



Journal of Advanced Research in Social and Behavioural Sciences

Journal homepage:
<https://karyailham.com.my/index.php/jarsbs/index>
ISSN: 2462-1951



Structural Modeling of Determinant Factors Influencing Online Scam Victimization in Malaysia: A DEMATEL Approach

Mohammad Nasrul Hakim Roslan^{1,*}, Ramlan Mustapha¹, Muhammad Hafis Mohd Hussain¹, Surita Hartini Mat Hassan¹, Mohd Nasir Ayub¹, Mohd Azim Zainal²

¹ Academy of Contemporary Islamic Studies, Universiti Teknologi MARA, Kampus Raub Pahang, Malaysia

² College of Computing and Mathematics, Universiti Teknologi MARA Pahang Branch Raub, Pahang, Malaysia

ARTICLE INFO

Article history:

Received 3 March 2026

Received in revised form 24 May 2026

Accepted 2 June 2026

Available online 3 July 2026

Keywords:

Scam; DEMATEL; social media influence; digital platforms; digital literacy; cyber fraud

ABSTRACT

The rise of online scam victimization in Malaysia presents a growing socio-economic concern, intensified by increasing digitalization and widespread use of online platforms. Existing literature often focuses on individual factors such as digital literacy, financial knowledge, and psychological susceptibility separately, resulting in limited insight into their interconnected effects. This study addresses this limitation by applying the DEMATEL approach to examine the causal structure among key determinants of scam victimization. Data from a multidisciplinary expert panel were used to evaluate four main factors: low digital literacy, low financial literacy, psychological and emotional influences, and the role of social media and digital platforms. The results show that social media and digital platforms function as the primary driving force within the system, influencing all other factors both directly and indirectly. In contrast, the remaining factors are classified as outcomes shaped by the digital environment rather than independent causes. These findings reposition online scam victimization as a systemic issue rooted in platform dynamics rather than individual weakness alone. The study contributes methodologically through the application of DEMATEL and offers practical insights for policymakers to develop more comprehensive, platform-aware, and targeted prevention strategies.

1. Introduction

Cheating and fraudulent practices have long been embedded in human history, predating the emergence of the digital age. Across different periods, individuals have devised a wide range of deceptive methods to exploit others, yet the underlying motive has remained largely consistent financial gain. From traditional schemes in earlier societies to more structured forms of deception, the intent to unlawfully obtain money has persisted as a central feature of fraudulent behavior.

* Corresponding author.

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

Scams and fraudulent activities have evolved substantially over recent decades, emerging as one of the most complex, widespread, and financially profitable forms of organised crime worldwide. Evidence reported by Amerhauser and Goodwin [1] indicates that approximately 57% of the global adult population encountered at least one scam incident within the preceding twelve months. Furthermore, available estimates indicate that scams and fraud collectively generated financial proceeds exceeding US\$1 trillion in 2024, underscoring the scale and economic significance of this growing criminal phenomenon.

With the rapid advancement of technology, however, the nature and execution of such activities have undergone a profound transformation. The rise of digital platforms has not only expanded opportunities for communication and commerce but has also created new avenues for exploitation [2]. These developments illustrate a significant shift from conventional fraud to complex, technology-driven crimes, highlighting the growing challenges faced by individuals, institutions, and legal systems in addressing modern forms of deception.

Fraud refers to any act of deception or wrongdoing committed intentionally to obtain personal or organizational gain, while simultaneously causing losses to other parties, particularly in financial terms. It involves the abuse of trust, manipulation of data, or acts of betrayal such as asset misappropriation and the preparation of false or misleading financial reports.

The significant increase in cyber fraud cases reflects a worrying trend in which digital technology, despite offering convenience in financial and commercial activities, has also become a medium exploited by irresponsible individuals or criminal syndicates. These increasingly sophisticated fraud schemes have a substantial impact on the national economy, while simultaneously placing greater pressure on authorities to address the issue through improvements in legal frameworks and the implementation of more effective enforcement mechanisms.

The term *scam* carries two primary meanings: first, it refers to the act of deceiving or defrauding an individual, and second, it denotes the act of obtaining something particularly money through deceptive practices. Financial scamming has emerged as a growing and increasingly prevalent phenomenon that is now formally recognised as a criminal offence.

Asian criminal syndicates have established themselves as dominant players in the global landscape of cyber-enabled fraud, money laundering, and illicit banking activities, while increasingly strengthening their cooperation with other major organized crime groups worldwide. Malaysia recorded a highly connected digital landscape in late 2025, with 44.0 million active cellular mobile connections, equivalent to 122% of the total population, although some of these connections were limited to voice and SMS services without internet access. In the same period, there were 35.4 million internet users, reflecting an internet penetration rate of 98.0%. Additionally, Malaysia had 30.7 million social media user identities in October 2025, accounting for 85.0% of the total population [3].

1.1 Types of Scams

1.1.1 Mail scams.

Mail scams involve fraudulent schemes conducted through traditional postal services or electronic mail. These scams typically include false prize notifications, investment offers, charity appeals, or requests for personal and financial information. Perpetrators often exploit the perceived legitimacy of written communication to gain victims' trust, using official-looking documents, logos, or fabricated endorsements to deceive recipients into making payments or disclosing sensitive information.

The experts highlights a growing and alarming trend in email-based cyber threats, demonstrating that one in four email messages is now classified as malicious or unwanted spam. This indicates a significant increase in user exposure to potentially harmful digital content. The report further reveals that 83% of malicious Microsoft 365 documents contain QR codes that redirect users to phishing websites, reflecting the rising use of QR-based social engineering tactics by cybercriminals. Additionally, 20% of organizations experience at least one Account Takeover (ATO) incident every month, emphasizing ongoing weaknesses in account security management [4].

The study also shows that nearly half of organizations have not implemented DMARC policies, leaving them vulnerable to email spoofing, phishing, and business email compromise. This vulnerability is reinforced by findings that almost one-quarter of HTML attachments are malicious, while more than three-quarters of organizations do not actively apply sufficient preventive measures against email threats. Moreover, Bitcoin extortion scams have emerged as a growing concern, accounting for 12% of malicious PDF attachments. Overall, these findings highlight the urgent need for organizations to strengthen their email security frameworks in response to increasingly sophisticated cyber threats.

1.1.2 Telephone scams.

Telephone scams are perpetrated through voice calls or text messages, whereby offenders impersonate legitimate entities such as government agencies, financial institutions, or service providers. These scams commonly rely on urgency, fear, or authority to pressure victims into immediate action, such as transferring funds, revealing one-time passwords, or confirming personal details. Advances in technology, including caller ID spoofing and automated calling systems, have further increased the effectiveness and scale of telephone-based fraud.

1.1.3 Doorstep scams.

Doorstep scams involve face-to-face deception, in which perpetrators approach victims, often elderly or vulnerable individuals at their residences. These scams may include false claims related to home repairs, utility services, or official inspections. By exploiting social norms of politeness and trust, offenders persuade victims to make immediate payments or allow access to their homes, which may result in financial loss or theft of property. Doorstep crime refers to situations where consumers are intentionally overcharged for poor-quality goods or services. This may involve demanding payment for unnecessary repairs, causing damage to property to create or justify paid work, charging for tasks that were never completed, abandoning work before it is finished, or using intimidation or coercive tactics to pressure individuals into paying money [4].

1.1.4 Online scams.

Online scams are executed through digital platforms such as websites, social media, e-commerce platforms, and messaging applications. Common forms include phishing attacks, love scams, fake online marketplaces, fraudulent investment schemes, romance scams, and impersonation scams. The anonymity and wide reach of the internet enable scammers to target many victims across geographical boundaries, making detection and enforcement more challenging. For online romance scams refer to deceptive relationships formed through websites, where perpetrators build romantic trust with unsuspecting victims to manipulate them into sending money [5]. These offenders often simulate genuine romantic involvement before ultimately exploiting the victim for financial gain. The

Nasdaq 2024 Global Financial Crime Report indicates that global losses attributable to online romance scams reached approximately US\$3.8 billion in 2023 [6].

Despite the increasing prevalence of online scams in Malaysia, existing studies have largely examined determinant factors such as low digital literacy, low financial literacy, psychological and emotional vulnerabilities, and the influence of social media and digital platforms in isolation. Most prior research relies on conventional statistical methods, which are limited in capturing the complex interrelationships among these factors. These determinants do not operate independently; rather, they interact within a broader system that shapes an individual's susceptibility to online scam victimization. For instance, low digital literacy may amplify the negative effects of misleading information disseminated through social media, while psychological and emotional factors can further weaken an individual's ability to critically evaluate financial risks. Without a comprehensive understanding of these interconnected dynamics, efforts to mitigate online scams may remain fragmented and less effective.

To address this gap, this study adopts the Decision-Making Trial and Evaluation Laboratory (DEMATEL) approach to structurally model the cause effect relationships among the key determinant factors influencing online scam victimization in Malaysia. Unlike traditional approaches, DEMATEL enables the identification of both direct and indirect influences, distinguishing between cause factors and effect factors within a complex system. Therefore, this study aims to examine how low digital literacy, low financial literacy, psychological and emotional factors, and the influence of social media and digital platforms interact and contribute to consumer vulnerability to scams. By mapping these structural relationships, the study seeks to provide deeper insights into the most influential drivers of scam susceptibility, offering more targeted and effective strategies for policymakers and stakeholders in combating online fraud in Malaysia.

2. Research Questions

"What are the key determinant factors influencing online scam victimization in Malaysia specifically low digital literacy, low financial literacy, psychological and emotional factors, and the influence of social media and digital platforms and how do these factors interact and contribute to victim susceptibility as analysed through a DEMATEL structural modelling approach?"

3. Literature Review

Scam and fraud have become increasingly prominent subjects of study within the fields of criminology, law, and cyber security. Existing literature highlights the rapid evolution of fraudulent activities, particularly with the advancement of digital technologies that enable cross-border crimes. Globally, researchers have examined various forms of scams, including online fraud, phishing, and financial deception, emphasizing their economic and psychological impacts.

A recent report BioCatch. [7] highlights the rapid and widespread rise of scams globally. Drawing on data from financial institutions that collectively serve nearly 350 million consumers across five continents, the study reveals that scam attempts surged by 65% over the past year. This includes a 100% increase in voice phishing (vishing) incidents, a 63% rise in attempted romance scams, and a 42% jump in investment scam attempts.

The findings reveal that this form of crime spans across 20 industry sectors in 162 countries, with cyber incidents in the financial sector accounting for approximately 10 percent over the past decade. These incidents are predominantly concentrated within the banking and securities sectors. Notably, cyber-enabled fraud has nearly tripled during this period; however, its true scale remains

underestimated due to incomplete reporting practices and significant data gaps across jurisdictions [8].

The study further highlights that credit transfers and credit cards represent the most commonly used payment methods in fraudulent activities, with a noticeable increase in reported payment fraud across several jurisdictions. In addition, there has been a growing trend in cyber incidents and fraudulent schemes involving cryptocurrencies.

Taken together, these developments underscore that cybercrime should not be underestimated. Its scale, complexity, and impact position it as a serious threat, comparable in many ways to traditional physical crimes, thereby demanding equal attention from policymakers, financial institutions, and society at large.

Understanding who scammers are is equally important in examining the phenomenon. Scammers may operate as organized criminal groups with sophisticated infrastructures, or as individual actors working independently. Organized groups often function in coordinated networks, utilizing advanced technologies, data analytics, fake email and scripted communication strategies to target large numbers of victims efficiently. In contrast, lone actors may rely on simpler techniques but can still be effective, particularly when exploiting niche opportunities or specific vulnerabilities. The concept of *modus operandi* is critical in this context, as it refers to the characteristic methods and patterns used by scammers, which can evolve over time to adapt to changing technological and regulatory environments.

From a technical perspective, phishing and e-commerce fraud involve a combination of digital tools and deceptive practices. Phishing attacks often employ spoofed emails, fake websites, or malicious links designed to closely resemble legitimate sources, thereby tricking users into disclosing confidential information. Nearly 57% of scam victims in 2022 were deceived through links sent via various communication platforms [9]. Similarly, e-commerce fraud may involve the creation of counterfeit websites, fake listings on legitimate platforms, or manipulation of payment systems to divert funds. These tactics are frequently supported by automation, data harvesting, and the use of anonymization tools, which make detection and prevention more challenging.

In the Malaysian context, studies indicate a growing trend in cyber-enabled fraud, raising concerns regarding the adequacy of legal frameworks, enforcement mechanisms, and public awareness. According to a media statement issued by Berita Harian [10] which refers to a report by the Polis Diraja Malaysia (PDRM), a total of 35,368 cases of cybercrime related to online financial fraud were reported in 2024. This figure represents an increase of 2.53% compared to 2023, with estimated financial losses amounting to RM1.58 billion. Furthermore, in the first quarter of 2025 alone, Malaysia recorded 12,110 cases of online fraud involving various forms of scams, including fake e-commerce offers, non-existent loan schemes, and fraudulent investment schemes, with total losses reaching RM573.7 million.

It's reported that fraud-related losses in Malaysia, as estimated by cybersecurity firm Fortinet Malaysia, reached approximately RM2.7 billion in 2025, representing a 76 percent increase compared to 2024 [10]. This rise was particularly pronounced during festive periods such as Hari Raya Aidilfitri. The trend has been largely driven by phishing campaigns, fraudulent e-commerce platforms, and deceptive payment links. Alongside the growing adoption of digital payment methods, including *e-hari raya* transfers, cybercriminals have increasingly exploited QR codes and payment channels to divert transactions unlawfully. Furthermore, the Cyber999 Incident Response Centre recorded 2,020 incidents in the third quarter of 2025, marking a year-on-year increase of over 20 percent, with phishing and online fraud accounting for approximately 75 percent of the total cases.

4. Methodology

4.1 Research Design

This study adopts the Decision-Making Trial and Evaluation Laboratory (DEMATEL) approach, a well-established structural modeling technique originally developed by the Science and Human Affairs Program at the Battelle Memorial Institute in Geneva between 1972 and 1976 to address complex and interrelated global challenges [6]. Since its inception, DEMATEL has evolved into a powerful multi-criteria decision-making (MCDM) method, widely recognized for its ability to systematically examine interdependent relationships among factors within complex systems. Through the construction of structural models and impact–relation maps, the approach allows researchers to clearly interpret causal connections and assess the intensity of influence among variables [11].

At its foundation, DEMATEL is designed to transform qualitative expert judgments into quantitative insights, enabling a deeper understanding of interdependencies and feedback mechanisms within a system [12]. Unlike traditional analytical methods that often assume criteria are independent, DEMATEL explicitly incorporates the dynamic interactions and mutual influences that characterize real-world decision-making environments. This capability makes it especially valuable for identifying key factors and analyzing both their direct and indirect effects on other components within a system [13]. Moreover, the method has been extensively applied across diverse domains including supply chain management, environmental assessment, technology evaluation, and organizational performance analysis demonstrating its flexibility and effectiveness in tackling complex, multi-dimensional decision-making problems [14].

4.2 Study Factors

Drawing on an extensive review of the literature on scam-related vulnerabilities, four primary economic determinants were identified as the focus of this study:

1. Low Digital Literacy (F1)

This factor reflects individuals' limited ability to effectively use digital technologies, recognize online threats, and assess the credibility of digital information, which increases susceptibility to online scams.

2. Low Financial Literacy (F2)

This determinant captures the lack of essential financial knowledge and decision-making skills, particularly in evaluating financial risks, managing transactions, and identifying fraudulent schemes.

3. Psychological and Emotional Factors (F3)

This factor encompasses behavioral and cognitive aspects such as impulsivity, trust, fear, greed, and emotional vulnerability, which can significantly influence an individual's likelihood of falling victim to scams.

4. Influence of Social Media and Digital Platforms (F4)

This determinant highlights the role of online platforms in facilitating scam activities, including exposure to deceptive advertisements, phishing attempts, and manipulated content that can mislead users.

4.3 Sampling Technique

The selection of an appropriate sampling strategy represents a critical component in the implementation of the DEMATEL method, as the credibility and representativeness of expert judgments directly influence the validity and reliability of the resulting structural model. Among the available sampling techniques, purposive sampling also known as judgmental or expert sampling is most commonly employed in DEMATEL studies. This approach involves deliberately selecting participants based on their specialized knowledge, extensive professional experience, and in-depth understanding of the research domain [11].

Determining the optimal sample size in DEMATEL research remains a subject of ongoing discussion in the literature. However, a widely accepted guideline suggests involving between 5 and 15 experts, as this range ensures a practical balance between capturing diverse viewpoints and maintaining manageability in data collection and consensus building [15]. The selection of experts is generally based on specific criteria, such as having a minimum of five years of relevant professional experience, holding at least a master's degree, actively participating in related decision-making activities, and demonstrating expertise through academic publications or significant practical contributions [16].

In the context of this study, titled *"Structural Modeling of Determinant Factors Influencing Online Scam Victimization in Malaysia: A DEMATEL Approach,"* a panel of five experts was deemed sufficient and appropriate. To ensure balanced and comprehensive insights, the expert panel was intentionally designed to be multidisciplinary, encompassing key domains aligned with the identified determinant factors: (1) Low Digital Literacy (F1), (2) Low Financial Literacy (F2), (3) Psychological and Emotional Factors (F3), and (4) Influence of social media and Digital Platforms (F4).

Specifically, the panel comprised:

- a digital literacy and cybersecurity specialist (F1: Low Digital Literacy),
- a financial literacy and consumer finance expert (F2: Low Financial Literacy),
- a behavioral psychologist or cognitive scientist (F3: Psychological and Emotional Factors),
- a social media and digital platform analyst (F4: Influence of Social Media and Digital Platforms), and
- a public policy or cybercrime prevention expert (cross-cutting perspective across F1–F4).

This multidisciplinary composition ensures that each determinant factor is evaluated from multiple professional perspectives, thereby enhancing the robustness and reliability of the causal relationship assessments generated through the DEMATEL analysis.

4.4 Research Instrument

A pairwise comparison questionnaire was utilized as the main instrument for data collection. The instrument was developed to evaluate the direct relationships among the four determinant factors

identified in this study, namely Low Digital Literacy (F1), Low Financial Literacy (F2), Psychological and Emotional Factors (F3), and the Influence of social media and Digital Platforms (F4).

In this questionnaire, experts were requested to assess the extent to which one factor exerts influence over another. All possible pairs of factors were systematically compared, leading to the formation of an influence relationship matrix. To standardize the evaluation process, a five-point scale was applied to represent the intensity of influence, defined as follows:

- 0 = No influence
- 1 = Very low influence
- 2 = Low influence
- 3 = High influence
- 4 = Very high influence

This scaling system enables the transformation of expert judgments into quantitative values, which can then be analyzed using the DEMATEL technique.

3. DEMATEL Procedural Framework

The DEMATEL method is implemented through a structured five-step procedure that converts expert judgments into a model of causal relationships. First, a direct-relation matrix is constructed based on expert evaluations of the influence between factors using a predefined scale (e.g., 0 to 4). Second, the matrix is normalized to ensure all values fall within a comparable range. Third, a total-relation matrix is derived to capture both direct and indirect effects. Fourth, prominence (D + R) and relation (D – R) indices are calculated to determine the importance of each factor and to classify them as cause or effect factors. Finally, a causal diagram is developed to visually represent these relationships, supporting clearer interpretation and decision-making.

3.1 Step In Dematel

Step 1	Step 1: Generate the direct relation matrix To identify the model of the relations among the n criteria, an n × n matrix is first generated. The effect of the element in each row is exerted on the element of each column of this matrix. If multiple experts' opinions are used, all experts must complete the matrix. arithmetic mean of all of the experts' opinions is used and then a direct relation matrix X is generated. $X = \begin{bmatrix} 0 & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{1n} & \cdots & 0 \end{bmatrix}$
Step 2	Compute the normalized direct-relation matrix To normalize, the sum of all rows and columns of the matrix is calculated directly. The largest number of the row and column sums can be represented by k. To normalize, it is necessary that each element of the direct-relation matrix is divided by k. $k = \max \left\{ \max \sum_{j=1}^n x_{ij}, \sum_{i=1}^n x_{ij} \right\}$ $N = \frac{1}{k} * X$
Step 3	Compute the total relation matrix After calculating the normalized matrix, the fuzzy total-relation matrix can be computed as follows: $T = \lim_{k \rightarrow +\infty} (N^1 + N^2 + \cdots + N^k)$

	In other words, an $n \times n$ identity matrix is first generated, then this identity matrix is subtracted from normalized matrix and the resulting matrix is reversed. The normalized matrix is multiplied by the resulting matrix to obtain the total relation matrix. $T = N \times (I - N)^{-1}$
Step 4	set the threshold value The threshold value must be obtained in order to calculate the internal relations matrix. Accordingly, partial relations are neglected and the network relationship map (NRM) is plotted. Only relations whose values in matrix T is greater than the threshold value are depicted in the NRM. To compute the threshold value for relations, it is sufficient to calculate the average values of the matrix T. After the threshold intensity is determined, all values in matrix T which are smaller than the threshold value are set to zero, that is, the causal relation mentioned above is not considered. In this study, the threshold value is equal to 1.838
Step 5	Final output and create a causal diagram The next step is to find out the sum of each row and each column of T (in step 3). The sum of rows (D) and columns (R) can be calculated as follows: $D = \sum_{j=1}^n T_{ij}$ $R = \sum_{i=1}^n T_{ij}$ Then, the values of D+R and D-R can be calculated by D and R, where D+R represent the degree of importance of factor i in the entire system and D-R represent net effects that factor i contributes to the system.

4. Findings

Criteria	r_i	c_i	$r_i + c_i$	$r_i - c_i$	Cause / Effect
Low Digital Literacy	3.42	4.33	7.75	-0.92	Effect
Low Financial Literacy	3.79	4.19	7.98	-0.40	Effect
Psychological and Emotional Factors	4.20	4.23	8.43	-0.03	Effect
Influence of Social Media and Digital Platforms	4.81	3.46	8.27	1.35	Cause

Noted : Factors with $R-C > 0$ are classified as **CAUSE** (influencer); $R-C < 0$ are classified as **EFFECT** (receiver).

The table illustrates the DEMATEL cause–effect analysis using the $r_i - c_i$ values. A positive value signifies that a factor belongs to the cause group, indicating that it predominantly exerts influence on other factors. Conversely, a negative value places a factor in the effect group, meaning it is largely influenced by other elements within the system.

The findings reveal that the Influence of Social Media and Digital Platforms (F4) is the sole factor categorized within the cause group ($r - c = 1.35$), identifying it as the most influential driving force in the model. This highlights that exposure to digital platforms and social media ecosystems plays a pivotal role in shaping other vulnerabilities associated with online scam victimization.

On the other hand, Low Digital Literacy (F1) ((-0.92)), Low Financial Literacy (F2) ((-0.40)), and Psychological and Emotional Factors (F3) ((-0.03)) fall under the effect group. Among these, Low Digital Literacy emerges as the most affected factor, suggesting that it is strongly shaped by other variables particularly the dynamics of digital platforms. Low Financial Literacy also shows a considerable level of dependence, while Psychological and Emotional Factors appear relatively balanced, though still slightly more influenced than influential.

Overall, these results indicate that the digital environment especially social media and online platforms acts as the primary starting point within the system, driving the development of other risk factors. In contrast, individual vulnerabilities, such as literacy levels and psychological conditions, tend to manifest as outcomes influenced by this dominant external force.

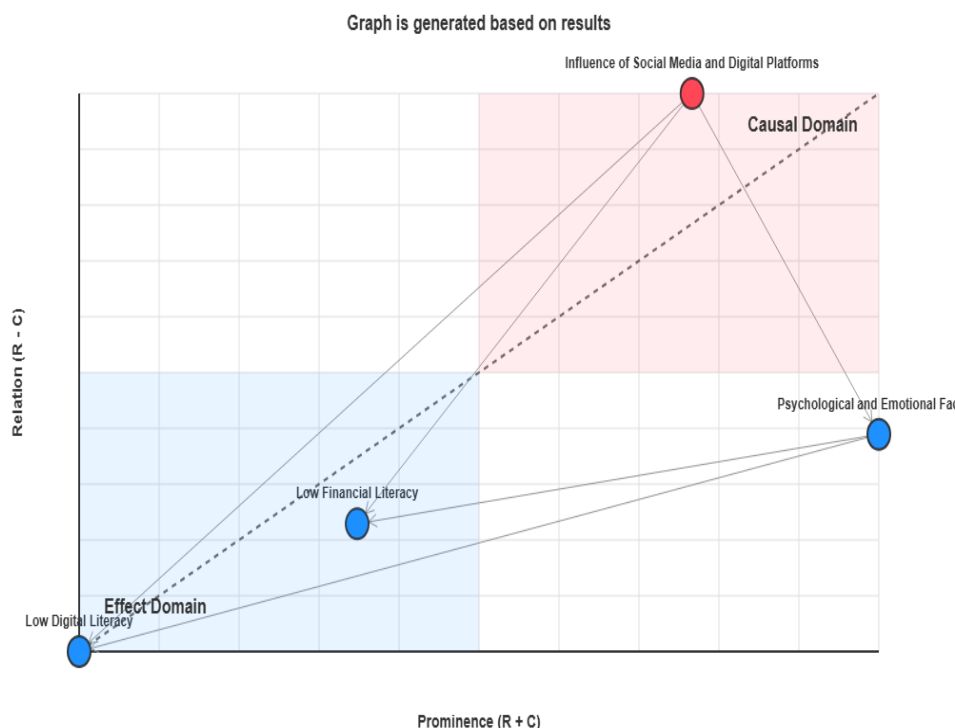


Fig. 2. Top 10 keyword

The network diagram (Figure 2) visualizes the positioning of each identified factor within a two-dimensional space defined by Prominence ($R + C$) on the horizontal axis and Relation ($R - C$) on the vertical axis. Prominence ($R + C$) reflects the overall significance of a factor in the system, capturing both its influence on other variables and the extent to which it is influenced. In contrast, Relation ($R - C$) differentiates the functional role of each factor, indicating whether it primarily acts as a causal driver (positive values) or as an effect or outcome (negative values).

Within this framework, the Influence of Social Media and Digital Platforms (F4) is situated in the upper-right quadrant, demonstrating both high prominence and a strong positive relational value. This position indicates that it is a key driving force within the system, exerting substantial influence on other factors while also maintaining high overall importance. It's alling with Tzeng *et al.*, [15], 63% of social media users and 3% of the general population reported having been victims of scams at least once. The study further explains that the risk of becoming a victim is associated with several psychological factors, including female gender, middle age, emotional instability, a tendency to idealize romantic relationships, a preference for thrill-seeking experiences, impulsive behavior, and a higher susceptibility to addiction.

In comparison, Psychological and Emotional Factors (F3) are located on the right side of the diagram but below the horizontal axis, placing them within the effect region. Although they exhibit relatively high prominence, their negative relational value suggests that they are primarily outcomes influenced by other factors rather than acting as main drivers. This implies that psychological and emotional conditions are significantly shaped by upstream influences in the system.

Meanwhile, Low Financial Literacy (F2) appears in the lower-left to central area of the diagram, indicating relatively lower prominence along with a negative relational value. This positioning suggests that it functions mainly as an effect factor with limited influence on other variables. Nonetheless, its connections within the network indicate that it still contributes meaningfully, albeit in a secondary capacity, to the overall system.

Finally, Low Digital Literacy (F1), positioned further toward the lower-left corner, displays both low prominence and a strongly negative relational value. This indicates that it is largely an outcome variable, minimally influencing other factors and instead being shaped by external drivers within the system.

Overall, the diagram reinforces the conclusion that the influence of digital platforms serves as the primary driving force, while psychological conditions and literacy-related factors predominantly emerge as consequences of these broader systemic interactions.

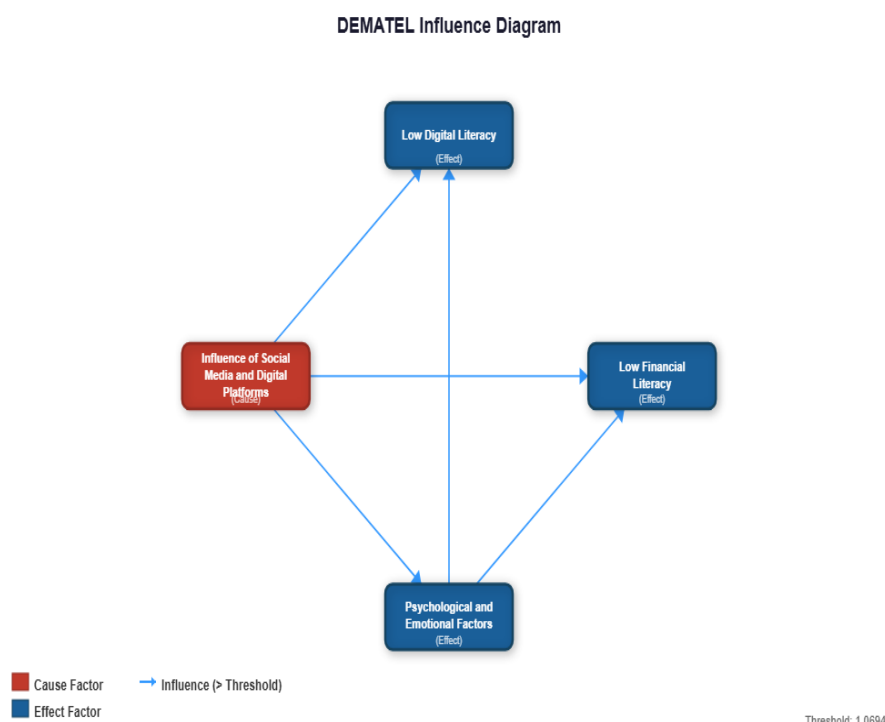


Fig. 3. Top keyword evolution over time

The findings reveal that the Influence of Social Media and Digital Platforms (F4) is the only factor classified within the cause group, positioning it as the central driving force in the network. It exhibits strong directional influence over several variables, including Low Digital Literacy (F1), Low Financial Literacy (F2), and Psychological and Emotional Factors (F3). This central role underscores its importance in shaping both cognitive and behavioral outcomes, suggesting that interactions with digital platforms significantly impact users' literacy levels and psychological states.

Among the identified influencing factors, Psychological and Emotional Factors (F3) hold a relatively central position due to their multiple incoming and outgoing relationships. While these factors are largely shaped by exposure to social media and digital platforms, they also have a significant impact on Low Digital Literacy (F1) and Low Financial Literacy (F2). This suggests a mediating role, whereby psychological and emotional responses may intensify or reinforce existing limitations in digital and financial literacy.

This observation is further supported by a reported case in *Free Malaysia Today (FMT)* [17], which described a love scam incident involving a victim who, influenced by trust and emotional attachment, began communicating with an individual claiming to be from Yemen via Facebook and later continued the interaction on WhatsApp. Between 5 February 2024 and 25 March 2024, the victim carried out 166 transactions, transferring a total of RM925,850 into 15 different bank accounts, ultimately resulting in a financial loss of nearly RM1 million.

Similarly, Low Financial Literacy (F2) is identified as an effect factor, influenced both directly by digital platforms and indirectly through psychological and emotional conditions. This suggests that financial literacy is shaped by a combination of external informational exposure and internal cognitive or emotional processes [18].

In the same vein, Low Digital Literacy (F1) appears as an effect factor that is directly influenced by both Influence of Social Media and Digital Platforms (F4) and Psychological and Emotional Factors (F3). Its position highlights a strong dependency on both technological environments and individual psychological conditions. Modern society is increasingly reliant on gadgets and social media platforms. However, knowledge related to digital security remains limited. Users are often unaware of the risks of exposing their personal data to unauthorized parties. This situation increases the likelihood of cybercrime occurrences. According to Reda, [19], a low level of awareness plays a significant role in the rise of such cases.

Overall, the diagram emphasizes that the influence of social media and digital platforms serves as the primary source of causality within the system, driving changes across both literacy and psychological domains. In contrast, digital and financial literacy, along with psychological outcomes, largely emerge as consequences of this dominant influence, with psychological factors additionally functioning as a secondary mediator that reinforces these effects.

5. Discussion and Conclusions

5.1 Discussion

This study applies the DEMATEL method to identify the relationships among key factors influencing the risk of online scam victimization in Malaysia, including low digital literacy, low financial literacy, psychological and emotional factors, as well as the influence of social media and digital platforms. The analysis highlights that these factors are interconnected within a complex system rather than operating independently.

The findings reveal that the influence of social media and digital platforms emerges as the primary cause factor, making it the dominant driver of online scam incidents. This indicates that the digital environment plays a crucial role in shaping users' exposure to fraudulent content, social manipulation, and increasingly sophisticated scam techniques [21]. Platform characteristics such as recommendation algorithms, anonymity, and rapid information dissemination further intensify this risk.

In contrast, low digital literacy, low financial literacy, and psychological and emotional factors are classified as effect factors influenced by external conditions. Among these, low digital literacy shows the strongest impact, suggesting that insufficient digital knowledge can weaken users' ability to recognize cyber threats. Psychological and emotional factors, meanwhile, act as reinforcing elements that further increase vulnerability, particularly in emotionally driven scams involving trust and relationships. For instance, criminals often employ impersonation tactics by posing as law enforcement officers and falsely claiming that victims are involved in criminal cases, which pressures victims into complying with instructions such as transferring money and disclosing their financial account information [20].

In conclusion, this study emphasizes that online scam victimization should be understood from a broader system perspective. It is not solely the result of individual weaknesses but is also shaped by the structure of the digital ecosystem. Therefore, effective prevention strategies should go beyond individual awareness and also address platform-level mechanisms alongside improving users' digital literacy and awareness.

5.2 Conclusion

This study contributes to the field of online scam research by applying the DEMATEL method to analyse the cause-and-effect relationships among key factors in Malaysia. The analysis reveals that the influence of social media and digital platforms acts as the dominant cause factor, while other factors such as low digital literacy, low financial literacy, and psychological and emotional factors function as effect factors within the system.

These findings highlight that online scam victimization is not merely the result of individual weaknesses, but rather the outcome of complex interactions between users and the digital environment. Therefore, prevention strategies should go beyond individual education and also incorporate stronger platform governance, improved system security design, and stricter regulatory enforcement of the digital ecosystem.

By clearly distinguishing between cause and effect factors, this study provides a more systematic framework for policymakers and relevant stakeholders to implement more targeted and effective intervention measures.

5.3 Limitations of the Study

This study has several limitations despite its significant contributions. First, the use of the DEMATEL method, which relies on expert judgment, may introduce a degree of subjectivity, although mitigation measures were applied through the involvement of a multidisciplinary expert panel. In addition, the study only considers four key factors, excluding other relevant variables such as regulatory enforcement, technological safeguards, and socio-cultural influences, which may also play important roles in online scam phenomena. Furthermore, the findings are specific to the Malaysian context and may not be directly generalizable to other countries.

Finally, the cross-sectional nature of the study does not allow for the observation of dynamic changes in relationships among factors over time, particularly as scam tactics and the digital environment continue to evolve.

5.4 Recommendations for Future Research

Future research can be further extended through several additional approaches. First, new variables such as institutional trust, regulatory effectiveness, and platform design features could be incorporated to broaden the scope of the analytical model.

Second, hybrid approaches that integrate DEMATEL with Structural Equation Modeling (SEM) or the Analytic Network Process (ANP) may be employed to statistically validate and more precisely assess causal relationships. Longitudinal studies are also recommended to examine how the structure of factors evolves over time, particularly in response to changes in platform policies, governmental interventions, and levels of public awareness.

In addition, cross-national comparative studies could be conducted to determine whether similar findings hold in different cultural and regulatory contexts. Finally, integrating empirical data such as

platform records or victim narratives could strengthen the robustness of the analysis and enhance the policy relevance of the findings.

Acknowledgement

This research did not receive any grant funding.

References

- [1] Amerhauser, K., & Goodwin, A. (2026, March 16). *A world of deceit: Mapping the landscape of the global scam centre phenomenon*. Global Initiative Against Transnational Organized Crime. <https://globalinitiative.net/analysis/mapping-global-scam-center-phenomenon/>
- [2] Pitchan, Muhammad Adnan, Siti Zobidah Omar, and Akmar Hayati Ahmad Ghazali. "Amalan keselamatan siber pengguna Internet terhadap buli siber, pornografi, e-mel phishing dan pembelian dalam talian." *Jurnal Komunikasi: Malaysian Journal of Communication* 35, no. 3 (2019): 212-227. <https://doi.org/10.17576/JKMJC-2019-3503-13>
- [3] DataReportal, "Digital 2026: Malaysia," *DataReportal*, 2026. [Online]. Available: https://datareportal.com/?utm_source=DataReportal&utm_medium=Country Article Hyperlink&utm_campaign=Digital 2026&utm_term=Malaysia&utm_content=Home Page Link. Accessed: Apr. 10, 2026.
- [4] Day, Tim. "Lost in the system: Locating rogue trading incidents in police statistics." *Crime prevention and community safety* 17, no. 3 (2015): 189-204. [doi: 10.1057/cpcs.2015.10](https://doi.org/10.1057/cpcs.2015.10).
- [5] Whitty, Monica T., and Tom Buchanan. "The online romance scam: A serious cybercrime." *CyberPsychology, Behavior, and Social Networking* 15, no. 3 (2012): 181-183. <http://dx.doi.org/10.1089/cyber.2011.0352>
- [6] Nasdaq Inc.; Verafin, 2024 *Global Financial Crime Report* (2024), <https://static.poder360.com.br/2024/03/relatorio-crimes-financeiros-nasdaq-2024.pdf> (accessed April 10, 2026).
- [7] BioCatch. "Banking Scams Up 65% Globally in Last Year." Published October 15, 2025. <https://www.biocatch.com/press-release/banking-scams-up-65-globally-in-last-year>
- [8] Khiaonarong, Tanai, and Shanyuan Zheng. "The rise of cyber events and digital fraud in the financial sector." (2026).
- [9] Petrosyan, A. 2023. Scam encounter rate in selected countries 2022, by vector. Statista. <https://www.statista.com/statistics/1389388/scam-rate-in-selected-countries-by-vector/> /. Accessed 10 April 2026
- [10] Berita Harian. (2026). *Kerugian akibat 'scam' cecah RM2.7 bilion tahun lalu, memuncak pada musim perayaan*. <https://www.bharian.com.my/bisnes/lain-lain/2026/03/1524795/kerugian-akibat-scam-cecah-rm27-bilion-tahun-lalu-memuncak-pada>
- [11] Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Sage Publications.
- [12] Wu, Wei-Wen, and Yu-Ting Lee. "Developing global managers' competencies using the fuzzy DEMATEL method." *Expert systems with applications* 32, no. 2 (2007): 499-507. <https://doi.org/10.1016/j.eswa.2005.12.005>
- [13] Tzeng, Gwo-Hshiung, Cheng-Hsin Chiang, and Chung-Wei Li. "Evaluating intertwined effects in e-learning programs: A novel hybrid MCDM model based on factor analysis and DEMATEL." *Expert systems with Applications* 32, no. 4 (2007): 1028-1044. <https://doi.org/10.1016/j.eswa.2006.02.004>
- [14] Si, Sheng-Li, Xiao-Yue You, Hu-Chen Liu, and Ping Zhang. "DEMATEL technique: a systematic review of the state-of-the-art literature on methodologies and applications." *Mathematical problems in Engineering* 2018, no. 1 (2018): 3696457. <https://doi.org/10.1155/2018/3696457>
- [15] Tzeng, Gwo-Hshiung, Cheng-Hsin Chiang, and Chung-Wei Li. "Evaluating intertwined effects in e-learning programs: A novel hybrid MCDM model based on factor analysis and DEMATEL." *Expert systems with Applications* 32, no. 4 (2007): 1028-1044. <https://doi.org/10.1016/j.eswa.2006.02.004>
- [16] Shieh, Jiunn-I., Hsin-Hung Wu, and Kuan-Kai Huang. "A DEMATEL method in identifying key success factors of hospital service quality." *Knowledge-Based Systems* 23, no. 3 (2010): 277-282. <https://doi.org/10.1016/j.knosys.2010.01.013>
- [17] *Free Malaysia Today (FMT)*, "Woman loses nearly RM1mil to love scam," accessed: Apr. 10, 2026. URL : <https://www.freemalaysiatoday.com/category/nation/2025/05/13/woman-loses-nearly-rm1mil-to-love-scam>
- [18] *Berita Harian Online*, "95 peratus kes penipuan kewangan atas kebenaran sendiri," Apr. 2026. [Online]. Available: <https://www.bharian.com.my/berita/nasional/2026/04/1529272/95-peratus-kes-penipuan-kewangan-atas-kebenaran-sendiri>. Accessed: Apr. 10, 2026.
- [19] N. M. Reda, "Jangan leka jenayah penipuan kewangan masih berleluasa," *Bernama / Astro Awani*, Dec. 2023. [Online]. Available: <https://www.astroawani.com/berita-malaysia/jangan-leka-jenayah-penipuan-kewangan-masih-berleluasa-451907>. Accessed: Apr. 10, 2026.

- [20] N. A. M. Amin, "Wanita rugi RM1.08j diperdaya 'pegawai polis'," *Sinar Harian*, 2023. [Online]. Available: <https://www.sinarharian.com.my/article/642027/berita/semasa/wanita-rugi-lebih-rm108juta-diperdaya-pegawai-polis>. Accessed: Apr. 10, 2026.
- [21] Coluccia, Anna, Andrea Pozza, Fabio Ferretti, Fulvio Carabellese, Alessandra Masti, and Giacomo Gualtieri. "Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review." *Clinical practice and epidemiology in mental health: CP & EMH* 16 (2020): 24. <https://doi.org/10.2174/1745017902016010024>

APPENDIX

Structural Modeling of Determinant Factors Influencing Online Scam Victimization in Malaysia: A DEMATEL Approach

Method: DEMATEL

Scale: Scale 0-4 (DEMATEL/ISM)

Date: 3/3/2026

Soalan Pairwise Comparison

No	Influencing Factors	Factor Influenced	Scale
1	Low Digital Literacy (F1)	Low Financial Literacy (F2)	0 / 1 / 2 / 3 / 4
2	Low Digital Literacy (F1)	Psychological and Emotional Factors (F3)	0 / 1 / 2 / 3 / 4
3	Low Digital Literacy (F1)	Influence of Social Media and Digital Platforms (F4)	0 / 1 / 2 / 3 / 4
4	Low Financial Literacy (F2)	Low Digital Literacy (F1)	0 / 1 / 2 / 3 / 4
5	Low Financial Literacy (F2)	Psychological and Emotional Factors (F3)	0 / 1 / 2 / 3 / 4
6	Low Financial Literacy (F2)	Influence of Social Media and Digital Platforms (F4)	0 / 1 / 2 / 3 / 4
7	Psychological and Emotional Factors (F3)	Low Digital Literacy (F1)	0 / 1 / 2 / 3 / 4
8	Psychological and Emotional Factors (F3)	Low Financial Literacy (F2)	0 / 1 / 2 / 3 / 4
9	Psychological and Emotional Factors (F3)	Influence of Social Media and Digital Platforms (F4)	0 / 1 / 2 / 3 / 4
10	Influence of Social Media and Digital Platforms (F4)	Low Digital Literacy (F1)	0 / 1 / 2 / 3 / 4
11	Influence of Social Media and Digital Platforms (F4)	Low Financial Literacy (F2)	0 / 1 / 2 / 3 / 4
12	Influence of Social Media and Digital Platforms (F4)	Psychological and Emotional Factors (F3)	0 / 1 / 2 / 3 / 4

Senarai Items / Factors

Kod	Nama Item
F1	Low Digital Literacy
F2	Low Financial Literacy
F3	Psychological and Emotional Factors
F4	Influence of Social Media and Digital Platforms