Architecture
Image Studies

Vol.6, Issue 4, pp.442-449, 2025
DOI: https://doi.org/10.62754/ais.v6i4.597

https://journals.ap2.pt/index.php/ais/index

Assessing Citizens' Readiness and Utilization of the National Scam Response Centre (NSRC) in Combating Online Scams: The Moderating Effect of Education

Nalini Munusamy[1], Muslimin Wallang[2]

Abstract

The increasing prevalence of online scams poses significant threats to financial security, trust in digital systems, and national economic stability. To address this growing concern, Malaysia established the National Scam Response Centre (NSRC) as a centralized platform for scam reporting and intervention. Despite the NSRC's potential, limited empirical research has examined factors influencing its utilization. This study investigates the impact of citizens' readiness factors including awareness, perceived risk, performance expectancy, effort expectancy, and social influence on NSRC utilization, while also examining the moderating role of education. Drawing upon Protection Motivation Theory (PMT), Perceived Risk Theory (PRT), and the Unified Theory of Acceptance and Use of Technology (UTAUT), a survey was administered to 416 respondents across Malaysia. Partial Least Squares Structural Equation Modelling (PLS-SEM) was employed for data analysis. The results reveal that all five readiness factors significantly influence NSRC utilization, with awareness being the strongest predictor. Education was found to significantly moderate the relationship between awareness and utilization but did not moderate other predictors. The findings underscore the importance of enhancing public awareness and digital literacy to strengthen citizen engagement with NSRC services.

Keywords: *Online Scams, National Scam Response Centre, Awareness, Perceived Risk, UTAUT, PLS-SEM.*

Introduction

The rapid advancement of digital technologies has brought about unprecedented opportunities for economic growth, social interaction, and innovation. However, alongside these benefits, cybercrime particularly online scams have emerged as a global threat. Online scams, including phishing, investment fraud, identity theft, and social engineering, not only result in substantial financial losses but also erode public confidence in digital systems. In Malaysia, the Commercial Crime Investigation Department (CCID) and the Malaysian Communications and Multimedia Commission (MCMC) have reported sharp increases in scam cases, reflecting the growing urgency of effective response mechanisms.

To address this concern, Malaysia established the National Scam Response Centre (NSRC) in 2022. The NSRC serves as a centralized hub for scam reporting and rapid intervention, providing the public with a hotline (997) that coordinates with law enforcement, banks, and telecommunications providers. Despite the NSRC's strategic role, limited research has investigated the determinants of citizen utilization of its services.

Existing scholarship on technology adoption and protective behaviour emphasizes awareness, risk perception, perceived ease of use, perceived usefulness, and social influence. Yet, little is known about how these factors affect scam reporting in Malaysia. Moreover, socio-demographic variables such as education may shape citizens' readiness and ability to act, but empirical evidence remains sparse.

This study aims to address these gaps by examining the factors influencing the utilization of the NSRC. Specifically, it investigates the impact of awareness, perceived risk, performance expectancy,

[1] Ghazali Shafie Graduate School of Government, University Utara Malaysia, Kedah, Malaysia, Email: nalini_munusamy2@gsgsg.uum.edu.my
[2] School of Government, University Utara Malaysia, Kedah Malaysia, Email: muslimin@uum.edu.my

effort expectancy, and social influence on NSRC utilization, while testing the moderating role of education. The study is guided by two research objectives: (1) To examine the relationship between citizen readiness and the utilization of the National Scam Response Centre (NSRC) in combating online scams. (2) To identify the role of policing strategies in enhancing public engagement with the NSRC.

Theoretical Basis and Conceptual Framework

The research is based on three theoretical perspectives: Protection Motivation Theory (PMT), Perceived Risk Theory (PRT), and the Unified Theory of Acceptance and Use of Technology (UTAUT). These frameworks create a holistic view for understanding the preparedness of citizens when engaging with the National Scam Response Centre (NSRC) to combat online scams.

Protection Motivation Theory (PMT)

PMT (Rogers, 1975) suggests that people enact protective behaviors when they assess a threat as serious, and believe they can act effectively in response to it. Two cognitive processes drive such behaviours: threat appraisal (the seriousness of the threat and personal vulnerability), and coping appraisal (the effectiveness of response and self-efficacy). In this study, PMT informs the construct of awareness, which represents citizens' knowledge of scams and awareness of NSRC's functions. When citizens perceive scams to be serious and capable of responding to scam alerts, they will be more likely to take part in protective mechanisms, such as the NSRC hotline.

Perceived Risk Theory (PRT)

PRT articulates behavioral reactions to uncertainty and potential loss (Bauer, 1960). With scams, the individual concerned has potential risks regarding financial loss, identity theft, or retaliation by scammers. There would also be potential risks to reporting, such as data privacy and doubts about the security of the institution. Therefore, in this study, perceived risk is included as an antecedent to NSRC use to recognize that increased risk may either promote reporting, or deter reporting based on the contextual situation.

Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT (Venkatesh et al., 2003) provides a robust model for understanding technology adoption. Four constructs are particularly relevant: performance expectancy (belief that using the NSRC will reduce scams and provide value), effort expectancy (ease of using the system), social influence (perceptions of encouragement from peers, government campaigns, or media), and facilitating conditions (availability of resources and support). In this study, performance expectancy, effort expectancy, and social influence are applied to explain citizen readiness for NSRC utilization.

Education as a Moderating Variable

Education is posited as a moderator in this framework. Higher education levels are associated with greater digital literacy, stronger information-processing abilities, and greater confidence in navigating online systems. Thus, education is expected to strengthen the relationship between readiness factors and NSRC utilization, particularly between awareness and utilization, as educated citizens may be better equipped to translate awareness into concrete reporting behaviors.

Conceptual Framework

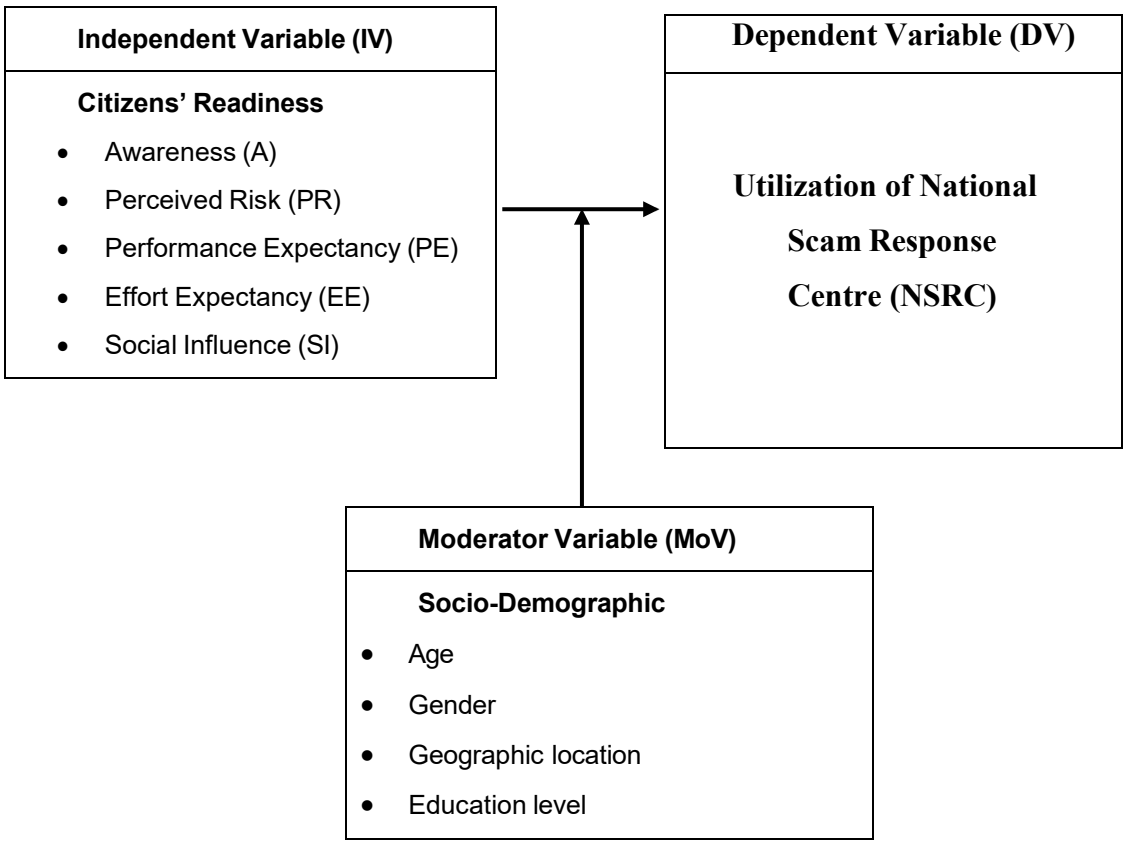

Figure 1: Conceptual Framework

Methodology

In this study, the researchers utilized a formal quantitative, cross-sectional research design, using a formalized survey to test the hypothesized relationships. A total of 416 targeted respondents were recruited from multiple regions across Malaysia. The researchers ensured that the selected sample was reflective of the population based on the sociodemographic groups of gender, age, education, and geographically where the respondents were recruited, by strategically recruiting based on the educational qualification of having a minimum degree. The questionnaire selected and developed by the research team, measured six constructs of interest: awareness, perceived risk, performance expectancy, effort expectancy, social influence, and NSRC utilization. All attitudinal scale items were measured using five-point scale Likert items. A robust pilot study was conducted by the researchers to ensure reliability and validity of the instrument. There were multiple steps in the analysis of the participants, the data was processed utilizing Partial Least Squares Structural Equation Modelling (PLS-SEM) via SmartPLS 4, which included, 1) evaluation of the measurement model, 2) evaluation of the structural model, and lastly, 3) moderation analysis.

Results

Respondent Profile

The demographic profile of the respondents (Table 1) provides important context for interpreting the findings. The sample of 416 respondents comprised predominantly males (63.9%), while females accounted for 36.1 percent. The age distribution showed that the largest group was between 31 and 40 years (53.6%), reflecting the working-age population most exposed to digital transactions and, consequently, to online scams. A significant proportion (23.1%) were aged between 51 and 60, while 16.6 percent were over 61, suggesting that older generations are also increasingly vulnerable.

In terms of education, the majority held SPM (35.1%) and STPM (33.4%), while 24.5 percent had diploma or degree qualifications. Only a small fraction (7%) held certificate-level education. This distribution is particularly relevant given the study's focus on education as a moderating variable. The majority of respondents resided in urban areas (63.7%), reflecting higher digital exposure compared to rural respondents (36.3%).

Table 1. Demographics of Respondents (N = 416)

Variable	Category	Frequency	Percentage (%)
Gender	Male	266	63.9
	Female	150	36.1
Age	20–30 years	8	1.9
	31–40 years	223	53.6
	41–50 years	20	4.8
	51–60 years	96	23.1
	> 61 years	69	16.6
Education	Certificate	29	7.0
	SPM	146	35.1
	STPM	139	33.4
	Diploma/Degree	102	24.5
Location	Urban	265	63.7
	Rural	151	36.3

Descriptive Statistics

Table 2 presents descriptive statistics for the six constructs. Awareness (M = 3.56, SD = 1.09), perceived risk (M = 3.65, SD = 1.13), and performance expectancy (M = 3.61, SD = 1.08) were rated at moderate levels. This suggests that while respondents were aware of the existence of scams and the NSRC, they were not highly confident in their knowledge or in the system's effectiveness.

In contrast, effort expectancy (M = 3.67, SD = 1.09), social influence (M = 3.71, SD = 0.86), and NSRC utilization (M = 3.85, SD = 1.11) were rated high. These findings suggest that respondents generally perceived the NSRC to be user-friendly and supported by their social environment, and they also expressed trust and willingness to engage with it.

The distinction between moderate and high ratings is important: it shows that while citizens are generally supportive of the NSRC and find it accessible, gaps remain in raising public knowledge and confidence in its overall effectiveness.

Table 2. Descriptive Analysis of Constructs

Construct	Mean	SD	Level
Awareness	3.56	1.09	Moderate
Perceived Risk	3.65	1.13	Moderate
Performance Expectancy	3.61	1.08	Moderate
Effort Expectancy	3.67	1.09	High
Social Influence	3.71	0.86	High
NSRC Utilization	3.85	1.11	High

Measurement Model

The findings related to the dimensions of measurement model related to each study construct are shown in Table 3. Reliability levels were satisfactory, with Cronbach's alpha ranging from 0.879 to 0.961, which is greater than the minimum standard of 0.70. Composite reliability (CR) levels were also high ranging from 0.908 to 0.968 indicating sufficient internal consistency. Average Variance Extracted (AVE) was much greater than the minimum standard of 0.50, ranging from 0.622 to 0.836, indicating convergent validity. This suggests that the measurement tools in this research were both reliable and valid, lending empirical support for further exploration of the structural model.

Table 3. Construct Reliability and Validity

Construct	Cronbach's Alpha	CR	AVE
Awareness	0.949	0.961	0.831
Perceived Risk	0.946	0.958	0.822

Performance Expectancy	0.961	0.968	0.836

Table 1. Demographics of Respondents (N = 416)

Variable	Category	Frequency	Percentage (%)
Gender	Male	266	63.9
	Female	150	36.1
Age	20–30 years	8	1.9
	31–40 years	223	53.6
	41–50 years	20	4.8
	51–60 years	96	23.1
	> 61 years	69	16.6
Education	Certificate	29	7.0
	SPM	146	35.1
	STPM	139	33.4
	Diploma/Degree	102	24.5
Location	Urban	265	63.7
	Rural	151	36.3

Descriptive Statistics

Table 2 presents descriptive statistics for the six constructs. Awareness (M = 3.56, SD = 1.09), perceived risk (M = 3.65, SD = 1.13), and performance expectancy (M = 3.61, SD = 1.08) were rated at moderate levels. This suggests that while respondents were aware of the existence of scams and the NSRC, they were not highly confident in their knowledge or in the system's effectiveness.

In contrast, effort expectancy (M = 3.67, SD = 1.09), social influence (M = 3.71, SD = 0.86), and NSRC utilization (M = 3.85, SD = 1.11) were rated high. These findings suggest that respondents generally perceived the NSRC to be user-friendly and supported by their social environment, and they also expressed trust and willingness to engage with it.

The distinction between moderate and high ratings is important: it shows that while citizens are generally supportive of the NSRC and find it accessible, gaps remain in raising public knowledge and confidence in its overall effectiveness.

Table 2. Descriptive Analysis of Constructs

Construct	Mean	SD	Level
Awareness	3.56	1.09	Moderate
Perceived Risk	3.65	1.13	Moderate
Performance Expectancy	3.61	1.08	Moderate
Effort Expectancy	3.67	1.09	High
Social Influence	3.71	0.86	High
NSRC Utilization	3.85	1.11	High

Measurement Model

The findings related to the dimensions of measurement model related to each study construct are shown in Table 3. Reliability levels were satisfactory, with Cronbach's alpha ranging from 0.879 to 0.961, which is greater than the minimum standard of 0.70. Composite reliability (CR) levels were also high ranging from 0.908 to 0.968 indicating sufficient internal consistency. Average Variance Extracted (AVE) was much greater than the minimum standard of 0.50, ranging from 0.622 to 0.836, indicating convergent validity. This suggests that the measurement tools in this research were both reliable and valid, lending empirical support for further exploration of the structural model.

Table 3. Construct Reliability and Validity

Construct	Cronbach's Alpha	CR	AVE
Awareness	0.949	0.961	0.831
Perceived Risk	0.946	0.958	0.822
Performance Expectancy	0.961	0.968	0.836

Effort Expectancy	0.948	0.960	0.829
Social Influence	0.879	0.908	0.622
NSRC Utilization	0.935	0.947	0.721

Structural Model

The structural model explained 72.9 percent of the variance in NSRC utilization ($R^2 = 0.729$), which is considered substantial in behavioural and social sciences research. This indicates that the five predictors collectively accounted for nearly three-quarters of the variance in utilization, highlighting the robustness of the model.

Table 4 shows the path coefficients and effect sizes. Awareness exerted the strongest positive influence on NSRC utilization ($\beta = 0.305$, $t = 7.761$, $p < 0.001$, $f^2 = 0.177$), confirming it as the most critical driver of citizen engagement. This finding indicates that when citizens are more informed about scams and the NSRC's role, they are significantly more likely to use the service.

Perceived risk also significantly influenced utilization ($\beta = 0.238$, $t = 4.914$, $p < 0.001$, $f^2 = 0.074$). This suggests that heightened concerns about scams—whether financial, reputational, or personal security risks—motivate individuals to take preventive action by reporting to the NSRC.

Effort expectancy ($\beta = 0.199$, $t = 4.184$, $p < 0.001$, $f^2 = 0.050$) and performance expectancy ($\beta = 0.187$, $t = 5.303$, $p < 0.001$, $f^2 = 0.065$) were also significant predictors, demonstrating that perceptions of usability and system effectiveness play key roles in shaping utilization. This underscores the importance of ensuring that the NSRC reporting process remains simple, accessible, and efficient.

Social influence had the weakest but still significant effect ($\beta = 0.108$, $t = 2.924$, $p = 0.003$, $f^2 = 0.026$). This implies that encouragement from peers, family, community, and government campaigns has a role, but less impact compared to awareness or perceived risk.

These results confirm that cognitive (awareness, perceived risk), functional (effort and performance expectancy), and contextual (social influence) factors all contribute to explaining NSRC utilization.

Table 4. Path Coefficients and Effect Sizes

Hypothesis	Path	β	t-value	p-value	f^2	Result
H1	Awareness → Utilization	0.305	7.761	<0.001	0.177	Supported
H2	Effort Expectancy → Utilization	0.199	4.184	<0.001	0.050	Supported
H3	Perceived Risk → Utilization	0.238	4.914	<0.001	0.074	Supported
H4	Performance Expectancy → Utilization	0.187	5.303	<0.001	0.065	Supported
H5	Social Influence → Utilization	0.108	2.924	0.003	0.026	Supported

Moderation Analysis

The moderating effect of education was tested across the five predictor variables (Table 5). Only the interaction between education and awareness was statistically significant ($\beta = 0.193$, $t = 5.905$, $p < 0.001$). This indicates that education strengthens the positive relationship between awareness and utilization. In other words, citizens with higher education levels were more likely to act on their awareness of scams and use the NSRC effectively.

For the other predictors which are perceived risk, social influence, performance expectancy, and effort expectancy was not significant. This suggests that education does not influence how these factors translate into NSRC utilization.

The selective moderating role of education highlights that while education enhances the awareness, utilization pathway, other readiness factors operate more universally across different education levels.

Table 5. Moderating Effect of Education

Hypothesis	Interaction	β	t-value	p-value	Result
H6	Education × Awareness	0.193	5.905	<0.001	Significant
H7	Education × Perceived Risk	- 0.091	1.887	0.059	Not Significant
H8	Education × Social Influence	0.044	1.540	0.124	Not Significant
H9	Education × Performance Expectancy	- 0.004	0.106	0.916	Not Significant
H10	Education× Effort Expectancy	- 0.065	1.322	0.186	Not Significant

Discussion

The results confirm that readiness factors significantly predict NSRC utilization. Awareness was the strongest predictor, indicating that citizens' knowledge of scams and NSRC functions is vital for engagement. Perceived risk also had a positive effect, suggesting that concerns about scams motivate citizens to report, even when fears about data security remain. Effort expectancy and performance expectancy highlight the importance of system usability and effectiveness perceptions. Social influence, though weaker, underscores the role of peers, government campaigns, and media.

Education moderated only the relationship between awareness and utilization. This finding demonstrates that higher education enhances the likelihood of translating awareness into action, reflecting the importance of digital literacy in combating scams.

Conclusion

This study provides empirical evidence that awareness, perceived risk, performance expectancy, effort expectancy, and social influence significantly influence NSRC utilization. Among these, awareness emerged as the strongest determinant. Education played a selective moderating role, strengthening the effect of awareness on utilization.

The findings highlight the need for targeted awareness campaigns and digital literacy programs to promote active engagement with the NSRC. Simplifying reporting processes and building trust in the system are essential steps toward combating the rising tide of online scams in Malaysia.

References

[1] Action Fraud UK. (2020). Investment scam reports. https://www.actionfraud.police.uk

[2] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

[3] Alharbi, H., Alshammari, M., & Almobaireek, F. (2020). The role of demographic factors in technology adoption in rural and urban settings. International Journal of Technology, Policy and Management, 20(2), 120–137.

[4] Almetere, E., Kelana, B., & Mansor, N. (2020). Using UTAUT model to determine factors affecting Internet of Things acceptance in public universities. International Journal of Academic Research in Business and Social Sciences, 10(2), 691–706. https://doi.org/10.6007/ijarbss/v10-i2/6915

[5] Alshammari, A. (2024). The influence of emotions on employees' cybersecurity protection motivation behaviour: Examining the mediating effect of self-efficacy and moderating role [Doctoral dissertation, Aston University]. Aston Publications. https://publications.aston.ac.uk/id/eprint/47861/1/Alshammari_Abdulelah_-_2024.pdf

[6] American Psychological Association. (2017). Ethical principles of psychologists and code of conduct. American Psychological Association.

[7] Andrews, J., Ward, H., & Yoon, J. (2021). UTAUT as a model for understanding intention to adopt AI and related technologies among librarians. The Journal of Academic Librarianship, 47(5), 102437. https://doi.org/10.1016/j.acalib.2021.102437

[8] Antonenko, P. (2015). The instrumental value of conceptual frameworks in educational technology research. Educational Technology Research and Development, 63(1), 53–71. https://doi.org/10.1007/s11423-014-9363-4
[9] Arias-de la Torre, J., Vilagut, G., Ronaldson, A., Serrano-Blanco, A., Martín, V., Peters, M., & Alonso, J. (2021). Handling missing data in health-related quality of life measures: A methodological review. Quality of Life Research, 30(5), 1305–1323. https://doi.org/10.1007/s11136-020-02733-3
[10] Australian Cyber Security Centre. (2021a). Annual cyber threat report 2021. Australian Government.
[11] Bank Negara Malaysia. (2021). Report on investment scams in Malaysia. https://www.bnm.gov.my
[12] Bordage, G. (2009). Conceptual frameworks to illuminate and magnify. Medical Education, 43(4), 312–319. https://doi.org/10.1111/j.1365-2923.2009.03295.x
[13] Bravo, L., Sagredo, M., Martínez, T., Penna, C., Molina, J., Stanciu, I., & Nistor, N. (2020). Psychometric analysis of a measure of acceptance of new technologies (UTAUT), applied to the use of haptic virtual simulators in dental students. European Journal of Dental Education, 24(2), 223–234. https://doi.org/10.1111/eje.12559
[14] Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
[15] Button, M., & Whittaker, J. (2021). Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation. International Journal of Law, Crime and Justice, 65, 100480. https://doi.org/10.1016/j.ijlcj.2021.100480
[16] Chopdar, P., Korfiatis, N., Sivakumar, V., & Lytras, M. (2018). Mobile shopping apps adoption and perceived risks: A cross-country perspective utilizing the Unified Theory of Acceptance and Use of Technology. Computers in Human Behavior, 86, 109–128. https://doi.org/10.1016/j.chb.2018.04.017
[17] Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.
[18] Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage Publications.
[19] Cross, C., Richards, K., & Smith, R. (2016). Improving responses to online fraud victims: An examination of reporting and support (Final report for Criminology Research Grant 29/13-14). https://eprints.qut.edu.au/98346/1/29-1314-FinalReport.pdf
[20] Cybersecurity and Infrastructure Security Agency. (2020). Ransomware awareness. https://www.cisa.gov
[21] Dwivedi, Y., Rana, N., Tamilmani, K., & Raman, R. (2020). A meta-analysis based modified unified theory of acceptance and use of technology (meta-UTAUT): A review of emerging literature. Current Opinion in Psychology, 36, 13–18. https://doi.org/10.1016/j.copsyc.2020.03.008
[22] Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1–4.
[23] European Union Agency for Cybersecurity. (2020). The role of scam response centers in cybercrime prevention. https://www.enisa.europa.eu
[24] Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). Sage Publications.
[25] Haynes, S. N., Richard, D. C., & Kubany, E. S. (1995). Content validity in psychological assessment: A functional approach to concepts and methods. Psychological Assessment, 7(3), 238–247. https://doi.org/10.1037/1040-3590.7.3.238
[26] Hohwü, L., Lyshol, H., Gissler, M., Jonsson, S. H., Petzold, M., & Obel, C. (2021). Non-response bias in health surveys among children and adolescents: A systematic review. BMC Public Health, 21, 1045. https://doi.org/10.1186/s12889-021-10274-7
[27] Imenda, S. (2014). Is There a Conceptual Difference between Theoretical and Conceptual Frameworks?. Journal of Social Sciences, 38, 185 - 195. https://doi.org/10.1080/09718923.2014.11893249
[28] Jadhav, Y. M. (2024). Analyzing efficacy and enhancing accessibility: A study of India's national cybercrime reporting portal in addressing financial cybercrimes. International Journal of Scientific Research in Computer Science and Engineering. Retrieved from https://www.researchgate.net/profile/Yogesh-Jadhav-6/publication/379219569
[29] Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (2000). Consumer trust in an internet store: A cross-cultural validation. Journal of Computer-Mediated Communication, 5(2), 1-35.
[30] Johnson, B., & Christensen, L. (2017). Educational research: Quantitative, qualitative, and mixed approaches (6th ed.). Sage Publications
[31] Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. International Journal of Qualitative Methods, 8(4), 49–62. https://doi.org/10.1177/160940690900800406
[32] Jain, R., Culler, D., & Sarma, S. (2019). Digital fraud: A growing concern. Cybersecurity Journal, 12(1), 34–56.
[33] Kulesa, J., Induru, S., Hubbard, E., & Bhansali, P. (2024). The Conceptual Framework: A Practical Guide.. Hospital pediatrics. https://doi.org/10.1542/hpeds.2024-007794
[34] Malaysia Communications and Multimedia Commission. (2020). National Scam Response Centre annual report.
[35] Malaysia Cyber Security Agency (MyCERT). (2020). Cyber security report. https://www.mycert.org.my
[36] Malaysian Communications and Multimedia Commission (MCMC). (2020). Annual report. https://www.mcmc.gov.my

[37] Malaysian Communications and Multimedia Commission. (2021). Report on phishing scams in Malaysia. https://www.mcmc.gov.my
[38] Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management, 34(1), 1–13. https://doi.org/10.1016/j.ijinfomgt.2013.06.002
[39] Morgan, A., Dowling, C., Brown, R., & Mann, M., Voce, I. (2016). Evaluation of the Australian cybercrime online reporting network. QUT ePrints. https://eprints.qut.edu.au/121532/
[40] Müller, T., Lin, H., & Tan, G. (2020). Socio-demographic factors influencing digital public service usage: A study of online scam reporting. Journal of Social Informatics, 34(1), 112–125.
[41] Ong, K., Tan, J., & Mohd, R. (2020). Exploring public awareness and utilization of national cybersecurity services in Southeast Asia. Cybersecurity Review, 8(1), 42–55.
[42] Organization for Economic Cooperation and Development. (2020). International cooperation in combating online scams. https://www.oecd.org
[43] Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. (2017). Measures of social psychological attitudes (Vol. 1). Academic Press.
[44] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93–114.
[45] Royal Malaysia Police. (2021). Annual crime report on love scams. https://www.rmp.gov.my
[46] Singapore Police Force. (2021). Anti-Scam Centre's impact on victim recovery. https://www.police.gov.sg
[47] Song, C., Lee, J., & Roh, T. (2024). Exploring cloud storage service adoption through the dual perspectives: Protection Motivation Theory (PMT) and the extended Unified Theory of Technology Acceptance Model (UTAUT2). International Journal of Human–Computer Interaction, 41, 2745–2762. https://doi.org/10.1080/10447318.2024.2327219
[48] Sook, Y. (2019). Understanding the reluctance to report online scams in Malaysia. Journal of Cybersecurity Studies, 4(2), 115–130.
[49] Sung, W. J., & Lee, J. (2025). Socio-demographics and citizens' use of e-government services: A longitudinal analysis of the e-government survey data in Korea. Public Performance & Management Review. https://www.tandfonline.com/doi/abs/10.1080/15309576.2025.2465747
[50] Tabachnick, B. G., & Fidell, L. S. (2013). Using multivariate statistics (6th ed.). Pearson Education.
[51] Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International Journal of Medical Education, 2, 53–55.
[52] Tehseen, S., Ramayah, T., & Sajilan, S. (2020). Testing and controlling for common method variance: A review of available methods. Journal of Management Sciences, 7(2), 205–218. https://doi.org/10.20547/jms.2014.2007202
[53] U.S. Department of Health & Human Services. (2020). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. U.S. Government Printing Office.
[54] United Nations Office on Drugs and Crime (UNODC). (2020). Cybercrime and the global threat landscape. Retrieved from https://www.unodc.org
[55] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926
[56] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540
[57] Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178. https://doi.org/10.2307/41410412
[58] Venkatesh, V., Thong, J., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. Journal of the Association for Information Systems, 17(1), 328–376. https://doi.org/10.17705/1jais.00428
[59] Xia, Y., & Chen, Y. (2024). Driving Factors of Generative AI Adoption in New Product Development Teams from a UTAUT Perspective. International Journal of Human–Computer Interaction, 41, 6067 - 6088. https://doi.org/10.1080/10447318
[60] Zhao, Y., Wamba, S. F., & Kshetri, N. (2021). Digital divide and technology adoption: The role of demographic and socio-economic factors. Journal of Global Information Management, 29(2), 45–62. https://doi.org/10.4018/JGIM.2021040103.