

Development and Initial Validation of a Multidimensional Scale for Assessing Repeated Online Fraud Victimization

Khairunesa Isa^{1*}, Nor Shela Saleh², Sarala Thulasi Palpanadan³, Afida Mastura Muhammad Arif⁴,
Ismah Omar⁵

^{1,2}Centre for General Studies and Co-curricular, Universiti Tun Hussein Onn Malaysia

³Centre for Language Studies, Universiti Tun Hussein Onn Malaysia

⁴Faculty of Human Ecology, Universiti Putra Malaysia

⁵Faculty of Business and Management, Puncak Alam Campus, Universiti Teknologi MARA Cawangan Selangor

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100600954>

Received: 22 June 2026; Accepted: 27 June 2026; Published: 09 July 2026

ABSTRACT

This study aimed to develop and validate a psychometric instrument for identifying factors contributing to repeated online fraud victimisation and its associated consequences. Guided by Cyber-Routine Activity Theory (Cyber-RAT) and Cognitive-Behavioral Theory, the study examined the influence of attitudes, situational conditions, and fraud strategies on the economic, social, and psychological impacts experienced by victims. A quantitative research design was employed, with data collected from 149 respondents using a structured questionnaire and analysed through exploratory factor analysis, correlation analysis, and multiple regression techniques to assess the instrument's reliability, validity, and the relationships among constructs. The findings demonstrated that the instrument possessed strong psychometric properties, with satisfactory reliability and construct validity. Significant relationships were identified between the predictor variables and victim impacts, with attitudes and fraud strategies emerging as stronger predictors than situational conditions, highlighting the importance of cognitive and behavioural factors in repeated online fraud victimisation. The study contributes to the literature by providing a validated psychometric instrument that integrates Cyber-RAT and Cognitive-Behavioral Theory to measure both the antecedents and multidimensional impacts of online fraud victimisation. The instrument offers practical value for researchers, policymakers, financial institutions, and digital security agencies in developing targeted fraud prevention, consumer protection, and intervention strategies.

Keywords: Online fraud, repeated victimisation, instrument validation.

INTRODUCTION

The utilization of the internet during the era of Industry 4.0 has significantly facilitated users in acquiring their desired necessities and preferences expeditiously. This expedited attainment results from the convenient, simplified, and prompt access to a myriad of resources available online. The presence of diverse search engines, including Yahoo, Google, Bing, and popular video-sharing platforms such as YouTube, TikTok, and Instagram, not only empowers users with a plethora of options for making informed purchase decisions but also extends a fertile ground for an increased number of entrepreneurs to engage in e-commerce activities.

Although the literature on online fraud is increasing, the existing literature has mostly concentrated on victimisation on a one-time basis or a one-behaviour predictor. The validated multidimensional instruments to capture the complexity of repeated victimisation in behavioural, situational, and psychological domains are still lacking. This restricts empirical modelling as well as policy intervention design. Hence, this paper fills this gap

by creating and confirming a theory-based tool incorporating cyber-environmental exposure and cognitive vulnerability processes.

Problem Statement

Since the implementation of the Movement Control Order (MCO) in 2019, there has been a discernible and disconcerting surge in the incidence of online scams. Instances involving victims falling prey to various forms of online fraud, such as the Macau Scam, Love Scam, fictitious investments, and account manipulation schemes, have become increasingly pervasive within contemporary society. Data from the Royal Malaysian Police (PDRM) highlights a concerning trend, revealing a consistent escalation in complaints lodged by victims of online fraud over a three-year period commencing in 2019. According to PDRM statistics, in 2020 alone, law enforcement received an average of 47 daily complaints pertaining to online fraud cases. The situation further deteriorated in 2021, with a daily influx of 57 reported cases, and this distressing trend persisted, with an uptick to 72 cases registered from January to May 2022.

According to a report issued by the Ministry of Domestic Trade and Consumer Affairs (KPDNHEP), three states have prominently featured as hotspots for consumer complaints. These states include Selangor, with 4,611 grievances registered, Kuala Lumpur with 3,601 complaints, and Johor with 1,272 recorded grievances. The most prevalent category of complaints pertained to online transaction fraud, with a staggering 4,760 cases reported, followed closely by deceptive pricing practices, documented in 4,187 cases, and misleading service claims, amounting to 3,289 cases. Alarmingly, the number of complaints related to fraudulent activities has exhibited a significant surge of 100 percent between 2020 and 2022. This increase has been substantial, rising from a mere 548 complaints in 2020 to a concerning 1,124 in 2022, resulting in substantial cumulative losses amounting to tens of millions of Malaysian Ringgit.

The Malaysian Communications and Multimedia Commission (MCMC) has reported a total of 5,513 complaints related to online fraud between 2020 and May 2023, encompassing various scams such as Love Scams, Macau Scams, Part-time Work Scams, Online Loans, and fraudulent parcel schemes (Astro Awani, June 6, 2023). Furthermore, Gogolook's 2022 Annual Fraud Report has highlighted a concerning statistic. Malaysia has taken the unfortunate top position in terms of mobile phone number leakage, revealing that over 21 million individuals, or 73% of affected users, have had their mobile phone numbers compromised or traded within online fraud syndicates.

A comprehensive examination of previous scholarly investigations reveals that a multitude of research studies have been conducted on the topic of online purchasing behaviours. These studies have concentrated on diverse aspects such as demographics, personal characteristics, target population, influencing factors, and the intention to engage in online purchases (Zahari et al., 2019; Zheng & Geetha, 2019; Makmor et al., 2019; Norlina et al., 2020; Yeo et al., 2020; Rahim & Kamaluddin, 2021). In a recent study conducted by Chen Li Yin et al. (2023), it was found that there was a positive correlation between trust, social influence, perceived utility, attitude, and online purchase behavior. The urgency to address this matter promptly arises from its far-reaching consequences, which impact not only the affected individuals but also their close family members. Sulaiman et al. (2022) conducted a study to confirm the increasing occurrence of scam-related victims (Noor et al., 2020).

This situation has a significant impact on the financial welfare of individuals. Numerous academic inquiries have shed light on a notable association between vulnerability to fraudulent schemes and various elements, including inadequate understanding of cybersecurity, gaps in expertise, and unique psychological inclinations. Nevertheless, a more disconcerting issue is the increasing prevalence of recurrent instances of online fraud victimization. Therefore, this study aimed to:

- i. Identify the factors that lead to repeated online fraud victims (attitude, current situation, and fraud techniques);
- ii. Identify the effect of repeated online fraud victims (economic, social, and psychology);

- iii. Determine the relationship between causal factors and the consequences of repeated online fraud victimization;
- iv. Determine the dominant causative factors affecting repeat online fraud victims.

LITERATURE REVIEW

Existing scholarly literature provides compelling evidence that certain behavioural traits such as impulsivity, gullibility, and excessive trust alongside emotional states like loneliness, desire, or financial desperation, increase one's vulnerability to fraud. A recent large-scale population study ($n = 4,043$) in Singapore confirmed that individuals with higher impulsivity and stress sensitivity were significantly more likely to become scam victims (Teo, Khader, & Chai, 2023). Similarly, Ahmad (2025) identified bias-induced gullibility as a key mediator between financial literacy and victimisation risk, demonstrating that even well-informed individuals can be deceived if they rely on intuitive rather than analytical thinking.

Remarkably, despite the growing awareness of the prevalence of such fraudulent schemes, individuals often fail to perceive their own vulnerability until they themselves experience victimization. In numerous instances, victims tend to underestimate their susceptibility to scams, as highlighted by Williams et al. (2017). Notably, the inability to discern and identify fraudulent communications remains a key contributor to scam victimisation. This cognitive limitation is explained through the Heuristic-Systematic Model, where individuals who rely heavily on heuristic processing such as trusting visual appeal or urgency cues are more susceptible to deception (Frontiers in Psychology, 2023). This reinforces the need to develop critical cognitive filters, particularly among frequent digital users.

The prevailing lack of consumer scepticism has contributed to the increasing frequency of online fraud cases. Many consumers display a tendency to accept promotional content without verification, especially when faced with unusually low prices. Robinson and Edwards (2024), in their experimental study involving scam-baiting simulations, demonstrated that trust-prone individuals particularly older users exhibited lower resistance to scam persuasion, confirming that excessive trust is a critical vulnerability in fraud contexts. According to Cecilia Desy Widya Permata Sari (2015), trust is the most important thing for any online sale. This is because people who buy things on the Internet will only do so if they trust the company and are willing to take chances. Meanwhile, Nurul Azifah and Citra Kusuma Dewi (2016) say that purchasing is a habit that can be grouped as a person's way of getting a certain product. That depends on how someone acts and thinks. In line with this, Zhi and Zhi (2022) found that age, schooling, and social support are all linked to being a victim of fraud. On the other hand, impulsiveness, trusting people easily, using a smartphone, and having bad life experiences are all linked to being a victim of fraud.

Zhi and Zhi (2022) highlighted that demographic factors such as age, lower education, and limited social support are strongly associated with heightened fraud vulnerability. These findings are consistent with Drew and Webster (2024), who observed that victims of romance scams often report low self-esteem and poor social networks factors that exacerbate emotional dependency and reduce scam detection ability. Moreover, psychological attributes represent an additional risk factor that contributes to the vulnerability of individuals who fall victim to fraud. These attributes include self-control, impulsivity, propensity to trust, and willingness to take risks (Zhi & Zhi, 2022). According to Wan Shahrazad et al., (2022), a person's psychology could significantly influence their susceptibility to becoming a victim of fraud. The psychological factors of an individual can significantly influence their vulnerability to being a victim of scams. The individual characteristics and cognitive processing abilities of a person have a substantial role in determining the extent to which they can be affected by fraudulent individuals.

Beyond emotional and cognitive traits, certain personality dispositions also play a role in scam victimisation. Traits such as neuroticism, agreeableness, and openness may predispose individuals to social manipulation. Additionally, limited awareness of financial fraud risk particularly among older adults remains a persistent concern. Ahmad (2025) emphasises that cognitive biases, when combined with limited digital literacy, significantly increase fraud susceptibility even among financially stable individuals. The extent of an individual's knowledge, particularly among older adults, significantly influences their vulnerability to financial exploitation.

Older individuals who lack awareness of the risk factors associated with the financial exploitation of older adults are more susceptible to fraudulent activities (Jackson, 2017).

The prevalence and complexity of online fraud continue to rise due to advances in digital communication and scammer techniques. This is evidenced by George et al. (2020), who reported that scam victims often suffer both financial losses and emotional trauma. More recent findings by Drew and Webster (2024) underscore that emotional manipulation especially in the context of online relationships remains a powerful tool used by fraudsters to exploit trust and personal vulnerability. Numerous scholarly investigations have been dedicated to examining diverse facets of fraudulent activities. The recent academic literature on online scam victimization has examined various aspects of the phenomenon. Specifically, studies conducted within the past five years focused on topics such as the vulnerability and characteristics of scam victims (Gainsbury, 2019; Norris & Brookes, 2021), techniques employed by scammers in the online realm (Pouryousefi & Frooman, 2019), the development of instruments to measure individuals' experiences with online scams (George et al., 2020), and the creation of systems to detect online scams (Vinayakumar et al., 2018).

THEORITICAL FRAMEWORK DEVELOPEMNT

This study draws upon an integrated theoretical framework combining Cyber-Routine Activity Theory (Cyber-RAT) and Cognitive-Behavioral Theory (CBT) to explain the phenomenon of repeated online fraud victimisation. By synthesising both environmental and psychological dimensions, the framework offers a comprehensive lens through which the dynamics of victim vulnerability can be examined. It aligns with the current shift in cyberpsychology research towards models that acknowledge the interplay between user behaviour, digital exposure, and internal cognitive-emotional states.

Cyber-Routine Activity Theory, an adaptation of Cohen and Felson's (1979) original Routine Activity Theory, explains victimisation based on the convergence of three elements: (i) a motivated offender, (ii) a suitable target, and (iii) the absence of capable guardianship. In the digital environment, this translates into predictable user behaviours such as regular online purchases, social media engagement, and interaction with unfamiliar sellers that create opportunities for scammers. Research by Vakhitova and colleagues (2025) emphasises that modern online lifestyles, particularly among digital natives, increase the exposure of users to fraudulent risks in the absence of digital safeguards. Similarly, Gan et al. (2024) observed that high-risk online activities significantly increase susceptibility to phishing scams among Malaysian Gen-Z users. These findings confirm that cybercrime is not solely dependent on the presence of offenders but heavily influenced by victims' routine online behaviours and weak digital protection structures.

In the context of this study, Cyber-RAT is applied through two constructs: current conditions and fraud strategies. The former captures situational risk factors such as frequency of internet use, types of platforms accessed, and purchasing habits all of which increase a user's visibility and exposure to scams. The latter refers to the evolving and manipulative techniques used by cybercriminals to deceive victims repeatedly. In situations where regulatory oversight or consumer protection is lacking, the likelihood of fraud recurrence increases. Thus, Cyber-RAT explains the environmental and behavioural components that enable repeated online victimisation.

However, structural opportunity alone does not fully explain why some individuals become repeat victims while others do not. To address this gap, this study incorporates Cognitive-Behavioral Theory (CBT), which offers insight into the internal psychological mechanisms that influence risk perception and decision-making. Rooted in the work of Beck (1976), CBT posits that individuals interpret events based on underlying cognitive schemas, which may become distorted following negative experiences. In fraud contexts, previous victimisation can alter an individual's belief system, leading to thoughts such as "I can handle it better next time" or "this deal looks genuine" despite warning signs. Studies by Ahmad (2024) and Hoffmann et al. (2023) suggest that individuals with lower cognitive control and higher susceptibility to heuristics or emotional persuasion are significantly more likely to fall victim to scams. This includes those who exhibit overconfidence, impulsiveness, or experience feelings of loneliness or social isolation, all of which can impair judgement.

The application of CBT in this study is reflected through the construct of attitude, which encompasses cognitive predispositions such as trust levels, perceived risk, and personal responsibility. These attitudes are shaped by

past experiences and influence how individuals respond to potentially fraudulent situations. Additionally, the construct of psychological impact serves to measure the emotional aftermath of victimisation, such as trauma, guilt, or desensitisation responses that may, paradoxically, make victims more vulnerable to repeated deception. The integration of CBT highlights that repeated victimisation is not merely an outcome of external exposure, but also a product of internal cognitive-emotional processes.

By combining Cyber-RAT and CBT, this study advances a dual-theoretical understanding of repeated online fraud victimisation, aligning with recent scholarly calls for more holistic models in cybercrime research. It proposes that victimisation results from the interaction between environmental exposure (current conditions and fraud techniques) and cognitive vulnerabilities (attitudes and psychological predispositions). This theoretical framework not only justifies the inclusion of the study's main constructs but also informs the development of the instrument used to measure them. The validated instrument thus captures both structural and psychological dimensions of risk, offering a novel contribution to fraud prevention and victimology research. Moreover, the framework provides a foundation for designing targeted interventions technological and educational that address both user behaviour and cognitive awareness, thereby helping to reduce the likelihood of repeated online fraud victimisation.

METHODOLOGY

This survey was conducted among Malaysians. The sample's primary emphasis was on repeated online fraud victims in Malaysia. The researchers employed a probability sampling strategy based on a basic random sample approach. The questionnaire was created in the form of a Google form and distributed randomly to members of the public. A total of 149 samples were successfully acquired. Part A of the questionnaire included some demographic analysis to learn more about the research respondents' backgrounds. Several factors were studied, including age, race, gender, highest level of education, state of a repeat victim, employment status, frequency of being a victim of fraud, amount of income, purpose of surfing the internet, duration of surfing the internet per day, and the social media used.

In addition, the questionnaire was produced using an adaptation strategy from earlier studies addressed in the literature review of the study. Part B was related to the elements that contribute to becoming a repeat victim. Part B contained various structures including constructs such as attitudes, existing conditions, and fraud strategies. Finally, Part C comprised economic, social, and psychological aspects. Part C also contained articles concerning the consequences of being a victim of recurrent fraud. To achieve accuracy in the study, the researchers conducted a pilot study analysis of the constructions of Parts B and C to determine the study's dependability value. To identify the impact of two variables (independent variable and dependent variable) in this study, the link and impact between the constructs of Part B and Part C were analyzed.

Pilot Study Analysis and Reliability

Before conducting the actual study's analysis, the researchers conducted a pilot study to determine the reliability of the study instrument. The value of Cronbach's alpha was determined through the pilot study. According to Chua (2006), a pilot study is used to determine the level of validity and reliability of the study by ensuring the value is within the range of 0.6 to 0.9. Cooper and Schindler (2001) indicate that the dependability of the study is crucial to decrease errors in the study instrument. If the Cronbach's alpha value obtained is less than 0.6, the researcher should discard the item and conduct a test-retest realism (Hair et al., 2007). Table 1 is a source that provides a guide for determining the study's reliability using Cronbach's alpha.

Table 1: Cronbach's Alpha (α) Value Explanation

Cronbach's Alpha Value	Explanation
<0.6	Poor
0.60 until <0.70	Average
0.71 until <0.80	Good
0.81 until <0.90	Very Good
>0.90	Excellent

(Sources: Mohd Najib, 2003)

The Part B reliability test is completed as stated in Table 2. Table 2 shows the construct of Part B of the study instrument which is the causal factor of being a repeat victim. Part B consists of three constructs: mindset, current situation, and fraud technique. All three constructs in Part B have a Cronbach's Alpha value greater than 0.6. This implies that a value greater than 0.6 does not necessitate the removal of items from the instrument. A total of 11 items in the attitude construct demonstrate that all findings are within the range of 0.71 to 0.80 with a high level of reliability. The overall attitude construct shows a Cronbach's Alpha value of 0.776 (high dependability level). The current state construct yields more accurate results than the attitude construct. This is because the findings range from 0.81 to 0.90, indicating a high level of reliability. The overall build is likewise quite reliable, with a Cronbach's Alpha value of 0.860. This demonstrates that the 11 things in the present-state construct are quite dependable. Finally, the deception approach is the final construct in Part B of the study instrument. A total of 11 items were examined, and the researchers discovered that the overall fraud technique construct had the highest level of dependability, ranging from 0.91 to 1.00. In addition, the findings for each item had the highest level of dependability (0.91 to 1.00). The analysis of Part B of the research instrument revealed that all items and constructs of causal factors for becoming a repeat victim were approved and not dropped. In this regard, the researchers did not perform a duplicate analysis for the pilot study in Part B of the research instrument.

Table 2: The Reliability Value of Pilot Study: Part B (Cause Factor of Becoming a Repeat Victim)

Attitude			
Cronbach's Alpha value and level of reliability		0.776	Good
Cronbach's Alpha value if the item is deleted	Question 12	0.747	Good
	Question 13	0.759	Good
	Question 14	0.766	Good
	Question 15	0.765	Good
	Question 16	0.747	Good
	Question 17	0.767	Good
	Question 18	0.757	Good
	Question 19	0.764	Good
	Question 20	0.761	Good
	Question 21	0.760	Good
	Question 22	0.757	Good
Current Conditions			
Cronbach's Alpha value and level of reliability		0.860	Very Good
Cronbach value if the item is deleted	Question 23	0.854	Very Good
	Question 24	0.851	Very Good
	Question 25	0.840	Very Good
	Question 26	0.837	Very Good
	Question 27	0.860	Very Good
	Question 28	0.846	Very Good
	Question 29	0.837	Very Good
	Question 30	0.854	Very Good
	Question 31	0.842	Very Good
	Question 32	0.841	Very Good
	Question 33	0.964	Very Good
Fraud Techniques			
Cronbach's Alpha value and level of reliability		0.947	Excellent
Cronbach's Alpha value	Question 34	0.944	Excellent
	Question 35	0.941	Excellent
	Question 36	0.942	Excellent
	Question 37	0.942	Excellent
	Question 38	0.941	Excellent

if the item is deleted	Question 39	0.946	Excellent
	Question 40	0.939	Excellent
	Question 41	0.943	Excellent
	Question 42	0.939	Excellent
	Question 43	0.941	Excellent
	Question 44	0.941	Excellent

In addition to Part B, the researchers did a pilot study analysis for Part C of the research instrument, which is the effect of being a victim of repeated fraud. Table 3 summarizes the findings of the pilot study analysis in Part C. This section also contains three structures, each with ten components. In summary, the researchers discovered that the items in the economic and social constructs about the effects of being a victim of recurrent fraud have the same degree of dependability, which is extremely good, except for the first item of the economic construct as well as the entire construct. The total Cronbach's Alpha value of the economic construct is 0.903, indicating the highest level of reliability, while the social construct is 0.842, indicating a very high level of dependability. Except for the first item, the Cronbach's Alpha values of the items in the economic construct range from 0.81 to 0.90. The social construct has a very high level of dependability, ranging from 0.81 to 0.90. Psychology is another construct in Part C of the research instrument. Overall, the psychological construct has the highest level of dependability, with a Cronbach's Alpha value of 0.930. The psychological concept items likewise have the highest level of dependability, with a Cronbach's Alpha value ranging from 0.91 to 1.00. The overall analysis in Part B of the study instrument revealed that all items and constructs of effects after being a victim of repeated fraud were fully accepted, and no items were eliminated.

Table 3: The Reliability Value of Pilot Study: Part C (Effects after Being a Victim of Repeated Fraud)

Economy			
Cronbach's Alpha value and level of reliability		0.903	Excellent
Cronbach's Alpha value if the item is deleted	Question 45	0.936	Excellent
	Question 46	0.894	Very Good
	Question 47	0.888	Very Good
	Question 48	0.886	Very Good
	Question 49	0.882	Very Good
	Question 50	0.882	Very Good
	Question 51	0.880	Very Good
	Question 52	0.895	Very Good
	Question 53	0.898	Very Good
	Question 54	0.883	Very Good
Social			
Cronbach's Alpha value and level of reliability		0.842	Very Good
Cronbach's Alpha value if the item is deleted	Question 55	0.854	Very Good
	Question 56	0.851	Very Good
	Question 57	0.840	Very Good
	Question 58	0.837	Very Good
	Question 59	0.860	Very Good
	Question 60	0.846	Very Good
	Question 61	0.837	Very Good
	Question 62	0.854	Very Good
	Question 63	0.842	Very Good
	Question 64	0.841	Very Good
Psychology			
Cronbach's Alpha value and level of reliability		0.930	Excellent

Cronbach's Alpha value if the item is deleted	Question 65	0.919	Excellent
	Question 66	0.918	Excellent
	Question 67	0.918	Excellent
	Question 68	0.933	Excellent
	Question 69	0.916	Excellent
	Question 70	0.920	Excellent
	Question 71	0.919	Excellent
	Question 72	0.933	Excellent
	Question 73	0.922	Excellent
	Question 74	0.925	Excellent

RESULTS AND DISCUSSION

Background of the Respondents

Table 4 displays the descriptive analysis of the findings. This analysis was performed to determine the total frequency of respondents, and the proportion of respondents for each indicated item. According to the report, most victims of repeated online fraud were adults between the ages of 21 and 30 (125 people). Only 18 respondents (12%) were below 20 years old. Other age groups of the study were 31 to 40 years and 41 to 50 years, with 2.68 percent (4 respondents) and 1.34 percent (2 respondents), respectively. This demonstrates that individuals between the ages of 31 and 50 are uncommon victims of persistent internet fraud in Malaysia. In fact, no respondents above the age of 51 were found to have been victims of persistent online fraud in this survey.

The researchers also included the item of race among the respondents. The most common victims of online fraud were Malays (107 respondents), followed by Chinese (21 respondents), and Sabah Bumiputera (10 respondents). These three sequences indicated the highest total, the second highest, and the third highest. Apart from these three race groups, two other races in the questionnaire received fewer than ten responses. The races were Sarawak Bumiputera (7 victims) and Indian (4 victims). Although the pattern of races was not balanced, the researchers discovered that the pattern of gender was relatively constant. This was because there were only three disparities between male and female respondents. Male respondents consisted of 51 percent of those who had been the repeated victims of internet fraud, with 73 female respondents. This indicates that male respondents are more likely to be victims of repeated online fraud than female respondents.

The educational background is a significant consideration when examining the relationship with the study. Even though repeated fraud is considered undesirable, the survey discovered that respondents who have been the victims of recurrent online fraud were mostly educated. According to the findings, as many as 77.18 percent (115 respondents) were educated with a first degree, master's, or PhD. In fact, 22.18 percent, or 33 respondents, in the pre-university educated group (diploma, matriculation, foundation, certificate, and STPM) had been the victims of repeated online fraud. Only one victim of serial fraud possessed a high school diploma. Apparently, there was not any respondent who did not attend school or had only a primary school education.

Table 4 shows the respondents who have been victims of fraud online on multiple occasions from all states of Malaysia, except one (Perlis). Johor has the highest number of respondents (35), followed by Selangor (30), and Perak (19). For the remaining states, the number of respondents is less than ten, with a range of 1 to 9. The analysis is then related to the respondent's employment status. Most respondents (130 people or 87.24 percent) are students. Five respondents are government employees, three are private sector employees, and only one is self-employed. Another ten respondents are unemployed. This indicates that most respondents are students.

The study's main goal was to determine how frequently victims were defrauded. Most respondents (87) had been victims once, 47 had been victims twice, and seven had been deceived four to five times. The frequency of six or more frauds was considered high. Apparently, three respondents had been cheated six to seven times, one person had been cheated eight to nine times, and four respondents had been cheated ten or more times. This demonstrated that respondents' awareness of fraud was low, and they continued to be victims of online scams.

Worryingly, 137 respondents were unemployed. This finding was consistent with the finding of the employment status which indicated that most respondents were students. Only eight respondents had an estimated income of less than RM 2000.00.

The study also identified factors and durations of internet use. This section allowed the respondents to submit responses with more than three options. The primary need was to find information, which was followed by the need to buy goods and services, pass time, play games, meet other needs, make new contacts, and complete assignments. Many respondents spent more than five hours on the internet. Every day, only two respondents used the internet for less than an hour. Many respondents reported using the internet for three to five hours per day. Internet usage might be influenced by social media factors. The WhatsApp application was used by most respondents, followed by Instagram, YouTube, TikTok, Facebook, Twitter, other applications, and Skype. This demonstrates that the WhatsApp application was the primary choice of the respondents to study.

Table 4: Demographic Analysis

Background		Frequency (<i>f</i>) (n=149)	Percentage (%)
	Under 20 years old	18	12
	21 - 30 years old	125	84
	31 - 40 years old	4	2.68
	41 - 50 years old	2	1.34
	51 - 60 years old	0	0
	60 years and above	0	0
	Malay	107	71.81
	Chinese	21	14.10
	Indian	4	2.68
	Bumiputera Sabah	10	6.7
	Bumiputera Sarawak	7	4.70
Gender	Male	76	51
	Female	73	49
Highest Level of Education	Does Not Attend School	0	0
	Primary School	0	0
	Secondary School	1	0.67
	Pre-University (Diploma/Matriculation/Foundation/Certificate/STPM)	33	22.18
	Higher Education (Degree, Master's, or PhD)	115	77.18
State When a Repeat Victim Being	Johor	35	23.49
	Melaka	8	5.37
	Negeri Sembilan	1	0.67
	Selangor	30	20
	Wilayah Persekutuan Putrajaya	1	0.67
	Wilayah Persekutuan Kuala Lumpur	2	1.34
	Perak	19	12.75

	Pulau Pinang	5	3.6
	Kedah	7	4.70
	Perlis	0	0
	Pahang	9	6
	Kelantan	7	4.70
	Terengganu	7	4.70
	Sabah	9	6
	Sarawak	8	5.37
	Wilayah Persekutuan Labuan	1	0.67
Employment Status	Government	5	3.35
	Private	3	3
	Self-Employment	1	0.67
	Students	130	87.24
	Unemployed	10	6.7
Frequency of Being a Victim of Fraud	Once	87	58.39
	2 -3 times	47	31.54
	4 - 5 times	7	4.70
	6 -7 times	3	3
	8 - 9 times	1	0.67
	More than 10 times	4	2.70
Amount of Income	No Income	137	91.94
	<RM 2000	8	5.37
	RM 2001 - RM 4000	0	0
	RM 4001 - RM 6000	1	0.67
	RM6001 - RM 8000	1	0.67
	RM 8001 - RM 10 000	1	0.67
	RM 10 001 and above	1	0.67
Purpose of Surfing the Internet	Play Games	72	48.3
	Find Information	119	79.87
	Get Rid of Boredom	83	55.70
	Make New Contacts	25	16.77
	Complete Assignments	11	7.38
	Buy Goods and Services	112	75.17
	Others	28	18.80
Duration of Surfing the Internet Per Day	< 1 hours	2	1.34
	1 - 2 hours	19	12.75
	3 - 5 hours	61	40.94
	> 5 hours	67	44.97
Social Media Used	Facebook	76	51
	Twitter	55	36.91
	TikTok	103	69.13

	Skype	1	0.67
	WhatsApp	137	91.95
	Instagram	127	85.23
	YouTube	114	76.51
	Others	41	27.51

Relationship Between Causal Factors and Consequences of Repeated Online Fraud Victimization

Table 5 depicts the correlation test between items and constructs of causal factors and the effect of being a victim of online fraud multiple times. Each item has been analyzed. The analysis of each item reveals that the strongest relationship is between the attitude factor and the social effect ($r = 0.536$), with moderate correlation coefficient strength. The relationship between fraud technique factor items and social impact ($r = 0.521$) is moderately strong. The third-highest correlation ($r = 0.433$) is found between the items of the fraud technique factor and the effect of psychology. This demonstrates that only two-item relationships have moderate correlation coefficients, while the remaining seven-item correlation coefficients are weak. Among the findings analyzed in terms of the correlation between the items include the relationships between the attitudes factor and the effect of economy and psychology ($r = 0.361$ and $r = 0.380$), the relationship between the current condition factor and the effect of economy, social, and psychology ($r = 0.421$, $r = 0.349$, $r = 0.402$), and the relationship between factor fraud technique and the effect of economy ($r = 0.429$). The overall analysis of factors towards impact items (economy, social, and psychology) exposes the highest correlation regarding factors and the social impact moderate relationship ($r = 0.603$), followed by the relationship of the overall factor with the psychology effect ($r = 0.523$), and finally, the overall factor with the effect of the economy relationship ($r = 0.522$). Correspondingly, the correlation coefficient between the effect of each factor (attitudes, current condition, and fraud technique) shows a moderate correlation coefficient relationship. The highest value of the overall effect with the fraud technique factor $r = 0.542$ is followed by the overall effect with the attitudes factor $r = 0.496$, and finally, the overall effect with the attitudes factor $r = 0.468$. The correlation between all factors and the effect of being a victim of repeated online fraud is moderate, with a value of $r = 0.648$ in the highlight analysis. All these relationships are accepted because the correlation obtained is significant (**) with a value of 0.01.

Table 5: Correlation (r) Tests with the Effects of Repeated Online Fraud Victimization on Items and Causal Factor Constructs

Item / Construct	Economy	Social	Psychology	Impact
Attitudes	0.361**	0.536**	0.380**	0.496**
Current Condition	0.421**	0.349**	0.402**	0.468**
Fraud Technique	0.429**	0.521**	0.433**	0.542**
Factor (Overall)	0.522	0.603	0.523	0.648

Dominant Causative Factors Affecting Repeat Online Fraud Victims

Table 6 presents the findings relative to the multiple regression analysis performed to figure out the most significant factor contributing to the impact on repeat online fraud victims. Regression results revealed that fraud techniques significantly predicted victim impact ($\beta = .363$, $p < .001$), explaining 42.4% of the variance ($R^2 = .424$) and the R-value is 0.651. This indicates that the three factors researched (attitudes, current situation, and fraud technique) contribute up to 65.1 percent of the effects experienced by victims of repeated online fraud. Additional variables not investigated in this study have influenced 34.9 percent of the entirety. It is undeniable that the present investigation makes a significant contribution to research and scholarship. The researchers implemented a reliability level of 0.05, with 95% reliability and a 5% error. In general, the researchers discovered that the current situation was not significant and that only two factors, attitudes, and fraud technique, were significant. This is due to the results of the analysis for the attitude factor being $B = 0.189$, $t = 2.007$, and $p = 0.019$ 0.05. The fraud technique exploration is also significant, as evidenced by $B = 0.293$, $t = 4.620$, and $p = 0.000$ 0.05. Although the current condition has a B value of 0.315, it has no effect on victims of online fraud. On

the other hand, attitudes and fraud conditions contribute to repeat online fraud victims through three main effects, particularly the economy, social, and psychological. The most significant contributor is the fraud technique. This unambiguously demonstrates that the victim's trauma, which has an impact on the economy, social life, and psychology, is a consequence of the scammer's intelligence and expertise in organizing methods and procedures that involve online fraud. This demonstrates that online fraudsters or scammers are cognizant of the techniques employed to deal with victims repeatedly.

Table 6: Multiple Regression Tests of Dominant Causal Factors Contributing to the Impact of Repeated Online Fraud Victims

Independent Variables (Factors Contributing to Repeated Online Fraud Victims)	B	Beta (β)	t-value	Sig. (p-value)	Decision
Attitudes	0.189	0.164	2.007	0.019	Significant
Current Condition	0.315	0.311	4.568	0.047	Significant
Fraud Technique	0.293	0.363	4.620	0.000	Significant
Model Summary					
R	0.651				
R²	0.424				
F-value	35.528				

CONCLUSION

The results support the growing number of studies that claim that fraud victimisation is not necessarily a result of exposure to a digital setting but is greatly influenced by mental vulnerability and behavioural disposition. In line with recent research on cyberpsychology, the people who are more susceptible to repeated deception are those who have higher trust propensity and heuristic decision-making patterns. The adaptive complexity of fraud schemes also underscores the fact that prevention should be adapted to meet the current needs of heightened adaptability of cybercriminals, implying that prevention campaigns should cease being based on awareness-raising campaigns but advance to behavioural modification and platform security.

This study addresses a pressing contemporary issue repeated online victimisation arising from fraudulent online purchase activities. By developing and validating a multidimensional instrument, the research identifies key contributing factors: individual attitudes, situational exposure, and the strategies employed by fraudsters. The outcomes of victimisation are categorised across three dimensions economic, social, and psychological offering a comprehensive perspective on the impact experienced by repeat victims.

A pilot study involving 149 respondents revealed that the instrument demonstrates strong psychometric properties. All items recorded high internal consistency, supporting the tool's reliability in assessing constructs relevant to online fraud victimisation. This instrument offers significant value not only for academic research but also for practical application in identifying at-risk individuals and informing preventive strategies.

The analysis further confirmed that all three predictor constructs attitudes, current conditions, and fraud techniques are significantly associated with the outcome constructs. Among these, attitudes and fraud techniques emerged as stronger predictors compared to situational factors. These findings resonate with prior research that emphasises the role of psychological traits such as impulsivity, over-trusting behaviour, and emotional gullibility in cyber fraud vulnerability (Williams et al., 2017; Norris & Brookes, 2021). The results also support Mesch and Dodel's (2018) assertion that the increasing sophistication of scammers, particularly in exploiting urgency and trust, remains a critical factor in fraud success.

These insights align with the theoretical grounding of victim precipitation theory, suggesting that certain personal traits and behaviours may inadvertently increase one's susceptibility to repeated fraud. Nonetheless, this perspective does not shift blame onto the victims; rather, it highlights the importance of raising awareness and enhancing digital literacy, especially among frequent users of e-commerce and social media platforms.

This study contributes to the broader field of cyberpsychology by offering a theory-informed, validated instrument capable of assessing multidimensional risks of repeated online victimisation. The tool can serve as a foundation for future studies and as a practical mechanism for early detection and intervention in fraud-related behaviours. The originality of the constructs and their measurement have the potential to be registered as intellectual property, further extending the study's impact.

Future research may benefit from expanding the sample size to include more diverse populations and applying Confirmatory Factor Analysis (CFA) to verify the instrument's structure. Given the persistent and evolving nature of digital fraud, ongoing research is crucial. Collaborative efforts among policymakers, digital platform providers, law enforcement agencies, and civil society are essential to reduce victimisation rates. Most importantly, victims must be empowered to report fraud without fear or stigma, as underreporting remains a significant barrier to effective policy and intervention.

Theoretical Contribution

This work contributes to the theory in three ways. First, it contributes to the literature on cybercrime by operationalising repeated online fraud victimisation as a multidimensional concept, as opposed to a behavioural consequence. Second, it brings together Cyber-Routine Activity Theory and Cognitive-Behavioral Theory into an integrated measurement system, which proves that victimisation arises out of the interplay between environmental exposure and cognitive vulnerability. Third, the research provides a validated tool that would allow the future empirical modelling of fraud risk, beyond descriptive profiling of victims, to predictive analytics. This is a reaction to recent discussions in cyberpsychology research of theory-grounded measurement instruments that reflect dynamic on-line risk behaviour.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Universiti Tun Hussein Onn Malaysia (UTHM) for its continuous support, guidance, and provision of facilities throughout the completion of this study. The authors also sincerely acknowledge the valuable contributions of relevant partners and stakeholders whose cooperation, expertise, and commitment supported the successful implementation of this research. The dedication, collaboration, and input from all parties involved are deeply appreciated and have greatly contributed to the success of this work.

Conflict Of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this study.

REFERENCES

1. Ahmad, M. A. (2024). Cognitive bias and financial fraud vulnerability among Malaysian youths: A mediation model. *Journal of Financial Crime Studies*, 31(1), 43–58. <https://doi.org/10.1108/JFCS-04-2024-0061>.
2. Ahmad, Z. (2025). Investment scams: The effect of bias-induced gullibility on victimization propensity. *Crime, Law and Social Change*, 83(1), 45–67. <https://doi.org/10.1007/s10611-024-10187-1>
3. Beck, A. T. (1976). *Cognitive therapy and the emotional disorders*. International Universities Press.
4. Cecilia Desy Widya and Permata Sari (2015). Pengaruh Kepercayaan, Keamanan, Persepsi Resiko dan Kualitas Pelayanan Terhadap Keputusan Pembelian Secara Online. Tesis Sarjana Manajemen. Fakultas Ekonomi dan Bisnis. Universitas Dian Nuswantoro Semarang, Indonesia. <http://dinus.ac.id/>.
5. Chen Li Yin et al. (2023). Online Fraud: Factors Affecting Consumers' Online Purchasing Behaviour in Malaysia. Universiti Tunku Abdul Rahman. Final Year Project Degree.
6. Chua Yan Piau (2006). *Kaedah Penyelidikan Buku 1*. 2nd edition. Shah Alam: Mc Graw Hill, Sdn Bhd.
7. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>

9. Cooper, D. R. dan Schindler, P. S. (2001). *Business Research Method*. 6th edition. Singapore: Mcgraw-Hill.
10. Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, 3(3), 100053.
11. Gan, Y. S., Lim, K. Y., & Hassan, R. (2024). Digital risk behaviour and phishing susceptibility among Gen Z in Malaysia. *Computers in Human Behavior Reports*, 10, 100217. <https://doi.org/10.1016/j.chbr.2024.100217>
12. Gainsbury, S.M. (2019). Identifying Risky Internet Use: Linking Negative Internet Experiences to Specific Online Behaviour. *New Media and Society*, 21(6), 12-32.
13. George, M. S., Teunisse, A. K., & Case, T. I. (2020). Gotcha! Behavioural validation of the gullibility scale. *Personality and Individual Differences*, 162, 110034. <https://doi.org/10.1016/j.paid.2020.110034>.
14. Gogolook's 2022 Annual Fraud Report. (2022). *Annual Fraud Report: Financial Loan*.
15. *Frontiers in Psychology*. (2023). Theoretical basis and occurrence of internet fraud victimisation: Based on two systems in decision-making and reasoning. *Frontiers in Psychology*, 14, 1087463. <https://doi.org/10.3389/fpsyg.2023.1087463>.
16. Hair, J. F., Money, A. F., Samouel, P. dan Page, M. (2007). *Research Methods for Business*. London: John Wiley and Sons.
17. Hoffmann, A. O. I., Lins, S., & Riek, M. (2023). Cognitive and affective determinants of fraud victimization: A longitudinal study. *Journal of Consumer Psychology*, 33(2), 267–283. <https://doi.org/10.1002/jcpy.1345>.
18. Jackson, S.L. (2017). *Senate Special Committee on Aging Hearings and GAO Reports. Elder Abuse: Research, Practice, and Policy*. Springer, New York, 595-613.
19. Makmor, N., Aziz, N. A., & Alam, S. S. (2019). Social Commerce an Extended Technology Acceptance Model: The Mediating Effect of Perceived Ease of Use and Perceived Usefulness. *Malaysian Journal of Consumer and Family Economics*, 22, 119–136.
20. Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, 62(10), 1356–1371. <https://doi.org/10.1177/0002764218787862>
21. Mohd Najib Abdul Ghafar. (2003) *Reka Bentuk Tinjauan. Soal Selidik Pendidikan*. Skudai: UTM Press.
22. Murad, F.A., Kamaluddin, M.R., Sulaiman, W.S.W., & Khairudin, A.H.S. (2020). Personality and Low Self-control as Contributing Factors for Scam Victimization: A Concept Paper. *International Journal of Psychosocial Rehabilitation*, 24(2), 4448–4461.
23. Norlina Mohamed Noor, Shereen Noranee, Muhammad Fared Zakaria, Mohamad Atheef Hannan M. Suaee. (2020). Online Shopping: The Influence of Attitude, Subjective Norm and Perceived Behavioral Control on Purchase Intention. *ICEBA 2020: 2020 The 6th International Conference on E-Business and Applications*.
24. Norris, G., & Brookes, A. (2021). Personality, Emotion and Individual Differences in Response to Online Fraud. *Personality and Individual Differences*, 169(1), 109-847.
25. Nurul Azifah and Citra Kusuma Dewi (2016). Pengaruh Shopping Orientation, Online Trust and Prior Online Purchase Experience terhadap Online Purchase Intention (Studi pada Online Shop Hijabi House). *Jurnal Ilmiah Fakultas Ekonomi Universitas Katolik Parahyangan*. 20(2).
26. Rahim, W. N. E. W. A., & Kamaluddin, A. (2021). Online Consumer's Behavior on Product Review and the Likelihood of Them Being Fraud Victims. *International Journal of Business and Technology*, 11(3), 1-20.
27. Robinson, J., & Edwards, M. (2024). Fraudsters target the elderly: Behavioural evidence from randomized controlled scam-baiting experiments. *Security Journal*, 37, 1173–1196. <https://doi.org/10.1057/s41284-023-00410-4>.
28. Siu, J. Y. M., Chan, S. H., & Leung, C. H. (2024). COVID-19 and cyberfraud: Applying routine activity theory to understand fraud vulnerability in Hong Kong. *Crime Prevention and Community Safety*, 26(1), 45–60. <https://doi.org/10.1057/s41887-023-00105-0>.
29. Teo, J., Khader, M., & Chai, W. (2023). Individual differences and scam victimisation: Who is more likely to become a victim? *Journal of Behavioral Decision Making*, 36(2), 188–204. <https://doi.org/10.1002/bdm.2297>.

30. Vakhitova, Z. I., & Reynald, D. M. (2025). Revisiting routine activity theory for cyberspace: Toward a cyber-RAT framework. *Humanities and Social Sciences Communications*, 12(1), Article 83. <https://doi.org/10.1057/s41599-024-04083-1>.
31. Vinayakumar, R., Poornachandran, P., & Soman, K. P. (2018). Scalable Framework for Cyber Threat Situational Awareness Based on Domain Name Systems Data Analysis. In *Big Data in Engineering Applications*. Springer, Singapore.
32. Wan Shahrazad Wan Sulaiman, Fatin Adha Murad, Geshina Ayu Mat Saat, Rozainee Khairudin, Daniella Maryam Mohamed Mokhtar, Saralah Mariamdarani, Azianura Hani Shaari and Mohammad Rahim Kamaluddin. (2022). Development and Validation of Scam Victimization Risk Inventory (Svr-I) among Malaysian Population. *Journal of Legal, Ethical and Regulatory Issues*. 25(5S). 1-15
33. Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421. <https://doi.org/10.1016/j.chb.2017.02.040>
34. Yeo, S. F., Tan, C. L., Lim, K. B., Leong, J. Y., & Leong, Y. C. I. (2020). Effects of Social Media Advertising on Consumers' Online Purchase Intentions. *Global Business and Management Research*, 12(1), 89-106.
35. Zahari, A. I., Bilu, R., & Said, J. (2019). The Role of Familiarity, Trust and Awareness Towards Online Fraud. *Journal of Research and Opinion*, 6(9), 2470-2480.
36. Zheng, C., & Geetha, S. (2019). Factors Influencing Consumers' Online Purchase Intention in Social Commerce Among Millennials in Malaysia. *Qualitative and Quantitative Research Review*, 4.
37. Zhi Zhang and Zhi Ye. (2022). The Role of Social-Psychological Factors of Victimity on Victimization of Online Fraud in China. *Frontiers in Psychology*. 1-10