting.

The principal practical implication is that preventive cyber education should be designed as behaviour training rather than information distribution. The principal theoretical implication is that crypto-scam prevention can be understood as a citizenship-capacity issue because safe digital-financial participation requires critical judgement, lawful institutional navigation, responsible action, and contribution to collective security. For future research in the Polda Metro Jaya context, the next step is empirical testing with actual cryptocurrency users, using behaviour-centred measures and a model that distinguishes police education, risk appraisal, crypto literacy, efficacy, and protective action.

### Authors' contributions

Candra Gunawan: Conceptualisation, methodology, literature search and screening, data extraction and appraisal, formal analysis, visualisation, writing – original draft, and writing – review and editing. Chryshnanda Dwilaksana: Supervision, validation, and writing – review and editing. Supardi Hamid: Supervision, validation, and writing – review and editing. Yopik Gani: Supervision, validation, and writing – review and editing. All authors read and approved the final manuscript.

### Competing interests

Conflicts of Interest: The authors declare no conflicts of interest.

### Funding Statement

This research did not receive funding.

### Ethics Approval

This systematic literature review used published and publicly available scholarly or institutional sources and did not involve human participants, personal data collection, or experimental intervention. Ethical approval was therefore not required.

### References

- Alderman, T., Ariel, B., & Harinam, V. (2024). Can a police-delivered intervention improve children's online safety? A cluster randomised controlled trial on the effect of the ThinkUKnow programme in primary and secondary Australian schools. *Journal of Experimental Criminology*, 20, 617–634. <https://doi.org/10.1007/s11292-023-09551-3>
- Armawi, A., & Wahidin, D. (2020). Optimalisasi peran internet dalam mewujudkan digital citizenship dan implikasinya terhadap ketahanan pribadi siswa [Optimising the role of the internet in realising digital citizenship and its implications for students' personal resilience]. *Jurnal Civics: Media Kajian Kewarganegaraan*, 17(1), 29–39. <https://doi.org/10.21831/jc.v17i1.30146>
- Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice*, 37(3), 427–451. <https://doi.org/10.1177/10439862211001628>

- Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access*, 9, 148353–148373. <https://doi.org/10.1109/ACCESS.2021.3123894>
- Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. <https://doi.org/10.1016/j.jisa.2018.08.002>
- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17–33. <https://doi.org/10.1108/JCRPP-12-2019-0070>
- Dulisse, B. C., Connealy, N., & Logan, M. W. (2024). ‘Get rich quick,’ scheme or script? The effect of cryptoculture on the susceptibility of fraud victimization among cryptocurrency purchasers. *Journal of Criminal Justice*, 94, Article 102273. <https://doi.org/10.1016/j.jcrimjus.2024.102273>
- Dulisse, B., Fitch, C., & Connealy, N. (2026). The scammer’s playbook: Exploring the psychological techniques and tactics used by scammers in the social engineering of cryptocurrency fraud. *Journal of Economic Criminology*, 11, Article 100211. <https://doi.org/10.1016/j.jeconc.2026.100211>
- Dulisse, B., Fitch, C., Denis, J., & Connealy, N. (2025). Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency. *Journal of Economic Criminology*, 9, Article 100178. <https://doi.org/10.1016/j.jeconc.2025.100178>
- Engle, T. A., Connealy, N., & Dulisse, B. C. (2026). Trust me bro: An examination of the influence of cryptocurrency literacy and overconfidence on victimization and financial loss. *Technology in Society*, 86, Article 103277. <https://doi.org/10.1016/j.techsoc.2026.103277>
- Engle, T. A., Maher, C. A., & Jones, M. (2025). Afraid of the unknown: Crypto literacy and fear of online fraud. *Journal of Economic Criminology*, 7, Article 100135. <https://doi.org/10.1016/j.jeconc.2025.100135>
- Hadan, H., Zhang-Kennedy, L., Nacke, L. E., & Mäkelä, V. (2024). Gamification and gaming in cryptocurrency education: A survey with cryptocurrency investors and potential investors. *Simulation & Gaming*, 55(2), 196–223. <https://doi.org/10.1177/10468781231223762>
- Ibrushi, D., Palacios Diaz, M., & Wang, S. (2026). Financial literacy and fraud vulnerability in digital finance: Evidence from the 2024 NFCS. *Finance Research Letters*, 94, Article 109674. <https://doi.org/10.1016/j.frl.2026.109674>
- Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance*, 44, Article 100977. <https://doi.org/10.1016/j.jbef.2024.100977>
- Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, 123, 40–55. <https://doi.org/10.1016/j.ijhcs.2018.10.004>
- Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security*, 127, Article 103089. <https://doi.org/10.1016/j.cose.2022.103089>

- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, Article 102267. <https://doi.org/10.1016/j.cose.2021.102267>
- Maulana, M. Y., & Milanti, A. A. (2023). A systematic literature review on civic engagement program through citizenship education. *Jurnal Civics: Media Kajian Kewarganegaraan*, 20(2), 341–358. <https://doi.org/10.21831/jc.v20i2.66024>
- Nurjanah, N., Abdulkarim, A., Komalasari, K., Bestari, P., & Suwandi, M. A. (2024). Critical literacy of young citizens in the digital era. *Jurnal Civics: Media Kajian Kewarganegaraan*, 21(2), 352–358. <https://doi.org/10.21831/jc.v21i2.70232>
- Otoritas Jasa Keuangan. (2026, April 7). *OJK minta masyarakat pahami fundamental data sebelum investasi kripto: Pembukaan Bulan Literasi Kripto (BLK) 2026* [OJK asks the public to understand fundamental data before investing in crypto: Opening of Crypto Literacy Month 2026] [Press release]. [https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Pembukaan-Bulan-Literasi-Kripto-\(BLK\)-2026.aspx](https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Pembukaan-Bulan-Literasi-Kripto-(BLK)-2026.aspx)
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, Article n71. <https://doi.org/10.1136/bmj.n71>
- Perdana, A., & Jiow, H. J. (2024). Crypto-cognitive exploitation: Integrating cognitive, social, and technological perspectives on cryptocurrency fraud. *Telematics and Informatics*, 95, Article 102191. <https://doi.org/10.1016/j.tele.2024.102191>
- Prasetyo, W. H., Naidu, N. B. M., Tan, B. P., & Sumardjoko, B. (2022). 'It really needs to be given to students': Digital citizenship understanding amongst student teachers qualitative NVivo analysis. *Jurnal Civics: Media Kajian Kewarganegaraan*, 19(1), 9–20. <https://doi.org/10.21831/jc.v19i1.46888>
- Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, Article 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security*, 150, Article 104206. <https://doi.org/10.1016/j.cose.2024.104206>
- Qu, J., Lin, K., Wu, Y., & Sun, I. Y. (2024). Fear and perceived risk of cyber fraud victimization among Chinese university students. *Crime, Law and Social Change*, 82, 543–562. <https://doi.org/10.1007/s10611-024-10155-9>
- Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., Koffel, J. B., & PRISMA-S Group. (2021). PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic reviews. *Systematic Reviews*, 10, Article 39. <https://doi.org/10.1186/s13643-020-01542-z>
- Robinson, C. G., Logan, M. W., Dulisse, B. C., & Connealy, N. T. (2026). Cops and crypto: Law enforcement knowledge, experience, and capacity in cryptocurrency crime. *Journal of Criminal Justice*, 103, Article 102596. <https://doi.org/10.1016/j.jcrimjus.2026.102596>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Setyawan, A., Setyabudi, C. M., & Nita, S. (2023). Strategy to build public awareness in preventing online fraud crimes in the jurisdiction of the Cimahi Police. *International*

*Journal of Social Service and Research*, 3(10), 2641–2649.  
<https://doi.org/10.46799/ijssr.v3i10.563>

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, 9(1), 26–46.  
<https://doi.org/10.4018/IJISP.2015010102>

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11, Article 1.  
<https://doi.org/10.1186/s40163-021-00163-8>

Wei, L., Peng, M., & Wu, W. (2021). Financial literacy and fraud detection: Evidence from China. *International Review of Economics & Finance*, 76, 478–494.  
<https://doi.org/10.1016/j.iref.2021.06.017>

Wicaksono, R. B., & Prasetyo, W. H. (2023). Digital competence for students in the networking society 5.0: A systematic review. *Jurnal Civics: Media Kajian Kewarganegaraan*, 20(2), 412–425. <https://doi.org/10.21831/jc.v20i2.51673>

Xiao, X., Li, X., & Zhou, Y. (2022). Financial literacy overconfidence and investment fraud victimization. *Economics Letters*, 212, Article 110308.  
<https://doi.org/10.1016/j.econlet.2022.110308>