Jurnal Komunikasi: Malaysian Journal of Communication
https://ejournal.ukm.my/mjc
Volume 42(2) 2026: 553-573

Digital Deception: A Qualitative Investigation of Online Scam Victims' Experiences and Coping Mechanisms

NUR HAFIFAH JAMALLUDIN*
ATEERAH ABDUL RAZAK
HASNAH BINTI AB.KADIR
WAN YUSOFF WAN SHAHARUDDIN
ARIEZAL AFZAN HASSAN
Universiti Malaysia Kelantan

ABSTRACT

Cyber scams have emerged as a critical global threat, leading to substantial financial loss, profound psychological distress, and a systemic erosion of trust in digital transactions. This study investigates the lived experiences of online scam victims to uncover recurring patterns in fraudulent methodologies, immediate victim responses, and the efficacy of institutional remedies. Theoretically grounded in Protection Motivation Theory (PMT), the research examines how cognitive processes specifically treat appraisal (perceived severity and vulnerability) and coping appraisal (self-efficacy and response efficacy) shape individuals' behavioral adaptations following victimization. Employing a qualitative research design, semi-structured interviews were conducted with 15 scam victims, and the data was analysed using a systematic thematic approach supported by NVivo software. The findings reveal that fraudsters systematically exploit social trust, urgency, and disinformation, resulting in severe emotional trauma and financial instability. While victims often adopt immediate coping strategies, such as reporting incidents to authorities, many express significant frustrations with the perceived inadequacy of law enforcement and institutional responses. The study highlights the vital necessity of enhancing digital literacy, fostering institutional accountability, and integrating psychological support into victim assistance frameworks. By providing empirical insights into victim narratives, this research contributes to cybercrime literature and offers a robust basis for legislative and policy improvements aimed at mitigating the impact of digital deception.

Keywords: *Cybercrime, online scams, protection motivation theory, victim experiences, digital fraud prevention.*

INTRODUCTION

With the rise of digital transactions, cyber scams have become increasingly sophisticated, exploiting users through various fraudulent schemes, including phishing, fake online marketplaces, and financial fraud (Agir et al., 2022; Weulen Kranenbarg et al., 2025). The rapid advancement of technology and the widespread adoption of digital financial services have provided fraudsters with new opportunities to deceive individuals. Victims of these scams often suffer significant financial losses, identity theft, and emotional trauma, making cyber fraud a critical issue in cybersecurity research (Azman et al., 2014; Irvin-Erickson, 2024). As digital transactions become more integral to daily life, the risk of falling victim to cyber fraud continues to escalate, necessitating further research into its impact and mitigation strategies.

Despite the growing number of cyber scams, there remains a lack of qualitative research capturing the victim's perspective on how they experience, respond to, and recover from online fraud (Cole, 2024; Jansen & Leukfeldt, 2018). Most existing studies primarily focus

*Corresponding author: hafifah.j@umk.edu.my
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30
Received: 6 March 2026 | Accepted: 12 May 2026 | Published: 30 June 2026

on technical countermeasures, such as fraud detection algorithms and cybersecurity policies, leaving a gap in understanding human vulnerabilities and behavioural responses (Galinec et al., 2025). Victims often report inadequate legal support and financial recovery options, leading to emotional distress and a diminished sense of trust in digital transactions (Zhu & Chang, 2023). The lack of effective consumer protection measures exacerbates the problem, as many victims struggle to seek justice or recover lost funds (Wang, 2025). Given this gap, it is crucial to analyse the lived experiences of scam victims to develop more effective intervention strategies. This study aims to address this issue by providing a deeper understanding of scam victims' experiences and proposing strategies to enhance scam prevention efforts.

This research is significant in three key areas: (1) academic contribution; (2) policy implications; and (3) social impact. Academically, the study enhances cybercrime literature by providing empirical qualitative data on scam victims' experiences, which can contribute to a more comprehensive understanding of online fraud (de Bruijn & Janssen, 2017). From a policy perspective, the findings can inform policymakers about the need for stronger consumer protection laws, improved financial security measures, and public awareness campaigns to combat cyber fraud effectively (Senarak, 2021; Wulandari et al., 2025). On a societal level, the study helps individuals recognize scam tactics, develop resilience against digital fraud, and improve overall cybersecurity awareness (Liang & Xue, 2009; Wang & Topalli, 2024). By addressing these key areas, this research contributes to both theoretical and practical efforts to mitigate cybercrime and enhance public safety in digital transactions.

LITERATURE REVIEW

Cyber Fraud and the Evolution of Online Scams

Cyber scams have been extensively examined from both technical and behavioural perspectives, with considerable emphasis placed on fraud detection systems, cybersecurity frameworks, and regulatory mechanisms (Gould et al., 2023; Niman et al., 2023). However, existing literature has largely overlooked the lived experiences of victims, resulting in a limited understanding of how individuals encounter, interpret, and respond to online fraud (Zwilling et al., 2022). This gap is significant, as victim-centred insights are essential for developing more effective prevention and intervention strategies. Addressing this limitation, the present study adopts a human-centred perspective by incorporating victims' narratives, thereby enriching the discourse on cyber fraud and its real-world implications.

The evolution of cyber fraud reflects a transition from relatively simple schemes, such as email-based fraud, to more sophisticated tactics involving phishing, social engineering, and digital identity theft (Weulen Kranenbarg et al., 2025) including cryptocurrency fraud as critical dimension of online scams (Pitchan et al., 2025). Contemporary fraudsters increasingly utilise advanced technologies, including artificial intelligence and automated phishing systems, to enhance the credibility and scalability of their attacks (Zhu & Chang, 2023). These developments have enabled fraudsters to exploit social trust and digital vulnerabilities more effectively, making it increasingly difficult for individuals to distinguish between legitimate and fraudulent communications (Misra & Khurana, 2017; Whitty, 2025). As digital transactions continue to expand globally, the dynamic nature of cyber fraud necessitates continuous adaptation in both technological safeguards and user awareness.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Psychological and Financial Impact of Cyber Fraud

Victimisation in cyber fraud cases extends beyond financial loss, encompassing significant psychological and emotional consequences (Firdaus et al., 2022; Gautam & Yadav, 2026). Studies indicate that victims often experience heightened levels of stress, anxiety, and trauma, particularly when substantial financial losses are involved (Irvin-Erickson, 2024; Oladiti et al., 2026; Van Schaik et al., 2017). These experiences are frequently accompanied by feelings of self-blame and embarrassment, which can intensify emotional distress and hinder recovery. In addition, victims may develop long-term trust issues with digital platforms, leading to reduced participation in online transactions such as e-commerce and internet banking (Galinec et al., 2025; Osman et al., 2024).

These psychological responses highlight that cyber fraud is not merely a technical or financial issue, but also a deeply personal and emotional experience. The impact of victimisation can influence individuals' future behaviour, particularly in terms of risk perception and trust in digital environments, thereby reinforcing the importance of understanding victim experiences in greater depth.

Institutional Response and Challenges in Fraud Recovery

Despite the implementation of fraud detection systems by financial institutions, victims often face considerable challenges in recovering lost funds (Agarwal et al., 2025). Many individuals report inadequate support from banks and law enforcement agencies, which further exacerbates their financial and emotional distress (Weulen Kranenbarg et al., 2025). Delays in response, lack of transparency, and limited recovery success contribute to a decline in public trust toward institutional mechanisms (Gajda, 2025).

Although governments have introduced cybercrime legislation and regulatory frameworks to address digital fraud, enforcement remains inconsistent across jurisdictions (Zhu & Chang, 2023). The transnational nature of cybercrime complicates legal processes, making it difficult to identify, prosecute, and penalise offenders effectively. The absence of a unified global legal framework further limits the ability of authorities to respond efficiently to cyber fraud cases (Sanusi et al., 2025). These institutional limitations highlight the need for more coordinated and effective responses to support victims and enhance trust in formal systems.

Digital Literacy and Preventive Behaviour

Digital literacy has emerged as a critical component in mitigating the risks associated with online scams. Studies have shown that individuals with higher levels of cybersecurity awareness are better equipped to recognise and avoid fraudulent schemes (Mwirigi et al., 2026; Sandra, 2026). Educational initiatives, including awareness campaigns, cybersecurity training programmes, and public service announcements, have been found to significantly reduce susceptibility to scams (Galinec et al., 2025; Irvin-Erickson, 2024). These initiatives enhance individuals' ability to critically evaluate online information and identify potential threats.

However, the effectiveness of digital literacy initiatives depends on their ability to adapt to evolving scam tactics. As cyber fraud becomes increasingly sophisticated, awareness programmes must be continuously updated to remain relevant and impactful (Alotaibi et al., 2016; Jamalludin et al., 2026), while still pushing the digital literacy agenda (Mohamed et al.,

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

2023). Therefore, a comprehensive approach that integrates technological innovation, policy enforcement, and public education is essential for reducing the impact of cyber fraud.

Theoretical Perspective: Protection Motivation Theory

This study is grounded in Protection Motivation Theory (PMT), which provides a robust framework for understanding how individuals respond to perceived threats (Rogers 1975). PMT posits that individuals engage in two key cognitive processes when faced with a threat: threat appraisal and coping appraisal (Sulaiman et al., 2026). Threat appraisal involves evaluating the severity of a threat and one's vulnerability to it, while coping appraisal refers to assessing the effectiveness of available responses and one's ability to execute them (Han et al., 2025).

In the context of cyber fraud, threat appraisal is reflected in how individuals perceive the seriousness of financial loss and their susceptibility to scams (Dodge et al., 2023). Victims who experience significant losses are likely to develop heightened perceptions of risk, which in turn trigger strong emotional responses such as fear, anxiety, and regret (Cheng, 2026). These emotional reactions play a crucial role in shaping subsequent behavioural decisions.

Coping appraisal, on the other hand, explains how individuals respond to scam incidents through actions such as reporting the incident, securing accounts, and seeking support (Carter & McNealey, 2025). It also encompasses individuals' confidence in their ability to manage the situation (self-efficacy) and their belief in the effectiveness of these actions (response efficacy) (Gautam & Yadav, 2026). However, perceived barriers, such as ineffective institutional support, may reduce the likelihood of adopting protective behaviours.

The application of PMT in this study provides a comprehensive lens to examine the relationship between threat perception, emotional response, and behavioural adaptation. By integrating this theoretical framework, the study moves beyond descriptive analysis and offers a deeper explanation of how individuals develop digital resilience following scam victimisation.

METHODOLOGY

Research Design and Theoretical Underpinning

This study adopts a qualitative research design to explore the lived experiences of online scam victims, with particular emphasis on their emotional responses, coping strategies, and behavioural adaptations following victimization. A qualitative approach is appropriate as it enables an in-depth understanding of subjective experiences, meanings, and interpretations that cannot be adequately captured through quantitative methods (Takona, 2024). Given the sensitive and personal nature of scam victimization, the use of qualitative inquiry allows participants to articulate their experiences in a nuanced and reflective manner.

The study is theoretically grounded in PMT, which explains how individuals respond to perceived threats through cognitive and behavioural processes. The theory posits that individuals evaluate threats based on threat appraisal, which includes perceived severity and vulnerability, and coping appraisal, which involves response efficacy, self-efficacy, and perceived barriers (Rogers 1975). In the context of online scams, this framework provides a robust lens to understand how victims interpret their experiences, react emotionally, and subsequently adapt their behaviours to mitigate future risks (Sulaiman et al., 2026). The integration of this theoretical perspective enhances the analytical depth of the study and strengthens its contribution to cybersecurity and victimology literature.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Sampling Strategy and Participants

This study employs purposive sampling to select participants who possess direct and relevant experience with online scams. This sampling strategy is widely used in qualitative research to ensure that participants are able to provide rich, meaningful, and experience-based insights relevant to the research objectives (Takona, 2024). Participants were selected based on specific inclusion criteria, namely: (1) individuals who have personally experienced an online scam; (2) are willing to share their experiences openly; and (3) are able to recall and articulate the incident in detail.

A total of 15 participants were recruited for this study. The sample size is considered appropriate for qualitative research, as the primary objective is to achieve depth of understanding rather than statistical generalisation. The determination of the sample size was guided by the principle of data saturation, which refers to the point at which no new themes or insights emerge from the data (Islam & Aldaihani, 2022). In this study, saturation was achieved as recurring patterns related to emotional responses, coping strategies, and behavioural adaptations became consistent across interviews. Existing qualitative research supports that saturation can be achieved within 12 to 15 participants when the study is focused and participants share similar experiential backgrounds. Therefore, the inclusion of 15 participants ensures both analytical depth and thematic completeness, meeting the expectations of rigorous qualitative inquiry.

Data Collection Procedure

Primary data were collected through semi-structured, in-depth interviews conducted over a period of approximately four to six weeks. This method was selected due to its effectiveness in capturing detailed personal narratives, particularly in contexts involving sensitive experiences such as financial loss and emotional distress. The semi-structured format allowed the researcher to maintain consistency across interviews while also providing flexibility to explore emerging themes and probe deeper into participants' responses.

Each interview lasted between 30 to 60 minutes and was conducted either face-to-face or via online communication platforms, depending on participants' availability and preference. Prior to the interviews, participants were provided with a clear explanation of the study's purpose and procedures, and informed consent was obtained. With participants' permission, all interviews were audio-recorded to ensure accuracy and completeness of the data. The recordings were subsequently transcribed verbatim to facilitate systematic analysis. In addition, field notes were taken during and after the interviews to capture contextual observations, non-verbal cues, and initial analytical reflections, thereby enriching the overall dataset.

Research Instrument

The primary research instrument used in this study was a semi-structured interview guide consisting of 24 open-ended questions – Table 1. The interview guide is important as it ensured conversations remained focused on specific subjects while providing prompts for research participants (Yusoh et al., 2024). The instrument was developed based on the objectives of the study, relevant literature on cybercrime and victimization, and key constructs derived from PMT. The design of the instrument ensured alignment with both threat appraisal and coping appraisal components, allowing for a comprehensive exploration of participants' experiences.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

The interview questions were organised into five main sections. The first section focused on participants' background and digital behaviour, including their level of engagement with online platforms. The second section explored the nature of the scam experience, including how the scam occurred and factors that contributed to its perceived legitimacy. The third section examined threat appraisal by capturing participants' perceptions of severity and vulnerability, as well as their emotional responses. The fourth section addressed coping appraisal by exploring participants' actions, perceived effectiveness of those actions, and challenges encountered. The final section focused on behavioural adaptation and prevention, including changes in online behaviour and recommendations for avoiding future scams.

The use of open-ended questions allowed participants to express their experiences freely and in their own words, thereby minimizing response bias and enhancing the richness of the data. This structure also ensured that the instrument was both theoretically grounded and empirically relevant.

Table 1: Research instrument (semi-structured interview guide)

Sections	Items
Section A: Background and Digital Behaviour	1. Can you describe your background (e.g., occupation, digital usage habits)? 2. How frequently do you engage in online transactions or digital activities? 3. What types of digital platforms do you commonly use?
Section B: Scam Experience (Threat Exposure)	4. Can you describe your experience of being involved in an online scam? 5. What type of scam did you encounter? 6. How did the scammer approach or manipulate you? 7. What made the situation appear legitimate or trustworthy? 8. When and how did you realise it was a scam?
Section C: Threat Appraisal (PMT)	9. How serious do you perceive the impact of the scam on your life? 10. Did you feel vulnerable to such scams before this incident? Why or why not? 11. What emotions did you experience after the incident (e.g., fear, anger, regret)? 12. How did the experience affect your sense of security in digital environments?
Section D: Coping Appraisal and Responses (PMT)	13. What actions did you take immediately after realising the scam? 14. Did you believe those actions would help reduce the damage? Why? 15. How confident were you in handling the situation? 16. What challenges did you face in responding to the scam? 17. Did you seek help from others (e.g., family, friends, authorities)?
Section E: Behavioural Adaptation and Prevention	18. How has this experience changed your online behaviour? 19. Do you feel more cautious when engaging in digital transactions now? 20. What preventive measures do you currently practice? 21. How do you evaluate the role of banks or authorities in handling scam cases? 22. Do you think existing support systems are adequate? Why? 23. What recommendations would you suggest to prevent online scams? 24. Is there anything else you would like to share about your experience?

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Data Analysis and Trustworthiness

Qualitative empirical data were analysed through thematic generation and coding procedures, which are widely recognised as rigorous approaches for interpreting experiential narratives. The analysis followed a structured empirical materials interpretation procedure adapted from Rashid et al. (2019), ensuring systematic organisation, validation, and interpretation of the qualitative dataset. The process is illustrated in Figure 1.

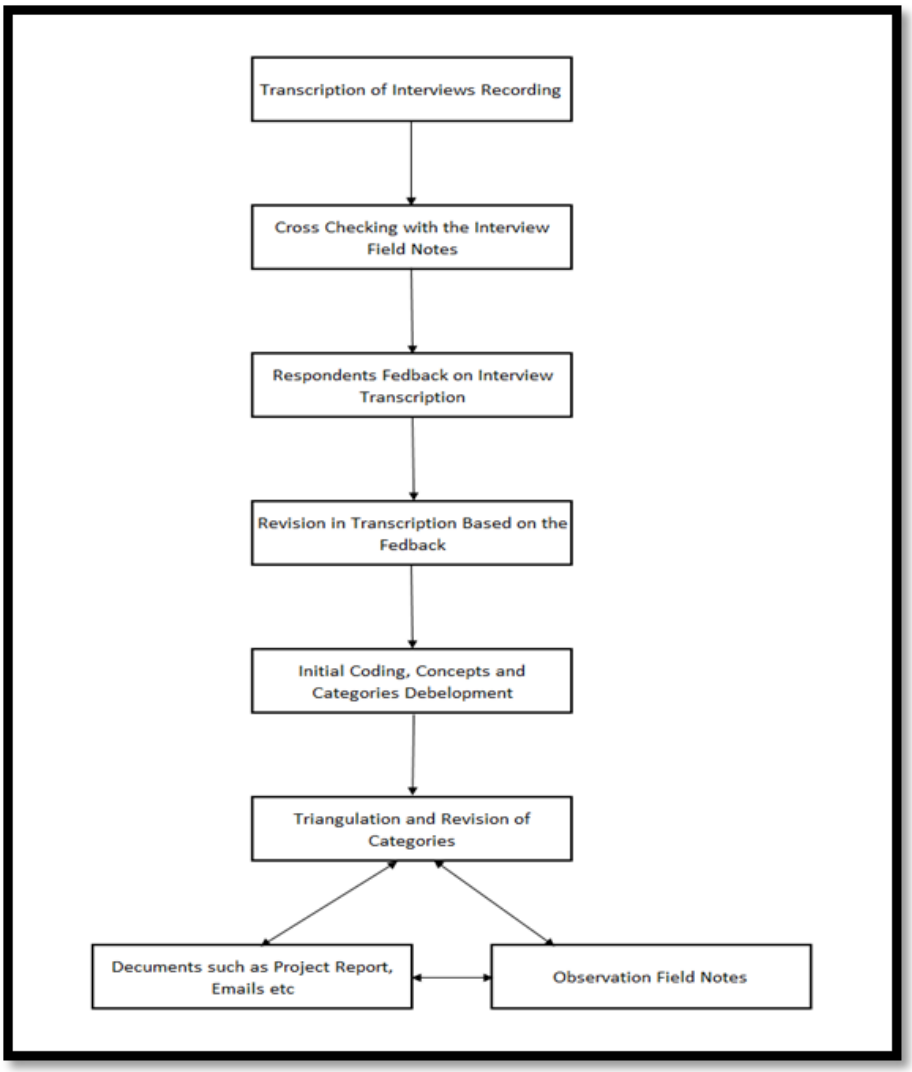


Figure 1: Empirical materials interpretation process for digital deception: A qualitative investigation of online scam victims' experiences and coping mechanisms adapted from Rashid et al. (2019)

The empirical materials for this study consisted primarily of semi-structured interview transcripts obtained from 15 participants who had experienced online scams, supported by interview field notes and researcher observations recorded during data collection. All interview recordings were transcribed verbatim to create a comprehensive textual dataset for analysis. The transcription process represented the first stage of analysis, transforming raw audio recordings into analysable empirical material.

Following transcription, cross-checking procedures were conducted between interview transcripts and field notes to ensure accuracy, contextual completeness, and consistency of participants' responses. Participants were subsequently invited to review

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

selected interview summaries to confirm the accuracy of interpretations, a process commonly referred to as member checking. Feedback received from participants was incorporated through revisions of the transcripts, enhancing credibility and reducing interpretive bias.

The revised transcripts were then imported into NVivo software to facilitate systematic data organization, coding, and categorization (Allsop et al., 2022; Rashid et al., 2019). Initial coding involved identifying meaningful units of data representing participants' experiences with online scams. These codes were progressively refined into sub-concepts, broader concepts, and finally thematic categories aligned with the research objectives. This iterative process ensured analytical transparency and enabled patterns to emerge organically from participants' narratives.

To enhance methodological rigor, triangulation was employed throughout the analytical process. Interview findings were continuously compared with field notes and observational reflections to validate emerging categories. The triangulation procedure strengthened the robustness of interpretations by integrating multiple sources of empirical evidence rather than relying solely on interview data. This approach ensured that identified themes reflected consistent patterns across data sources, thereby improving the credibility and dependability of findings (Rashid et al., 2019).

In addition to the empirical interpretation procedure, thematic analysis was conducted following the six-step framework proposed by Adu (2019). The process involved: (1) familiarization with the data through repeated reading of transcripts; (2) generation of initial codes capturing significant features of participants' experiences; (3) identification of potential themes; (4) detailed review and refinement of themes; (5) definition and naming of final themes; and (6) production of the analytical report supported by verbatim quotations.

An inductive analytical approach was adopted, allowing themes to emerge directly from participants' lived experiences rather than imposing predetermined theoretical categories (Proudfoot, 2023). This inductive orientation was particularly appropriate for exploring online scam victimization, as it enabled a deeper understanding of emotional responses, coping strategies, and behavioural adaptations grounded in participants' narratives. Similar approaches have been recommended for qualitative health and social research to ensure findings remain closely connected to empirical data (Fereday & Muir-Cochrane, 2006).

To further enhance reliability, inter-coder consistency procedures were applied. A subset of interview transcripts was independently reviewed and coded, followed by discussion and reconciliation of discrepancies to ensure coding consistency and analytical accuracy. This procedure strengthened confirmability and reduced subjective bias in theme development.

The combined use of empirical materials interpretation, triangulation, and systematic thematic analysis ensured that the research findings were derived from a transparent, validated, and methodologically rigorous analytical process. By integrating multiple analytical stages supported by NVivo software, the study achieved a comprehensive interpretation of online scam victims' lived experiences, reinforcing the credibility, dependability, and trustworthiness of the research outcomes.

In addition, to ensure methodological rigor, this study adopted trustworthiness criteria which emphasize credibility, transferability, dependability, and confirmability as standards for qualitative research quality (Adu, 2019; Ahmed, 2024) – Table 2. Multiple validation strategies were integrated throughout the research process to enhance the authenticity and reliability of findings derived from participants' lived experiences of online scam victimization.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Table 2: Trustworthiness criteria

Trustworthiness Criteria	Purpose	Strategies Applied in This Study	Evidence in Current Research
A. Credibility	Ensures findings accurately represent participants' realities	1. Semi-structured in-depth interviews with 15 scam victims 2. Member checking conducted after transcription 3. Prolonged engagement during interviews 4. Use of verbatim quotations	Participants validated interview summaries; themes grounded in real experiences
B. Transferability	Allows readers to determine applicability to similar contexts	1. Thick description of participants' experiences 2. Detailed explanation of scam contexts and victim responses 3. Clear participant selection criteria	Enables comparison with cyber fraud victims in other digital environments
C. Dependability	Demonstrates consistency and stability of research procedures	1. Systematic interview protocol 2. Audit trail documenting coding decisions 3. NVivo-assisted thematic analysis 4. Inter-coder review process	Transparent analytical procedures allowing methodological replication
D. Confirmability	Ensures findings emerge from data rather than researcher bias	1. Data triangulation (interviews, field notes, observations) 2. Reflexive analytical process 3. Documentation of theme development	Findings supported by multiple empirical data sources

Ethical Considerations

Ethical considerations were strictly observed throughout the research process. Participants were provided with clear information about the study and gave informed consent prior to participation. Confidentiality and anonymity were ensured using pseudonyms Participants were also informed of their right to withdraw from the study at any time. All data was securely stored in password-protected systems to protect participants' privacy.

RESULTS AND DISCUSSION

Nature and Types of Scams

Online scams take various forms, exploiting different vulnerabilities in digital transactions – Table 3. One of the most common types reported by victims is online shopping fraud, where individuals pay for products that are either never delivered or significantly different from what was advertised. As one informant shared, "*My friend got scammed from a seller that sells clothes. The seller offered a fair price, which was too cheap compared to the market price. My friend lost 1.5K from that accident*." Another respondent recalled, "*I bought discounted*

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

electronics from an online store and realised the website was a scam after making the payment" These scams highlight the risks associated with purchasing items from unverified online sources and underscore the need for increased consumer awareness.

Another prevalent form of fraud is phishing and identity theft, where victims receive fraudulent emails, calls, or messages that appear to be from legitimate organizations, such as banks or service providers. One victim noted, "*I have received a lot of phishing emails through my Yahoo email. I have been hacked once when Yahoo had a global information leak*." Another reported, "*I got an email, SMS notification asking for CODE PIN for one of my accounts*." A particularly deceptive scheme involved a scammer sending a text invitation for a neighbour's wedding, as one informant stated, "*My dad received a text invitation to our neighbour's wedding, which seemed genuine at first*". However, it turned out to be a scam attempting to collect his phone number and other personal details. These cases illustrate the evolving sophistication of phishing techniques used to steal personal information.

Investment and job scams were also frequently reported by victims. Fraudulent investment opportunities and part-time job offer often promise quick financial gains but eventually lead to financial loss. One victim recounted, "*I once received a part-time job scam. I only needed to like and subscribe to certain YouTube channels. At first, I got paid, but then I had to pay a fee to continue. That's when I realised it was a scam*." Similarly, another informant described being lured into an investment scam through Telegram, stating, "*I got an invitation to join an investment group on Telegram and received various messages to attract potential victims to invest*." These scams demonstrate how fraudsters manipulate financial aspirations and trust to deceive individuals.

Another common fraud tactic is loan and prize scams, where victims are tricked into paying processing fees for non-existent loans or rewards. One respondent shared, "*My uncle needed a personal loan. He saw an online advertisement offering up to RM50K. He transferred RM2K first, then another RM5K, but never received the loan. The scammer disappeared*." Another victim almost fell for a fake prize scam, stating, "*I received a WhatsApp call from 'Digi Centre' saying I had won 3 months of free bills. They asked for my Celcom app OTP. I almost fell for it*." These scams prey on financial desperation and excitement, convincing victims to act hastily without verifying legitimacy.

Lastly, romance scams exploit victims' emotions to deceive them into sending money. One informant shared, "*My mom spent almost RM15K on a guy she met online. He asked her to transfer money to two suspicious accounts. After realizing she was scammed, she went to the police, but it was too late*." Another respondent reported, "*Someone disguised as a friend asked for help, and then my money was scammed by that unknown person*." These cases highlight the psychological manipulation tactics employed in romance scams, which often lead to significant financial and emotional distress.

Online scams continue to evolve as cybercriminals leverage advanced technology and psychological tactics to exploit victims (Weulen Kranenbarg et al., 2025; Zwilling, 2022). The increase in online shopping fraud and phishing scams highlights the growing need for digital literacy among consumers (Gould et al., 2023). Studies have shown that a lack of awareness and security measures contributes significantly to online fraud cases (Cole, 2024; Van Schaik et al., 2017). Victims often experience financial and emotional distress, as fraudsters manipulate trust and urgency to pressure individuals into acting impulsively. Preventative measures, such as multi-factor authentication, financial transaction alerts, and awareness campaigns, are essential in mitigating risks (Misra & Khurana, 2017; Zhu & Chang, 2023). Law

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

enforcement agencies and financial institutions must also strengthen their efforts in detecting and addressing fraudulent activities to enhance consumer protection.

Psychological and Emotional Impact

Victims of online scams experience significant emotional distress, including fear, frustration, and loss of trust in digital transactions. As one respondent put it, "*It's scary and traumatic." Another victim expressed anger, stating, "I was very angry about this cybercrime*." The financial impact can be devastating, with some individuals losing substantial amounts of money. One informant recounted, "*My friend reported a scam involving RM15,000. It devastated the family's finances and trust in the authorities*." Such experiences can also lead to long-term psychological consequences, as one victim stated, "*I have never trusted online sellers again since my experience of being scammed*." These findings indicate that scam victimization goes beyond financial loss, affecting mental well-being and digital trust.

The emotional and psychological distress experienced by scam victims is well-documented in cybersecurity and criminology literature. Studies indicate that financial fraud often results in severe emotional consequences, including anxiety, depression, and a diminished sense of security in digital environments (Klimek, 2026; Harrison et al., 2022; Niman et al., 2023). Victims of online scams frequently report feelings of shame and helplessness, which can deter them from seeking help or reporting incidents to authorities (Klimek, 2026; Firdaus et al., 2022). Additionally, financial losses, especially large sums can lead to prolonged financial instability, further exacerbating stress and reducing trust in online transactions (Irvin-Erickson, 2024). Research suggests that improving public awareness of scams and providing psychological support services for victims can mitigate these negative effects (Gautam & Yadav, 2026; Harrison et al., 2022; Oladiti et al., 2026). Addressing scam victimization requires a multi-faceted approach that combines legal interventions, financial protections, and mental health resources to support affected individuals effectively.

Victims' Responses and Coping Strategies

Victims often take immediate actions after realizing they have been scammed, such as blocking the scammer, reporting the incident, and contacting financial institutions to prevent further losses. One victim shared, "*I reported to the police about the theft of money online against my friend amounting to RM15,000*." Another respondent described their response after their social media account was hacked, stating, "*My brother's social media account got hacked. He immediately filed a report with the bank to block all banking services and changed all information*." However, in many cases, the scam had already caused irreversible financial damage, as another victim noted, "*My father called the bank immediately when he realised he had been scammed, but it was too late*."

Seeking support from family, friends, and online communities is another common coping strategy. One respondent explained, "*I advised my parents not to click on suspicious links. If they are not sure, they ask me first*." Others adopted technological solutions, as one victim shared, "*I installed the TrueCaller app for my parents so they can track scammer calls*." These strategies highlight the importance of collective awareness and digital vigilance in preventing future scams.

Legal and institutional responses vary, with some victims filing police reports while others find law enforcement unhelpful. One informant stated, "*The police told my uncle that they receive up to 6 similar scam cases daily, but they couldn't track the scammer*." Another

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

victim expressed frustration, saying, "*I went to the police station to report a scam, but they said there wasn't much they could do*." These responses indicate a gap in effective legal frameworks and law enforcement resources to address cyber fraud.

The psychological and financial toll of online scams can have long-term effects on victims, influencing their mental well-being and trust in digital transactions. Studies show that scam victims often experience anxiety, depression, and post-traumatic stress symptoms due to financial losses and the sense of betrayal (Sanusi et al., 2025; Senarak, 2021). The erosion of trust in online platforms may lead to digital avoidance behaviors, where individuals become hesitant to engage in e-commerce or financial transactions online. Furthermore, research highlights that victims who suffer significant financial losses often feel abandoned by authorities, exacerbating feelings of helplessness and frustration (Agarwal et al., 2025; Liang & Xue, 2009). Psychological support services and targeted intervention strategies, such as scam awareness programs and improved fraud prevention mechanisms, are crucial in mitigating these negative consequences (de Bruijn & Janssen, 2017; Gajda, 2025). Addressing the emotional impact of online scams requires a multi-faceted approach, combining financial protection, legal support, and mental health assistance to help victims recover both economically and psychologically.

Perceptions of Law Enforcement and Financial Institutions

Victims often feel that authorities and banks provide limited recourse and insufficient action in recovering lost money. One informant shared, "*A scam from a fake bank. I made a police report quickly and went to the bank to block my account*." However, another victim noted the ineffectiveness of reporting fraud, stating, "I lost RM900 in 5 minutes after clicking a link. Reporting it did not help. These experiences reflect a widespread lack of confidence in institutional fraud response mechanisms.

Additionally, respondents highlighted the need for improved cybersecurity education and stronger consumer protection policies. One victim emphasised; "*authorities should run more awareness campaigns about scams. Many people do not know how to identify them*". Another suggested, "*I hope the government strengthens cybersecurity laws to punish fraudsters more severely*." These insights reveal the growing demand for stricter regulatory measures and enhanced public education efforts to combat cyber fraud.

The perceived ineffectiveness of authorities and financial institutions in addressing online scams contributes to a lack of trust in formal fraud response mechanisms. Research indicates that many victims feel frustrated by slow or ineffective institutional actions, which often result in minimal financial recovery (Mwirigi et al., 2026). A study by Sandra (2026) found that law enforcement agencies face significant challenges in tracking down fraudsters due to the cross-border nature of cybercrime. Furthermore, inadequate consumer protection policies leave victims vulnerable to recurring fraud incidents (Weulen Kranenbarg et al., 2025). To address these issues, experts emphasize the importance of collaborative efforts between governments, financial institutions, and cybersecurity organizations in strengthening fraud detection and response systems (Jamalludin et al., 2026). Increased investment in digital literacy campaigns can also empower consumers to recognize and avoid scams before falling victim to them. By implementing stricter cybersecurity regulations and enhancing consumer education, authorities can work towards restoring public confidence and reducing the prevalence of online scams.

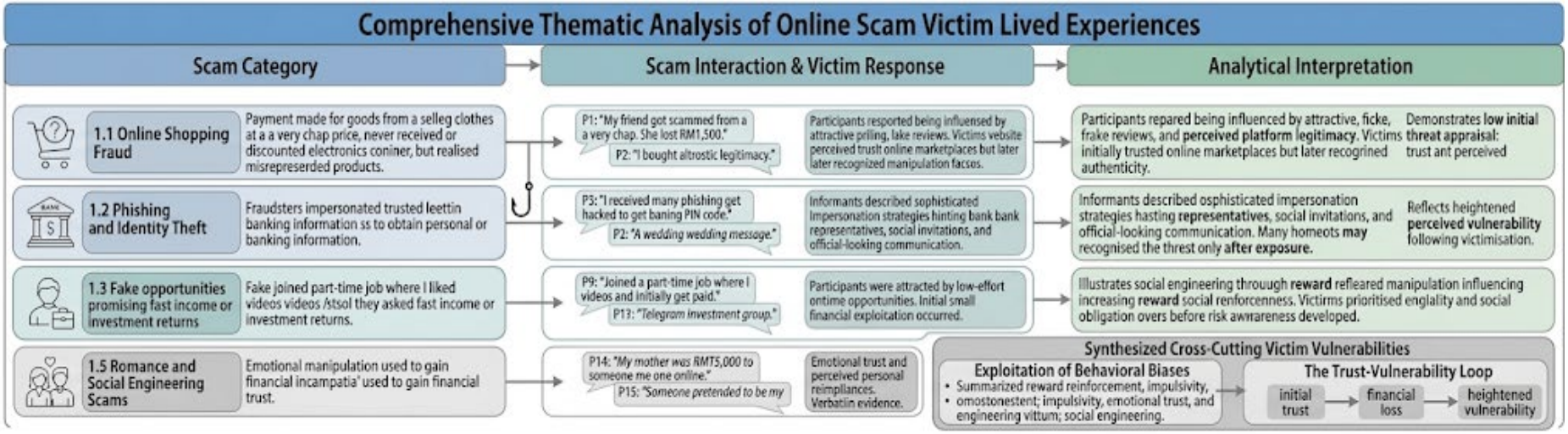
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Table 3: Thematic analysis: Lived experiences of online scam victims

No.	Thematic Analysis	Definition	Informants' Responses (Verbatim Evidence)	Analytical Interpretation
1.1 Online Shopping Fraud	Payment made for goods never received or misrepresented products.	P1: "My friend got scammed from a seller selling clothes at a very cheap price. She lost RM1,500."P2: "I bought discounted electronics online but realised the website disappeared after payment."P3: "The seller kept delaying delivery until the account vanished."P4: "I trusted the reviews, but they were fake."	Participants reported being influenced by attractive pricing, fake reviews, and perceived platform legitimacy. Victims initially trusted online marketplaces but later recognised manipulation tactics.	Demonstrates **low initial threat appraisal**; scams exploited trust and perceived authenticity.
1.2 Phishing and Identity Theft	Fraudsters impersonate trusted institutions to obtain personal or banking information.	P5: "I received many phishing emails through Yahoo and got hacked once."P6: "I received SMS asking for my banking PIN code."P7: "A wedding invitation message turned out to be a scam collecting personal details."P8: "Someone called claiming to be from my bank requesting verification."	Informants described sophisticated impersonation strategies including bank representatives, social invitations, and official-looking communication. Many recognised the threat only after exposure.	Reflects heightened **perceived vulnerability** following victimisation.
1.3 Investment and Job Scams	Fake opportunities promising fast income or investment returns.	P9: "I joined a part-time job where I liked YouTube videos and initially got paid."P10: "Later they asked me to pay a fee to continue."P11: "I was invited to a Telegram investment group promising high profit."	Participants were attracted by low-effort income opportunities. Initial small rewards increased credibility before financial exploitation occurred.	Illustrates social engineering through **reward reinforcement** increasing scam effectiveness.
1.4 Loan and Prize Scams	Victims pay processing fees or share OTPs for fake loans or rewards.	P12: "My uncle transferred RM7,000 for a loan that never existed."P13: "I almost shared my OTP after a fake Digi prize call."	Victims experienced urgency pressure involving financial relief or rewards. Requests for advance payment or OTP verification were common manipulation tactics.	Shows exploitation of financial need and urgency triggering impulsive decision-making.
1.5 Romance and Social Engineering Scams	Emotional manipulation used to gain financial trust.	P14: "My mother sent RM15,000 to someone she met online."P15: "Someone pretended to be my friend asking urgently for money."	Emotional trust and perceived personal relationships increased compliance. Victims prioritised empathy and social obligation over risk evaluation.	Highlights emotional manipulation influencing decision processes before risk awareness developed.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-01

Figure 2: Thematic analysis: Lived experiences of online scam victims



E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Digital Literacy and Scam Prevention

Many victims reported learning to recognize red flags and exercise greater caution in digital interactions. One informant stated, "*Now I always verify evidence before believing anything online."* Another noted answer from the informant*; "I never answer calls from unknown numbers anymore*." Avoiding suspicious links and calls has also become a key protective measure, as one victim shared, "*If I see an unfamiliar number, I don't pick up*." Others take proactive steps to educate family and friends, as one respondent noted, "*I warn my family and friends never to transfer money before verifying in person.*" Another added, "*I always tell my mom to ask me before she clicks on any suspicious links*." These findings highlight the importance of digital awareness and community-based prevention strategies in reducing scam susceptibility. These findings collectively emphasize the growing sophistication of online scams, their psychological and financial consequences, and the crucial role of digital literacy and institutional reforms in preventing cyber fraud.

Digital literacy plays a critical role in mitigating online scams, as informed users are better equipped to recognize fraudulent tactics and adopt preventive measures. Research suggests that individuals who receive cybersecurity education are significantly less likely to fall victim to scams (Carter & McNealey, 2025; Novianti & Chariri, 2025). Raising awareness about common scam indicators such as unsolicited messages, too-good-to-be-true offers, and urgent requests for personal information can empower individuals to make safer digital decisions (Maina, 2026).

Additionally, peer education and community-based initiatives have proven effective in spreading digital safety practices, as social networks often serve as the first line of defense against fraud (Cheng, 2026; Zwilling et al., 2022). However, while personal vigilance is essential, institutional reforms, such as stricter cybersecurity regulations and improved fraud reporting systems, are equally necessary to reduce cybercrime prevalence (Sirohi & Misra, 2024). A comprehensive approach combining education, legal measures, and financial security protocols is essential in protecting individuals from evolving digital threats.

Comprehensive Findings: Threat Appraisal through Protection Motivation Theory

Findings indicate that participants perceived online scams as highly severe, particularly due to financial losses and psychological distress. Victims reported losing substantial amounts of money, which significantly impacted their financial stability and emotional well-being. From the perspective of PMT, this reflects high perceived severity, where individuals recognise the serious consequences of a threat (Gautam & Yadav, 2026; Rogers 1975; Sulaiman et al., 2026).

In addition, many participants admitted that they did not initially perceive themselves as vulnerable, often trusting online platforms or offers that appeared legitimate. However, after the incident, their perception of vulnerability increased significantly (Han et al., 2025). This shift demonstrates how direct victimisation reshapes individuals' risk awareness, aligning with PMT's assertion that threat experience strengthens vulnerability perception.

CONCLUSION

This study provides a comprehensive exploration of online scam victimisation, highlighting the complex interplay between emotional responses, cognitive evaluations, and behavioural adaptations. The findings demonstrate that online scams have significant psychological and social implications, extending beyond financial loss. By applying PMT, the study offers a

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-01

theoretically grounded explanation of how individuals respond to digital threats and adapt their behaviours accordingly.

The study contributes to the literature by extending the application of PMT to the context of cybercrime, emphasising the role of emotional responses in shaping behavioural outcomes. It also provides practical insights for policymakers and stakeholders. From a policy perspective, there is a need to strengthen institutional mechanisms for handling scam cases, particularly in improving response time and effectiveness. For instance, technologies such as artificial intelligence (AI) and big data analytics should be considered for adoption to improve detection of suspicious transaction trends with greater accuracy (Pitchan, et al., 2025). In this sense, financial institutions and law enforcement agencies should enhance collaboration to provide more efficient support to victims. In addition, digital literacy programmes should be expanded to equip individuals with the skills needed to identify and avoid scams. This effort could be further enhanced through continuous public awareness campaigns to reflect evolving scam tactics. As emotional distress remains a significant consequence of scam victimisation, psychological support services should also be incorporated into victim assistance frameworks. In short, a holistic approach that integrates technological, institutional, and psychological interventions is essential to effectively address the growing threat of online scams.

ACKNOWLEDGEMENT

The article is based on research funded by the Universiti Malaysia Kelantan, Skim Geran Penyelidikan UMK Fundamental (UMK FUND): R/FUND/A0400/02016A/001/2024/01225. This study was also supported by the Institut Penyelidikan dan Pengurusan Kemiskinan (InsPeK) and the Faculty of Language Studies and Human Development, Universiti Malaysia Kelantan, Malaysia.

BIODATA

Nur Hafifah Jamalludin is a lecturer at Universiti Malaysia Kelantan. Her PhD's, Master's and Bachelor's degrees in Communication (Human Sciences) with a specialisation in Organizational Communication from International Islamic University Malaysia. Her areas of expertise include cyber resiliency, cybercrime, cyber security, and social media usage, particularly its effects on adults and other related fields. Email: hafifah.j@umk.edu.my

Ateerah Abdul Razak is a Senior Lecturer at Universiti Malaysia Kelantan and Associate Fellow at InsPeK. Specialising in social psychology and community well-being, she leads an FRGS Hikmah Socialization Model project, authors academic books, received the MAPIM KPT-15 Best-Selling Book Award (2024), and contributes to community resilience and digital society research. Email: ateerah@umk.edu.my

Hasnah Ab.Kadir, PhD, is senior lecturer at Universiti Malaysia Kelantan. She holds a PhD of Communication from International Islamic University Malaysia. Among her areas of expertise are Communication, Organisation Communication, Business Communication, New Media and various related fields. Email: hasnah.ak@umk.edu.my

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Wan Yusoff Wan Shaharuddin is a Senior Lecturer at the Faculty of Language Studies and Human Development, Universiti Malaysia Kelantan. He holds a PhD in Communication and specialises in interpersonal communication, academic writing, and social communication research, with active involvement in teaching, supervision, and scholarly publications. Email: yusoff.ws@umk.edu.my

Ariezal Afzan Hassan is a Lecturer at the Faculty of Language Studies and Human Development, Universiti Malaysia Kelantan. He holds a Master's degree in Professional Communication from the University of Sydney and specialises in public relations, communication studies, and English language education, with active research and innovation involvement. Email: ariezal@umk.edu.my

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

REFERENCES

Adu, P. (2019). *A step-by-step guide to qualitative data coding*. Routledge. https://doi.org/10.4324/9781351044516

Agarwal, R., Dwivedi, S., & Singh, A. (2025). Five emerging strategies to detect and control fraud: Multiple case studies. *International Insurance Law Review*, *33*(S5), 57–71. https://doi.org/10.2139/ssrn.5692623

Agir, N., Effendi, M., & Matore, E. M. (2022). Literasi dan kewarganegaraan digital: Konsep dan strategi implementasi dalam pendidikan di Malaysia [Digital literacy and citizenship: Concepts and implementation strategies in education in Malaysia]. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *7*(3), Article e001367. https://doi.org/10.47405/mjssh.v7i3.1367

Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *2*, Article 100051. https://doi.org/pbzw

Allsop, D. B., Chelladurai, J. M., Kimball, E. R., Marks, L. D., & Hendricks, J. J. (2022). Qualitative methods with NVivo software: A practical guide for analyzing qualitative data. *Psych*, *4*(2), 142–159. https://doi.org/10.3390/psych4020013

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research*, *6*(2), 660–666. https://doi.org/10.20533/ijisr.2042.4639.2016.0076

Azman, H., Salman, A., Razak, N. A., Hussin, S., Hasim, M. S., & Hassan, M. A. (2014). Determining digital maturity among ICT users in Malaysia. *Jurnal Komunikasi: Malaysian Journal of Communication*, *30*(1), 22–34. https://doi.org/gg5bf5

Carter, T., & McNealey, R. L. (2025). Protection motivation and cybersecurity intentions: A visual conjoint experiment. *Journal of Experimental Criminology*, *21*(1), 1–28. https://doi.org/10.1007/s11292-025-09717-1

Cheng, H. H. (2026). E-Banking identity protection: A protection motivation and future-oriented emotion perspective. *International Journal of Human–Computer Interaction*, *42*(4), 2542–2567. https://doi.org/10.1080/10447318.2025.2530063

Cole, R. (2024). A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States. *Journal of Economic Criminology*, *6*, Article 100108. https://doi.org/10.1016/j.jeconc.2024.100108

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., Jr., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849–868. https://doi.org/rcrz

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/gcdvss

Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, *13*, Article 947234. https://doi.org/10.3389/fpsyg.2022.947234

Gajda, W. (2025). Legal foundations for developing anti-fraud policies in enterprises: Challenges and perspectives. *Public Administration and Law Review*, *6*(1), 90–98. https://doi.org/10.36690/2674-5216-2025-2-90-98

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Galinec, D., Steingartner, W., & Kozina, A. (2025). National cybersecurity strategy action plan implementation for cyber resilience: Qualitative exploration and achievements. *WSEAS Transactions on Business and Economics*, *22*, 1290–1304. https://doi.org/10.37944/23207.2025.22.105

Gautam, R., & Yadav, S. (2026). Psychological impact of cyber-crime on victims. *Current Psychology*, *45*(3), 240–251. https://doi.org/10.1007/s12144-025-08873-x

Gould, K. R., Carminati, J. Y. J., & Ponsford, J. L. (2023). "They just say how stupid I was for being conned": Cyberscams and acquired brain injury: A qualitative exploration of the lived experience of survivors and close others. *Neuropsychological Rehabilitation*, *33*(2), 325–345. https://doi.org/10.1080/09602011.2021.2016447

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: Evidence from China. *Frontiers in Public Health*, *13*, Article 1677024. https://doi.org/rcr2

Harrison, J., Hough, J., & Wood, M. (2022). *Experiences of victims of fraud and cyber crime* (Research Report No. 129). Home Office, Government of the United Kingdom. https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime

Irvin-Erickson, Y. (2024). Identity fraud victimization: A critical review of the literature of the past two decades. *Crime Science*, *13*(1), Article 3. https://doi.org/rcr3

Islam, M. A., & Aldaihani, F. M. F. (2022). Justification for adopting qualitative research method, research approaches, sampling strategy, sample size, interview method, saturation, and data analysis. *Journal of International Business and Management*, *5*(1), 1–11. https://doi.org/10.37227/jibm-2021-09-1494

Jamalludin, N. H., Kadir, H. A., Mohamed, A. F., Razak, A. A., & Abd Latif, S. F. (2026). Cybersecurity awareness and protective behaviour among young adult digital users: An educational perspective. *JETech: Journal of Education and Technology*, *2*(1), 40–45. https://doi.org/10.65678/jetech.v2i1.318

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228. https://doi.org/10.21428/88de04a1.976bcaf6

Klimek, L. (2026). Vertical and horizontal cooperation in combatting organised fraud in Slovakia. In *Financial crime and the office of the European Public Prosecutor* (pp. 92–116). Routledge. https://doi.org/10.4324/9781003403302-6

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90. https://doi.org/10.2307/20650279

Maina, C. W., Bashokoh, M. I., & Koponicsné Györke, D. (2026). A bibliometric analysis of digital financial literacy and its role in reducing online financial fraud in the European Union. *International Journal of Financial Studies*, *14*(1), Article 18. https://doi.org/10.3390/ijfs14010018

Misra, R. K., & Khurana, K. (2017). Employability skills among information technology professionals: A literature review. *Procedia Computer Science*, *122*, 63–70. https://doi.org/10.1016/j.procs.2017.11.342

Mohamed, S., Ghazali, W. N. W. M., & Nasir, N. S. M. (2023). Digital literacy and poverty: Investigating the digital experience of children living at Pusat Perumahan Rakyat (PPR). *Journal of Media and Information Warfare*, *16*(2), 50–67. https://doi.org/10.17576/ebangi.2022.1901.03

Mwirigi, P. K., Odini, C., & Rotich, D. C. (2026). The impact of digital literacy and technological tools on elderly health information practices. *African Journal of Emerging Issues*, *8*(1), 1–38. http://www.ajoeijournals.org/

Niman, S., Parulian, T. S., & Rothhaar, T. (2023). Online love fraud and the experiences of Indonesian women: A qualitative study. *International Journal of Public Health Science*, *12*(3), 1200–1208. http://doi.org/10.11591/ijphs.v12i3.22617

Novianti, I. D., & Chariri, A. (2025). Cybersecurity awareness and digital minimalism towards cyber fraud prevention in generation Z. *E-Jurnal Akuntansi*, *35*(9), 2428–2442. https://doi.org/10.24843/EJA.2025.v35.i09.p14

Oladiti, A. A., Ojebisi, A. O., & Akanni, J. O. (2026). Evaluation of cybercrime and internet-related fraud activities among undergraduate students of Emmanuel Alayande University of Education, Oyo State, Nigeria. *Federal University Gusau Faculty of Education Journal*, *6*(2), 314–322. https://doi.org/10.64348/zije.2026329

Osman, Z., Alwi, N. H., & Ahmad Khan, B. N. (2024). Psychological impact on the public susceptible to online scams. *International Journal of Academic Research in Business and Social Sciences*, *14*(5), 989–1014. https://doi.org/10.6007/ijarbss/v14-i5/21324

Pitchan, M. A., Salman, A., & Arib, N. M. (2025). A systematic literature review on online scams: Insights into digital literacy, technological innovations, and victimology. *Jurnal Komunikasi: Malaysian Journal of Communication*, *41*(1), 107–124. https://doi.org/10.17576/jkmjc-2025-4101-07

Proudfoot, K. (2023). Inductive/deductive hybrid thematic analysis in mixed methods research. *Journal of Mixed Methods Research*, *17*(3), 308–326. https://doi.org/10.1177/15586898221126816

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case study method: A step-by-step guide for business researchers. *International Journal of Qualitative Methods*, *18*, 1–13. https://doi.org/10.1177/1609406919862424

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sandra, L. (2026). Modeling adolescent online risk-taking through digital literacy and parental mediation in Indonesia. *Cogent Psychology*, *13*(1), Article 2624803. https://doi.org/10.1080/23311908.2026.2624803

Sanusi, A., Sanusi, I., Yinusa, S., & Abugh, I. (2025). Fraud risk management and organizational resilience: An empirical analysis controlling for organizational culture. *World Journal of Advanced Research and Reviews*, *26*(2), 2446–2458. https://doi.org/10.30574/wjarr.2025.26.2.1512

Senarak, C. (2021). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *The Asian Journal of Shipping and Logistics*, *37*(4), 345–360. https://doi.org/10.1016/j.ajsl.2021.10.002

Sirohi, N., & Misra, G. (2024). Vulnerability of individuals to economic crime and the role of financial literacy in its prevention: Evidence from India. *Crime, Law and Social Change*, *82*(1), 165–196. https://doi.org/10.1007/s10611-024-10138-w

Sulaiman, N. S., Hussain, S., & Fauzi, M. A. (2026). Cybersecurity practices among Malaysian government employees: The role of protection motivation theory and responsibility norms. *Asian Education and Development Studies*, *15*(1), 114–136. https://doi.org/rcr4

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30

Takona, J. P. (2024). Research design: Qualitative, quantitative, and mixed methods approaches. *Quality & Quantity*, *58*(1), 1011–1013. https://doi.org/gt4v2k

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Wang, F. (2025). Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. *International Review of Victimology*, *31*(1), 91–116. https://doi.org/10.1177/02697580241234331

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: Qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/grrm7h

Whitty, M. T. (2025). A systematic literature review of profiling victims of cyber scams: Setting up a framework for future research. *Cogent Social Sciences*, *11*(1), Article 2563781. https://doi.org/10.1080/23311886.2025.2563781

Wulandari, M. P., Wachid, I. B., Dahlia, S. I. T. I., Bahesa, S. B. P., & Arista, K. G. W. S. W. (2025). Digital public relations in Indonesia in the age of AI and big data: Theoretical and practical insights from a five-dimensional framework. *Jurnal Komunikasi: Malaysian Journal of Communication*, *41*(2), 405–427. https://doi.org/rcr5

Yusoh, M. H., Ghazali, W. N. W. M., Manan, K. A., Mohamed, S., Nasir, N. S. M., & Idris, H. (2024). Mapping out factors that undermining vaccine uptake in Malaysia: A multiple perspective. *IIUM Medical Journal Malaysia*, *23*(1), 106–114. https://doi.org/10.31436/imjm.v23i01.2334

Zhu, W., & Chang, K. (2023). Artificial intelligence in cyber fraud detection: Trends and challenges. *International Journal of Cybersecurity Research*, *21*(1), 34–49. https://doi.org/10.19107/cybercon.2023.11

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-30