Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 11(2) 2026

Journal of Computing Research and Innovation

Factors Predisposing Individuals to Scam Victimization: A Case Study in Seremban, Negeri Sembilan

Aqeelah Balqis Abdul Samad[1], Nornadiah Mohd Razali[2*], Siti Aishah Mohd Shafie[3], Az'lina Abdul Hadi[4]

[1,2,3,4]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara Cawangan (UiTM) Negeri Sembilan Branch, Seremban Campus, 70300 Seremban, Negeri Sembilan, Malaysia.*

ARTICLE INFO

Article history:
Received 30 June 2025
Revised 5 March 2026
Accepted 6 March 2026
Online first
Published 1 September 2026

Keywords:
Scam Victimization
Awareness
Logistic Regression
Trust
Technological Literacy

DOI:
10.24191/jcrinn.v11i2.563

ABSTRACT

Scam, which include investment schemes, job offer fraud, Macau scams, love scams, and internet shopping scams has become an alarming problem in Malaysia. Scammers frequently utilize internet platforms or pose as officials to trick victims into sending money or disclosing private information. In response to these issues, this study investigated the factors that predispose individuals to scam victimization. Questionnaire was distributed to a total of 385 samples encompassed individuals from various demographic backgrounds residing in Seremban, Negeri Sembilan. Factors such as age, income level, level of awareness, trust, and technological literacy were regressed towards scam victimization (had or had never been a scam victim) in a logistic regression analysis. Upon completion of the study, the results revealed that age, level of awareness and technological literacy contributed significantly to scam victimization. Hence, this study concluded that promoting critical thinking, enhancing technological literacy, and encouraging responsible online behaviour are essential steps in reducing scam victimization.

1. INTRODUCTION

An illegal tactic is called a scam. The goal of scams is to deceive and swindle to obtain money from victims through illegal methods, and they can take many different forms, from complex false investment schemes to fraudulent phone calls and messages. Online scams and financial frauds include a wide range of illegal acts, from ransomware attacks and cryptocurrency scams to phishing emails and identity theft (Kipngetich, 2025). Scams target individuals of all ages, socioeconomic origins, and income levels. Nowadays, scammers' psychological manipulation tactics have advanced, making it more difficult for victims to identify and steer clear of scams (Liu et al., 2025). The growth of digital platforms and the speed at which technology is advancing have made it easier for scammers to take advantage of gullible people. The rise of artificial intelligence (AI) has further complicated the landscape, enabling scammers to create more convincing fraudulent content, such as deepfake videos and voice imitations. All these advancements make it increasingly difficult for individuals to distinguish between genuine and fraudulent communications.

[2*] Corresponding author. *E-mail address*: nornadiah@uitm.edu.my
https://doi.org/10.24191/jcrinn.v11i2.563

The implication of scams on the victims can go beyond than just monitory losses. In addition to monetary losses, victims may experience mental discomfort, such as tension and feelings of embarrassment. Furthermore, they may experience severe psychological effects, such as feeling overburdened and confined. According to Kubilay et al. (2023), scams are detrimental to the victims both in terms of direct monetary cost and indirect costs such as loss of trust in financial service, loss of confidence in financial matters and mental health problems including depression and stress, emphasizing the need for heightened awareness and preventive measures.

Scam victimisation has been a growing concern, mirroring a global trend of rising internet fraud. As reported in the 2024 Asia Scam Report, more than 50% of people report being victims of scams weekly, across Asia, with an estimated total loss of US$688.42bil over the last 12 months (Juremi, 2024). In Malaysia specifically, as of August 2024, Malaysian Communications and Multimedia Commission had deleted over 32,000 posts on scams and fraud, a significant rise from just over 6,000 posts in 2023. Malaysia has the greatest rate of online fraud victimisation in Asia, with victims being retargeted more than 2.5 times on average, according to the Global Anti-Scam Alliance's Asia Scam Report 2024. Scams involving SMS contests, phone call impersonations, online impersonation investments, lotteries, phishing schemes, and internet shopping were prevalent in Malaysia. A sustained growing trend is seen from the 12,110 cases of online fraud that occurred in the first quarter of 2025 alone, with losses RM573.7 million (Bernama, 2025). These numbers highlight how urgent it is to fight crimes related to scams and put in place efficient defences.

Despite the alarming statistics, a significant number of scam incidents remain unreported. The State of Scam Report 2024 revealed that 70% of scam victims in Malaysia did not report their cases to the authorities, often due to scepticism about the effectiveness of reporting processes. These underreporting hampers the efforts to combat scams and protect potential victims. Increasing the awareness towards scams and understanding the factors that contribute to scam victimization are required as a method of developing successful prevention. Therefore, this study investigated the level of awareness towards scam and factors predisposing individuals to scam victimization, focusing on the people in Seremban, Negeri Sembilan.

2. LITERATURE

This section elaborates the factors predisposing individuals to scam victimization as evidenced in the previous studies.

2.1 Age

It is expected that among all generations, older adults are more vulnerable to various type of scams (Button et al., 2014). Scammers frequently target older folks because they are thought to be less tech-savvy and are more likely to be socially isolated. Ueno et al. (2021) determined whether cognitive decline is a risk factor for scam vulnerability in older adults and found that mild cognitive decline is a risk factor for scam vulnerability in older adults. This shows that older adults have a high risk of scam victimization. Yu et al. (2022), in another study, found that older populations are consequently more vulnerable to scams or unexpected financial shocks. On the contrary, Shang et al. (2022) concluded in their study that there was no evidence of older adults being more vulnerable to scams victimization. According to data gathered by the Federal Trade Commission among US citizens, the impact of age varies depending on the type of fraud, with older persons more likely to fall victim to tech support (helpdesk) fraud and prize fraud, while younger people are more likely to fall victim to online shopping fraud (Federal Trade Commission, 2022).

2.2 Income level

Many studies concluded that people with lower income levels can be more vulnerable to scams that promise immediate cash relief. Economic vulnerability and income level are frequently correlated, and this

https://doi.org/10.24191/jcrinn.v11i2.563

can influence a person's propensity to fall for scams. Gao et al. (2020) has proven this theory by concluding that households facing credit constraints (which is heavily tied to lower income) have a significantly higher probability of becoming scam victims. This is supported by Beach et al. (2023) who introduced two methods to assess financial exploitation vulnerability and discovered that adults with lower income are more vulnerable to financial exploitation. As reviewed by Koning et al. (2024), the effect of income on scams may vary depending on the type of fraud whereby victims of lottery scams may have lower incomes than average, while victims of investment scams may have higher incomes than average.

2.3 Level of awareness

Scam awareness is essential to protect people from falling for scams and as a shield from losing their money. A study conducted by Cole et al. (2015) investigated the email users' level of awareness and knowledge gaps regarding the steps that should be taken in the event that they become victims of scam emails. The results revealed that the participants who were lack of scam awareness were not able to identify a few different practices to identify the scam email. Email users may be at risk from this lack of awareness since they may not be cautious while utilising other online services and may become targets of well-known scams that were not carried out through email (Cole et al. 2015). Another study by Holtfreter et al. (2008) found that individuals who practised scam awareness and were aware of the possible risks involved in their daily activities were less likely to become scam victims.

2.4 Trust

In the context of a scam, trust means the individual's trust towards the scammer causes them to be the prey of the scam. Zhang and Ye (2022) has proven through a multiple linear regression analysis that trust is significantly related to scam victimization in China. People with greater trust are more prone to fall for imitation schemes of authority, making them to be more likely to fall for scams. Another study regarding trust in financial institutions and its impact on scam victimization by Button et al. (2014) found that people who had trust in their banks and financial advisors were less inclined to check unusual requests on their own, leaving them more vulnerable to impersonation schemes. Other than that, Holtfreter et al. (2008) found that low self-control and intense levels of trust significantly increase the likelihood of falling for scams.

2.5 Technology literacy

Technological literacy is the ability to use, understand, manage, and analyse technology in a safe, efficient, and responsible manner. Using technology to assess, generate and integrate information is a part of this literacy. Increasing technology literacy can dramatically lower the likelihood of falling victim to a scam (Tennant et al., 2022). Research has proven that people with lower levels of technology literacy may be more susceptible to scams. People who are not skilled at spotting fake websites or phishing attempts are more likely to become victims. For instance, Anderson and Rainie (2018) discovered that people who have high technological literacy are more capable of identifying and avoiding online scams. Muniam et al. (2025) revealed that individuals who adopted technological literacy well are better at recognising and avoiding scams. Other than that, a study by Beach et al. (2023) and Alotaibi and Furnell (2018) exposed that individuals who are aware of cybersecurity practices and less experience with technology are less likely to become victims of online fraud, highlighting the necessity of education and training to improve technological literacy.

https://doi.org/10.24191/jcrinn.v11i2.563

3. METHODOLOGY

3.1 Research methodology

A cross-sectional study was conducted to collect all data regarding the factors of scam victimization from the population at a single point of time. The purpose of this study design was to collect data that would be pertinent to finding the answer to the research questions. The data was gathered over a period of two months; from October 2024 until November 2024. The population involved the people in Seremban, Negeri Sembilan. A total of 385 samples encompassed individuals from various demographic backgrounds residing in Seremban, Negeri Sembilan were considered in the study. The sample size is calculated by using Cochran's formula. Due to unattainability of the sampling frame, convenience sampling was employed to choose the samples. Consequently, the findings were interpreted with caution due to concerns regarding limited representativeness of the sample. A pilot study was conducted prior to the main study to evaluate the internal consistency of the instruments.

3.2 Research instrument

An online questionnaire was created using a Google Form for the purpose of data collection. The questionnaire was divided into five sections. Section A consists of three questions enquiring the demographic profile of the respondents. Section B consists of one question only regarding the experience towards the online payment scam victimization (whether or not the respondent has ever been a scam victim). Section C contains five items measuring the level of awareness of the respondents towards scam. Section D consists of five items measuring the trust and finally section E consists of five items measuring the technological literacy of the respondents. The level of awareness, trust, and technological literacy were measured using a five-point Likert scale where 1= strongly disagree, 2=disagree, 3=neutral, 4=agree and 5=strongly agree. The online questionnaire was distributed to the respondents through social media platforms such as WhatsApp, Telegram, and Facebook.

3.3 Statistical analysis

To ensure the reliability of the instrument, a reliability analysis was conducted for the factors measured using the Likert scale, namely level of awareness, trust, and technological literacy. Cronbach's alpha was used to assess internal consistency, with values exceeding 0.70 indicating acceptable reliability.

The demographic characteristics (age and income level) of the respondents were described using descriptive analysis such as frequency and percentage. The mean was calculated to define the level of awareness of the respondents towards scam victimization. According to Mauricio and Barbosa (2009), the level of awareness can be classified into two categories: high and low, whereby mean scores of three or higher indicated high awareness, while mean scores below three were interpreted as demonstrating low awareness.

The binary logistic regression analysis was employed to achieve the main objective of this study, which was to identify the factors predisposing individuals to scam victimization. The general binary logistic regression model was written as,

$$\text{logit} = \ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \varepsilon \quad (1)$$

where,

p = the probability of being a scam victim
X_1 = Age

https://doi.org/10.24191/jcrinn.v11i2.563

X_2 = Income level (Low)
X_3 = Income Level (Medium)
X_4 = Level of awareness score
X_5 = Trust score
X_6 = Technological literacy score

The Likert-scale items measuring level of awareness, trust and technological literacy were combined to form composite scores by calculating their total. These composite scores were then treated as continuous independent variables in the binary logistic regression analysis.

The logistic regression model was estimated using IBM SPSS. The model was assessed for its goodness-of-fit based on two statistical tests, namely the Omnibus test as well as Hosmer and Lemeshow (HL) test. The Omnibus test checked if the independent variables, as a group, significantly predict the outcome. It tests the null hypothesis that all regression coefficients are zero, meaning the independent variables have no predictive power. A significant omnibus test (p-value < α=0.05) indicates that at least one of the independent variables in the model has a statistically significant relationship with the dependent variable. In other words, the model with independent variables provides a better fit than a model without any independent variables (Hosmer et al., 2013). Meanwhile, the HL test checks how well a logistic regression model fits the observed data. It tests the hypothesis that there is no difference between observed and predicted event rates. Therefore, a non-significant test (p-value > α=0.05) means that the model's predictions do not significantly differ from the observed outcomes, indicating a good fit (Hosmer et al., 2013).

Prior to assessing the model's goodness-of-fit, the Variance Inflation Factor (VIF) and Tolerance (TOL) values of each independent variable was calculated and observed to ensure the absence of multicollinearity. A multicollinearity problem is said to exist if the VIF values is more than 10 and TOL value is less than 0.2 (Hair et al., 2010).

Finally, Wald's statistic was used to identify the factors that significantly predisposing individuals to scam victimization, and odds ratio was described to further understands the relationship between the significant factors and scam victimization.

4. RESULTS AND DISCUSSIONS

This section presents the results of reliability analysis, description of respondents by their demographic profile, the awareness level of the respondents towards scam victimization and the results of the logistic regression analysis.

4.1 Reliability of the scale

Table 1 presents the results of the reliability analysis. Based on the table, the Cronbach's alpha values for all factors measured using the Likert scale, namely level of awareness, trust and technological literacy, exceeded 0.70 for both pilot and actual studies. This indicates that the instruments used to measure level of awareness, trust and technological literacy demonstrate acceptable reliability.

https://doi.org/10.24191/jcrinn.v11i2.563

Table 1. Cronbach's alpha values for pilot and actual study

Variable	Cronbach's Alpha	
	Pilot Study	Actual Study
Awareness	0.794	0.755
Trust	0.781	0.742
Technological literacy	0.783	0.747

4.2 Demographic profile of the respondents

As indicated in Table 2, 56.3% of the respondents were young adult (18-25 years old), 31.1% of the respondents were adult (26-44 years old), 9.1% of the respondents were from the middle age category (45-59 years old) and the rest were senior citizens (60 and above). Aside from that, most of the respondents (45.2%) came from the medium-income group (RM5001-RM10,000 per month), 33.8% of the respondents came from the low-income group (RM0-RM5000 per month), while the remaining came from the high-income group (RM 10,001 and above).

Table 2. The distribution of respondents by their age group and income level

Variable	Classification	Frequency	Percentage
Age Group	Young Adult	228	56.3
	Adult	126	31.1
	Middle Age	37	9.1
	Old	14	3.5
Income Level	Low	137	33.8
	Medium	183	45.2
	High	85	21.0

4.3 Level of awareness towards scam

Based on the cut-off point from Mauricio and Barbosa (2009), the level of awareness of the respondents was identified as shown in Table 3. The mean of the overall awareness of the respondents is 3.15, indicating that, on average, the respondents were highly aware of scam victimization. Looking at the specific statement to measure the awareness, the mean values for all statements are more than three. This suggests that the respondents were highly aware of the tactics used by the scammers (mean = 3.21), the red flags of a potential scam (mean = 3.11), seeking information regarding the protection of scams (mean = 3.12), how and where to report a scam (mean = 3.07) and the impact of scams on individuals and society (mean = 3.26). Therefore, the result showed that the awareness of scams had already been spread widely among the people in Seremban. There is no doubt that it should be a basic awareness of everyone.

Table 3. Level of awareness of the respondents towards scam

Items	Mean	Awareness Level
I aware the tactics used by scammers, such as fake emails, phone calls, or websites.	3.21	High
I can identify the red flags of a potential scam, such as requests for personal information or urgent requests for money.	3.11	High
I regularly seek information about how to protect myself from scams from sources such as news, social media, or official websites.	3.12	High
I know how and where to report a scam if I encounter one.	3.07	High
I aware that scams have a significant impact on individuals and society.	3.26	High
Overall	3.15	High

https://doi.org/10.24191/jcrinn.v11i2.563

4.4 Identification of factors predisposing individuals to scam victimization

Table 4 shows the results of the binary logistic regression analysis. The values of VIF are less than 10, while TOL values are more than 0.2 for all quantitative independent variables. Therefore, the multicollinearity problem does not exist. The Omnibus test suggests that the model containing only the constant has a poor fit (p-value=0.000). This implies that the model with independent variables performs better than the model with constant only. In addition, the non-significant of the HL test (p-value=0.353) implies that the estimated model fits the data at an acceptable level. The model accounts for 5.8% of the variation in scam victimization (Cox-and-Senall $R^2 = 0.058$).

Table 4. Results of logistic regression analysis

Variable	Coefficient	Wald Statistic	P-value	VIF	TOL
Constant	0.853	1.582	0.209	1.060	0.944
Age	0.026	4.657	0.031	1.060	0.944
Income Level (Low)	-0.011	0.002	0.964		
Income Level (Medium)	0.038	0.019	0.889		
Level of Awareness	-0.042	7.148	0.008	1.046	0.956
Trust	0.020	0.392	0.531	2.048	0.488
Technological Literacy	-0.069	4.097	0.043	2.105	0.475
Goodness-of-fit Test					
Omnibus Test			0.000		
Hosmer and Lemeshow (HL) Test			0.353		
Cox-and-Snell R^2			0.058		

The Wald statistics provides an index of the significance of each independent variable in the equation. Based on the p-value of the Wald test, age (p-value=0.031), level of awareness (p-value=0.008), and technological literacy (p-value=0.043) are significant since their p-values are less than 0.05. This means that the variables have a significant contribution to scam victimization. In contrast, income level (p-value=0.964 for low income; p-value=0.889 for medium income) and trust (p-value=0.531) do not contribute significantly to scam victimization. The findings contradicting the previous studies which concluded that income level and trust significantly influence scam victimization. Based on these results, the estimated binary logistic regression model for this study can be written as,

$$\log\left(\frac{p}{1-p}\right) = 0.853 + 0.026 * \text{Age} - 0.042 * \text{Awareness} - 0.069 * \text{Technological literacy} \quad (2)$$

The relationship between the significant independent variables with scam victimization can be further described based on the odds ratio shown in Table 5. Based on the odd ratio values, the odds of the people in Seremban included in the sample being a scam victim increase by 2.6% for every one-year increase in age (OR=1.026). Consistent with the finding obtained by Button et al. (2014), Ueno et al. (2021) and Yu et al. (2022), this study has proven that older people are more prone to scams. Conversely, the odds of the people in Seremban included in the study being a scam victim decrease by 4.2% for every one-unit increase in the awareness score (OR=0.958). This result agrees with the previous research by Cole et al. (2015) and Holtfreter et al. (2008) who concluded that individuals who practice scam awareness were less likely to become a scam victim.

https://doi.org/10.24191/jcrinn.v11i2.563

Table 5. Odds ratio for significant factors

Variable	Odds Ratio
Age	1.026
Level of Awareness	0.958
Technological Literacy	0.933

Moreover, the odds of the people in Seremban being a scam victim decrease by 6.7% for every one-unit increase in technological literacy score (OR=0.933). Hence, this result is in line with the previous study by Anderson and Rainie (2018), Alotaibi and Furnell (2018) and Muniam et al. (2025) where people with high technological literacy could avoid becoming scam victims. The classification table was not included in the discussion, as the primary objective of this study was to identify the significant factors predisposing individual to scam victimization rather than to evaluate predictive performance.

5. CONCLUSION AND RECOMMENDATIONS

This study examined the factors predisposing individual to scam victimization, revealing that age, level of awareness and technological literacy play significant roles in determining susceptibility to scam. Similar to most of the previous studies, the findings from this study highlight that older individuals with limited scam awareness and lower technological literacy are more vulnerable to deception. Additionally, income and trust are found to be not significantly influence scam victimization. This is contradicted with most of the previous studies which believe that both variables do contribute to scam victimization. The insignificance of the variables in this study may be due to several factors such as the sample size, sample selection, variation in the independent variables, distribution of the dependent variables and many more. Larger sample size may lead to more statistical power (Bhandari, 2021). Therefore, in future studies is suggested to increase the sample size and expand the sample selection by considering people from the other states of Malaysia as well. Probability sampling should also be considered so that generalization of results can be made to the population. In addition, future study is also recommended to ensure that the sample size for both categories of the dependent variable is balance to a certain possible extent. Highly imbalanced sample size can mask the effect of the independent variables that are genuinely predictive. As a concluding remark, the insights gained in the study underscore the need for targeted educational campaigns and preventive strategies, especially for high-risk populations. Enhancing technological literacy, promoting critical thinking, and encouraging responsible online behaviour are essential steps in reducing scam incidents. Ultimately, the study provides a foundation for policymakers, educators, and law enforcement to develop evidence-based interventions aimed at minimizing the impact of scams in society.

6. ACKNOWLEDGEMENTS/FUNDING

The authors would like to acknowledge the support of Universiti Teknologi MARA (UiTM) Cawangan Negeri Sembilan, Kampus Seremban for providing the facilities for this study. This study did not receive any specific funding from public, commercial or non-profit funding agencies. Approval has been granted from the UiTM Research Ethics Committee to conduct the study.

https://doi.org/10.24191/jcrinn.v11i2.563

7. CONFLICT OF INTEREST STATEMENT

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

8. AUTHORS' CONTRIBUTIONS

All authors have contributed significantly to the completion of this study. **Aqeelah Balqis Abdul Samad:** Conceptualisation, methodology and analysis. **Nornadiah Mohd Razali:** Conceptualisation, methodology and writing-original draft; **Siti Aishah Mohd Shafie:** writing-review and editing; **Az'lina Abdul Hadi:** writing-review and finalizing.

9. REFERENCES

Alotaibi, S., & Furnell, S. (2018). A study of cyber-security awareness in Saudi Arabia. *Journal of Information Security and Applications 40*, 15-20. https://10.1109/ICITST.2016.7856687.

Anderson, J., & Rainie, L. (2018). *The future of well-being in a tech-saturated world*. Pew Research Center. https://www.pewresearch.org/internet/2018/04/17/the-future-of-well-being-in-a-tech-saturated-world/.

Bhandari, P (2021). *Statistical power and why it matters: A simple introduction*. https://www.scribbr.com/statistics/statistical-power/

Beach, S. R., Czaja, S. J., & Schulz, R. (2023). Novel methods for assessment of vulnerability to financial exploitation (FE). *Journal of Elder Abuse & Neglect*, *35*(4-5), 151–173. https://doi.org/10.1080/08946566.2023.2281672.

Bernama (2025). *Increase in online fraud cases, nearly RM600 million losses recorded*. https://www.bernama.com/en/news.php?id=2414124.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *33*(4), 498-519. https://10.1057/sj.2012.11.

Cole, K., Kelly & Datar, T., & Rogers, M. (2015). Awareness of scam e-mails: An exploratory research study – Part 2. 115-125. *International Conference on Digital Forensics and Cyber Crime*. https://10.1007/978-3-319-25512-5_9.

Federal Trade Commission (2022). *Who experiences scams? A story of all ages.* https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages.

Gao, N., Ma, Y., & Xu, L. C. (2020). Credit constraints and fraud victimization: evidence from a representative Chinese household survey. *Policy Research Working Paper*. https://doi.org/10.1596/1813-9450-9460.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th Edition). Pearson Prentice Hall.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1),189 - 220. https://10.1111/j.1745-9125.2008.00101.x.

Hosmer, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). *Applied logistic regression* (3rd Edition). Wiley.

https://doi.org/10.24191/jcrinn.v11i2.563

Juremi, J (2024). Target: The young and vulnerable (2024). *The Star*. https://www.thestar.com.my/news/focus/2024/11/24/target-the-young-and-vulnerable.

Liu, X. F., Ai, Y., Jiang, L. C., Wang, X. & Wu, Y. (2025). Understanding the human element in scams: a multidisciplinary approach. *Journal of Information Technology Case and Application Research*, *27*(1), 9-24. https://doi.org/10.1080/15228053.2024.2439192.

Kipngetich, A. (2025). A review of online scams and financial fraud in the Digital Age. *GSC Advanced Research and Reviews*, *22*(01), 302-329. https://doi.org/10.30574/gscarr.2025.22.1.0025.

Koning, L., Junger, M., & Veldkamp, B. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, *30*(3), 443-479. https://doi.org/10.1177/02697580231215839.

Kubilay, E., Raiber, E., Spantig, L., Cahlikova, J. & Karia, L. (2023). Can you spot a scam? Measuring and improving scam identification ability. *Journal of Development Economics*, *165*, 103147. https://doi.org/10.1016/j.jdeveco.2023.103147.

Mauricio, B. A., Barbosa, R. R. (2009). Ontologies in knowledge management support: A case study. *Journal of the American Society for Information Science and Technology*, *60*(10), 2032-2047. https://doi.org/10.1002/asi.21120.

Muniam, R., Jaafar, N. S., Belaman, J. A. X., Suppiah, P. C. & Hussin, A. A. (2025). Education on scam awareness through digital literacy. *International Journal of Advanced Research in Education and Society*, 7(4), 39-47. https://doi.org/10.55057/ijares.2025.7.4.4.

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers In Psychology*, *13*, 912242. https://doi:10.3389/fpsyg.2022.912242.

Ueno, D., Daiku, Y., Eguchi, Y., Iwata, M., Amano, S., Ayani, N., Nakamura, K., Kato, Y., Matsuoka, T., & Narumoto, J. (2021). Mild cognitive decline is a risk factor for scam vulnerability in older adults. *Frontiers in Psychiatry*, *12*, 685451. https://10.3389/fpsyt.2021.685451.

Yu, L., Mottola, G., Barnes, L. L., Valdes, O., Wilson, R. S., Bennett, D. A., & Boyle, P. A. (2022). Financial fragility and scam susceptibility in community dwelling older adults. *Journal of Elder Abuse & Neglect*, *34*(2), 93-108. https://10.1080/08946566.2022.2070568.

Zhang, Z. & Ye, Z. (2022). The role of socio-psychological factors of victimity on victimization of online fraud in China. *Front. Psychol*, 13. https://doi.org/10.3389/fpsyg.2022.1030670.

https://doi.org/10.24191/jcrinn.v11i2.563