Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

ANALYSIS OF FACTORS INFLUENCING ONLINE FRAUD VICTIMIZATION AMONG UNIVERSITY STAFF

Nur Niswah Naslina Azid@Maarof[1*]
Nur Ashyefa Husna Nor Hazri[2]
Az'lina Abdul Hadi[3]
Nornadiah Mohd Razali[4]
Siti Noorul Ain Nor Azemi[5]

[1] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kelantan, 18500 Machang, Kelantan, Malaysia (E-mail: niswah@uitm.edu.my)
[2] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kelantan, 18500 Machang, Kelantan, Malaysia (E-mail: 2022664264@student.uitm.edu.my)
[3] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Negeri Sembilan, 70300 Seremban, Negeri Sembilan, Malaysia (E-mail: azlinahadi@uitm.edu.my)
[4] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Negeri Sembilan, 70300 Seremban, Negeri Sembilan, Malaysia (E-mail: nornadiah@uitm.edu.my)
[5] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia (E-mail: noorulain@uitm.edu.my)
*Corresponding author: niswah@uitm.edu.my

Article history
Received date : 4-10-2025
Revised date : 5-10-2025
Accepted date : 27-10-2025
Published date : 5-11-2025

To cite this document:
Azid@Maarof, N. N. N., Nor Hazri, N. A. H., Abdul Hadi, A., Mohd Razali, N., & Nor Azemi, S. N. A. (2025). Analysis of factors influencing online fraud victimization among university staff. *Journal of Islamic, Social, Economics and Development (JISED),* 10 (78), 35 – 44.

Abstract: *Online fraud and scams are defined as deceptive acts in which individuals are induced to disclose confidential information in response to fraudulent requests, resulting in financial or emotional harm. These activities have emerged as a critical global issue. This study investigates the determinants of fraud victimization among university staff, with an emphasis on the roles of psychological factors, consumer behaviour, awareness level, technological awareness and access, and social influence. Using a quantitative approach, data were collected via structured questionnaires from 105 staff members. Analytical procedures comprised descriptive statistics, Pearson correlation analysis, and multiple linear regression modelling. The findings reveal that psychological factors and technological awareness exert significant effects on fraud victimization. These results highlight the necessity of targeted awareness interventions and the enhancement of digital literacy as strategic measures to reduce vulnerability to online fraud.*

Keywords: *fraud victimization, psychological, consumer behaviour, awareness level, technological awareness*

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

Introduction

Online fraud and scams have emerged as a critical global issue, with Malaysia experiencing a sharp rise in cybercrime alongside the rapid expansion of internet usage and digital platforms. Ansar et al. (2021) define online scams as deceptive acts in which individuals are induced to disclose confidential information in response to fraudulent requests, resulting in financial or emotional harm. Between 2021 and April 2024, over 95,800 Malaysians collectively lost RM3.18 billion to scams, including investment fraud and identity theft that increasingly exploit technologies such as artificial intelligence (Isamudin, 2024).

Despite government initiatives, such as the establishment of the National Scam Response Centre and nationwide awareness campaigns, public knowledge remains limited; 64% of respondents in CelcomDigi's National Scam Awareness Survey (2024) were unaware of these resources, while 66% had experienced scam attempts, often through impersonation phone calls. Scammers frequently target urban populations via platforms such as Facebook and Mudah.my (Mohamad et al., 2023) and employ sophisticated methods, including social engineering and AI-driven phishing, that exploit psychological triggers such as fear and urgency. Low digital literacy, emotional vulnerability, and enforcement challenges despite legal provisions under Malaysia's Penal Code with further heighten susceptibility (Rahman, 2020).

Against this backdrop, the present study investigates psychological factors, consumer behaviour, awareness level, technology awareness and access, and social influences associated with fraud victimization among university staff with the goal of informing targeted prevention strategies and enhancing digital safety within the higher education context.

Literature Review

Research indicates that nearly half of adult internet users have reported being drawn into an online scam or fraud, highlighting the spread through nature of this issue (Ofcom, 2022). The psychological impacts of victimization can be intense, leading to long-term effects such as anxiety and distrust in online interactions (Koning et al., 2023). Previous studies have found that psychological traits such as impulsiveness and trust can significantly increase vulnerability to online fraud. For instance, Zhang and Ye (2022) found that individuals with high impulsiveness are associated with a higher risk of fraud victimization. Impulsive people are more prone to trust the con artists behind complex frauds because they are more receptive to outside influences than to their own logical reasoning when making decisions.

Research focusing on older adults indicates that intelligence decline can increase vulnerability to online fraud (Chen et al., 2025). The experiences with online scams can lead to increased scepticism and reduced trust in e-commerce platforms (Norton, 2023). Consumers who actively seek information about security measures are less likely to fall victim to scams (Ofcom, 2022).

Awareness may be defined in two ways: awareness about scams and the capacity to put that information into effect (Nauni, 2022). Having knowledge about common scam tactics is essential. Many scams use similar tricks to deceive people, such as pretending to be a trusted company or creating fake websites that look real. Studies show that individuals who are informed about these tactics are more likely to spot them and avoid falling victim (Patil & Arra, 2022). Many individuals might say they are aware of scams but still fall for them when they encounter them due to sharing personal information too freely or clicking on links without thinking (Althibyani & Al-Zahrani, 2023). Technological awareness and access are another important factor in protecting individuals from online fraud. Technological awareness refers to

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

how familiar people are with cybersecurity tools, such as antivirus software and two-factor authentication (Alrobaian et al., 2023). Social influence adds another layer, as advice or warnings shared by family, friends, or coworkers can significantly shape how individuals respond to online threats (Balakrishnan et al., 2025). The advice or experiences shared by friends, family, or social media influencers can shape on the understanding of online safety (Norris et al., 2019). Influencers or community leaders who share their experiences with fraud can raise awareness among their followers.

Methodology

This section elaborates the population and sample, instrument, and methods of analyses used in this study.

Population and Sample

This cross-sectional study focused on university staff selected for their extensive reliance on online platforms and corresponding vulnerability to cybercrime.

To ensure the reliability of the sample for this study, the researcher considered the inclusion and exclusion criteria. The inclusion criteria included the respondents who are current staff of UiTM Cawangan Kelantan comprising academic, non-academic, and contract staff with access to their official UiTM email accounts. Besides that, the selected respondents were active internet users engaging in routine activities such as online communication, financial transactions, or work-related digital tasks. The last criteria are providing informed consent to participate in the study. Exclusion criteria comprised individuals who were not employed at UiTM Cawangan Kelantan. Moreover, those staffs that reported with minimal or no use of online platforms were also excluded from the study. The researcher also omitted those respondents did not consent to participate or submitted incomplete responses.

The minimum required sample size was calculated using the Raosoft online sample-size calculator (Raosoft, 2004) based on the finite population of UiTM Cawangan Kelantan staff of 677, a 95% confidence level, a 5% margin of error, and a conservative response distribution of 50%. Under these assumptions, the Raosoft output yielded a minimum sample size of 246 respondents. Because the Raosoft estimate provides the statistically required minimum but does not account for potential nonresponse or unusable questionnaires, a conservative 10% inflation factor was applied to safeguard statistical power and representativeness in field conditions, yielding 246×1.10=270.6246 respondents, which was then rounded up to a final recruitment target of 271 respondents.

The study faced limitations in reaching the intended sample size of 271 due to participants' reluctance to participate. Nevertheless, 105 valid responses were obtained, which exceeded the minimum threshold required for regression analysis given the limited number of predictors. According to Tabachnick and Fidell's (2019) guideline, the minimum sample size for regression can be estimated using the formula $N \geq 50+8m$ where m represents the number of predictors. Based on this rule-of-thumb, the sample size achieved in this study was deemed adequate for the planned analyses. Data were collected via a structured online questionnaire distributed through official staff email accounts to ensure confidentiality, controlled access, and participant eligibility.

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

Instrument

The construct of extensive reliance on online platforms and corresponding vulnerability to cybercrime was operationalized through questionnaire with 25 items. These items with five major constructs include psychological factors, consumer behaviour, awareness levels, social influence and technological awareness presented as exploratory variables while fraud victimization as dependent variable. All the constructs were adopted from an established questionnaire with a ten-point scale ranging from scale 1 (Strongly disagree) to 10 (Strongly agree). The following table indicates the information on the dependent variable and the respective factors.

Table 1: Constructs Reliance on Fraud Victimization

Dependent Variable	Number of Question	Adopted From
Fraud Victimization	5	Whitty, 2019
Independent Variable	5	
Psychological Factors	5	Sur et al., 2021
Consumer Behaviour	5	Jalil & Sinnamon, 2020
Awareness Level	5	Qu et al., 2024
Technological Awareness	5	Getz et al., 2024
Social Influence	5	Shang et al., 2023

Methods of Analysis

Descriptive and advanced statistical techniques were applied in this study to address the stated objectives.

Descriptive Analysis

In this study, the data were analysed using a frequency table with the aim of presenting the demographic profile of the respondents, which includes gender, age, educational level, income. level, marital status and experienced online scam.

Multiple Linear Regression

A regression analysis was applied to examine the determinants of those that entice people to become victims of online fraud. There were five (5) independent variables, hence the regression model can be expressed as follows;

$$Y_1 = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \varepsilon$$

where,

y : Fraud victimization
X_1 : Psychological factors
X_2 : Consumer behaviour,
X_3 : Awareness level,
X_4 : Technology awareness and access,
X_5 : Social Influence
β_0, β_1, β_2, β_3, β_4, and β_5 are the regression coefficients
ε is the independent model error with follows $N \sim (0, \sigma^2)$.

Assumptions of Multiple Linear Regression

To ensure the accuracy of the model and validity of the results, several assumptions must be fulfilled. For that purpose, a normal probability plot was applied to check for the normality

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

assumption of the residuals. The homogeneity of the variance assumption was assessed by using a scatter plot of residuals versus predicted values, while linearity assumption was assessed based on the Pearson linear correlation coefficient. In addition, the Tolerance and Variance Inflation Factor (VIF) were applied to check the presence of multicollinearity.

Results and Findings

This study involved 105 respondents with a balanced gender distribution, comprising 56 females (53.3%) and 49 males (46.7%). Most respondents were aged between 30 and 49 years, with equal representation in the 30-39 and 40-49 age groups (27.6% each), while the smallest group was those aged 60 and above (6.7%). This minority group represents those staff who have retired but continue working on a contract basis. Educational attainment was generally high, with the majority holding a Diploma (30.5%), followed by Master's (22.9%), Bachelor's (21.9%), PhD (14.3%), and SPM (10.5%). Income levels varied, with the largest proportion earning RM2001-RM4000 (23.8%), followed by RM6001-RM8000 (21.0%) and RM4001-RM6000 (17.1%), while only 9.5% earned below RM2000. Nearly half were married (49.5%), with 25.7% single and 24.8% divorced. Notably, 36.2% had experienced online scams. Overall, the respondents were slightly female dominated, largely middle-aged, well-educated, and socioeconomically diverse. The results were summarized in Table 2 below.

Table 2: Descriptive Statistics

Variable	Class Variable	*n*	Percentage (%)
Gender	Male	49	46.7
	Female	56	53.3
Age	20-29	21	20
	30-39	29	27.6
	40-49	29	27.6
	50-59	19	18.1
	60 above	7	6.7
Educational level	SPM	11	10.5
	Diploma	32	30.5
	Degree	23	21.9
	Master	24	22.9
	PhD	15	14.3
Income level	Below RM2000	10	9.5
	RM2001-RM4000	25	23.8
	RM4001-RM6000	18	17.1
	RM6001-RM8000	22	21.0
	RM8001-RM10000	18	17.1
	Above RM10000	12	11.4
Marital Status	Single	27	25.7
	Married	52	49.5
	Divorced	26	24.8
Experienced online scam	Yes	38	36.2
	No	67	63.8

Pearson correlation analysis was performed to assess the relationship between the dependent variable (fraud victimization) and the independent variables: psychological factors, consumer behaviour, awareness level, technological awareness and access, and social influence. As presented in Table 3, all independent variables demonstrated a statistically significant positive

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

correlation with fraud victimization at 0.05 significance level. Psychological factors exhibited the strongest association (r=0.376, p< 0.01), followed closely by technological awareness and access (r=0.356, p< 0.01), both indicating moderate positive relationships. In contrast, consumer behaviour (r = 0.241, p = 0.013), awareness level (r = 0.272, p = 0.005), and social influence (r=0.288, p=0.003) showed statistically significant but weaker positive correlations. These results suggest that the identified factors are meaningfully associated with fraud exposure among university staff.

Table 3: Pearson Correlation

Independent Variable	Pearson Correlation (r)	Sig. (2-tailed)	Strength of Relationship
Psychological Factors	0.376	0.000	Moderate Positive (Significant)
Consumer Behaviour	0.241	0.013	Weak Positive (Significant)
Awareness Level	0.272	0.005	Weak Positive (Significant)
Technological Awareness	0.356	0.000	Moderate Positive (Significant)
Social Influence	0.288	0.003	Weak Positive (Significant)

The multiple linear regression analysis examined the influence of five independent variables; psychological factors, consumer behaviour, awareness level, technological awareness and access, and social influence on fraud victimization among staff. Using the stepwise regression method, the final model incorporating these two predictors demonstrated a moderate correlation (R=0.465) and explained 21.6% of the variance (adjusted R^2=0.200). Both predictors showed positive and significant effects: psychological score (B=0.243, β=0.308, p=0.001) and technological awareness score (B=0.221, β=0.281, p= 0.002). The model was statistically significant (F = 14.033, p < 0.001). No multicollinearity issues were detected (tolerance > 0.9, VIF =1.06). These findings confirm both variables as key predictors of fraud victimization. The fraud prevention strategies should prioritize strengthening psychological resilience and promoting responsible technology use to mitigate victimization risks.

Table 4: Regression Coefficients

Predictor	B	Beta	t	Sig.	Interpretation	Tolerance	VIF
Psychological factor	0.243	0.308	3.404	0.001	Significant positive effect	0.941	1.063
Technological awareness and access	0.221	0.281	3.107	0.002	Significant positive effect	0.941	1.063

The regression diagnostics in Figure 1 indicated that the residuals were approximately normally distributed, as shown by the Normal P-P Plot, with no significant deviations or outliers. The scatterplot of residuals displayed a random, balanced spread around zero, confirming constant variance. Thus, the assumptions of normality and homoscedasticity were satisfied.

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

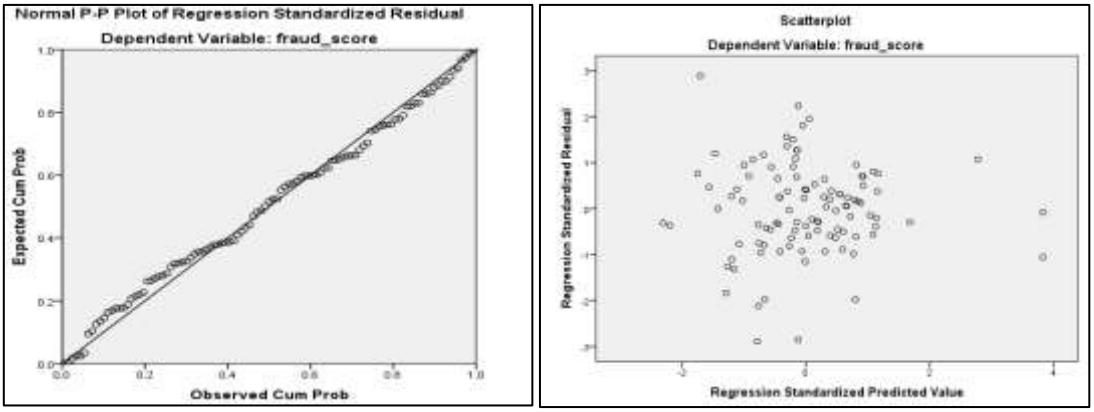

Figure 1: Normal P-P Plot and Scatterplot

Discussion of Results

A multiple linear regression analysis performed in this study to achieve the objective revealed that psychological factors and technological awareness and access emerged as significant predictors, while the other factors were not significant. These findings demonstrate mixed or context-dependent effects for awareness, consumer behaviour, and social influence, but they are partially consistent with previous research that frequently identifies individual cognitive/affective qualities and digital capability/exposure as important predictors of fraud susceptibility.

Consistent with many prior studies, this study reports the robust effects of psychological vulnerabilities (impulsive, trust, affect) and technological awareness on fraud victimization. A positive relationship between fraud victimization and psychological factors implies that university staff who exhibit higher impulsivity or trust propensity, or who rely more on intuitive processing, may respond more readily to persuasive cues in fraud attempts. Conversely, those with higher self-control and scepticism may better detect red flags. On the other hand, a positive relationship between fraud victimization and technological awareness and access implies that staff with higher technological awareness can better identify anomalies such as spoofed domains, unusual permissions and atypical sender behaviour. Hence, they are able to apply protective practices better than those without technological awareness.

Meanwhile, there is conflicting research on social influence and generic awareness. The Pearson correlation coefficient revealed a favourable correlation between fraud victimization and awareness, customer behaviour, and social influence. However, these effects became non-significant in the multiple linear regression model, probably due to shared variation with psychological characteristics and technology knowledge. Other characteristics like limited variability (possible ceiling effects), and probable nonlinearity might have also lessened their distinct contributions.

In addition, while some research revealed null effects for generic awareness, others find beneficial protective effects of skills-based, specialized training. Social influence can be less pronounced in academic or professional settings, but it frequently manifests itself in consumer audiences or younger generations. Effects frequently vary by setting (corporate vs. academic), attack type (phishing vs. investment scams), and measurement granularity. The results produced in this study are consistent with the idea that operational, skills-focused capabilities and individual psychological dispositions are more proximal predictors in workplace fraud scenarios.

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

Conclusion

This study examined the influence of psychological factors, consumer behavior, awareness level, technological awareness and access, and social influence on fraud victimization among university staff. Statistical analyses revealed that only psychological factors and technological awareness and access were significant positive predictors of fraud victimization. Individuals with higher psychological vulnerability and greater access to technology were more likely to fall victim to fraud, while consumer behavior, awareness level, and social influence were not significant predictors. The regression model accounted for 21.6% of the variance in fraud victimization, a level considered acceptable in social science research. All regression assumptions, including normality, homoscedasticity, and multicollinearity, were met, confirming the model's validity. The findings underscore the importance of addressing psychological vulnerabilities and technological exposure in fraud prevention strategies. Despite its limitations, the study offers valuable insights for universities and organizations seeking to strengthen protection against scams, particularly in increasingly digital environments. By focusing on these key predictors, institutions can design targeted interventions, raise awareness, and promote digital resilience to reduce the risk of victimization.

Acknowledgements

1. The authors would like to thank the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Cawangan Kelantan, for its support.
2. We also want to express our gratitude to the UiTM Research Ethics Committee for helping to make this study a success. No grants were obtained to support this study.

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

References

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing, 7(2), 73*. https://doi.org/10.3390/bdcc7020073.

Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. *Sustainability, 15*(15), 11512. https://doi.org/10.3390/su151511512

Ansar, S. A., Yadav, J., Dwivedi, S. K., Pandey, A., Srivastava, S. P., Ishrat, M., Khan, M. W., Pandey, D., & Khan, R. A. (2021). A critical analysis of fraud cases on the Internet. *Turkish Journal of Computer and Mathematics Education, 12*(1), 424–445.

Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLoS ONE, 20*(1), e0317232. https://doi.org/10.1371/journal.pone.0317232

CelcomDigi. (2024). *National Scam Awareness Survey 2024*. CelcomDigi Berhad.

Chen, H., He, M., Xu, X., & Atkin, D. (2025). Examining older adults' vulnerability to online health scams: Insights from routine activity theory. *Frontiers in Public Health, 13*, 1585851. https://doi.org/10.3389/fpubh.2025.1585851

Isamudin, D. (2024). RM3.2b lost to online scams between 2021 and April 2024 – Gobind. https://www.nst.com.my/business/economy/2024/08/1090337/rm32b-lost-online-scams-between-2021-and-april-2024-gobind

Koning, L., Junger, M., & Veldkamp, B. (2023). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *Sage Journals, 30*(3). https://doi.org/10.1177/02697580231215839

Mohamad, Z., Ismail, Z., & Thani, A. K. A. (2023). Determinants of fraud victimizations in Malaysian e-commerce: A conceptual paper. *International Journal of Academic Research in Business and Social Sciences, 13*(12). https://doi.org/10.6007/ijarbss/v13-i12/20395

Nauni, M. (2022). Raised awareness helps detecting and preventing online shopping scams (By P. Hartel, Singapore University of Technology and Design, SUTD Institutional Review Board, Ms Jasmine, Professor Pieter Hartel, & Mr Jaddoo Yeaz Elias). https://mayanknauni.com/wpcontent/uploads/2022/08/Thesis_Paper_Mayank_Nauni_v13.pdf

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology, 34*(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5

Norton. (2023). *Norton Cyber Safety Pulse Report: Scams in the digital age*. https://us.norton.com/blog/emerging-threats/pulse-report-september-2023

Ofcom. (2022). *Online scams and fraud research – Technical report*. Ofcom. https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-fraud-and-scams/online-scams-and-fraud-research-technical-report?v=329361

Patil, S., & Arra, S. (2022). Detection of phishing and user awareness training in information security: A systematic literature review. In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 780–786. https://doi.org/10.1109/ICIPTM54933.2022.9753912

Rahman, M. R. A. (2020). Online scammers and their mules in Malaysia. *Jurnal Undang-Undang Dan Masyarakat, 26*, 65–72. https://doi.org/10.17576/juum-2020-26-08.

Raosoft, 2004, Raosoft, Inc., http://www.raosoft.com/samplesize.html.

Tabachnick, B. G., & Fidell, L. S. (2019). Using multivariate statistics, 7th Ed, Pearson.

Volume: 10 Issues: 78 Special Issue [November, 2025] pp. 35 - 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.academicinspired.com/jised
DOI: 10.55573/JISED.107804

Zhang, Z. & Ye, Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China. *Front Psychol*, 13:1030670. https://doi:10.3389/fpsyg.2022.1030670