International Journal Software Engineering and Computer Science (IJSECS)
6 (1), 2026, 25-33
Published Online April 2026 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v6i1.6345.

RESEARCH ARTICLE Open Access

Preventing Crypto Scams Through Digital Literacy and Cyber Security

Muhammad Dzaky Maulana [1*], **Agus Juhana** [2]

[1*,2] Department of Multimedia Education, Indonesia University of Education, Bandung City, West Java Province, Indonesia.

**Corresponding author*: muhammaddzakymaulana@upi.edu

Received: January 15, 2026; Accepted: February 2, 2026; Published: April 1, 2026.

Abstract: Blockchain-based financial technology has reshaped how digital transactions are conducted, yet its rapid adoption has simultaneously expanded the attack surface for a specific class of cybercrime — cryptocurrency fraud. This study examines how digital literacy education and cybersecurity practices, when applied in combination, can reduce the vulnerability of crypto asset holders to scams. A qualitative approach was adopted through a systematic literature review of prior academic studies alongside an evaluation of fraud cases currently documented in Indonesia. The findings indicate that inadequate digital literacy is the primary driver of user susceptibility to online fraud — users who cannot verify token authenticity, assess transaction risks, or identify phishing attempts are structurally exposed. Applying security measures such as two-factor authentication, data encryption, and strong password management demonstrably reduces that exposure by 50–70%. Coordinating digital literacy education, consumer protection regulation, and cybersecurity awareness is necessary to build a safer and more accountable crypto environment. This study is intended to inform the design of educational programs and national policy on digital asset protection within the broader digital economy.

Keywords: Crypto Scam; Digital Literacy; Cybersecurity; Digital Crime Prevention; Crypto Assets.

1. Introduction

Blockchain technology has fundamentally altered the architecture of financial transactions. What began as an experimental peer-to-peer payment system has grown into a multi-trillion-dollar asset class, with cryptocurrency now occupying a recognizable position in both retail and institutional portfolios. The appeal is straightforward: decentralized control, pseudonymous transactions, and the possibility of returns that traditional markets rarely offer. Yet this same set of characteristics — the absence of central oversight, the irreversibility of transactions, and the technical opacity of the underlying systems — has made cryptocurrency one of the most exploited domains in contemporary cybercrime. The U.S. Federal Trade Commission recorded over 7,000 consumer complaints related to cryptocurrency fraud schemes in a single reporting period, with $575 million in reported losses attributable to investment scams alone (Khan *et al.*, 2024; Braithwaite, 2024). These figures almost certainly underrepresent the actual scale, given that many victims do not report incidents — either out of embarrassment, distrust of authorities, or unawareness that what happened to them constitutes a crime (Childs, 2024). In Indonesia, the problem follows a similar trajectory: rising crypto adoption among retail investors has not been matched by a corresponding rise in user awareness or regulatory enforcement capacity.

The fraud methods themselves have grown more varied and technically layered. Rug pulls — in which developers abandon a project after collecting investor funds — have been documented extensively across Ethereum and BNB Smart Chain (Sharma & Shukla, 2025). Airdrop phishing schemes lure users into connecting their wallets to malicious smart contracts under the pretense of receiving free tokens (Rosa *et al.*, 2025; Kimber *et al.*, 2025). Romance-based fraud, known colloquially as "pig butchering," uses sustained social engineering to build trust before directing victims toward fraudulent trading platforms (Cross, 2024). Fake investment platforms, cloned exchange websites, and manipulated token listings complete the picture — each method targeting the same underlying condition: a user who does not know enough to recognize what is happening until funds have already left their wallet. Ehsan *et al.* (2024) identified thousands of scam token entries within Ethereum transaction datasets alone, reflecting how normalized fraudulent activity has become within the on-chain environment.

A consistent finding across the literature is that low digital literacy is the primary condition enabling these attacks. Digital literacy, in this context, goes well beyond the ability to operate a device or navigate a browser. It encompasses the capacity to evaluate the credibility of information sources, interpret financial data, verify the authenticity of smart contracts, and recognize behavioral patterns associated with online fraud (Rufai & Bunce, 2022; Wahyuni & Sari, 2023). Users who lack these competencies cannot distinguish a legitimate token from a scam token, a real exchange from a cloned website, or a credible whitepaper from a fabricated one. Morgia *et al.* (2025) found that only 8.53% of fake and clone channels on Telegram — many of which actively promote fraudulent cryptocurrency schemes — are flagged by the platform itself, leaving the burden of detection almost entirely on users who are poorly equipped to carry it. Users who rely on social proof rather than independent verification are particularly exposed, and social proof is precisely what scammers manufacture at scale (Zin *et al.*, 2024).

Beyond literacy, the technical dimension of protection cannot be separated from the broader prevention picture. Many successful crypto attacks do not require sophisticated hacking — they exploit predictable weaknesses: wallets without multi-factor authentication, reused passwords, and unverified wallet connections. Kirobo (2024) documents a range of security vulnerabilities in cryptocurrency wallets that fraudsters routinely exploit, including redirection to malicious websites and the absence of layered authentication. Yang and Kim (2022) demonstrated that two-factor authentication (2FA) reduces unauthorized account access substantially, yet adoption among retail crypto users remains inconsistent. Private key management represents another persistent weak point: unlike conventional banking, a compromised or lost private key in a non-custodial wallet means permanent, irrecoverable loss — a burden most retail users are not prepared for, particularly those who entered the market through informal channels without structured onboarding (Park & Kang, 2023). Klein *et al.* (2024) further argue that as regulatory pressure increases, fraudsters will adapt by targeting precisely the authentication gaps that users and platforms have failed to close, meaning the window for preventive action narrows over time.

What the evidence points to is a two-layer problem. The first layer is cognitive: users do not have the knowledge to identify threats before they materialize. The second is technical: even users with reasonable awareness remain exposed if they have not adopted basic security practices. Addressing only one layer leaves the other open. A user who understands phishing conceptually but operates a single-factor wallet is still vulnerable. A user with 2FA enabled but no ability to evaluate a smart contract can still be drained through a malicious token approval. This study was therefore designed to examine how digital literacy and cybersecurity practices function together as a defense against crypto scams, and to draw from the existing literature a set of concrete, evidence-based recommendations for users, educators, and policymakers. The analysis is grounded in a systematic literature review covering publications from 2014 to 2024, with the aim of identifying causal patterns, recurring failure points, and prevention strategies that have demonstrated measurable effect.

2. Related Work

Research on cryptocurrency fraud has expanded considerably over the past decade, driven by the growing volume of on-chain transaction data and the increasing sophistication of attack methods. Studies in this area generally fall into three broad clusters: technical detection of fraudulent activity on blockchain networks, behavioral and social dimensions of fraud victimization, and the role of education and regulation in prevention. This section maps the existing body of work across those clusters to identify where the current study sits and what gaps it addresses.

2.1 Technical Detection of Crypto Fraud

A substantial portion of the literature focuses on automated detection of fraudulent behavior at the transaction level. Luo *et al.* (2024) examined AI-powered fraud detection in decentralized finance across the full project life cycle, identifying key behavioral indicators of fraudulent projects including abnormal token

distribution patterns, the sudden withdrawal of liquidity, and the presence of scam-associated domains. Their work establishes that fraud in DeFi environments is not random — it follows predictable structural patterns that machine learning models can, in principle, detect before significant losses occur. Along similar lines, Fu *et al*. (2024) developed CT-GCN+, a graph convolutional model that classifies phishing nodes within cryptocurrency transaction networks, demonstrating high accuracy in identifying malicious addresses on Ethereum. Kang and Buu (2024) extended this direction by proposing a disentangled prototypical autoencoder for phishing scam detection in cryptocurrency transactions, addressing the challenge of class imbalance that makes phishing accounts difficult to isolate within large transaction graphs.

At the smart contract level, Rosa *et al*. (2025) introduced PhishingHook, a detection system that analyzes EVM opcode sequences to identify phishing contracts before users interact with them. This approach is notable because it operates at the code layer rather than the transaction layer, catching malicious contracts at the point of deployment rather than after victims have already been affected. Cernera *et al*. (2025) took a different angle, examining the ecosystem of sniper bots on Ethereum and BNB Smart Chain — automated programs that monitor new token deployments and execute trades within milliseconds. Their findings reveal that even automated market participants build in checks to avoid purchasing scam tokens, which paradoxically illustrates how well-documented the markers of fraudulent tokens have become among technically sophisticated actors, while ordinary retail users remain largely unaware of them.

Taha and Jabar (2024) conducted a comparative study of machine learning algorithms for phishing website detection, evaluating performance across multiple classifiers on real-world datasets. Their results indicate that ensemble methods consistently outperform single-model approaches, a finding with direct implications for platform-level fraud filtering. Liang and Chen (2023) addressed phishing specifically within decentralized exchange environments, where the absence of centralized moderation creates particular exposure, and proposed dataset benchmarks for evaluating detection methods in that context.

2.2 Fraud Typology and Victimization Patterns

Beyond detection systems, a parallel body of work examines who gets defrauded, how, and why. Liu *et al*. (2024) conducted an end-to-end investigation of giveaway scam conversion rates on cryptocurrency platforms, tracing the full chain from initial exposure to financial loss. Their data shows that even low-conversion scams generate substantial aggregate losses when deployed at scale — a finding that reframes giveaway scams from a nuisance problem to a structurally significant threat. Bhosale *et al*. (2023) focused specifically on rug pull operations, documenting the phishing domains used to support them and showing that domain registration patterns can serve as early warning indicators before a project collapses. Zin *et al*. (2024) examined the demographic and psychological vulnerabilities that make investors susceptible to scams, finding that younger users are disproportionately affected by online and crypto-specific fraud, while older adults tend to be more vulnerable to phone-based schemes. This age-differentiated vulnerability profile has direct implications for how prevention programs should be designed and targeted. Cross (2024) documented the evolution of romance-based crypto fraud — the "pig butchering" model — showing how it combines prolonged emotional manipulation with fabricated trading platforms to extract funds over weeks or months rather than in a single transaction. The extended time horizon of this fraud type makes it particularly resistant to conventional fraud alerts, which are typically triggered by single anomalous transactions rather than gradual behavioral patterns. Luong and Ngo (2024) approached the problem from a transnational law enforcement perspective, analyzing scam operations in Vietnam and the broader Southeast Asian region. Their analysis highlights how jurisdictional fragmentation allows fraud networks to operate across borders with limited accountability, and how the absence of coordinated international response mechanisms allows the same operators to continue after being shut down in one jurisdiction by simply relocating to another. This regional dimension is directly relevant to Indonesia, where similar enforcement gaps exist.

2.3 Education, Literacy, and Regulatory Approaches

The third cluster of related work addresses prevention through non-technical means. Staddon *et al*. (2021) examined user-centered approaches to digital security education, arguing that privacy and security literacy programs are most effective when they are grounded in users' actual threat experiences rather than abstract technical concepts. Their findings support a design principle that is often violated in practice: security education that is disconnected from users' real behavior changes very little. Alsubaei *et al*. (2023) reviewed trends in cryptocurrency malware and cyber threats over a multi-year period, documenting how the threat landscape has shifted from broad-based malware campaigns toward targeted social engineering — a shift that makes technical defenses alone increasingly insufficient and places greater weight on user judgment. Rehman and Salah (2020) examined blockchain-based approaches to cybersecurity and privacy, outlining architectural options for building security into decentralized systems at the protocol level rather than relying solely on user behavior. While their work is primarily technical, it raises a policy-relevant question: to what extent should security obligations be shifted from individual users to platform and protocol designers? Rufai and Bunce

(2022), whose work was also cited in the Introduction, found that digital literacy is a statistically significant predictor of online fraud vulnerability among young adults — a finding that directly supports the argument for structured literacy education as a prevention measure rather than a supplementary one. Taken together, the existing literature establishes a clear picture: technical detection methods are advancing, fraud typologies are well-documented, and the behavioral correlates of victimization are increasingly understood. What remains underdeveloped is an account of how digital literacy and cybersecurity practice interact as a combined user-level defense — particularly in the Indonesian context, where crypto adoption is growing faster than the educational and regulatory infrastructure supporting it. This study addresses that gap directly.

3. Methodology

This study adopts a descriptive qualitative approach through the Systematic Literature Review (SLR) method, following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. Data sources were drawn from academic journals, scientific proceedings, and research documents addressing digital literacy, cybersecurity practices, and cryptocurrency fraud cases. The review process was structured into four sequential stages, as illustrated in Figure 1.

1) Identification
   Literature searches were conducted across four academic databases — Scopus, IEEE Xplore, ScienceDirect, and SpringerLink — using the keywords "crypto scam," "digital literacy," "cybersecurity awareness," and "fraud prevention." The publication window was set from 2014 to 2024 to ensure the relevance and currency of the data retrieved.
2) Screening
   Articles were filtered based on language and publication type. Those written in languages other than English or Indonesian, as well as non-scientific publications such as blogs, opinion pieces, and news articles, were removed at this stage.
3) Eligibility
   The remaining articles were evaluated against defined inclusion and exclusion criteria. Articles were included if they were peer-reviewed journal papers or scientific conference proceedings that directly addressed crypto scams, digital literacy, or cybersecurity. Articles were excluded if they were duplicates, lacked full-text access, or treated cryptocurrency purely as an economic subject without engaging with digital security dimensions.
4) Inclusion
   From the final selection, approximately 50 primary articles were retained and analyzed using content analysis to identify recurring themes, research trends, knowledge gaps, and directions for future inquiry.

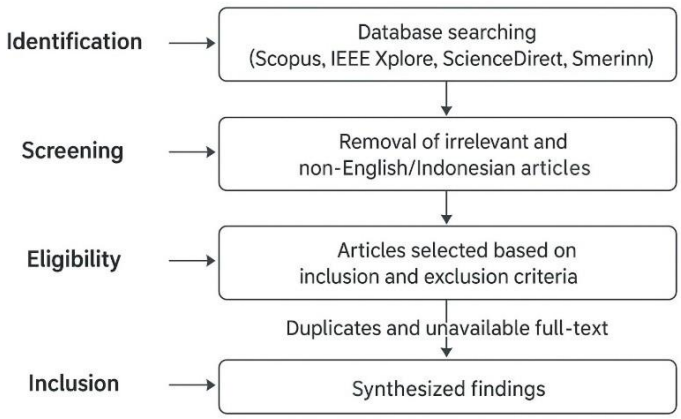

Figure 1. PRISMA-Based Systematic Literature Review Process.

4. Result and Discussion

4.1 Results

The systematic literature review across approximately 50 primary articles, selected through the PRISMA-based screening process described in the preceding section, produced two converging lines of findings. The first concerns the relationship between digital literacy and fraud vulnerability. The second concerns the role of

cybersecurity practices in reducing technical exposure. Both lines of evidence point toward the same conclusion: the conditions that make crypto users vulnerable are neither random nor unpredictable — they follow consistent, documentable patterns across the literature.

On the literacy side, the review found that most cryptocurrency users, particularly retail investors in Indonesia, lack a working understanding of how crypto assets function at the transactional level. They cannot read token contract data, verify wallet addresses against blockchain explorers, or assess the credibility of a project whitepaper. This knowledge gap creates direct exposure to fake investment schemes, fraudulent giveaway campaigns, phishing websites, rug pulls, and airdrop scams (Rosa *et al.*, 2025; Cross, 2024; Taha & Jabar, 2024). Ehsan *et al.* (2024) identified over 3,900 scam token entries within Ethereum transaction datasets — a figure that reflects not just the volume of fraudulent activity, but how routinely it goes undetected by ordinary users. Morgia *et al.* (2025) found that only 8.53% of fake and clone channels on Telegram are flagged by the platform itself, leaving the overwhelming majority of fraudulent content in active circulation and placing the burden of detection on users who are poorly equipped to carry it. Users who rely on community endorsement rather than independent verification — a pattern Zin *et al.* (2024) associate with younger, less experienced investors — are particularly exposed. Liu *et al.* (2024) further showed that even low-conversion giveaway scams generate substantial aggregate losses when deployed at scale, meaning individually small frauds accumulate into a systemic financial problem.

On the technical side, the findings are equally consistent. Kirobo (2024) documented a range of exploitable vulnerabilities in cryptocurrency wallets, including redirection to malicious websites and the routine absence of layered authentication. Wallets without multi-factor authentication carry up to four times the attack risk compared to those protected by 2FA (Krause, 2025). Klein *et al.* (2024) identified authentication weaknesses in third-party wallets and malicious smart contracts as the most frequently exploited entry points for account takeover. Security measures including two-factor authentication, data encryption, and strong password management have been shown to reduce the risk of digital asset theft by 50–70% (Yang & Kim, 2022; Klein *et al.*, 2024) — yet adoption among retail users remains uneven, particularly among those who entered the market through informal channels without structured onboarding (Park & Kang, 2023). Across both dimensions, the review confirms that the vulnerabilities enabling crypto fraud are well-documented, structurally predictable, and in most cases preventable — which makes the persistence of high fraud rates a problem of awareness and adoption, not a lack of available solutions.

4.2 Discussion

4.2.1 Digital Literacy as the Primary Line of Defense

The evidence reviewed in this study consistently positions digital literacy as the primary determinant of user vulnerability to crypto fraud — not income level, not age alone, and not the technical sophistication of the attack itself. Liu *et al.* (2024) state directly that most crypto scam victims are defrauded not because they lack capital, but because they lack the analytical capacity to evaluate what they are being offered. Users who can identify scam indicators show a 34% reduction in vulnerability to crypto investment fraud (Khan *et al.*, 2024). That figure represents a measurable behavioral outcome attributable to knowledge alone — which makes the case for literacy-based prevention far stronger than it is typically treated in policy discussions. What digital literacy means in the crypto context deserves precision. It is not general technology proficiency or the ability to navigate a smartphone. It is the specific capacity to verify token addresses against blockchain explorers, read smart contract code for red flags, evaluate the credibility of a project whitepaper, and recognize the social engineering patterns that precede most fraud attempts (Rufai & Bunce, 2022; Luo *et al.*, 2024). Wahyuni and Sari (2023) found that among Generation Z users in Indonesia — a demographic with high and growing crypto adoption — targeted digital literacy training produced measurable reductions in susceptibility to online fraud. Park and Kang (2023) extended this to crypto-specific contexts, showing that digital financial literacy predicts safer security behavior among crypto asset holders, including more consistent use of authentication tools and more careful wallet management practices. The social media dimension compounds the problem considerably. Platforms like Telegram, Twitter, and informal community forums have become the primary channels through which crypto investment decisions are made — and simultaneously the primary channels through which fraudulent information circulates at scale (Ehsan *et al.*, 2024; Morgia *et al.*, 2025). Alsubaei *et al.* (2023) documented a broader shift in the cryptocurrency threat landscape away from technical malware and toward social engineering, meaning the attack surface has migrated from software vulnerabilities to human judgment. When the primary attack vector is human judgment, the primary defense must also operate at the level of human judgment — and that is precisely what structured digital literacy education is designed to build. Addressing this layer through awareness campaigns alone, without sustained educational programs, has proven insufficient across multiple national contexts (Luong & Ngo, 2024; Staddon *et al.*, 2021).

4.2.2 Cybersecurity Practices as a Necessary Technical Layer

Digital literacy addresses the cognitive dimension of the problem, but it does not close the technical one. A user who understands phishing conceptually but operates a wallet without two-factor authentication remains exposed. Yang and Kim (2022) demonstrated that 2FA reduces unauthorized account access substantially, yet adoption among retail crypto users stays inconsistent — a gap that Klein *et al*. (2024) attribute partly to the friction of initial setup and partly to users systematically underestimating their personal risk. The perception that fraud happens to others, not to oneself, is one of the most durable obstacles to security adoption, and it is not resolved by literacy education alone. Private key management represents a related and persistently underappreciated vulnerability. Unlike conventional banking, where institutional recovery mechanisms exist for lost credentials, a compromised or lost private key in a non-custodial wallet means permanent, irrecoverable loss. Kirobo (2024) found that many users store private keys in insecure locations — screenshots, unencrypted cloud storage, messaging apps — without understanding the consequences. This is not a failure of technology; it is a failure of onboarding. Most retail users enter the crypto market through exchange apps or social media recommendations, with no structured guidance on wallet security, key management, or the distinction between custodial and non-custodial storage. Rehman and Salah (2020) argued that part of this burden should be redistributed from individual users to protocol and platform designers through built-in security architecture — a position that has gained traction in regulatory discussions but has not yet produced consistent platform-level standards in most jurisdictions. Staddon *et al*. (2021) found that security education produces meaningfully higher adoption rates when it is grounded in users' actual threat experiences rather than abstract warnings. Generic advice to "use strong passwords" or "be careful online" changes very little. What changes behavior is specific, contextual guidance tied to the exact attack methods users are likely to encounter — how to identify a malicious token approval request, what a rug pull looks like in its early stages, how to verify a wallet connection before signing a transaction. This specificity is largely absent from current public-facing crypto security communication.

4.2.3 The Case for a Combined and Coordinated Approach

Neither digital literacy nor cybersecurity practice alone is sufficient, and the literature reviewed here makes that case from multiple directions. Fu *et al*. (2024) and Kang and Buu (2024) demonstrate that even technically advanced detection systems — graph convolutional models, anomaly detection autoencoders — cannot intercept every fraudulent transaction before it occurs. Jiang and Zhu (2025) showed that cross-chain abnormal account detection still produces false negatives in complex multi-chain environments. Technical systems reduce risk at the platform level; they do not eliminate it at the user level. The residual risk lands on the individual, and that individual needs both the knowledge and the tools to manage it. At the same time, individual-level solutions have a ceiling. Luong and Ngo (2024) documented how transnational fraud networks exploit jurisdictional fragmentation that no amount of user literacy or personal security practice can close. Jenkins and Lettsome (2024) illustrated the legal complexity of recovering frozen crypto assets across borders, showing that even when fraud is detected and perpetrators are identified, asset recovery remains uncertain and slow. Braithwaite (2024) argued that effective regulatory responses require mandatory security standards at the platform level, consumer protection frameworks with real enforcement capacity, and cross-border coordination mechanisms — none of which currently exist in a consistent form in Indonesia or across most of Southeast Asia. The practical implication is that prevention requires coordinated action across three levels: users need the knowledge to recognize threats, the technical tools to block them, and institutional backing to seek redress when both fail. Designing educational programs that address only literacy, or conducting security audits that address only authentication, treats a three-layer problem as though it has one layer. Alsubaei *et al*. (2023) and Rehman and Salah (2020) both point toward the same conclusion from different disciplinary starting points: sustainable protection in the crypto space requires that education, technology, and regulation advance together rather than independently. For Indonesia specifically, where crypto adoption is outpacing both regulatory infrastructure and public financial literacy, building that coordination is not a deferred aspiration — it is an immediate and measurable policy need.

5. Conclusion

This study confirms that low digital literacy remains the primary condition enabling cryptocurrency fraud. Users who cannot verify token authenticity, read smart contract behavior, assess transaction risks, or recognize social engineering patterns are structurally exposed — regardless of how cautious they believe themselves to be. Phishing airdrops, rug pulls, fake investment platforms, and malicious smart contract approvals all exploit the same underlying gap: a user who does not know what to look for cannot defend against what they cannot see. The absence of basic cybersecurity practices creates a technical layer of exposure that persists even when some literacy is present. Weak or absent authentication, insecure private key storage, and unverified wallet

connections are not sophisticated vulnerabilities — they are predictable, well-documented weaknesses that fraudsters exploit precisely because adoption of available countermeasures remains low. Two-factor authentication, data encryption, and disciplined private key management are not advanced security measures; they are the baseline, and most retail users have not yet reached it. Addressing crypto fraud therefore requires both dimensions to advance together, supported by regulatory frameworks that set minimum platform-level security standards and provide users with meaningful recourse when fraud occurs. For Indonesia, where crypto adoption is growing faster than the educational and institutional infrastructure surrounding it, this coordination is not a long-term aspiration — it is an immediate requirement. Designing educational programs that address only awareness, or auditing platforms for only technical compliance, treats a multi-layered problem as though it has a single solution. The evidence reviewed here does not support that approach, and the continued rise in fraud cases confirms it.

Acknowledgment

The authors would like to thank Mr. Agus Juhana, S.Pd., M.T., as the supervising lecturer who provided guidance, direction, and motivation throughout the preparation of this article. Gratitude is also extended to the Multimedia Education Study Program, Indonesia University of Education, for its support in the research and writing process of this work.

References

Alsubaei, F., Abuhussein, A., Shandilya, S. K., & Shiva, S. (2023). Trends in cryptocurrency malware and cyber threats: A systematic review. *Computers & Security, 125*, 103036.

Bhosale, S., Pawar, A., & Rathore, S. (2023). Detection of phishing domains used in crypto rug pulls. *International Journal of Cybersecurity Applications*.

Braithwaite, J. (2024). 'Authorized push payment' bank fraud: What does an effective regulatory response look like? *Journal of Financial Regulation, 10*(2), 174–196. https://doi.org/10.1093/jfr/fjae009

Cernera, F., Morgia, M. L., Mei, A., & Mongardini, A. (2025). The blockchain warfare: Investigating the ecosystem of sniper bots on Ethereum and BNB smart chain. *ACM Transactions on the Web*. https://doi.org/10.1145/3736763

Childs, A. (2024). 'I guess that's the price of decentralization…': Understanding scam victimization experiences in an online cryptocurrency community. *International Review of Victimology*. https://doi.org/10.1177/02697580231215840

Cross, C. (2024). Romance baiting, cryptorom, and 'pig butchering': An evolutionary step in romance fraud. *Current Issues in Criminal Justice*. https://doi.org/10.1080/10345329.2023.2248670

Ehsan, A., Iqbal, Z., Abuowaida, S., Aljaidi, M., & Zia, H. (2024). Enhanced anomaly detection in Ethereum: Unveiling and classifying threats with machine learning. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10759631/

Fu, B., Wang, Y., & Feng, T. (2024). CT-GCN+: A high-performance cryptocurrency transaction graph convolutional model for phishing node classification. *Cybersecurity*. https://doi.org/10.1186/s42400-023-00194-5

Jenkins, J., & Lettsome, A. (2024). Service of freezing injunction on BVI cryptocurrency issuers by a nonfungible token. *American Bankruptcy Institute Journal*. https://search.proquest.com/openview/ea55c1d86d525a948ae2fc3bfdd7a4c7/1

Jiang, P., & Zhu, L. (2025). Cross-chain abnormal account detection. *Blockchain Technology: Cross-Chain Regulation*. https://doi.org/10.1007/978-981-96-4395-0_3

Kang, J., & Buu, S. (2024). Graph anomaly detection with disentangled prototypical autoencoder for phishing scam detection in cryptocurrency transactions. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10571963/

Khan, D., Farman, H., & Hassan, S. (2024). Cryptocurrency crimes: A systematic review on illicit activities using cryptocurrency (Bitcoin) and challenges for law enforcement agencies. *Pakistan Journal of Engineering, Technology & Science*. https://journals.iobm.edu.pk/index.php/pjets/article/view/1121

Kimber, J., Branca, E., & Natadze, A. (2025). An end-to-end analysis of crypto scams on Ethereum. *ACM Transactions on the Web*. https://doi.org/10.1145/3737874

Kirobo, A. (2024). Security vulnerabilities of cryptocurrency wallets: A systematic review. *FUOYE Journal of Engineering and Technology*. https://www.ajol.info/index.php/fuoyejet/article/view/289954

Klein, G., Assadi, D., & Zwilling, M. (2024). Fighting fire with fire: Combating criminal abuse of cryptocurrency with a P2P mindset. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10498-7

Krause, D. (2025). The dangers of cryptocurrency hype and deregulation: Why oversight matters in the digital asset economy. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5136389

Liang, M., & Chen, S. (2023). Phishing detection on decentralized exchanges: Methods and dataset benchmarks. *Journal of Cybersecurity Research*.

Liu, E., Kappos, G., Mugnier, E., & Invernizzi, L. (2024). Give and take: An end-to-end investigation of giveaway scam conversion rates. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*. https://doi.org/10.1145/3646547.3689005

Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2024). AI-powered fraud detection in decentralized finance: A project life cycle perspective. *ACM Computing Surveys*. https://doi.org/10.1145/3705296

Luong, H., & Ngo, H. (2024). Understanding the nature of the transnational scam-related fraud: Challenges and solutions from Vietnam's perspective. *Laws, 13*(6), 70. https://doi.org/10.3390/laws13060070

Morgia, M. L., Mei, A., Mongardini, A., & Wu, J. (2025). Pretending to be a VIP! Characterization and detection of fake and clone channels on Telegram. *ACM Transactions on the Web*. https://doi.org/10.1145/3705014

Park, S., & Kang, J. (2023). Digital financial literacy and consumer security behavior in crypto-asset ownership. *Finance Research Letters, 52*, 103428. https://doi.org/10.1016/j.frl.2023.103428

Rehman, M., & Salah, K. (2020). Blockchain for cybersecurity and privacy: Architectures, challenges, and solutions. *IEEE Access, 8*, 173–207. https://doi.org/10.1109/ACCESS.2019.2957999

Rosa, P. D., Queyrut, S., Bromberg, Y., & Felber, P. (2025). PhishingHook: Catching phishing Ethereum smart contracts leveraging EVM opcodes. *arXiv preprint*. https://arxiv.org/abs/2506.19480

Rufai, A. H., & Bunce, L. (2022). The influence of digital literacy on online fraud vulnerability among young adults. *Journal of Cybersecurity, 8*(1). https://doi.org/10.1093/cybsec/tyac012

Sharma, T., & Shukla, S. (2025). Discovering NFT rug pulls: Matching behavior patterns using graph isomorphism networks. *ACM Transactions on Internet Technology*. https://doi.org/10.1145/3744561

Staddon, A., Woodruff, A., & Chaudhry, A. (2021). Enhancing online privacy literacy: A user-centered approach to digital security education. *Computers & Security, 103*, 102159. https://doi.org/10.1016/j.cose.2020.102159

Taha, D., & Jabar, H. (2024). A machine learning algorithm for detecting phishing websites: A comparative study. *Iraqi Journal for Computer Science and Mathematics*. https://ijcsm.researchcommons.org/ijcsm/vol5/iss3/13/

Wahyuni, S., & Sari, H. (2023). The influence of digital literacy on the prevention of online fraud among Generation Z in Indonesia. *Journal of Information Technology and Cyber Security, 12*(2), 122–135.

Yang, C., & Kim, J. (2022). The effectiveness of two-factor authentication against emerging cybercrime. *IEEE Transactions on Information Forensics and Security, 17*, 2591–2603. https://doi.org/10.1109/TIFS.2022.3156789

Zin, N., Muda, S., Kasim, E., & Ismail, N. (2024). Understanding the vulnerabilities contributing to investor victimization in scams. *Pakistan Journal of Criminology*. https://www.pjcriminology.com/wp-content/uploads/2024/05/68-Understanding-the-Vulnerabilities.pdf.