



Journal of Advanced Research in Business and Management Studies

Journal homepage:
<https://karyailham.com.my/index.php/arbms/index>
ISSN: 2462-1935



The Digital Trap: Conceptualizing Investment Scam Vulnerability among Malaysian Young Professional

Muhammad Zikry Hishamudin¹, Norlaila Md Zin^{2,*}, Eley Suzana Kasim¹, Fazlida Mohd Razali¹

¹ Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Malaysia

² Institute of Leadership and Development (ILD), Negeri Sembilan, Malaysia

ARTICLE INFO

ABSTRACT

Article history:

Received 9 July 2026

Received in revised form 29 September 2026

Accepted 30 September 2026

Available online 12 October 2026

Keywords:

Digital investment scam; Investment scam vulnerability; Social Cognitive Theory; Protection Motivation Theory; Digital financial literacy; Young working adults; Malaysia

Digital financial services have expanded investment opportunities while increasing exposure to sophisticated investment scams. Despite growing research on investment scam, existing studies examined vulnerability from isolated perspectives, such as financial literacy, behavioural traits, or demographic characteristics. As a result, study on investment scam vulnerability remain fragmented. This conceptual paper proposes an integrated framework to explain digital investment scam vulnerability among Malaysian young working adults by drawing on Social Cognitive Theory, Protection Motivation Theory, and Digital Financial Literacy. The framework argues that vulnerability is shaped by the interaction of individual characteristics, environmental influences, and protective appraisal, with digital financial literacy influencing the effectiveness of protective responses. By integrating these complementary perspectives, the paper extends the current understanding of investment scam vulnerability beyond single-factor explanations and provides a theoretical foundation for future empirical research. The proposed framework also offers practical insights for policymakers, regulators, and financial educators in developing more targeted investor protection and digital financial literacy initiatives.

1. Introduction

The rapid digitalisation of financial services has changed how individuals invest, save, and manage their wealth [1]. Mobile investment applications, online trading platforms, digital banking, and social media have made investment opportunities more accessible than ever before [2]. While these developments have increased financial inclusion and encouraged greater participation in digital investment, they have also created new opportunities for financial fraud. Among digital financial crime, investment scams have become one of the most significant threats to individual investors, causing substantial financial losses and undermining public confidence in digital financial markets [3].

* Corresponding author.

E-mail address: norlaila249@uitm.edu.my

Unlike traditional investment fraud, digital investment scams exploit technology to deceive potential victims through online platforms, social media, instant messaging applications, and fraudulent investment websites [2]. These schemes frequently imitate legitimate financial institutions, promote unrealistic investment returns, and use persuasive digital communication to create a false sense of trust and urgency [3-8]. As scammers continue to adopt increasingly sophisticated technologies and psychological manipulation techniques, distinguishing legitimate investment opportunities from fraudulent schemes has become more difficult for ordinary investors.

Malaysia has experienced a similar trend. The increasing adoption of digital financial services has been accompanied by a steady rise in investment scam cases despite continuous regulatory efforts, public awareness campaigns, and financial education initiatives [9,10]. This situation suggests that technological advancement alone does not explain why investment scams continue to succeed. More importantly, it raises an important question: why do some individuals remain vulnerable to digital investment scams while others facing similar circumstances do not?

Young working adults represent a particularly relevant population for addressing this question. As one of the most digitally connected groups in society, they actively use online platforms to obtain financial information, manage personal finances, and explore investment opportunities [11]. Their growing financial independence and willingness to participate in digital investment markets expose them to both legitimate financial products and fraudulent schemes [13,21]. Previous studies have shown that this group frequently encounters investment-related content through social media, online communities, and digital influencers, increasing both investment participation and exposure to scams [7,12]. Although digital engagement creates valuable financial opportunities, it also increases the likelihood of interacting with misleading or deceptive investment information.

Existing research has identified numerous factors associated with investment scam victimisation, including financial literacy, trust, risk-taking behaviour, cognitive bias, and social influence. While these studies have improved understanding of investment scams, they have largely examined these factors independently. Such fragmented approaches overlook the reality that vulnerability is rarely driven by a single characteristic. Instead, susceptibility to investment scams is likely to emerge from the interaction of individual characteristics, environmental influences, and psychological responses within digital financial environments.

This paper argues that digital investment scam vulnerability should be understood as a multidimensional phenomenon rather than the outcome of isolated behavioural or demographic factors. Accordingly, it proposes an integrated conceptual framework that combines SCT, PMT, and DFL to explain how individual factors, environmental influences, protective appraisal, and digital financial literacy collectively shape vulnerability among Malaysian young working adults. By integrating these perspectives, this paper contributes to the growing literature on digital financial fraud while providing a theoretical foundation for future empirical research and more effective investor protection strategies.

2. Investment Scam Vulnerability: Existing Perspectives and Research Gap

Investment fraud vulnerabilities have attracted digital financial services to continue reshaping investment behavior [13,14]. Rather than viewing scam victimisation as the result of a single weakness, recent studies suggest that vulnerability arises from a combination of factors influencing how individuals perceive, evaluate, and respond to investment opportunities [15,16]. Thus, scholars have approached investment scam vulnerability from different perspectives, emphasising individual characteristics, environmental conditions, and psychological processes [6,17]. Although each perspective has contributed valuable insights, they have largely developed independently, resulting

in a fragmented understanding of why some individuals are more susceptible to digital investment scams than others.

Early research primarily focused on individual characteristics that influence financial judgement and investment decision-making [6]. Factors such as trust propensity, risk propensity, financial literacy, cognitive bias, and overconfidence have frequently been associated with increased susceptibility to fraudulent investment schemes [17-19]. Individuals with a greater tendency to trust investment information may be less likely to verify the legitimacy of an investment opportunity, while those with higher risk tolerance are generally more willing to pursue investments promising exceptional returns despite greater uncertainty. Likewise, cognitive biases, including overconfidence and fear of missing out, may encourage impulsive investment decisions by shifting attention away from potential warning signs [8,15]. Collectively, these findings suggest that personal characteristics play an important role in shaping investment behaviour and vulnerability.

However, focusing solely on individual characteristics provides only a partial explanation. Investment decisions influenced by external environments that shape the information individuals receive and the choices they make [4,20]. The rapid growth of digital platforms has significantly changed how investment opportunities are promoted, discussed, and evaluated [12,13]. Social media, online communities, financial influencers, and digital communication channels have become important sources of investment information, allowing fraudulent schemes to spread rapidly and gain credibility through repeated exposure and social endorsement [4,21]. At the same time, regulatory initiatives and scam prevention programmes seek to reduce exposure by improving investor awareness and strengthening consumer protection [2,10]. These environmental influences demonstrate that vulnerability is not determined solely by personal characteristics but is also shaped by the broader digital ecosystem in which investment decisions are made.

More recently, researchers have recognised that vulnerability also depends on how individuals interpret and respond to potential threats [9,20,22,23]. From this perspective, scam victimisation is influenced not only by what individuals know or the environment in which they operate, but also by their ability to recognise fraudulent cues, assess potential consequences, and adopt appropriate protective responses [9,20,24]. Individuals exposed to the same investment opportunity may therefore behave differently because they evaluate risks differently [18,25]. This psychological perspective has provided valuable insight into the cognitive mechanisms underlying investment decisions, highlighting the importance of protective appraisal in reducing susceptibility to fraudulent investment schemes.

Taken together, these perspectives indicate that investment scam vulnerability is a multidimensional phenomenon. Nevertheless, the existing literature continues to examine behavioural, environmental, and psychological influences as largely independent explanations [15, 26,27]. Such separation limits our understanding of digital investment scams, where investment decisions are simultaneously shaped by personal judgement, social environments, and cognitive evaluations. As digital financial ecosystems become increasingly interconnected, explaining vulnerability through a single perspective is unlikely to capture the complexity of real-world investment decisions.

Addressing this limitation requires a more integrated perspective that explains not only what influences vulnerability but also how these influences interact. Rather than treating individual characteristics, environmental conditions, and protective responses as competing explanations, this paper argues that they represent complementary dimensions of the same phenomenon [11,15]. Integrating these perspectives provides a more comprehensive conceptualisation of investment scam vulnerability and offers a stronger theoretical foundation for understanding why certain individuals remain vulnerable despite increasing financial awareness and regulatory intervention.

3. Towards an Intergrated Conceptualisation of Investment Scam Vulnerability

The research suggests that investment scam vulnerability cannot be adequately explained through individual, environmental, or psychological perspectives alone [15,26]. While each perspective contributes valuable insights, none can fully capture the complexity of investment decision-making in a digital financial environment, where individuals constantly interact with technology, information, and social networks [4,13]. Consequently, vulnerability should be viewed as a multidimensional construct that emerges from the interaction of multiple influences rather than from a single behavioural or contextual factor.

Within digital investment settings, individuals rarely make decisions based solely on personal judgement [18,28]. Investment opportunities are increasingly discovered through social media, online communities, financial influencers, and digital platforms that shape perceptions of credibility and risk [12,21]. At the same time, personal tendencies, such as trust, risk-taking, and sensitivity to missed opportunities, influence how investment information is interpreted [18, 19]. These influences are further moderated by an individual's ability to recognise potential threats and evaluate appropriate protective responses. Understanding investment scam vulnerability therefore requires a framework that captures these interconnected processes rather than treating them as independent explanations.

Social Cognitive Theory (SCT) provides an appropriate foundation for explaining how individual characteristics and environmental influences jointly shape behaviour [29]. The theory proposes that behaviour develops through the reciprocal interaction between personal factors and external environments. Applied to digital investment, SCT suggests that vulnerability is influenced not only by who individuals are but also by the information they consume, the social networks they engage with, and the digital environments in which investment decisions occur. This perspective explains why individuals exposed to similar investment opportunities may develop different levels of vulnerability.

Although SCT explains the origins of behaviour, it provides limited insight into how individuals cognitively evaluate fraudulent investment opportunities once they are encountered [30]. Protection Motivation Theory (PMT) complements this perspective by explaining how individuals assess potential threats and determine appropriate protective responses [6,20,22]. Individuals who perceive greater scam-related risks and believe they possess the ability to identify and avoid fraudulent schemes are more likely to resist deceptive investment offers [24,31]. Conversely, those with weaker protective appraisal may remain susceptible despite possessing similar levels of investment knowledge or digital experience.

While behavioural tendencies, environmental influences, and protective appraisal provide a comprehensive explanation of vulnerability, their effectiveness may differ according to an individual's level of digital financial literacy [31]. Digital financial literacy extends beyond financial knowledge by encompassing the competencies required to access, evaluate, and safely use digital financial services. Individuals with stronger digital financial literacy are generally better equipped to verify investment information, recognise fraudulent signals, and apply protective strategies when navigating digital investment environments [14]. Rather than acting as a direct determinant of vulnerability, digital financial literacy may strengthen the effectiveness of protective appraisal by enabling individuals to translate awareness into safer financial decisions.

Drawing these perspectives together, this paper conceptualises digital investment scam vulnerability as:

an individual's susceptibility to fraudulent investment schemes arising from the interaction of individual characteristics, environmental influences, and psychological protective mechanisms within digital financial environments.

This conceptualisation moves beyond conventional explanations that attribute vulnerability to isolated behavioural traits or limited financial knowledge. Instead, it recognises vulnerability as a dynamic condition shaped by the continuous interaction between individuals and their digital financial environment [4,31-33]. Such a perspective provides a more comprehensive explanation of why people with similar financial knowledge or demographic backgrounds may respond differently when confronted with the same fraudulent investment opportunity.

Based on this integrated perspective, the proposed framework positions individual characteristics and environmental influences as antecedents of protective appraisal, which subsequently influences investment scam vulnerability. Digital financial literacy is proposed as a contextual capability that strengthens or weakens the effectiveness of protective appraisal in reducing vulnerability. Figure 1 presents the proposed conceptual framework.

4. Proposed Conceptual Framework

Figure 1 presents the proposed conceptual framework for explaining digital investment scam vulnerability among Malaysian young working adults. The framework integrates Social Cognitive Theory (SCT), Protection Motivation Theory (PMT), and Digital Financial Literacy (DFL) to provide a holistic explanation of investment scam vulnerability. Consistent with SCT, individual and environmental factors are proposed as the primary antecedents shaping individuals' responses to digital investment opportunities. PMT complements this perspective by explaining how these factors influence protective appraisal, which subsequently affects investment scam vulnerability. Digital Financial Literacy is incorporated as a moderating capability that may strengthen or weaken the effectiveness of protective appraisal in reducing vulnerability.

Unlike previous studies that examined these perspectives independently, the proposed framework conceptualises investment scam vulnerability as the outcome of interconnected behavioural, environmental, and psychological processes operating within digital financial environments. Consequently, understanding vulnerability requires recognising how these factors interact rather than treating them as isolated determinants.

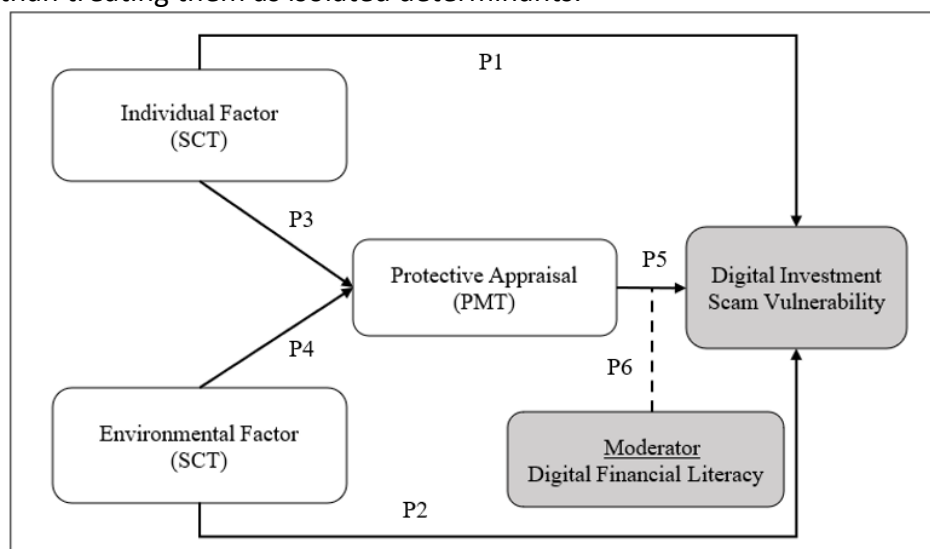


Fig. 1. Conceptual framework of digital investment scam vulnerability

Proposed Propositions

Based on the proposed framework, the following propositions are advanced.

- P1 : Individual factors are associated with digital investment scam vulnerability
- P2 : Environmental factors are associated with digital investment scam vulnerability.
- P3 : Individual factors influence protective appraisal.
- P4 : Environmental factors influence protective appraisal.
- P5 : Protective appraisal mediates the relationship between individual and environmental factors and digital investment scam vulnerability.
- P6 : Digital Financial Literacy moderates the relationship between protective appraisal and digital investment scam vulnerability, such that higher levels of Digital Financial Literacy strengthen the protective effect of protective appraisal.

These propositions provide a theoretical basis for future empirical research and offer a structured framework for examining the multidimensional nature of investment scam vulnerability within digital financial environments.

5. Discussion

The proposed framework contributes to the investment scam literature by shifting the focus from isolated determinants of scam victimisation to a more integrated understanding of vulnerability. Previous studies have predominantly examined behavioural characteristics, environmental influences, or psychological responses independently, resulting in fragmented explanations of why some individuals are more susceptible to fraudulent investment schemes than others. By integrating SCT, PMT, and DFL, this paper argues that vulnerability is better understood as the product of interacting individual, environmental, and cognitive processes rather than the consequence of a single factor.

From a theoretical perspective, the framework extends existing knowledge in two important ways. First, it broadens the application of SCT beyond explaining financial behaviour to conceptualising vulnerability within digital investment environments. Rather than focusing solely on behavioural outcomes, the framework demonstrates how personal characteristics and environmental conditions jointly influence individuals' susceptibility to fraudulent investment schemes. Second, integrating PMT introduces a psychological mechanism that explains how individuals evaluate investment-related threats and determine appropriate protective responses. This integration provides a more comprehensive explanation than either theory can offer independently.

The inclusion of Digital Financial Literacy further strengthens the framework by recognising that financial knowledge alone may not be sufficient to protect individuals from increasingly sophisticated scams. Instead, digital financial literacy represents the capability to apply financial knowledge effectively within digital environments, enabling individuals to identify misleading information, verify investment opportunities, and make safer financial decisions. This perspective helps explain why individuals with comparable levels of financial knowledge may experience different levels of vulnerability.

Beyond its theoretical contribution, the proposed framework has practical implications for regulators, financial institutions, and educators. Current anti-scam initiatives often emphasise awareness campaigns or financial education as universal solutions. However, the proposed

framework suggests that effective intervention requires a more comprehensive approach that simultaneously addresses behavioural tendencies, environmental influences, psychological preparedness, and digital financial capability. Such an approach may support the development of more targeted investor protection strategies, particularly for young working adults who are highly engaged in digital financial activities.

Finally, the framework provides several opportunities for future research. Empirical studies may validate the proposed relationships using different demographic groups, investment contexts, or national settings. Future research may also examine additional behavioural or technological factors that influence investment scam vulnerability as digital financial ecosystems continue to evolve.

6. Conclusion

Digital investment scams represent one of the most significant challenges associated with the rapid digitalisation of financial services. Although previous studies have identified numerous factors related to investment scam victimisation, existing explanations remain fragmented because they largely examine behavioural, environmental, and psychological influences independently. This conceptual paper addresses that limitation by proposing an integrated framework grounded in Social Cognitive Theory, Protection Motivation Theory, and Digital Financial Literacy.

By conceptualising investment scam vulnerability as a multidimensional phenomenon shaped by the interaction of individual characteristics, environmental influences, and protective appraisal, the proposed framework offers a more comprehensive explanation of why individuals differ in their susceptibility to fraudulent investment schemes. The framework not only contributes to the theoretical development of investment scam research but also provides a foundation for future empirical studies and more effective investor protection strategies within increasingly digital financial environments.

Acknowledgement

This research was not funded by any grant.

References

- [1] Rangapur, Aman, Haoran Wang, and Kai Shu. "Investigating online financial misinformation and its consequences: A computational perspective." *arXiv preprint arXiv:2309.12363* (2023).
- [2] Napitupulu, Josua Halomoan, Mompang L. Panggabean, Hulman Panjaitan, and Wiwik Sri Widiarty. "An integrated legal framework for digital investment fraud prevention in Indonesia." *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (2025): 540-567.
- [3] International Criminal Police Organization: INTERPOL Global Financial Fraud Assessment. (2024)
- [4] Xiao, Jingjia, Qing Xiao, and Hong Shen. ""It Felt Real" Victim Perspectives on Platform Design and Longer-Running Scams." *arXiv preprint arXiv:2510.02680* (2025).
- [5] Aziz, A.A.A., Shah, N.K.M., Yatim, A.I.A., Juned, A.M., Yusof, A.H.S.M., Sharifudin, M.A.S.: The Forensic Linguistics of Fear-Based Messaging: Deconstructing Narrative Structures in Malaysian Investment Scam Promotional Materials. *International Journal of Research and Innovation in Social Science (IJRISS)*. VII, 1175–1189 (2025). <https://doi.org/10.47772/IJRISS>
- [6] Whitty, Monica Therese. "A systematic literature review of profiling victims of cyber scams: Setting up a framework for future research." *Cogent Social Sciences* 11, no. 1 (2025): 2563781. <https://doi.org/10.1080/23311886.2025.2563781>
- [7] Ofcom: Understanding Online Financial Harm: A Review of Fraud and Disinformation Exposure Across Demographic Groups in the UK. (2025)

- [8] Kan, M., Fonzo, P. Di, Paleja, M., Raza, A., Carriaga, R., Trebebov, S.: Artificial Intelligence and Retail Investing: Scams and Effective Countermeasures, <https://www.osc.ca/en/investors/artificial-intelligence-and-retail-investing-scams-and-effective-countermeasures>
- [9] Munusamy, Nalini, and Muslimin Wallang. "Assessing Citizens' Readiness and Utilization of the National Scam Response Centre (NSRC) in Combating Online Scams: The Moderating Effect of Education." *Architecture Image Studies (AIS)* 6, no. 4 (2025): 442. <https://doi.org/10.62754/ais.v6i4.597>
- [10] Muhammad, F., Shaarani, A.Z.M., Hussin, M.Y.M., Awang, S.A., Hamdan, R.: Scam Awareness Gaps: A Survey on Malaysian Youth's Digital Habits and Knowledge. *International Journal of Religion*. 5, 3130–3141 (2024). <https://doi.org/10.61707/28kb8w07>
- [11] Rizky, Ahmad, Lestari Wulandari, Nurul Azizah, and Fiona Walsh. "Financial Behavior and Risk Tolerance as Determinants of Investment Decision Making among Young Adults in Urban Areas." *Journal of Economics and Management* 3, no. 2 (2025): 60-68. <https://doi.org/10.70716/ecoma.v3i2.249>
- [12] Ramli, Rosniza, Salwa Muda, Eley Suzana Kasim, Norlaila Md Zin, Norhidayah Ismail, and Hazlina Mohd Padil. "Examining the relationship between social media and intention to invest in an investment scams among students." *Information Management and Business Review* 15, no. 4 (2023): 387-393.
- [13] Hilmi, Ahmad Humaizi. "From WhatsApp to Fake Trading Apps: How Digital Platforms Are Reshaping Investment Fraud in Malaysia."
- [14] Ruiz, Juan Rafael. "Who gets scammed? The roles of financial literacy, digital financial security, and overconfidence in Europe." *International Review of Economics & Finance* (2026): 104913. <https://doi.org/10.1016/j.iref.2026.104913>
- [15] Park, Youngjin. "Fear of missing out and online scam vulnerability: a sequential interlayering multimethod approach." *Telematics and Informatics* (2026): 102377. <https://doi.org/10.1016/j.tele.2026.102377>
- [16] Houtti, Mo, Abhishek Roy, Venkata Narsi Reddy Gangula, and Ashley Marie Walker. "A survey of scam exposure, victimization, types, vectors, and reporting in 12 countries." *arXiv preprint arXiv:2407.12896* (2024).
- [17] Baharudin, Zainur Nadiyah, Noor Aznaim Abd Latib, Muhamad Hasif Yahaya, Muhamad Syahrul Deen Ahmad Rosli, and Aeshah Mohd Ali. "Determinants of financial literacy and investment fraud: a systematic literature review." *Al-Qanadir: International Journal of Islamic Studies* 34, no. 04 (2025): 274-282. <https://doi.org/10.64757/alqanadir.2025.3404/1200>
- [18] Tjondro, Elisa, Cherrylia Ester, Yovita Gisella Sardjono, and Adhityawati Kusumawardhani. "Investment scam vulnerability among university students: the role of personality traits and risk tolerance." *Cogent Education* 12, no. 1 (2025): 2464309. <https://doi.org/10.1080/2331186X.2025.2464309>
- [19] Ahmad, Zauwiyah. "Investment scams: the effect of bias-induced gullibility on victimization propensity: Z. Ahmad." *Crime, Law and Social Change* 83, no. 1 (2025): 17. <https://doi.org/10.1007/s10611-024-10187-1>
- [20] Anderson, Matthew. "Exploring the contribution of victims, offenders and protection mechanisms to the online investment fraud victimisation process." PhD diss., University of New South Wales (Australia), 2025.
- [21] Rauf, Mujtaba, Muhammad Moosa Naeem, and Syed Majid Hussain. "Social Media and Investment Scams: Examining Social Media Platforms as a Tool for Investment Scams among University Students in Pakistan." *The Regional Tribune* 4, no. 4 (2025): 190-204. <https://doi.org/10.55737/trt/fl25.171>
- [22] Zainiar, Noor Aishah, and Siti Nur Edayu Hashim. "A Review of Social Engineering Threats in the Age of AI: Understanding Human Vulnerabilities Through Protection Motivation Theory (PMT)." *Journal on Technical and Vocational Education* 10, no. 2 (2025): 570-583.
- [23] Luu, Veronica, Lesley Land, and Wynne Chin. "Safeguarding against romance scams—using protection motivation theory." (2017): 2429.
- [24] Kuah, Chin Yoke, Xian Wen Lee, Hia Nya Lim, and Yi Yan Vivian Lim. "Awareness On Online Financial Scams: A Case Study in Malaysia." *International Journal of Advanced Research in Economics and Finance* 6, no. 1 (2024): 101-116. <https://doi.org/10.55057/ijaref.2024.6.1.8>
- [25] Lemay, David John, Ram B. Basnet, and Tenzin Doleck. "Examining the Relationship between Threat and Coping Appraisal in Phishing Detection among College Students." *J. Internet Serv. Inf. Secur.* 10, no. 1 (2020): 38-49. <https://doi.org/10.22667/JISIS.2020.02.29.038>
- [26] Zarina Taha, A., Chen, W., Kenny, S.L.C.: Financial Literacy as a Moderator in Consumer Financial Decision-Making: A Systematic Literature Review. *International Journal of Advanced Research in Economics and Finance*. (2025). <https://doi.org/10.55057/ijaref.2025.7.2.13>
- [27] Pothupitiya, Rathnapriya Samitha. "Scammer Exchange: A Critical Discourse Analysis." *International Journal of Research and Innovation in Social Science* 9, no. 12 (2025): 3719-3732 <https://doi.org/10.47772/IJRISS>
- [28] Supti, Tourjana Islam, Khaled M. Khan, Ala Yankouskaya, Israa Abuelezz, Mahmoud Barhmagi, Aiman Erbad, and Raian Ali. "Examining the role of Self-Construal on Cybersecurity Attitudes and perceptions of vulnerability." *Journal of Applied Security Research* 20, no. 3 (2025): 355-381. <https://doi.org/10.1080/19361610.2025.2466000>

- [29] Balakrishnan, Vimala, Umayma Ahhmed, and Faris Basheer. "Personal, environmental and behavioral predictors associated with online fraud victimization among adults." *PLoS one* 20, no. 1 (2025): e0317232. <https://doi.org/10.1371/journal.pone.0317232>
- [30] Batra, Gunjan, Khawaja Saeed, and Botong Xue. "Driver of User's Security Behaviors: Avoidance or Motivation." (2026).
- [31] Junaidi, Junaidi, and Rismawati Rismawati. "Analysis of the Influence of Society Vulnerability to Online Fraud." (2025). <https://doi.org/10.2139/ssrn.5343445>
- [32] Herrero, Juan, Andrea Torres, Pep Vivas, Antonio Hidalgo, Francisco J. Rodríguez, and Alberto Urueña. "Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization." *International journal of environmental research and public health* 18, no. 7 (2021): 3763. <https://doi.org/10.3390/ijerph18073763>
- [33] Lazarus, Suleman, Jack M. Whittaker, Michael R. McGuire, and Lucinda Platt. "What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021)." *Journal of Economic Criminology* 2 (2023): 100013. <https://doi.org/10.1016/j.jeconc.2023.100013>