INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 11, (2026) E-ISSN: 2222-6990

Validating the Knowledge, Attitude, and Practice (KAP) Model for Online Scam Prevention: A Confirmatory Factor Analysis among Muslim University Students in Malaysia

Noor Fariza Mohd Hasini, Salbiah Nur Shahrul Azmi, Shahrul Niza Samsudin

Faculty of Business, Hospitality & Technology, Universiti Islam Melaka, Kuala Sungai Baru, 78200 Melaka, Malaysia

Email: fariza@unimel.edu.my, salbiahnur@unimel.edu.my, shahrulniza@unimel.edu.my

Nor Izzuani Izhar

Faculty of Education, Universiti Islam Melaka, Kuala Sungai Baru, 78200 Melaka, Malaysia

Email: izzuani@unimel.edu.my

Nor Ainee Idris

Centre for Language and General Studies, Universiti Islam Melaka, Kuala Sungai Baru, 78200 Melaka, Malaysia

Email: ainee@unimel.edu.my

Azwan Amirulsyafiq Abu Hassan

Royal Malaysia Police, Seberang Perai Tengah, Pulau Pinang, Malaysia

Email: azwanamirulsyafiq@gmail.com

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i11/29350

Published Date: 22 November 2026

Abstract

A total of 107,716 online fraud cases were recorded in Malaysia between 2020 and 2023, with losses exceeding RM 3.2 billion. This record necessitates a framework to combat how vulnerabilities function cognitively, attitudinally, and behaviourally. This study validates a measurement model for preventing online fraud based on the Knowledge, Attitude, and Practice (KAP) framework interpreted through the lens of Maqasid al-Shariah. The data were collected from 182 students at Universiti Islam Melaka (UNIMEL) via a cross-sectional survey. Confirmatory Factor Analysis (SPSS AMOS 26) assessed individual constructs, model fit, convergent validity, and discriminant validity. The final instrument retained 17 items across four constructs (Knowledge, Attitude, Practice, and Online Scam). Reliability was strong (α = 0.783–0.905). Convergent validity held (AVE = 0.592–0.673; CR = 0.808–0.911). Discriminant

validity met the Fornell-Larcker criterion. Model fit was acceptable (CMIN/DF = 2.531, RMSEA = .092, CFI = .919). This study contributes the first empirically validated KAP measurement model for online scam prevention in the Malaysian context, providing a psychometrically sound instrument for future structural equation modelling and enriching Islamic scholarly discourse on digital ethics and cybercrime prevention.
Keywords: Confirmatory Factor Analysis, Knowledge, Attitude, Practice, Online Scam

Introduction

Conferring to Cybersecurity Malaysia (2023), the MyCERT Cyber999 platform documented that online scam accounted for 3,087 out of 4,898 cybercrime cases, representing the single largest category of cybercrime in the country. This trajectory is further underscored by the National Security Council (NSC, 2024), which documented 107,716 online scam cases between 2020 and 2023, resulting in financial losses amounting to RM 3.2 billion. Moreover, more than 7,600 cyber incidents were recorded in 2025, including 5,751 scam cases (CyberSecurity Malaysia, 2026). Despite sustained intervention by Polis Diraja Malaysia (PDRM) and relevant authorities through public awareness campaigns, legislative measures, and educational programmes, the incidence of online scams remains to intensify.

From the perspective of Maqasid al-Shariah, the five fundamental objectives of Islamic law as articulated by Imam Al-Ghazali and later developed by Ibn Ashur, this crisis directly threatens Hifz al-Mal (protection of wealth) and Hifz al-Nafs (protection of life and dignity), both of which are considered inviolable in Islamic law. Despite increasing scholarly attention to the issues of online scams, existing literature reveals a fragmented understanding of the psychological, behavioural, and social dimensions of online scam susceptibility, particularly within the Malaysian context (Dinya Solihati et al., 2023; Abdul Wahab, Pitchan & Salman, 2023; Aoun et al., 2026). Prevailing response strategies; encompassing both technological safeguards and user education programmes have demonstrated limited efficacy in preventing victimisation (Koibichuk et al., 2021; Alias et al., 2022; Parti et al., 2026). This gap is particularly pronounced among university students, a demographic characterised by high digital platform engagement and consequently elevated exposure to online scam risks (Tade & Aliyu, 2011; Whitty, 2019; Yen et al., 2025).

From an Islamic perspective, Islam places the acquisition and application of knowledge (Ilm) at the centre of individual and collective responsibility. The Quran clearly commands the pursuit of knowledge in Surah Al-Alaq (96:1-5), and Islamic scholars have long emphasised that knowledge must be harnessed for the protection and betterment of society; a principle directly relevant to equipping Muslims with the awareness and skills to resist online scam.

The motivation for undertaking this study stems from academic, theoretical, and practical considerations. From an academic perspective, understanding of the psychological, behavioural, and social factors that contribute to vulnerability to online scams remains limited, particularly among Muslim university students in Malaysia, who are highly engaged with digital platforms. From a theoretical perspective, although the Knowledge, Attitude, and Practice (KAP) model provides a framework for understanding the relationships among knowledge, attitudes, and protective practices, its suitability as a measurement model for online scam prevention among Muslim university students in Malaysia requires empirical validation. Furthermore, the conceptual alignment between the KAP model and Islamic

principles, which emphasise knowledge, intention, and action, provides a theoretical rationale for examining the applicability of this model to this population. From a practical perspective, the increasing number of online scam cases despite various awareness and protective initiatives indicates the need for more evidence-based preventive approaches. Establishing the validity and reliability of a KAP instrument is essential for systematically measuring levels of knowledge, attitudes, and protective practices, thereby helping to identify areas requiring improvement in education and preventive interventions. Accordingly, this study seeks to validate the KAP measurement model for online scam prevention among Muslim university students in Malaysia, thereby establishing a robust measurement foundation for future research and the development of prevention strategies.

In addressing these gaps, this study adopts the Knowledge, Attitude, and Practice (KAP) model as its primary theoretical framework. The KAP model, originally developed in the field of public health (Launiala, 2009), posits that an individual's level of knowledge about a phenomenon shapes their attitudinal disposition towards it. The KAP model provides a framework for understanding how awareness of online scam influences cautious digital attitudes, which translate into protective online behaviours. Importantly, the model resonates strongly with Islamic pedagogical principles. Knowledge is the foundation of righteous action, and the cultivation of correct attitudes is considered inseparable from virtuous practice. The equivalent between the KAP model and the Islamic triad of knowledge, intention, and action renders this framework particularly appropriate for studying online scam prevention within a Muslim-majority population.

No prior empirical study has rigorously validated the psychometric properties of a KAP-based measurement model for online scam prevention among Malaysian Muslim university students. The absence of a validated instrument represents a critical methodological gap, as sound structural analysis requires a well-specified and validated measurement model (Hair et al., 2010). Specifically, this study pursues these objectives: (i) to examine the factor structure and psychometric properties of the Knowledge, Attitude, and Practice constructs in relation to online scam prevention; (ii) to assess the convergent and discriminant validity of the KAP measurement model; and (iii) to evaluate the overall goodness-of-fit of the CFA measurement model for online scam prevention among Malaysian Muslim university students. By achieving these objectives, this study contributes a validated, theoretically and Islamically grounded measurement instrument as the foundation for subsequent structural analysis and informed evidence-based, value-aligned strategies for online scam prevention in Malaysia.

Literature Review

Online Scam Crimes in Malaysia

Online scams, also defined as deceitful schemes committed through digital channels (Abdul Karim & Lyndon, 2023). National Security Council (NSC, 2024) documented a total of 107,716 online scam cases between 2020 and 2023, resulting in financial losses amounting to RM 3.2 billion. The losses recorded are increasing with total losses reaching RM 1.73 billion in 2022 alone, and a further 29% increase recorded between January and September 2023 (NSC, 2024). The increasing trend of online scam cases in Malaysia is increasingly worrying when 47,854 cases were recorded as of September 2025 (Bernama, 2025).

Online scams in Malaysia exhibit various methods, involving online shopping scams, fake loan offers, investment deception, romantic scams, job vacancy scams, and impersonation

schemes (PDRM Melaka, 2024). These tactics necessitate continuous education and proactive engagement from all sectors of society (Bashir et al., 2022). Despite the organisation of 3,689 crime prevention programmes by the PDRM through the Commercial Crime Investigation Department (CCID) between January and May 2023 alone (CCID Bukit Aman, 2023), victimization rates remain high.

Characterised by high levels of digital platform engagement, university students are disproportionately exposed to online scam risks (Tade & Aliyu, 2011; Whitty, 2019; Jusoh & Nizar, 2022; Yen et al., 2025). In Malaysia, the increasing adoption of digital banking, e-commerce, and social media among youth populations amplifies this vulnerability, underscoring the need for targeted research into online scam prevention (MCMC, 2023).

From the views of Maqasid al-Shariah; the five essential objectives of Islamic law, online scams directly threaten Hifz al-Mal (protection of wealth) and Hifz al-Nafs (protection of dignity and wellbeing), both of which are considered unbreakable (Al-Ghazali, 1993; Ibn Ashur, 2006). Battling online scams consequently creates a joint obligation (Fardu Kifayah) within the Muslim community, and scholarly review into effective prevention strategies represents an input to Maslahah (public interest), a cornerstone of Islamic jurisprudence (Al-Shatibi, 2006).

The Knowledge, Attitude, and Practice (KAP) Model

The Knowledge, Attitude, and Practice (KAP) model is a theoretical framework for understanding the behavioural factors of health, social, and security-related phenomena. This KAP model posits that knowledge about a phenomenon shapes an individual's attitudinal disposition toward it, influencing their resultant behavioural practices. This sequential, tripartite relationship; wherein knowledge informs attitude, and attitude drives practice renders the KAP model particularly appropriate for examining online scam prevention behaviours, as it captures both the cognitive and volitional dimensions of protective behaviour (Bennett, 1976; Launiala, 2009; Pitchan et al., 2022). The model has been successfully applied across diverse domains including public health (Launiala, 2009), environmental behaviour (Ramayah et al., 2012), and most recently, cybersecurity contexts (Abdul Wahab et al., 2023), reflecting its versatility as an explanatory framework.

Knowledge and Online Scam Prevention

Knowledge establishes the initial dimension of the KAP model. Past studies constantly determine that those with better knowledge on cybercrime are well equipped to identify, evade, and retort to online scam intimidations (Patil & Arra, 2022). This shielding knowledge includes comprehending of common types of scams, recognition of deceitful indicators, and alertness of suitable precautionary actions (Althibyani & Al-Zahrani, 2023; Dinya Solihati et al., 2023). Kimpe et al. (2022) demonstrated that individuals who perceive themselves as well-informed are less likely to feel vulnerable to cybercrime and more likely to adopt effective security measures. Abdul Wahab et al. (2023) further established a direct correlation between public knowledge levels and online scam prevalence.

Attitude and Online Scam Prevention

The attitude dimension of the KAP model captures the attitudinal temperaments that arbitrate between knowledge and behaviour. In cybersecurity, attitudes toward online safety include readiness to take security practices, recognition of the importance of cybersecurity measures, and cautious temperament toward online communications (Hagger et al., 2020; Aoun et al., 2026). Online users' awareness of threats and the apparent practicality of cyber consciousness influence their readiness to occupy in protecting behaviours (Qahri-Saremi & Turel, 2023; Wang, 2026). Social media settings encourage imprudent engagement, flagging watchful attitudes to mistrustful content (Frauenstein et al., 2023). Abdul Wahab et al. (2023) stated insights of crime prevention campaigns and emotive retorts to awareness initiatives. Optimistic attitudes toward awareness programs associate with enhanced personal cybersecurity practices. Conversely, community contentment contributes to increased online scams. Therefore, the Islamic principle of Ihtiyat advocates for a preventive method, bring into line with these attitudinal dimensions.

Practice and Online Scam Prevention

The practice dimension of the KAP model represents the behavioural indicator of knowledge and attitude, encircling the concrete actions individuals take to protect themselves from online scam threats. Nadry et al. (2025) conceptualise these secure online practices as the behavioural dimension of cybersecurity awareness, reflecting how individuals apply their knowledge and attitudes in real-world digital interactions. Effective cybersecurity practices include the use of security software, organization of strong passwords, avoidance of suspicious links, and cautious conduct of unsought communications (Uthoff, 2022).

However, Nadry et al. (2025) further indicate that although individuals may determine moderate to high levels of cybersecurity knowledge and positive attitudes, their actual online practices often remain inconsistent, particularly in detecting and responding to phishing attempts. This gap underscores the need for innovative approaches to foster protective practices, as explored in recent literature. Empirical studies consistently demonstrate that individuals who implement these practices are significantly better protected against online victimisation (Mahmud & Siarap, 2013; Parti et al., 2026).

Innovative approaches to fostering protective practices have been explored in recent literature. Priya and Ranganathan (2022) propose interactive learning platforms, including simulation-based card games, as effective tools for cultivating cybersecurity awareness and practice. Tache et al. (2021) emphasise the role of specialised training and certified auditors in high-risk financial sectors. Abdul Wahab et al. (2023) further demonstrate that individuals who participate in awareness campaigns are more likely to adopt cautious behaviours, share protective knowledge with their networks, and maintain vigilance against scam attempts fostering a culture of collective responsibility and resilience. In the present study, the practice construct is operationalised through four retained items measuring knowledge-driven protective action, advocacy for public dissemination of prevention information, avoidance of suspicious links, and reporting behaviour to authorities; reflecting both individual protective practices and communal responsibility dimensions.

The practice of defending oneself and the community from harm in Islamic perspective is not simply discretionary nevertheless compulsory under the principle of La Darar wa La Dirar (no harm shall be inflicted or reciprocated), one of the five basic maxims of Islamic law (Al-Suyuti,

2013). This principle establishes a direct religious foundation for the adoption of practical protective measures against online scams, reinforcing the practice dimension of the KAP model from an Islamic ethical perspective.

Measurement Validation in KAP Research - Justification for CFA

A serious yet often disregarded dimension of KAP-based research is the rigorous validation of the measurement instruments used to operationalise knowledge, attitude, and practice constructs. Without a psychometrically validated measurement model, structural relationships between KAP dimensions cannot be meaningfully or reliably estimated (Hair et al., 2010). Confirmatory Factor Analysis (CFA) within the Structural Equation Modeling (SEM) framework represents the gold standard approach for measurement model validation, enabling the systematic assessment of construct validity through the evaluation of factor loadings, Average Variance Extracted (AVE), Composite Reliability (CR), and both convergent and discriminant validity (Fornell & Larcker, 1981; Byrne, 2010). Existing studies have largely relied on adapted instruments from related cybersecurity and public health fields without subjecting them to rigorous CFA-based validation (Dinya Solihati et al., 2023; Abdul Wahab et al., 2023). This gap represents a significant methodological limitation, as construct validity is a fundamental prerequisite for the credibility and generalisability of research findings (Nunnally & Bernstein, 1994). The present study directly addresses this gap by conducting a comprehensive CFA to validate the KAP measurement model for online scam prevention, thereby contributing a psychometrically sound and theoretically grounded instrument for future research in this domain.

Conceptual Framework

Drawing upon the KAP model, Launiala, (2009) and its alignment with Islamic principles of knowledge, attitude, and practice, the conceptual framework of this study suggests that knowledge, attitude, and practice constitute three distinct yet interrelated latent constructs that collectively operationalise individual readiness to prevent online scam victimisation. The online scam construct serves as the dependent variable, capturing respondents' perceptions of online scam risk and impact. The theoretical relationships among these constructs are grounded in the KAP model's sequential logic wherein knowledge acquisition shapes attitudinal orientation, which in turn manifests in protective behavioural practices as well as in the Islamic pedagogical triad of Ilm (knowledge), Niyyah (intention/attitude), and Amal (action/practice). This framework serves as the foundation for the CFA measurement model validated in the present study, and subsequently for the Structural Equation Model to be tested in future research.

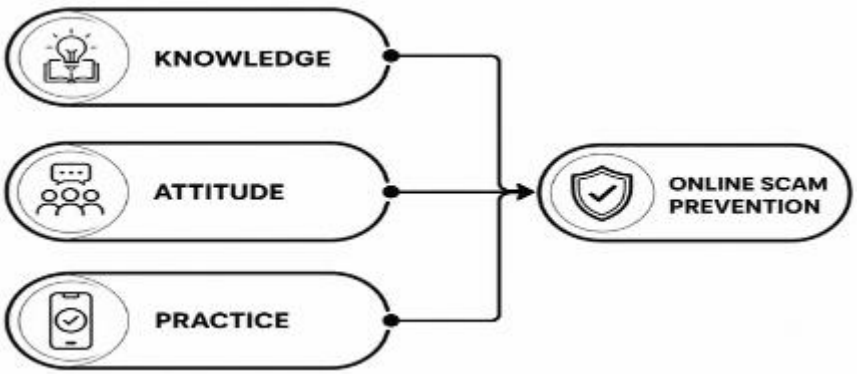

Figure 1 Conceptual Framework for Online Scam Prevention
Source: Author's compilation (2026)

Methodology

Research Design

This study employs a quantitative research design rooted in the positivist tradition to measure and validate phenomena via systematic empirical observation. It uses a cross-sectional survey design to gather data at a single point from a representative sample, favouring its efficiency and replicability for CFA. Grounded in the KAP theoretical framework, data analysis is conducted using IBM SPSS AMOS version 26 for CFA.

Population and Sampling

The target population includes 2,487 undergraduate and postgraduate students at Universiti Islam Melaka (UNIMEL), noted for high digital engagement and online scam exposure. Being an Islamic institution, UNIMEL provides a relevant context for studying online scam prevention through Islamic ethical lenses. The university's students are crucial for societal and policy discussions on digital citizenship. A purposive sampling strategy selected students actively using digital platforms for an exploratory quantitative study, with data collected via self-administered online questionnaires in July 2025.

Sample Size Justification

A sample of 182 valid responses was analyzed, deemed adequate based on various benchmarks for Structural Equation Modeling (SEM) studies. While Krejcie and Morgan (1970) suggest a sample of 346 for a population of 3,500, their formula is not suitable for SEM. Hair et al. (2010) recommend a minimum sample size of 100 to 200 respondents, which the current sample meets comfortably. Additionally, the respondent-to-parameter ratio is approximately 10.7:1 with 17 variables, exceeding the recommended ratios of 5:1 and 10:1. Comrey and Lee's (1992) scale rates a sample of 182 as approaching the fair-to-good threshold. These justifications confirm the adequacy of the sample for CFA based on established guidelines.

Research Instrument

Data were collected through a structured, self-administered questionnaire in Malay language to improve comprehension among Malaysian university students. The questionnaire had two sections: demographic information and measurement items related to KAP and Online Scam. Measurement items were based on extensive literature reviews, and a five-point Likert scale was used. The initial instrument included 19 items, but after CFA, two items were removed, resulting in a validated instrument of 17 items. Content validity was ensured through expert reviews, and a pilot study with a Cronbach's Alpha of 0.936 confirmed reliability before the main data collection.

Data Collection and Data Analysis Procedure

Main data collection took place in July 2025 at an Online Scam seminar at UNIMEL, with prior ethical clearance obtained. Participants were informed about the study's purpose and confidentiality through an online consent statement, ensuring no personally identifiable information was collected. Questionnaires, distributed via Google Forms through university channels and WhatsApp, yielded 182 valid responses. Responses with over 10% missing data or random answering patterns were excluded before analysis. Data were analysed in two

stages using IBM SPSS version 26 and IBM SPSS AMOS version 26. Preliminary analyses included descriptive statistics and reliability assessments in SPSS, followed by confirmatory factor analysis in AMOS, adhering to the two-step approach as per established guidelines.

Pilot Testing

A pilot study was conducted with 30 respondents drawn from the same target population at UNIMEL prior to the main data collection. The pilot study served two purposes. First, to assess the clarity and comprehensibility of questionnaire items among the target population. Second, to evaluate the preliminary internal consistency of the measurement instrument. Based on pilot feedback, minor linguistic adjustments were made to two items to improve clarity. The overall Cronbach Alpha of 0.936 obtained from the pilot study confirmed strong internal consistency of the instrument and the questionnaire was deemed ready for main data collection (Nunnally & Bernstein, 1994).

Measurement Items and Constructs

Table 1

Measurement Items and Constructs

Construct	Item	Item Description
Knowledge	K1	I have knowledge regarding online scam crime.
	K2	I am aware of the modus operandi of online scam crime.
	K3	I know how to identify online scam crime.
	K4	I am aware of the dangers of online scam crime.
	K5	I know methods to protect personal information from online scam crime.
Attitude	A1	I read privacy policies and terms before using online services.
	A2	I seek references before using online services to avoid scams.
	A3	I am confident in the privacy security of links I browse.
	A4	I am careful using online services due to awareness of scam dangers.
	A5	I am confident using online services due to existing cyber laws.
Practice	P1	I know methods to overcome online scams with my knowledge.
	P2	I agree prevention information should be widely disseminated.
	P4	I will report to authorities if I become a scam victim.
	P5	I will report to authorities if I become a scam victim.
Online Scam	OS1	Online scam risk increases with frequency of internet use.
	OS2	Online scam risk increases with frequency of social media use.
	OS4	Online scams have negative effects on individuals, families, and society.

Note: Items P3 and OS3 were removed following CFA re-specification. P3: "I use applications to detect unknown numbers" was deleted due to a factor loading of 0.494 (< 0.50). OS3: "Individuals are at risk if they lack exposure to online scam information" was deleted due to construct heterogeneity and inadequate loading following model re-specification.

Results and Discussions

This study utilizes the KAP model aligned with Islamic principles to suggest that knowledge, attitude, and practice are interrelated constructs that enhance individual preparedness against online scams. The dependent variable, online scam, reflects respondents' views on scam risks and effects. The framework is based on the sequential logic of the KAP model, where knowledge influences attitude and subsequently leads to protective actions, and the Islamic triad of Ilm (knowledge), Niyyah (intention/attitude), and Amal (action). This serves as the basis for the CFA measurement model used in the study.

Prior to CFA analysis, the internal consistency of all four constructs was assessed using Cronbach Alpha coefficients. As presented in Table 2, the knowledge construct demonstrated excellent reliability (α = 0.905). Attitude followed closely (α = 0.888), then practice (α = 0.866) both reflecting good internal consistency. The online scam construct yielded an acceptable reliability coefficient (α = 0.783). All values exceeded the minimum threshold of 0.70 recommended by Nunnally and Bernstein (1994), confirming adequate internal consistency across all constructs prior to CFA validation. The overall instrument reliability of α = 0.936, obtained during the pilot study, further corroborates the strong internal consistency of the measurement instrument as a whole.

CFA Diagram

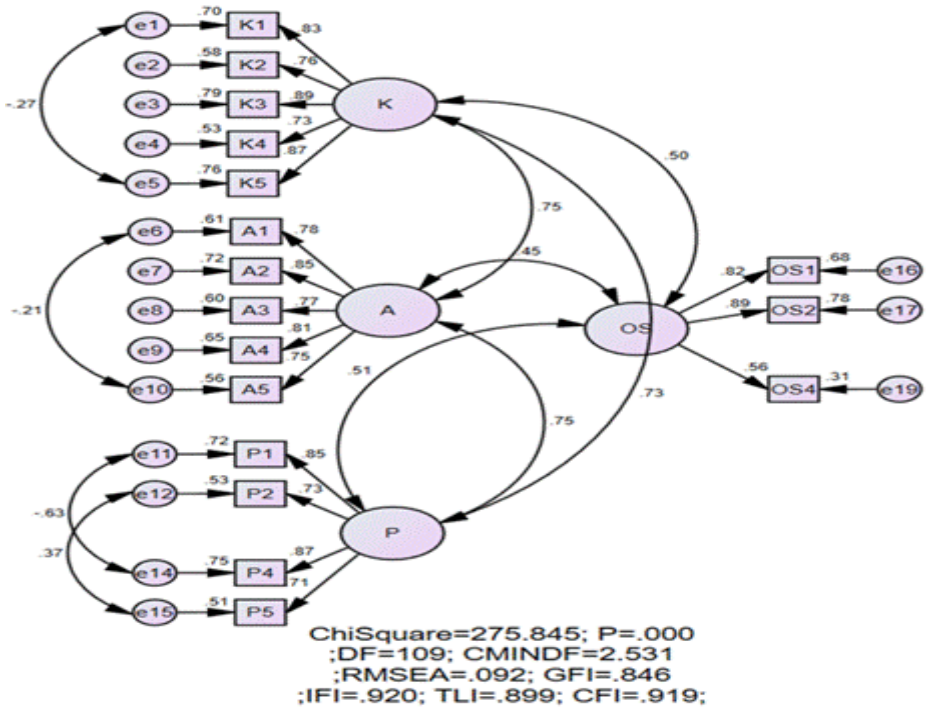

Diagram 1 CFA Model for Online Scam

Table 2
Results of Confirmatory Factor Analysis: Factor Loadings, Reliability and Validity

Construct	Item	Standardized Loading (λ)	Cronbach α	AVE	CR
Knowledge	K1	0.835	0.905	0.673	0.911
	K2	0.763			
	K3	0.892			
	K4	0.728			

	K5	0.872			
Attitude	A1	0.779	0.888	0.627	0.893
	A2	0.851			
	A3	0.772			
	A4	0.806			
	A5	0.747			
Practice	P1	0.851	0.866	0.627	0.870
	P2	0.728			
	P4	0.866			
	P5	0.711			
Online Scam	OS1	0.822	0.783	0.592	0.808
	OS2	0.886			
	OS4	0.560			

Note: All standardized factor loadings exceed the minimum threshold of 0.50 (Hair et al., 2010). All AVE values exceed 0.50 (Fornell & Larcker, 1981). All CR values exceed 0.70 (Hair et al., 2010). All Cronbach Alpha values exceed 0.70 (Nunnally & Bernstein, 1994).

Table 3
Model Fit Indices Summary

Construct / Model	**CMIN**	**P**	**DF**	**CMIN/DF**	**RMSEA**	**GFI**	**IFI**	**TLI**	**CFI**
Knowledge	6.981	.222	5	1.396	.047	.986	.997	.993	.997
Attitude	6.605	.252	5	1.321	.042	.987	.997	.993	.997
Practice	0.684	.710	2	0.342	.000	.998	1.004	1.012	1.000
Online Scam	.000	-	0	Just-ID	-	1.000	1.000	-	-
Overall Model	275.845	.000	109	2.531	.092	.846	.920	.899	.919

Table 4
Discriminant Validity Matrix

Construct	**Knowledge**	**Attitude**	**Practice**	**Online Scam**
Knowledge	0.820			

Attitude	.750	0.792		
Practice	.731	.754	0.792	
Online Scam	.502	.449	.512	0.769

Knowledge Construct

The knowledge construct demonstrated the strongest psychometric properties among the four latent variables in the measurement model. Excellent internal consistency (α = 0.905). Strong convergent validity (AVE = 0.673, CR = 0.911). Individual construct model fit indices substantially exceeded all recommended thresholds (CMIN/DF = 1.396, RMSEA = .047, CFI = .997). All five indicators (K1–K5) returned standardised factor loadings ranging from 0.728 to 0.892, confirming the unidimensional and reliability of the Knowledge construct as operationalised in this study.

Among the five knowledge items, K3, which assessed respondents' ability to identify online scam crimes emerged as the strongest indicator (λ = 0.892). K5 followed, measuring knowledge of personal information protection methods (λ = 0.872). Practical knowledge, particularly the ability to recognize and protect against online scams, is crucial among Malaysian university students, supporting findings by Althibyani and Al-Zahrani (2023) and others that digital skills reduce victimization. The study emphasizes operational knowledge over declarative knowledge, impacting online scam prevention education. The robust knowledge construct aligns with the KAP model, highlighting its significance in shaping protective behavior against cybercrime. Additionally, from an Islamic perspective, the findings resonate with the imperative to seek knowledge (Ilm), as outlined in Surah Al-Alaq. Knowledge of scam prevention among Muslim students at UNIMEL reflects an application-focused approach, reinforcing Islamic principles relevant to digital ethics and cybercrime prevention.

Attitude Construct

The attitude construct demonstrated strong psychometric properties. Good internal consistency (α = 0.888). Satisfactory convergent validity (AVE = 0.627, CR = 0.893). Excellent individual construct fit (CMIN/DF = 1.321, RMSEA = .042, CFI = .997). All five attitude items (A1–A5) returned standardised factor loadings ranging from 0.747 to 0.851 and all exceeding the minimum threshold of 0.50 (Hair et al., 2010).

The attitude construct, particularly dimension A2, highlights the inclination among UNIMEL students to verify information before utilizing online services to mitigate scam risks, achieving a high indicator value (λ = 0.851). This is supported by dimension A4, which captures cautious online behavior due to scam awareness (λ = 0.806). These findings indicate that verification and awareness-driven caution are significant attitudinal dimensions reflecting intentional information-seeking behavior before digital engagement. This aligns with the cognitive-rational model suggested by Hagger et al. (2020) and Wang (2026), which states that rational processing of risk information leads to vigilant and self-protective attitudes.

Abdul Wahab et al. (2023) similarly found that proactive verification and vigilance are linked to reduced susceptibility to online scams in Malaysia. Additionally, dimension A5 (λ = 0.747)

reflects respondents' confidence in using online services, bolstered by Malaysian cyber laws, though its lower value suggests that legal confidence is a secondary factor in shaping online safety attitudes among students. This could indicate a gap in public awareness regarding Malaysian cybercrime legislation, such as the Computer Crimes Act 1997 and the Communications and Multimedia Act 1998, which policymakers should address.

From an Islamic ethical perspective, the attitudes observed correspond with the concept of Niyyah (intention/attitude), emphasizing that the moral worth of actions ties to the underlying intent. Islamic principles like Ihtiyat (precaution) and Sadd al-Dhara'i (blocking harmful means) advocate for a cautious approach in potentially harmful interactions, mirroring the findings regarding verification and caution. The robust indicators A2 and A4 reinforce this connection, positioning online scam prevention behaviors within an Islamic ethical framework.

Practice Construct

The practice construct demonstrated good internal consistency (α = 0.866), satisfactory convergent validity (AVE = 0.627, CR = 0.870), and excellent individual construct fit following the removal of item P3 (CMIN/DF = 0.342, RMSEA = .000, CFI = 1.000). The four retained items (P1, P2, P4, P5) returned standardised factor loadings ranging from 0.711 to 0.866. The strongest practice indicator was P4, measuring respondents' avoidance of suspicious links, yielding a loading of 0.866. Next, P1, which assessed knowledge-driven protective action (λ = 0.851). These findings reveal that UNIMEL students prioritize avoidance of suspicious digital content and employ personal knowledge as key protective practices, consistent with previous studies on effective cybersecurity behaviours.

P3, which assessed the use of detection applications for unknown phone numbers, was excluded from further analysis due to its inadequate statistical loadings and conceptual divergence from broader knowledge-driven practices. Items P2 and P5 showed acceptable loadings, highlighting the importance of public awareness and willingness to report scams, although less central than individual avoidance behaviours. From an Islamic perspective, these practices align with the KAP model's practice dimension, emphasizing Amal (righteous action) and the obligation to avoid harm, supported by principles such as La Darar wa La Dirar and Fardu Kifayah, which advocate for individual and communal protective actions.

Online Scam Construct

The online scam construct serving as the dependent variable in the KAP measurement model; demonstrated acceptable internal consistency (α = 0.783), satisfactory convergent validity (AVE = 0.592, CR = 0.808), and a just-identified individual construct model (df = 0). This is an expected and acceptable outcome for a three-indicator single-factor CFA model (Hair et al., 2010; Byrne, 2010). The three retained items (OS1, OS2, OS4) yielded standardised factor loadings of 0.822, 0.886, and 0.560 respectively.

The online scam construct underwent extensive re-specification, revealing a dimensionality in perceived risk among Malaysian university students. Initial models failed due to the OS3 item, which highlighted an awareness-based risk dimension distinct from frequency-based perceptions of scams. This insight suggests that future research should treat awareness-based

vulnerability separately. The strongest indicator, OS2, shows that students perceive increased scam risks with higher social media usage, emphasized by findings from the Malaysian Communications and Multimedia Commission (MCMC, 2023) regarding the predominance of social media as a scam channel. Targeted prevention messaging should therefore prioritize social media platforms.

OS4 (λ = 0.560) capturing perceptions of the negative societal impact of online scams on individuals, families, communities, and the nation; demonstrated the weakest loading within the construct. While acceptable, its relatively lower value suggests that the macro-level societal impact dimension is somewhat less psychometrically central to respondents' conceptualisation of online scam risk compared to the direct usage-frequency risk items. This may reflect a tendency among young adults to conceptualise online scam risk in personal rather than collective terms, a finding consistent with the individualised risk perception literature (Whitty, 2019; Taqbira & Susilo, 2026).

From an Islamic standpoint, online scams threaten Hifz al-Mal (protection of wealth) and Hifz al-Nafs (protection of dignity), key objectives of Maqasid al-Shariah. The damage inflicted by these scams not only impacts individual victims but also harms the broader community, aligning with the concept of Maslahah Ammah (public interest). The findings suggest that enhancing awareness of the community-level repercussions of online scams within an Islamic social responsibility framework is crucial for future educational efforts in Islamic higher education.

Convergent and Discriminant Validity

Convergent validity was confirmed across all four constructs, with AVE values between 0.592 (Online Scam) and 0.673 (Knowledge), and CR values from 0.808 (Online Scam) to 0.911 (Knowledge). The Knowledge construct showed stronger inter-construct correlations with Attitude (r = .750) and Practice (r = .731) than Online Scam did with any KAP constructs (r = .449 to .512). This supports the KAP model's logic that knowledge drives change in attitudes and behaviors, while online scam risk perceptions are distal outcomes. Moderate correlations (r .449 to .512) indicate that knowledge, attitudes, and practices are linked to online scam risk perception, suggesting other variables like prior victimization or social influence may need to be considered in future models.

Conclusions and Recommendations

This study contributes several significant theoretical contributions to the literature on online scam prevention and KAP-based research. First, it offers the first analytically validated CFA measurement model of the KAP construct specifically developed for the online scam prevention context in Malaysia: to address a critical methodological gap identified in the literature (Dinya Solihati et al., 2023; Abdul Wahab et al., 2023). The validated instrument offers a psychometrically sound and theoretically grounded tool for future research, enabling more rigorous structural analysis of the relationships among knowledge, attitude, practice, and online scam risk perception.

Second, this study demonstrates the empirical viability of the KAP model in the cybersecurity domain, extending its established applications in public health and environmental behaviour

research (Launiala, 2009; Ramayah et al., 2012) to the emerging field of online scam prevention. The satisfactory convergent and discriminant validity of all four constructs confirms that KAP dimensions are not only theoretically meaningful but empirically distinguishable in the online scam context—providing a solid foundation for subsequent structural hypothesis testing. Third, this study contributes to Islamic academic scholarship by demonstrating the conceptual and empirical alignment between the KAP framework and Islamic principles of Ilm (knowledge), Niyyah (intention), and Amal (action). By situating KAP-based online scam prevention research within the framework of Maqasid al-Shariah, this study opens a new interdisciplinary dialogue between cybersecurity research and Islamic ethics thus, contributing to the growing body of Islamic scholarship on digital governance and cyber ethics.

In brief, this study set out to validate the measurement model of the KAP construct for online scam prevention among undergraduate and postgraduate students at UNIMEL using CFA. Motivated by the alarming escalation of online scam cases in Malaysia with 107,716 cases between 2020 and 2023 resulting in losses of RM 3.2 billion (NSC, 2024), and the latest cases in 2025; and the critical absence of a psychometrically validated KAP-based measurement instrument in the Malaysian cybersecurity literature, this study addressed a significant methodological and theoretical gap with both scholarly and societal urgency.

Building on the study's findings and limitations, several future research directions are recommended such as cross-cultural, and cross-national CFA studies comparing the KAP measurement model across various Muslim-majority countries like Indonesia, Brunei, and Saudi Arabia which would provide valuable insights into the universality versus cultural specificity of the KAP construct in online scam prevention, thereby enriching both cybersecurity and Islamic scholarly literature.

References

Abdul Karim, M. Y., & Lyndon, N. (2023). Pandangan dunia pengguna perniagaan dalam talian tentang jenayah siber. Malaysian Journal of Social Sciences and Humanities (MJSSH), 8(7), e002392. https://doi.org/10.47405/mjssh.v8i7.2392

Abdul Wahab, E., Pitchan, M. A., & Salman, A. (2023). Pengetahuan, sikap dan amalan masyarakat di Kuala Lumpur terhadap kempen pencegahan jenayah penipuan dalam talian. Jurnal Komunikasi: Malaysian Journal of Communication, 39(1), 240–258. https://doi.org/10.17576/JKMJC-2023-3901-14

Afthanorhan, A., Awang, Z., Salleh, F., Ghazali, P. L., & Rashid, N. (2018). The effect of product quality, medical price and staff skills on patient loyalty via cultural impact in medical tourism. Management Science Letters, 8 (12), 1421-1428. https://doi.org/10.5267/j.msl.2018.10.004

Alias, N. S., Mahamood, A. F., Tengku Yakob, T. K., Ramli, A. J., Affandy, H. B., & Abdul Manaf, A. R. (2022). Fenomena phishing di Malaysia: Persepsi masyarakat, kesan dan kaedah mengatasi. Journal of Global Business and Social Entrepreneurship (GBSE), 8(24), 132–158. https://www.researchgate.net/publication/361205162

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, 11512. https://doi.org/10.3390/su151511512

Anderson, J.C., & Gerbing, D.W. (1988). Structural equation modelling in practice: A review and recommended two-step approach. Psychological Bulletin, 103(3), 411–423.https://doi.org/10.1037/0033-2909.103.3.411

Aoun, D., Rahal, R., Sfeir, L., & Al Maalouf, N. J. (2026). Understanding millennials' financial behavior: the role of fintech adoption, financial literacy, and the mediating effect of financial attitudes in a crisis-affected emerging economy. International Journal of Financial Studies, 14(35), 1–19. https://doi.org/https://doi.org/10.3390/ijfs14020035

Al-Alaq, 96:1-5

Al-Bukhari, M. I. (n.d.). Sahih al-Bukhari, Hadith 33 [English translation]. Sunnah.com. https://sunnah.com/bukhari:33

Al-Ghazali, Abu Hamid, Al-Mustafa min Ilm al-Usul. Beirut: Dar al-Kutub al-Ilmiyyah, 1993.

Al-Shatibi, I. (2006). Al-Muwafaqat fi Usul al-Shariah. Dar Ibn Affan.

Al-Suyuti, J. (2013). Al-Ashbah wa al-Nazair. Dar al-Kutub al-Ilmiyyah.

Bada, M., Sasse, A.M., & Nurse, J.R.C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society, 1, 118–131.

Bashir, A., Azwardi, A., Soebyakto, B. B., Atiyatna, D. P., Hamidi, I., Hamira, H., & Dwi, R. S. (2022). Raising awareness and knowledge of rural communities against lottery fraud and illegal online loans through telephone and short message services. Sricommerce: Journal of Sriwijaya Community Services, 3(2), 89–96. https://doi.org/10.29259/jscs.v3i2.83

Bennett, C. F. (1976). Analyzing impacts of extension programs. U.S. Department of Agriculture, Extension Service.

Berita RTM. (2024). 107,716 kes penipuan dalam talian dikesan dari 2020 hingga 2023. https://berita.rtm.gov.my/nasional/senarai-berita-nasional/senarai-artikel/107-716-kes-penipuan-dalam-talian-dikesan-dari-2020-hingga-2023

Bernama. (2025). Kes penipuan dalam talian meningkat, kerugian cecah RM1.9 bilion setakat September 2025. Bernama. https://www.bernama.com/bm/news.php?id=2479506

Byrne, B.M. (2010). Structural equation modelling with AMOS: Basic concepts, applications, and programming (2nd ed.). Routledge.

CCID Bukit Aman. (2023). Crime prevention programme statistics January–May 2023. Royal Malaysia Police.

Comrey, A.L., & Lee, H.B. (1992). A first course in factor analysis (2nd ed.). Lawrence Erlbaum Associates.

Creswell, J.W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative and mixed methods approaches (4th ed.). SAGE Publications.

CyberSecurity Malaysia. (2023). Mid-Year Report Threat Landscape 2023. https://www.cybersecurity.my/data/content_files/26/2511.pdf

CyberSecurity Malaysia. (2026). Reported incidents based on general incident classification statistics 2025. CyberSecurity Malaysia. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=4b9c0f37-f1d9-49e7-8c58-80e06499ce52

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour &

Information Technology, 41(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066

Dinya Solihati, K., Rizki, M., & Sari, N. (2023). The role of the government to improve financial literacy in efforts to prevent the use of illegal online loans. In The 4th International Conference on Governance, Public Administration, and Social Science (pp. 670–687). https://doi.org/10.18502/kss.v8i11.13581

Dusuki, A. W., & Abdullah, N. I. (2007). Maqasid al-Shariah, Maslahah, and Corporate Social Responsibility. The American Journal of Islamic Social Sciences, 24 (1), 25-45. http://dx.doi.org/10.35632/ajis.v41i1.3417

Elena, S. T., Amalia, M. D., & Monica, M. D. (2021). The role of the chartered accountant in diminishing the effects of cyber fraud. Journal of Financial Studies, 6(11), 141–155. http://dx.doi.org/10.55654/JFS.2021.6.11.11

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104

Frauenstein, E.D., Flowerday, S., Mishi, S., Warkentin, M., 2023. Unraveling the behavioral influence of social media on phishing susceptibility: a personality-habit-information processing model. Inf. Manag. 60 (7), 1–28. https://doi.org/10.1016/j.im.2023.103858

Hagger, M. S., Cameron, L. D., Hamilton, K., Hankonen, N., & Lintunen, T. (Eds.). (2020). The handbook of behavior change. Cambridge University Press. https://doi.org/10.1017/9781108677318

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

Hu, L., & Bentler, P.M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1–55. https://doi.org/10.1080/10705519909540118

Ibn Ashur, M.T. (2006). Treatise on Maqasid al-Shariah. International Institute of Islamic Thought (IIIT).

Jabatan Perangkaan Malaysia. (2022). Poket Stats Negeri Melaka ST3 2022.

Jusoh, W., & Nizar, W. N. (2022). Online Scams Awareness among Muslim University Students in Malaysia. Journal of Islamic, Social, Economics and Development, 7(43), 50–58. https://doi.org/10.55573/JISED.074305

Koibichuk, V., Ostrovska, N., Kashiyeva, F., & Kwilinski, A. (2021). Innovation technology and cyber frauds risks of neobanks: Gravity model analysis. Marketing and Management of Innovations, 1, 253–265. https://doi.org/10.21272/mmi.2021.1-19

Kosmo. (2024). 34,497 kes ‘scam’ babit lebih RM1.2 bilion kerugian pada 2023. https://www.kosmo.com.my/2024/03/18/34497-kes-scam-babit-lebih-rm1-2-bilion-kerugian-pada-2023/

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610.

Launiala, A. (2009). How much can a KAP survey tell us about people's knowledge, attitudes and practices? Some observations from medical anthropology research on malaria in pregnancy in Malawi. Anthropology Matters, 11(1), 1–13. https://www.anthropologymatters.com

Lawshe, C.H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Mahmud, M. H., & Siarap, K. (2013). Kempen pencegahan H1N1: Kajian tentang pengetahuan, sikap dan amalan penduduk di Timur Laut Pulau Pinang. Jurnal Komunikasi: Malaysian Journal of Communication, 29(1), 127–140. https://journalarticle.ukm.my/6425/

Maina, C. W., Bashokoh, M. I., & Györke, D. K. G. (2026). A bibliometric analysis of digital financial literacy and its role in reducing online financial fraud in the European Union. International Journal of Financial Studies, 14(18), 1–23. https://doi.org/https://doi.org/10.3390/ijfs14010018

Malaysian Communications and Multimedia Commission (MCMC). (2023). Internet Users Survey 2022. https://www.mcmc.gov.my/skmmgovmy/media/General/IUS-2022.pdf

Nadry, Z., Hakimi, M., Sirat, A. W., & Popal, Z. (2025). Strengthening cybersecurity awareness through education: The expanding role of cyber law in academic institutions. Jurnal Analisis Hukum, 8(2), 193–209.https://doi.org/10.38043/jah.v8i2.7086

National Security Council. (2024). Scam atas talian, jenayah utama abad ke-21. https://www.mkn.gov.my/web/ms/2024/01/25/scam-atas-talian-jenayah-utama-abad-ke-21/

Nunnally, J.C., & Bernstein, I.H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

Parti, K., Silis, S., Teaster, P., Rinehart, S., & Dye, C. (2026). "This is not a scam !": Assessment of an awareness raising program tackling older adults' scam victimization in a multi-method study. Qualitative Criminology, 15(1), 1–36. https://dc.swosu.edu/qc/vol15/iss1/1

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

PDRM Melaka. (2024). Statistik jumlah kes dan kerugian jenayah siber Kontinjen Melaka tahun 2023.

PDRM Melaka. (2024). Statistik mangsa jenayah siber mengikut pekerjaan Kontinjen Melaka tahun 2023.

Pitchan, M. A., Baco, M. A., Hassan, F., & Ghazali, A. H. A. (2022). Knowledge, Attitudes, Practices Towards Information Privacy & Security of Online Purchase by Youth. Jurnal Komunikasi: Malaysian Journal of Communication, 38(4), 250–267. https://doi.org/10.17576/JKMJC-2022-3804-14

Priya, P. M., & Ranganathan, A. (2022). Cyber awareness learning imitation environment (CALIE): A card game to provide cyber security awareness for various groups of practitioners. International Journal of Advanced Networking and Applications, 14(2), 5334–5341. https://www.ijana.in/papers/V14I2-3.pdf

Putra, M. C., & Rahayu, P. B. (2025). Correlation analysis of online fraud prevention efforts by the Tokopedia E-Commerce platform usage decisions. 55(2), 239–245.

Qahri-Saremi, H., Turel, O., 2023. Situational contingencies in susceptibility of social media to phishing: a temptation and restraint model. J. Manag. Inf. Syst. 40 (2), 503–540. https://doi.org/10.1080/07421222.2023.2196779

Ramayah, T., Lee, J.W.C., & Mohamad, O. (2010). Green product purchase intention: Some insights from a developing nation. Resources, Conservation and Recycling, 54(12), 1419–1427. https://doi.org/10.1016/j.resconrec.2010.06.007

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93–114.https://doi.org/10.1080/00223980.1975.9915803

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill-building approach (7th ed.). John Wiley & Sons.

Tade, O., & Aliyu, I. (2011). Social organisation of internet fraud among university students in Nigeria. International Journal of Cyber Criminology, 5(2), 860–875. https://www.cybercrimejournal.com/pdf/tadealiyui2011julyijcc.pdf

Taqbira, F., & Susilo, A. (2026). The relationship between financial literacy and risk perception on students' interest in using shoppee paylater in Surakarta City. JHSS (Journal of Humanities and Social Studies), 10(01), 1–7. https://doi.org/https://doi.org/10.33751/jhss.v10i1.137

Uthoff, C. S. (2022). Cyber intelligence: Actors, policies, and practices. Lynne Rienner Publishers.

Wang, F. (2026). A scoping review of online romance scams: Conceptual construction and comparative analysis. International Review of Victimology, 1–29. https://doi.org/10.1177/02697580251414141

Whitty, M.T. (2019). Online fraud victimisation among young adults. Journal of Financial Crime, 26(1), 211–225. https://doi.org/10.1108/JFC-09-2017-0088

Yen, N. T. H., Hanh, B. T., Hung, L. T., & Hang, T. T. T. (2025). The impact of financial technology on financial consumption decisions of university students in Hanoi. HaUI Journal of Science and Technology, 61(11), 115–122. https://doi.org/https://doi.org/10.57001/huih5804.2025.412

Zainuddin Awang. (2015). SEM Made Simple: A Gentle Approach to Learning Structural Equation Modeling (Z. Awang, Ed.). MPWS Rich Publication.