Jurnal Komunikasi: Malaysian Journal of Communication
https://ejournal.ukm.my/mjc
Volume 42(2) 2026: 494-510

Digital Literacy and Scam Susceptibility Among Youth: The Mediating Roles of Risk Awareness and Digital Responsibility

KAMARUZZAMAN ABDUL MANAN
MIHARAINI MD GHANI*
Universiti Sains Malaysia

ISMAIL SHEIKH YUSUF AHMED
Qatar University, Qatar

SITI NOR AMALINA AHMAD TAJUDDIN
Universiti Pendidikan Sultan Idris, Malaysia

ABSTRACT

The rapid expansion of digital platforms has significantly increased youths' exposure to online scams, rendering digital protection competencies a critical area of inquiry. Despite growing scholarly attention to cybercrime victimisation, limited research has examined how digital literacy shapes individuals' vulnerability to online scams through cognitive and behavioural mechanisms. Grounded in Protection Motivation Theory (PMT), this study investigates the relationship between digital literacy and scam susceptibility among Malaysian youth, with online risk awareness and perceived digital responsibility serving as mediating variables. A quantitative survey was administered to 383 youth respondents with active digital engagement. Data were analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM) via SmartPLS. The measurement model demonstrated satisfactory reliability and validity, whilst the structural model revealed that digital literacy dimensions particularly critical evaluation that significantly enhance online risk awareness and perceived digital responsibility. Both mediators were found to significantly reduce scam susceptibility, confirming their protective role in digital environments. Mediation analysis further indicated that risk awareness and digital responsibility partially mediate the relationship between digital literacy and scam susceptibility, underscoring the importance of cognitive and normative protective mechanisms. The findings contribute to communication and cyber-safety scholarship by extending PMT to the context of youth digital behaviour in Malaysia. Practically, the study emphasises the need for digital literacy education programmes that cultivate risk awareness and responsible online conduct, which can ultimately reduce youth vulnerability to online scams.

Keywords: *Digital literacy, online scam susceptibility, risk awareness, digital responsibility, protection motivation theory.*

INTRODUCTION

The digital revolution has fundamentally transformed the ways in which young people communicate, consume information, and conduct everyday transactions. Across Southeast Asia and particularly in Malaysia, youth are among the most digitally active demographic groups, with smartphone penetration and social media usage reaching unprecedented levels (MCMC, 2023). The rapid growth of digital media entertainment platforms has also facilitated media consumption globally (Sukmono et al., 2025). This pervasive connectivity, whilst enabling remarkable opportunities for education, commerce, and social interaction, has

*Corresponding author: miharaini@usm.my
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-27
Received: 6 March 2026 | Accepted: 12 May 2026 | Published: 30 June 2026

simultaneously created fertile conditions for the proliferation of online scams and cybercrime.

The Malaysian Communications and Multimedia Commission (MCMC, 2023) reported a substantial increase in online fraud cases, with financial losses running into hundreds of millions of *ringgit* (MYR) annually, disproportionately affecting younger victims who may be less experienced (Ho, 2025) in recognising deceptive digital tactics. Online scams have grown increasingly sophisticated in their execution. Perpetrators now employ psychologically manipulative strategies such as urgency framing, social proof, impersonation of trusted authorities, and platform migration (Manan et al., 2025), for instance, recruiting victims via WhatsApp or social media before migrating them to Telegram-based "investment" groups. These tactics are specifically designed to bypass rational evaluation and exploit emotional vulnerabilities, rendering even educated individuals susceptible. The consequences extend beyond financial harm to include psychological distress, loss of trust in digital systems, and reluctance to engage in legitimate digital services.

Digital literacy has emerged as one of the most frequently examined protective factors against online victimisation (Vo et al., 2026). Broadly defined, digital literacy encompasses not only functional or operational skills such as the ability to navigate digital platforms and manage account settings, but also the capacity for critical evaluation of online content and the consistent practice of safety and privacy behaviours (Juan et al., 2023). However, the theoretical mechanisms through which digital literacy translates into reduced scam vulnerability remain insufficiently theorised. Most studies treat digital literacy as a direct predictor of victimisation outcomes without examining the psychological and behavioural pathways that mediate this relationship (Luo et al., 2023).

This study addresses this gap by drawing on Protection Motivation Theory (PMT; Rogers, 1975), which provides a robust cognitive framework for understanding how individuals appraise threats and formulate protective responses. PMT posits that threat *appraisal, which comprises* threat awareness and perceived vulnerability, and coping appraisal which is self-efficacy and response efficacy jointly determine the likelihood of protective behaviour. In the context of online scams, online risk awareness can be conceptualised as a form of threat appraisal, whilst perceived digital responsibility reflects a coping orientation that motivates vigilant and ethical digital conduct. Both constructs are theorised to function as mediating mechanisms connecting digital literacy to scam susceptibility.

The present investigation is situated within the Malaysian youth context for several compelling reasons. First, Malaysia's high smartphone penetration rate and relatively young demographic profile make youth particularly exposed to digital fraud environments (MCMC, 2023). Second, despite increasing government-led anti-scam campaigns, empirical evidence regarding the psychological mechanisms underpinning scam resilience among youth remains scarce. Third, the multicultural composition of Malaysian society, combined with varying levels of access to quality digital education, creates a heterogeneous digital competency landscape that warrants systematic investigation (Tahir, 2025).

This study makes several distinct contributions. Theoretically, it extends PMT by integrating digital responsibility as a normative construct alongside risk awareness, expanding the theory's applicability to social media and cybercrime prevention contexts. Methodologically, it employs PLS-SEM to simultaneously test direct and indirect relationships

across multiple latent constructs. Practically, the findings offer actionable insights for policymakers, educators, and platform designers seeking to develop targeted digital literacy interventions that address both cognitive risk appraisal and behavioural responsibility among youth.

LITERATURE REVIEW OR RESEARCH BACKGROUND

Digital Literacy: Conceptualisation and Dimensions

Digital literacy is a multidimensional construct that has been defined and operationalised in various ways across the literature. Whilst early conceptualisations focused primarily on basic computer skills, contemporary frameworks emphasise a broader set of competencies necessary for effective, critical, and safe participation in digital environments (Buckingham, 2022). Gushevinalti and Suparman (2024) suggested that individuals from all professions must possess digital literacy competence to counter fake information. For the purposes of this study, digital literacy is operationalised across three theoretically grounded dimensions: operational skills, critical evaluation, and safety and privacy practices.

Operational skills refer to the functional ability to use digital tools, platforms, and applications for everyday purposes, such as managing privacy settings, navigating mobile payment systems, and recovering compromised accounts (Denysenko et al., 2024). These foundational competencies are widely regarded as prerequisites for more advanced forms of digital engagement. Critical evaluation encompasses the capacity to assess the credibility, accuracy, and intent behind online content and communications, including the ability to detect phishing attempts, verify suspicious messages, and resist manipulative narratives (Luo et al., 2023). Safety and privacy practices involve the consistent adoption of protective digital habits, such as using strong passwords, enabling multi-factor authentication, and exercising caution on public networks (Barnard et al., 2025).

Research has consistently demonstrated positive associations between higher digital literacy and reduced susceptibility to online misinformation, phishing, and fraud (Singh & Kumar, 2025). However, the mechanisms through which these competencies confer protection have not been fully elaborated. This study posits that digital literacy operates indirectly by cultivating risk awareness and promoting a sense of digital responsibility, which together function as cognitive-behavioural buffers against scam manipulation.

Online Risk Awareness and Scam Susceptibility

Online risk awareness refers to an individual's perceived understanding of the threats, vulnerabilities, and deceptive tactics prevalent in digital environments (Aiken et al., 2024). It encompasses knowledge of common fraud typologies, awareness of data exploitation techniques, and the ability to recognise the red flags associated with scam communications, such as urgency cues, requests for one-time passwords (OTPs), and unsolicited investment propositions. Risk awareness is closely aligned with the threat appraisal component of PMT (Rogers, 1983), which proposes that the perception of environmental dangers motivates individuals to adopt protective cognitive and behavioural responses.

Empirically, risk awareness has been identified as a significant protective factor against online fraud (Balakrishnan et al., 2025). Individuals who possess a clearer and more nuanced understanding of how scams operate are better positioned to scrutinise suspicious communications, delay impulsive responses, and seek verification from trusted sources. Conversely, low risk awareness, often characteristic of younger and less experienced users,

has been associated with higher rates of victimisation, particularly in relation to phishing, parcel scams, and social engineering attacks (Luo et al., 2023).

In the Malaysian context, the diversity of scam typologies poses particular challenges for youth. Job scams conducted via WhatsApp, investment scams hosted on Telegram channels, and impersonation scams involving fake government or financial institution representatives are among the most frequently reported fraud categories (MCMC, 2023). The technical sophistication and contextual plausibility of these scams mean that operational digital skills alone are insufficient to confer protection; rather, a heightened awareness of online risks, cultivated through digital literacy, is necessary (Ho, 2025).

Perceived Digital Responsibility and Protective Behaviour

Perceived digital responsibility is conceptualised in this study as an individual's internalised sense of accountability for their conduct in digital environments, encompassing the obligation to verify information before sharing, to report suspicious content, to protect personal data, and to contribute to safer online communities. This construct draws from normative frameworks in ethics of technology and aligns with the coping appraisal dimension of PMT, which emphasises the role of self-efficacy and response efficacy in motivating protective action (Rogers, 1983).

Responsible digital conduct has been linked to reduced engagement in risky online behaviours, including sharing unverified information and clicking on unverified hyperlinks (Maiko, 2025). When individuals perceive themselves as responsible digital citizens, they are more likely to exercise due diligence before engaging with unfamiliar communications, to maintain secure digital practices, and to resist social engineering manipulation. Importantly, digital responsibility is not solely a product of individual values but is also shaped by environmental factors, including digital literacy education, peer norms, and institutional messaging regarding cybersecurity (Manan et al., 2023).

Protection Motivation Theory as a Theoretical Framework

Protection Motivation Theory (Rogers, 1983) was originally developed to explain health-protective behaviour but has since been successfully applied across a range of risk domains, including information security, privacy protection, and cybersecurity compliance (Luo et al., 2023). PMT proposes that protective motivation is a function of threat appraisal, involving assessments of the severity and probability of a threat and coping appraisal, involving evaluations of the efficacy of available protective responses and one's capacity to perform them.

In the context of online scams, digital literacy can be understood as a foundational competency that enables both forms of appraisal. Specifically, higher digital literacy is expected to enhance threat appraisal by improving risk awareness, and to support coping appraisal by reinforcing a sense of digital responsibility. This theoretical positioning provides a coherent framework for hypothesising that risk awareness and digital responsibility function as mediating mechanisms between digital literacy and scam susceptibility.

Recent applications of PMT to cybersecurity contexts have yielded largely consistent support for these propositions (Almansoori et al., 2023). However, few studies have explicitly modelled digital responsibility as a distinct normative construct within the PMT framework, particularly in the context of youth and emerging digital economies. This study extends

existing PMT scholarship by incorporating perceived digital responsibility alongside risk awareness, thereby offering a more comprehensive account of the psychological mechanisms underpinning scam resilience.

Hypotheses Development

Drawing on the theoretical framework and empirical literature reviewed above, this study proposes the following hypotheses:

H1: Digital literacy dimensions (operational skills, critical evaluation, and safety and privacy practices) positively predict online risk awareness.

H2: Digital literacy dimensions positively predict perceived digital responsibility.

H3: Online risk awareness positively predicts perceived digital responsibility.

H4: Online risk awareness negatively predicts scam susceptibility.

H5: Perceived digital responsibility negatively predicts scam susceptibility.

H6: Online risk awareness mediates the relationship between digital literacy dimensions and scam susceptibility.

H7: Perceived digital responsibility mediates the relationship between digital literacy dimensions and scam susceptibility.

METHODOLOGY

Research Design and Sampling

This study adopted a quantitative cross-sectional survey design to examine the hypothesised relationships among digital literacy, online risk awareness, perceived digital responsibility, and scam susceptibility. A structured self-administered questionnaire was developed and distributed via online platforms, including WhatsApp, Instagram, and university student portals. The target population comprised Malaysian youth aged between 15 and 30 years who had active engagement with digital devices and online platforms.

Purposive sampling combined with snowball sampling was employed to recruit respondents. This sampling strategy was deemed appropriate given the targeted nature of the study population and the practical challenges of accessing a nationally representative youth sample. The final sample comprised 383 valid respondents after excluding incomplete or inconsistent responses. This sample size exceeds the minimum requirement suggested by Hair et al. (2018) for PLS-SEM analysis, providing adequate statistical power for the detection of small to medium effect sizes.

Measurement Instruments

All constructs were measured using multi-item Likert scales adapted from validated instruments in the extant literature. Operational skills (7 items) and critical evaluation (7 items) were adapted from the Digital Literacy Assessment Scale developed by Choi et al. (2023), safety and privacy practices (7 items), online risk awareness (6 items) was adapted from the risk perception scale used by Torres-Hernandez et al. (2022), whilst perceived digital responsibility (6 items) was adapted from the ethical digital citizenship framework proposed by Muhammad et al. (2025). Scam susceptibility (7 items) was operationalised using scenario-based items that assessed respondents' likelihood of engaging with common scam scenarios prevalent in the Malaysian context, including job scams, investment scams, and phishing communications.

Response options ranged from 1 (Strongly Disagree / Very Unlikely) to 5 (Strongly Agree / Very Likely). The questionnaire was piloted with 30 respondents to assess clarity and comprehension before the main data collection. Minor revisions were made to item wording based on pilot feedback.

Data Analysis

Data were analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM) with SmartPLS 4 software. PLS-SEM was selected over covariance-based SEM (CB-SEM) on the grounds that the study is primarily prediction-oriented, involves a complex model with multiple latent constructs and mediation pathways, and does not assume multivariate normality in the data (Hair et al., 2018). The analysis followed a two-stage procedure. First, the measurement model was evaluated to establish construct reliability (Cronbach's Alpha and Composite Reliability), indicator reliability (outer loadings), and convergent validity (Average Variance Extracted). Discriminant validity was assessed using the Heterotrait-Monotrait ratio (HTMT). Second, the structural model was estimated to test direct path coefficients and indirect mediation effects, with significance determined through bootstrapping with 5,000 subsamples.

RESULTS AND DISCUSSION

Demographic Profile of Respondents

A total of 383 respondents participated in this study. The demographic characteristics of the sample are presented in Table 1. In terms of gender, the sample comprised 233 female respondents (60.8%) and 150 male respondents (39.2%), indicating a slightly higher representation of female participants, which is consistent with patterns reported in similar youth digital behaviour surveys in Malaysia (MCMC, 2023). With regard to age, the majority of respondents fell within the 15–20 years age bracket (51.2%), followed by those aged 21–25 years (41.3%), whilst only 7.6% were between 26 and 30 years of age. This distribution reflects the study's youth-oriented focus.

In terms of educational background, secondary school students constituted the largest proportion (43.6%), followed by undergraduate students (32.1%), diploma holders (13.3%), and STPM or certificate holders (10.4%). Only a negligible proportion held postgraduate qualifications (0.5%). With respect to daily internet usage, the largest group reported using the internet for six to eight hours per day (40.7%), followed by three to five hours (31.6%) and more than nine hours (26.1%), confirming the high digital engagement of the sample. Regarding ethnicity, the sample was largely representative of the Malaysian population, with Malay respondents forming the plurality (48.8%), followed by Chinese (25.6%) and Indian (21.1%) respondents. Finally, income and allowance distribution reflected the predominantly student-based nature of the sample, with 38.1% reporting earnings below RM500 per month and 28.5% reporting no personal income.

Table 1: Demographic profile of respondents (N = 383)

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	150	39.2
	Female	233	60.8
Age	15–20 years old	196	51.2
	21–25 years old	158	41.3
	26–30 years old	29	7.6
Education Level	Secondary School	167	43.6
	Bachelor's Degree	123	32.1
	Diploma / Higher Diploma	51	13.3
	STPM / Certificate	40	10.4
	Master's Degree	2	0.5
Daily Internet Use	Less than 2 hours	6	1.6
	3–5 hours	121	31.6
	6–8 hours	156	40.7
	More than 9 hours	100	26.1
Ethnicity	Malay	187	48.8
	Chinese	98	25.6
	Indian	81	21.1
	Others	17	4.5
Monthly Income / Allowance	Less than RM500	146	38.1
	No personal income	109	28.5
	RM501–RM1000	35	9.1
	RM1001–RM2000	44	11.5
	RM2001–RM3000	36	9.4
	More than RM3000	13	3.4

Measurement Model Evaluation

To ensure the robustness of the measurement model, internal consistency reliability was assessed using Cronbach's Alpha (CA) and Composite Reliability (CR), whilst indicator reliability and convergent validity were examined using outer loadings and Average Variance Extracted (AVE), respectively. As summarised in Table 2, all constructs demonstrated satisfactory internal consistency, with CA values ranging from 0.828 to 0.983 and CR values ranging from 0.875 to 0.986, comfortably exceeding the recommended threshold of 0.70 (Hair et al., 2018). All items exhibited acceptable outer loadings, with the majority exceeding 0.75, indicating that each indicator contributes meaningfully to its respective construct.

Convergent validity was further confirmed, as all constructs achieved AVE values above the minimum criterion of 0.50 (Hair et al., 2018), ranging from 0.606 to 0.910.

Table 2: Internal consistency reliability, convergent validity and indicator reliability

Construct	Items	Outer Loading	Cronbach's Alpha	CR	AVE
Operational Skills	7 items	0.770–0.827	0.908	0.927	0.644
Critical Evaluation	7 items	0.746–0.860	0.919	0.935	0.675
Safety & Privacy Practices	7 items	0.738–0.834	0.891	0.915	0.606
Online Risk Awareness	6 items	0.803–0.865	0.918	0.936	0.709
Perceived Digital Responsibility	6 items	0.848–0.909	0.942	0.954	0.776
Scam Susceptibility	7 items	0.919–0.967	0.983	0.986	0.910

Discriminant validity was assessed using the Heterotrait–Monotrait ratio (HTMT), which is widely recommended as a stringent criterion for establishing empirical distinctiveness among constructs (Yong, 2023). As shown in Table 3, all HTMT values were below the conservative threshold of 0.85, confirming that each construct captures a unique conceptual domain. Furthermore, bootstrapped HTMT confidence intervals (Table 4) did not include the value of 1.00 for any construct pair, providing robust support for discriminant validity.

Table 3: Discriminant validity: heterotrait–monotrait ratio (HTMT)

	1	2	3	4	5	6
1. Operational Skills						
2. Critical Evaluation	0.742					
3. Safety & Privacy	0.691	0.734				
4. Online Risk Awareness	0.612	0.684	0.655			
5. Perceived Digital Responsibility	0.571	0.602	0.583	0.644		
6. Scam Susceptibility	0.329	0.301	0.317	0.388	0.351	

Table 4: Discriminant validity: HTMT confidence intervals (Bias Corrected)

Relationship	Original Sample (O)	Sample Mean (M)	Bias	2.50%	97.50%
Operational Skills → Critical Evaluation	0.742	0.741	−0.001	0.641	0.831
Operational Skills → Safety & Privacy	0.691	0.690	−0.001	0.589	0.785
Operational Skills → ORA	0.612	0.611	−0.001	0.502	0.708
Critical Evaluation → ORA	0.684	0.683	−0.001	0.584	0.771
Safety & Privacy → ORA	0.655	0.653	−0.002	0.551	0.742

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4202-27

ORA → PR	0.644	0.642	−0.002	0.548	0.731
PR → SSUS	0.351	0.349	−0.002	0.241	0.452
ORA → SSUS	0.388	0.386	−0.002	0.271	0.491

Overall Model Fit, Explanatory Power, and Predictive Relevance

The structural model was evaluated using the coefficient of determination (R^2), predictive relevance (Q^2), and the standardised root mean square residual (SRMR). As presented in Table 5, the model explained 37.2% of the variance in Online Risk Awareness ($R^2 = 0.372$) and 29.5% of the variance in Perceived Digital Responsibility ($R^2 = 0.295$), indicating meaningful explanatory power for the key psychological mechanisms in the model. The explained variance for Scam Susceptibility was comparatively smaller ($R^2 = 0.078$), which is theoretically plausible given that scam victimisation is influenced by a broad array of situational, contextual, and dispositional factors beyond individual competencies alone (Luo et al., 2023). All endogenous constructs achieved Q^2 values above zero, confirming the model's predictive relevance. The SRMR value of 0.072 falls below the recommended threshold of 0.08 (Hair et al., 2018), indicating acceptable overall model fit.

Table 5: Overall model fit, R^2 and Q^2

Endogenous Construct	**R^2**	**Q^2**	**SRMR**
Online Risk Awareness	0.372	0.241	
Perceived Digital Responsibility	0.295	0.193	
Scam Susceptibility	0.078	0.061	0.072

Model Path Analysis

Path coefficients were estimated through bootstrapping with 5,000 subsamples. The results are presented in Table 6 and discussed below in relation to the hypotheses. With respect to the effects of digital literacy dimensions on Online Risk Awareness (H1), Critical Evaluation emerged as the strongest predictor ($\beta = 0.461$, $t = 8.687$, $p < 0.001$), indicating that the capacity to appraise and scrutinise digital content confers the most substantial benefit in terms of threat perception. Operational Skills ($\beta = 0.172$, $t = 2.908$, $p = 0.004$) and Safety and Privacy Practices ($\beta = 0.196$, $t = 3.500$, $p = 0.001$) also significantly predicted Online Risk Awareness, providing support for H1. These findings resonate with Luo et al. (2023), who demonstrated that higher-order evaluative digital competencies are more strongly associated with threat sensitivity than operational skills alone.

Regarding the prediction of Perceived Digital Responsibility (H2), Critical Evaluation again demonstrated the strongest effect ($\beta = 0.308$, $t = 5.118$, $p < 0.001$), whilst the effect of Operational Skills was non-significant ($\beta = 0.081$, $t = 1.395$, $p = 0.163$), indicating that functional competence alone is insufficient to cultivate a sense of digital accountability. This finding is consistent with Recker et al. (2025), who argued that digital responsibility is shaped more by ethical and evaluative dispositions than by technical proficiency. H3 was also supported, as Online Risk Awareness significantly and positively predicted Perceived Digital Responsibility ($\beta = 0.216$, $t = 3.789$, $p < 0.001$), suggesting that recognition of digital threats motivates a more conscientious approach to online conduct.

Both mediating variables significantly reduced Scam Susceptibility. Online Risk Awareness demonstrated a significant negative effect (β = −0.176, t = 2.792, p = 0.005), supporting H4, whilst Perceived Digital Responsibility similarly reduced scam susceptibility (β = −0.150, t = 2.419, p = 0.016), supporting H5. These findings align with PMT's proposition that threat appraisal and coping orientation jointly mitigate risk-taking behaviour (Rogers, 1983).

Table 6: Model path analysis results

Relationship	β (O)	Sample Mean (M)	SD	T-Statistics	P-Value
Critical Evaluation → Online Risk Awareness	0.461	0.459	0.053	8.687	0.000
Operational Skills → Online Risk Awareness	0.172	0.171	0.059	2.908	0.004
Safety & Privacy → Online Risk Awareness	0.196	0.198	0.056	3.500	0.001
Critical Evaluation → Perceived Digital Responsibility	0.308	0.309	0.060	5.118	0.000
Operational Skills → Perceived Digital Responsibility	0.081	0.083	0.058	1.395	0.163
Online Risk Awareness → Perceived Digital Responsibility	0.216	0.215	0.057	3.789	0.000
Online Risk Awareness → Scam Susceptibility	−0.176	−0.178	0.063	2.792	0.005
Perceived Digital Responsibility → Scam Susceptibility	−0.150	−0.148	0.062	2.419	0.016

Mediation Analysis

Mediation effects were assessed using bootstrapped indirect effects with 5,000 subsamples. Results are presented in Table 7. Online Risk Awareness significantly mediated the effects of all three digital literacy dimensions on Perceived Digital Responsibility, with indirect effects for Critical Evaluation (β = 0.099, t = 3.122, p = 0.002), Operational Skills (β = 0.037, t = 2.015, p = 0.044), and Safety and Privacy Practices (β = 0.042, t = 2.306, p = 0.021) all reaching statistical significance, thereby supporting H6. Similarly, Online Risk Awareness significantly mediated the effects of digital literacy dimensions on Scam Susceptibility, confirming that the protective value of digital competence against scams is substantially channelled through heightened threat awareness. These findings are consistent with PMT's threat appraisal pathway and extend Luo et al. (2023)'s findings to the Malaysian youth context.

The sequential mediation pathway from Online Risk Awareness through Perceived Digital Responsibility to Scam Susceptibility was also significant (β = −0.032, t = 2.005, p = 0.045), supporting H7. This layered mechanism suggests that risk awareness does not solely operate as a direct buffer against scams but also reinforces a normative orientation towards responsible digital conduct, which in turn reduces vulnerability. This finding extends prior work by Ashrafi et al. (2025) by demonstrating that the integration of threat appraisal and responsibility-based coping yields an additive protective effect beyond individual pathways.

Table 7: Mediation analysis results

Indirect Relationship	Indirect Effect (β)	T-Statistics	P-Value
Critical Evaluation → ORA → PR	0.099	3.122	0.002
Operational Skills → ORA → PR	0.037	2.015	0.044
Safety & Privacy → ORA → PR	0.042	2.306	0.021
Critical Evaluation → ORA → SSUS	−0.081	2.676	0.008
Operational Skills → ORA → SSUS	−0.030	2.101	0.036
Safety & Privacy → ORA → SSUS	−0.034	2.294	0.022
ORA → PR → SSUS (Sequential)	−0.032	2.005	0.045

DISCUSSION

The findings of this study provide several important theoretical and practical insights into the mechanisms through which digital literacy influences scam susceptibility among Malaysian youth. Overall, the results support the central premise of Protection Motivation Theory (PMT), which posits that protective behaviour emerges through the interaction of threat appraisal and coping appraisal (Rogers, 1983). In the present model, digital literacy functions as a foundational competence that facilitates both cognitive recognition of online threats and behavioural responsibility in digital environments.

One of the most salient findings concerns the consistent dominance of critical evaluation across the structural paths in the model. Critical evaluation emerged as the strongest predictor of both online risk awareness and perceived digital responsibility, highlighting the central role of evaluative competencies in navigating complex digital environments. This finding reinforces the argument that digital literacy should not be conceptualised merely as the ability to operate technological devices but must also include the cognitive capacity to interpret, question, and critically assess digital information (Buckingham, 2022). In contemporary online ecosystems characterised by algorithmically curated content and persuasive digital messaging, the ability to distinguish legitimate communication from deceptive manipulation has become an essential survival skill.

The strong association between critical evaluation and online risk awareness suggests that youths who possess stronger analytical abilities are more capable of recognising subtle indicators of deception embedded in scam messages. These indicators may include urgency cues, unrealistic financial promises, impersonation of trusted institutions, or requests for sensitive personal information. Such findings align with previous studies indicating that individuals with stronger evaluative digital competencies are better equipped to detect phishing attempts and other forms of cyber deception (Luo et al., 2023). Importantly, this finding highlights that higher-order cognitive literacy, rather than mere technical familiarity with digital platforms, is the key mechanism through which digital literacy contributes to scam resilience.

In contrast, the relatively weaker influence of operational skills provides an important nuance to the digital literacy discourse. Whilst operational competence significantly predicted online risk awareness, its direct relationship with perceived digital responsibility was not statistically significant. This finding indicates that technical proficiency alone does not necessarily translate into responsible digital conduct. Youth may be highly skilled in navigating digital platforms, managing applications, and conducting online transactions, yet still lack the

ethical orientation or reflective judgement required to behave responsibly in digital spaces. Such a disconnect between digital capability and digital responsibility has been noted in previous research on digital citizenship, which emphasises that ethical awareness and social responsibility are distinct from technical competence (Recker et al., 2025).

This distinction carries important implications for digital literacy education. Many digital skills training programmes continue to prioritise operational training such as software usage, device management, and platform navigation. Whilst these competencies remain necessary, the findings of the present study suggest that such approaches may be insufficient to cultivate safe and responsible digital behaviour. Instead, educational initiatives should integrate critical media literacy, ethical reasoning, and reflective digital citizenship components that encourage individuals to consider the broader consequences of their online actions.

The positive relationship between online risk awareness and perceived digital responsibility further supports the theoretical propositions of PMT. Risk awareness, which represents the threat appraisal component of the theory, appears to stimulate a heightened sense of accountability in digital environments. Youth who recognise the potential dangers associated with online scams may develop stronger motivations to adopt cautious behaviours, verify information sources, and avoid engaging with suspicious digital communications. This finding suggests that awareness of digital threats not only promotes defensive reactions but also reinforces normative expectations about responsible digital conduct.

Both mediating variables, namely online risk awareness and perceived digital responsibility, were found to significantly reduce scam susceptibility. These results provide empirical support for the dual-process protective mechanism proposed by PMT, whereby both cognitive recognition of threats and behavioural coping strategies jointly influence protective decision-making (Rogers, 1983). Youth who are aware of scam tactics are more likely to pause and evaluate suspicious messages, whilst those who internalise a sense of digital responsibility may be more inclined to follow secure practices such as verifying requests, avoiding suspicious links, and protecting personal information.

The mediation analysis further revealed a sequential pathway, whereby digital literacy enhances risk awareness, which subsequently strengthens digital responsibility, ultimately reducing scam susceptibility. This layered mechanism offers a more nuanced understanding of how digital competence translates into real-world protection against online scams. Rather than operating as a direct safeguard, digital literacy appears to function through intermediate psychological processes that shape individuals' perceptions and behaviours in digital contexts. This finding extends prior research on cybersecurity behaviour by demonstrating that protective outcomes are best explained through interconnected cognitive and normative mechanisms rather than single-variable relationships (Ashrafi et al., 2025).

Another noteworthy observation concerns the relatively modest explanatory power of the model for scam susceptibility ($R^2 = 0.078$). Whilst statistically meaningful, this value indicates that scam vulnerability is influenced by a broader constellation of factors beyond individual digital literacy competencies. Situational characteristics of scams, such as urgency framing, emotional manipulation, and social engineering tactics, may significantly influence decision-making processes. For instance, individuals experiencing financial stress or emotional vulnerability may be more susceptible to fraudulent schemes regardless of their

level of digital competence. Similarly, peer influence and social proof mechanisms frequently employed in online scams may override rational risk assessment processes. These contextual influences highlight the complexity of cybercrime victimisation and suggest that digital literacy should be viewed as one component within a broader ecosystem of protective factors.

Within the Malaysian context, the findings of this study are particularly relevant given the rapid growth of digital platforms and the increasing sophistication of scam operations. Malaysian youth are among the most active users of social media and mobile financial services, making them attractive targets for cybercriminals (MCMC, 2023). Scam tactics such as investment fraud, job recruitment scams, and impersonation schemes often rely on persuasive communication strategies that exploit trust and urgency. As such, strengthening youths' ability to critically evaluate digital content and recognise deceptive patterns becomes a critical component of national cyber safety strategies.

From a policy perspective, the results suggest that anti-scam initiatives should adopt a multi-layered educational approach. Government agencies, educational institutions, and digital platforms should collaborate to design programmes that simultaneously address knowledge, awareness, and behavioural responsibility. Digital literacy campaigns that merely disseminate information about scams may be insufficient unless they also cultivate the cognitive and ethical competencies required to interpret and respond to such threats effectively. Integrating digital safety modules into school curricula, promoting peer-led digital awareness campaigns, and leveraging social media platforms for educational messaging may help strengthen youths' resilience against online fraud.

Furthermore, the role of platform design and technological interventions should not be overlooked. Digital platforms can contribute to scam prevention by embedding risk-alert mechanisms, transaction warnings, and verification prompts that encourage users to pause and reconsider potentially risky actions. Such "risk nudges" can support users' cognitive appraisal and complement individual-level digital literacy competencies.

In summary, the findings of this study advance our understanding of how digital literacy contributes to cyber safety among youth by demonstrating that its protective effects operate through the interconnected mechanisms of risk awareness and digital responsibility. The results underscore the importance of developing digital literacy frameworks that prioritise critical evaluation, ethical awareness, and responsible digital engagement. As online scams continue to evolve in complexity and scale, empowering youth with the cognitive and normative competencies required to navigate digital environments safely will remain a crucial priority for policymakers, educators, and technology developers alike.

CONCLUSION

This study set out to examine the relationships between digital literacy, online risk awareness, perceived digital responsibility, and scam susceptibility among Malaysian youth, employing Protection Motivation Theory as its guiding theoretical framework. Using PLS-SEM, the study confirmed that digital literacy dimensions, particularly critical evaluation and safety and privacy practices, significantly predict both online risk awareness and perceived digital responsibility, which in turn reduce susceptibility to online scams.

Several contributions emerge from this investigation. First, the study extends PMT to the context of youth digital behaviour and cybercrime prevention, demonstrating the applicability of threat appraisal and coping orientation constructs to the specific challenges

posed by online scams. Second, by introducing perceived digital responsibility as a distinct mediating construct, the study enriches the theoretical landscape by integrating normative dimensions of digital citizenship into the PMT framework. Third, the identification of a sequential mediation pathway through which risk awareness reinforces responsibility, which subsequently reduces scam vulnerability, offers a more nuanced understanding of the cognitive-behavioural mechanisms underpinning scam resilience.

From a practical standpoint, the findings carry clear implications for educational and policy interventions. Digital literacy programmes in schools and tertiary institutions should be redesigned to prioritise not only operational skills but also critical evaluation capacities and the cultivation of a sense of digital responsibility. Anti-scam campaigns by government agencies and financial institutions should similarly be framed to enhance youth's awareness of specific scam typologies while simultaneously reinforcing messages about digital accountability. Platform developers might consider incorporating risk-nudging features such as warnings about unverified senders or unusual transaction requests to support in-the-moment risk appraisal.

Several limitations of this study merit acknowledgement. The cross-sectional design precludes causal inference, and future longitudinal studies would strengthen the basis for causal claims regarding the directionality of observed relationships. The sample, whilst adequately sized for PLS-SEM, was recruited through purposive and snowball sampling and may not be fully representative of the broader Malaysian youth population. Additionally, scam susceptibility was assessed using scenario-based self-report items rather than behavioural measures, which may be subject to social desirability bias. Future research should consider employing experimental or longitudinal designs, expanding the sample to include rural youth and older adult populations, and incorporating objective measures of digital competence and actual victimisation history.

Notwithstanding these limitations, this study contributes meaningfully to the growing body of research on digital safety, youth communication behaviour, and cyber-risk management in developing digital economies. As online scams continue to evolve in sophistication and scale, the cultivation of critically literate, risk-aware, and digitally responsible youth represents one of the most promising pathways towards a safer and more resilient digital society.

ACKNOWLEDGEMENT

The article is based on research funded by a Universiti Sains Malaysia Short-Term Grant entitled "Digital Literacy and Cybercrime among Youth", (Grant No: R501-LRRND002-0000001169-0000). The authors sincerely appreciate this support, which enabled the research.

BIODATA

Kamaruzzaman Abdul Manan (PhD) is a senior lecturer at the School of Communication, Universiti Sains Malaysia. His research interests encompass digital communication, cybercrime victimisation, and media literacy among youth populations. Email: kamaruzzaman@usm.my

Miharaini Md Ghani is a lecturer at the School of Communication, Universiti Sains Malaysia, specialising in digital media, health communication, and quantitative research methods. Email: miharaini@usm.my

Ismail Sheikh Yusuf Ahmed (PhD) is affiliated with the Mass Communication Department at Qatar University. His expertise lies in the effects of digital technologies, strategic communication, advertising, quantitative research methods, and cross-cultural communication research. Email: iahmed@qu.edu.qa

Siti Nor Amalina Ahmad Tajuddin (PhD) is a lecturer at the Faculty of Human Development, Universiti Pendidikan Sultan Idris. Her research interests include educational technology, digital citizenship, and youth digital well-being. Email: sitinoramalina@fbk.upsi.edu.my

REFERENCES

Aiken, M. P., Davidson, J. C., Walrave, M., Ponnet, K. S., Phillips, K., & Farr, R. R. (2024). Intention to hack? Applying the theory of planned behaviour to youth criminal hacking. *Forensic Sciences*, *4*(1), 24–41. https://doi.org/10.3390/forensicsci4010003

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*(9), Article 5700. https://doi.org/10.3390/app13095700

Ashrafi, D. M., Sattar, M., & Jalal, R. (2025). What influences digital natives' susceptibility to cyber phishing scams? *Journal of Financial Crime*, *32*(6), 1211–1234. https://doi.org/10.1108/jfc-01-2025-0021

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

Barnard, G., Maczka, K., & Parsons, D. (2025). Digital safety practices and the psychological mechanisms of password protection. *Journal of Cyber-Risk and Protection*, *11*(2), 142–158.

Buckingham, D. (2023). *The media education manifesto* (2nd ed.). Polity Press.

Choi, J., Choi, S., Song, K., Baek, J., Kim, H., Choi, M., Kim, Y., Chu, S., & Shin, J. (2023). Everyday digital literacy questionnaire for older adults: Instrument development and validation study. *JMIR Publications*, *9*, Article e51616. https://doi.org/10.2196/51616

Denysenko, M., Khudoliy, L., & Laptiev, L. (2024). *Digital skills in a digital society: Requirements and challenges*. Scientific Center of Innovative Research. https://doi.org/10.36690/DSDS

Gushevinalti, & Suparman. (2024). Digital literacy to improve the professionalism of online media journalists in Bengkulu, Indonesia. *Jurnal Komunikasi: Malaysian Journal of Communication*, *40*(2), 61–74. https://doi.org/10.17576/JKMJC-2024-4002-04

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2018). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/ebr-11-2018-0203

Ho, S. (2025, August 20). No decline in online scam cases in Malaysia despite campaigns, says minister. *The Straits Times*. https://www.straitstimes.com/asia/se-asia/no-decline-in-online-scam-cases-in-malaysia-despite-campaigns-says-minister

Juan, D., Tao, C., & Lu, G. (2023). Analysis of the connotation of digital literacy and related literacy. *International Journal of New Developments in Education*, *5*(23), 1–10. https://doi.org/10.25236/ijnde.2023.052301

Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2023). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28–38. https://doi.org/10.1016/j.cose.2012.12.003

Maiko, C. R. M. A. (2025). Assessing awareness and practices on preventive measures against online scams among senior high school students. *International Journal of Multidisciplinary Research and Publications*, *7*(12), 578–581.

Malaysian Communications and Multimedia Commission (MCMC). (2023). Internet users survey 2023.

Manan, K. A., Li, J., Ahmad Tajuddin, S. N. A., & Samsudin, S. (2025). Factors influencing online impulsive buying intentions on Weibo: The mediating role of arousal. *Pertanika Journal of Social Sciences & Humanities*, *33*(5), Article 13. https://doi.org/rcjr

Muhammad, Z. U. H., & Sangkala, I. (2025). Digital citizenship framework: A systematic review of contemporary elements and implementation challenges. *Journal of Computer Interaction in Education*, *8*(1), 34–39.

Recker, J., Chatterjee, S., Sundermeier, J., & Tarafdar, M. (2025). Digital responsibility: Current perspectives and future directions. *Journal of the Association for Information Systems*, *26*(5), 1222–1238. https://doi.org/10.17705/1jais.00966

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114. https://doi.org/cb4jgn

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. R. Cacioppo & R. E. Petty (Eds.), *Social psychology: A sourcebook* (pp. 153–176). Guilford Press.

Singh, R., & Kumar, A. (2025). The impact of digital literacy on cybercrime awareness & victimization. *PJCriminology Journal*, *1*(1), 45–60.

Sukmono, F. G., Kencana, A. P. S., Fadillah, D., & Long, B. (2025). Empowering digital audiences: A uses and gratifications theory analysis of streaming platform selection among youth in Indonesia and China. *Jurnal Komunikasi: Malaysian Journal of Communication*, *41*(4), 19–39. https://doi.org/10.17576/JKMJC-2025-4104-02

Tahir, A. (2025, February 26). Digital danger: The growing cybercrime crisis among Malaysia's youth. *SinarDaily*. https://www.sinardaily.my/article/225616/culture/tech/digital-danger-the-growing-cybercrime-crisis-among-malaysias-youth

Torres-Hernández, n., García-Martínez, I., & Gallego-Arrufat, M. J. (2022). Internet risk perception: Development and validation of a scale for adults. *European Journal of Investigation in Health, Psychology and Education*, *12*(11), 1581–1593. https://doi.org/10.3390/ejihpe12110111

Vo, D. V., Nguyen, P. N. T., Huynh, V. T., & Nguyen, G. M. T. (2026). Cyberbullying among high school students: Digital literacy as a protective factor? *Social Psychology of Education*, *29*(7). https://doi.org/10.1007/s11218-026-10174-5

Yong, D. (2023). Testing the discriminant validity and heterotrait–monotrait ratio of correlation (HTMT): A case in Indonesian SMEs, macroeconomic risk and growth in the Southeast Asian countries. *Insight*, *1*(1), 12–25.