

Knowledge, Attitudes and Practices as Protective Factors against Commercial Crime Victimization Risk among Adults in Malaysia: A Behavioral Science Perspective

Thanabal Suppiah¹, Mohammad Rahim Kamaluddin¹ and Azahah Abu Hassan Shaari¹

¹Centre for Research in Psychology and Human Well-Being (PsiTra),
Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia,
43600 Bangi, Selangor, Malaysia

Abstract. Commercial crime victimization increasingly involves behavioral as well as technological vulnerabilities, requiring prevention strategies that extend beyond general awareness. This conceptual paper examines how knowledge, attitudes and practices (KAP) may function as protective factors against commercial crime victimization risk among adults in Malaysia. A narrative conceptual synthesis was undertaken by integrating the KAP framework with Social Cognitive Theory and Routine Activity Theory, supported by empirical and official literature relevant to fraud and scam victimization. The synthesis distinguishes exposure, susceptibility, risk and realized victimization, and proposes that knowledge, attitudes and practices are separate but interacting capacities. Routine activities shape exposure to offenders, social-cognitive processes explain how personal and environmental influences affect judgement, and KAP determines whether warning signs are recognized, threats are appraised realistically and protective actions are performed. Six propositions specify the expected relationships among these domains and victimization risk. The framework argues that prevention should address not only what individuals know, but also how they calibrate trust, respond to urgency and consistently verify transactions. It offers a theoretically grounded basis for future empirical testing and behaviorally informed commercial crime prevention in Malaysia.

Keywords: commercial crime; victimization risk; knowledge, attitudes and practices; Social Cognitive Theory; Routine Activity Theory; behavioral science

Email: sthana9667@yahoo.com

1.0 Introduction

Digital banking, electronic commerce, social media and instant messaging have expanded the speed and reach of legitimate transactions. The same infrastructures have also widened opportunities for commercial crime. Offenders can contact large numbers of potential targets, imitate trusted institutions and personalise deceptive messages with information gathered from digital traces. Susceptibility emerges from the interaction between individual

characteristics and persuasive online contexts(Williams & Beardmore, 2017). Technology alone therefore does not complete a scam. In many common forms of fraud, victimisation occurs only after an individual responds to a request, discloses credentials, installs an application or transfers funds. Commercial crime involves a behavioral decision point as well as a technological attack surface.

The Malaysian context makes this distinction particularly important. Official statistics recorded an increase in commercial crime from 30,536 cases in 2022 to 40,350 cases in 2023, with fraud accounting for most cases (Department of Statistics Malaysia, 2024). More recent official reports indicate continuing losses measured in billions of ringgit (Bank Negara Malaysia, 2026; Royal Malaysia Police, 2025). Although reporting periods and operational definitions differ across agencies, the direction is consistent: commercial crime represents a sustained public-safety and financial-well-being problem.

Public education has achieved substantial reach, but exposure to warnings does not necessarily produce safe action. Bank Negara Malaysia (2025) reported that nine in ten surveyed consumers were aware of scam warnings from banks, while most reported scam cases involved victims consciously transferring money to persons subsequently identified as scammers. This apparent awareness-action gap does not imply that victims knowingly accepted fraud. Rather, it suggests that information was not recognised as relevant, not believed strongly enough, or not converted into a protective response at the critical moment.

The knowledge-attitudes-practices (KAP) framework offers a useful starting point because it separates what people know, how they evaluate threats and what they actually do. However, a simple linear sequence more knowledge produces safer attitudes, which automatically produces safer practices is inadequate for deceptive and emotionally charged decisions. Individuals may recognise common scams but remain overconfident, underestimate their own susceptibility or abandon routine checks when confronted with urgency, authority, fear or anticipated reward. KAP is therefore better treated as a diagnostic set of interacting protective capacities than as a deterministic causal chain.

This paper develops an integrated conceptual framework in which KAP is linked to Social Cognitive Theory (SCT) and Routine Activity Theory (RAT). The paper has three objectives: (1) to clarify the conceptual boundary between exposure, susceptibility, victimisation risk and realised victimisation; (2) to explain how KAP may protect adults from commercial crime within a broader social and environmental context; and (3) to formulate propositions and practical implications for subsequent empirical investigation in Malaysia.

2.0 Conceptual synthesis method

This paper uses a narrative conceptual synthesis rather than a systematic review or meta-analysis. Literature was organised around four analytic questions: how commercial crime victimisation is defined; how exposure differs from susceptibility and realised loss; how knowledge, attitudes and protective practices relate to risk; and how personal, social and environmental conditions modify these relationships. Priority was given to peer-reviewed empirical studies and systematic reviews concerning fraud, scams, phishing and online influence, together with Malaysian studies and official statistics that establish local relevance.

The synthesis proceeded in three stages. First, concepts that are often used interchangeably awareness, exposure, perceived risk, susceptibility and victimisation were separated by their position in the victimisation process. Second, the explanatory contribution and limitations of KAP, SCT and RAT were compared. Third, the complementary elements of the three perspectives were integrated into a framework and translated into testable

propositions. The method is interpretive and theory-building; it does not estimate pooled effects or claim exhaustive coverage of all fraud literature.

3.0 Conceptual foundations

3.1 From exposure to realised victimisation

Commercial crime is used here as an umbrella term for deceptive offences involving transactions, money, property, trust or valuable information. The analytical focus is on offences that require some response from an individual target, including e-commerce, impersonation, investment, employment, loan, telecommunications and romance scams. These categories differ in narrative and target group, but typically share a sequence: attention is captured, credibility is constructed, emotion or urgency is induced, critical scrutiny is reduced and a consequential action is requested.

Exposure refers to encountering an attempted scam; targeting refers to being selected or contacted; susceptibility refers to a tendency to believe, comply or continue the interaction; victimisation risk is the relative likelihood that exposure progresses towards harmful compliance; and realised victimisation is the occurrence of loss, data compromise or other harm. (Koning et al., 2023) show why this separation matters: variables that increase contact with fraud attempts do not necessarily increase compliance after contact. A highly active internet user may face more attempts but also develop stronger detection skills. Conversely, an infrequent user may remain highly susceptible to one carefully designed approach.

Risk should therefore not be equated with prior victim status. A continuous risk construct can identify potentially modifiable tendencies before harm occurs. The Malaysian Scam Victimisation Risk Inventory operationalises risk through hasty decision-making, trust in inaccurate information and risk-taking tendency (Wan Sulaiman et al., 2022). Such an inventory supports prevention, although it cannot predict with certainty whether a particular person will be victimised in a specific context.

3.2 Knowledge as recognition capability

Protective knowledge includes more than familiarity with the word scam. It covers current modus operandi, warning signs, verification procedures, credential protection, reporting channels and immediate steps following a suspicious transaction. Objective knowledge what a person can correctly identify must also be distinguished from subjective knowledge how knowledgeable the person feels. This distinction is central because overconfidence may suppress verification. Malaysian evidence shows that overconfidence predicts online fraud victimisation and that perceived financial capability may exceed demonstrated literacy (Balakrishnan et al., 2025) Institute for Capital Market Research Malaysia, 2023).

Knowledge is thus protective when it is accurate, current, retrievable under pressure and calibrated to the limits of one's competence. It may fail when scam scripts evolve, when an individual recognises only stereotypical messages, or when confidence rises faster than detection ability. Knowledge should consequently be measured through scenario-based or objective items where possible, rather than solely through self-rated awareness.

3.3 Attitudes as threat appraisal and calibrated trust

Attitudes include perceived seriousness, realistic personal susceptibility, willingness to verify, tolerance of delay and the manner in which trust is assigned. A person may agree that

scams are serious while believing that only less capable people become victims. Such perceived immunity reduces motivation to pause or obtain a second opinion. Productive caution is not indiscriminate fear; it is calibrated scepticism that recognises personal fallibility without eliminating the trust required for normal social and commercial exchange.

Authority cues, social endorsement and emotional framing are particularly important. Offenders borrow credibility from institutional logos, job titles, testimonials, acquaintances or online communities. Malaysian evidence identifies social influence as a consistent predictor of online fraud victimisation (Basir et al., 2026), while the risk inventory highlights trust in inaccurate information (Santhidran et al., 2026). Attitude therefore includes an epistemic disposition: the readiness to distinguish independent evidence from signals designed to look credible.

3.4 Practices as enacted guardianship

Practices are observable or self-reported protective behaviors performed before, during and after suspicious contact. Examples include independently contacting an organisation, checking account or telephone details, inspecting links, refusing remote-access applications, protecting authentication codes, enabling security features, pausing before transfer and reporting attempted fraud. Within RAT, these practices function as guardianship because they interrupt the path from exposure to harmful compliance.

The main challenge is the intention-behavior gap. A respondent may endorse verification as important but fail to perform it when tired, rushed, emotionally invested or confronted by an apparent authority. Self-reported practice may also be inflated by social desirability. Consequently, practices are conceptually closest to immediate protection but require behaviorally specific measurement. Where feasible, future research should complement self-report with scenarios, simulations or transaction-level indicators.

4.0 Integrating KAP, Social Cognitive Theory and Routine Activity Theory

4.1 Complementary explanatory roles

Each perspective answers a different part of the victimisation problem. RAT explains the opportunity structure: motivated offenders encounter suitable targets in the absence of effective guardianship (Cohen & Felson, 1979). In digital settings, routine activities such as shopping, investing, job seeking and communicating with unknown contacts increase exposure. RAT is less specific about why two people facing the same message respond differently.

SCT addresses this difference through reciprocal interaction among personal factors, behavior and environment (Bandura, 1986). Knowledge, confidence and threat appraisal operate within the personal domain; security habits and verification are behavioral; platform design, social influence and institutional safeguards form part of the environment. SCT therefore corrects the overly linear interpretation of KAP: behavior can reshape knowledge and confidence, while environmental cues can override or reinforce both.

KAP contributes measurable and intervention-relevant capacities. Knowledge supports recognition, attitudes govern appraisal and trust, and practices enact protection. Integrated with RAT and SCT, these capacities are positioned between exposure and harmful action rather than treated as isolated individual traits. The framework also retains institutional responsibility: safer platform design, friction at high-risk transactions, clear verification

channels and timely support strengthen guardianship instead of placing the full burden on potential victims.

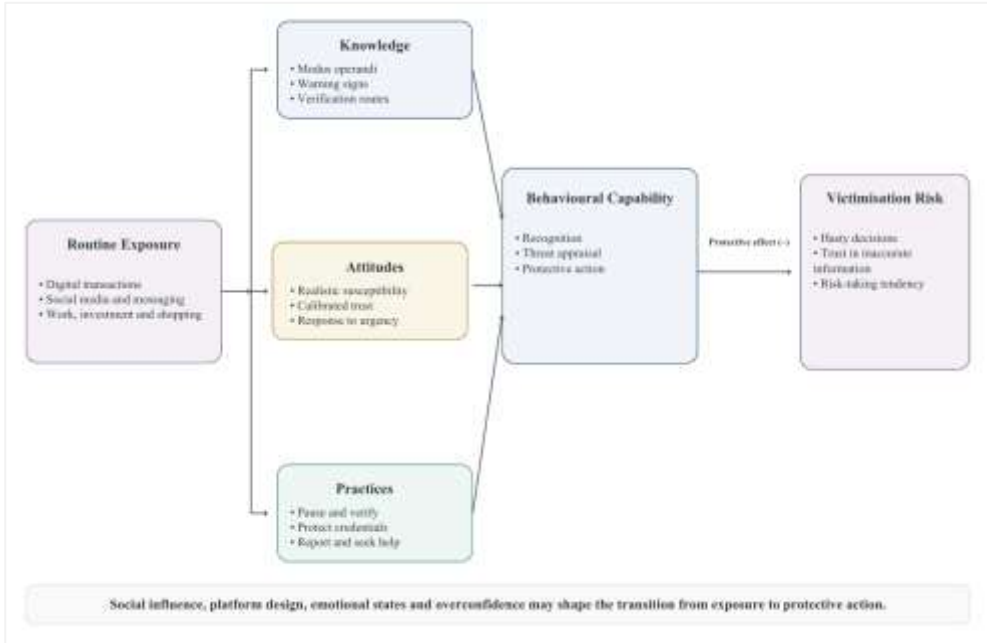


Fig. 1. Integrated behavioral framework of KAP and commercial crime victimisation risk.

4.2 Conceptual propositions

- P1.** Higher accurate and current objective knowledge is associated with lower commercial crime victimisation risk because it improves recognition of deceptive cues and knowledge of verification routes.
- P2.** The protective effect of knowledge is weakened when subjective confidence exceeds objective knowledge; overconfidence reduces help-seeking and independent verification.
- P3.** Attitudes characterised by realistic susceptibility, calibrated trust and resistance to urgency are associated with lower victimisation risk.
- P4.** Consistent protective practices are associated with lower victimisation risk and mediate part of the relationship between knowledge, attitudes and risk.
- P5.** Routine digital activities increase exposure opportunities, but the progression from exposure to harmful compliance depends on the interaction between KAP, environmental cues and available guardianship.
- P6.** Sociodemographic characteristics do not form a universal victim profile; their association with risk is conditional on exposure patterns, resources, scam type and protective capacity.

5.0 Discussion

The framework shifts the central question from “Who becomes a victim?” to “Under what conditions does exposure become harmful compliance, and which protective capacity fails?” This shift is important because demographic findings are inconsistent across scam types and

populations, including in systematic evidence concerning older adults(Burton et al., 2021). Age, gender, education and income may influence technology use, financial opportunity, social support and the narratives used by offenders, but they should not be interpreted as direct or immutable causes. A behaviorally grounded framework reduces stereotyping and victim blaming while preserving the value of subgroup analysis.

The synthesis also explains why awareness campaigns may show diminishing returns. Awareness is often treated as a proxy for knowledge, attitude and behavior simultaneously, yet these constructs are not interchangeable. A person can recall that scams exist without recognising a new script; recognise the script but trust an apparently authoritative caller; or distrust the caller but still transfer money under time pressure. Prevention must therefore diagnose the broken link rather than repeat generic warnings.

Existing Malaysian research supports the relevance of each component but has not fully integrated them.(Azmi et al., 2025) reported positive associations between KAP domains and cautious behavior, and subsequent mixed method work further applied KAP to online scam awareness and prevention. Balakrishnan et al. (2025) demonstrated that overconfidence and social influence remain relevant across two adult samples, while (Adeyinka-Ojo & Miraz, 2025) showed the relevance of routine activities to Malaysian e-commerce fraud exposure. Together, these findings justify a model that combines modifiable capacities with social context, but they do not establish causality or the relative contribution of each KAP domain to a validated risk outcome.

The distinction between exposure and susceptibility further prevents misleading conclusions. Frequent internet activity can increase the number of attempts detected and reported, creating an apparent association between knowledge and exposure. The same knowledge may nevertheless reduce compliance once an attempt occurs (Mukred et al., 2024). Future analyses should therefore avoid collapsing exposure, victim history, perceived risk and susceptibility into a single outcome.

6.0 Practical implications for prevention

The integrated framework suggests that commercial crime prevention should be layered, consistent with the view that effective fraud prevention requires a combination of strategies rather than a single awareness intervention (Button et al., 2023). Information remains necessary, but educational content should be current, scenario-based and action-oriented. Individuals need to practise identifying manipulated urgency, verifying identities through independent channels, refusing credential requests and pausing before irreversible transactions. Demonstrations and simulations may expose overconfidence more effectively than passive messages because they compare perceived skill with actual performance.

Domain	Primary gap	Behavioral response	Example indicator
Knowledge	Outdated or generic awareness	Recognise current cues and identify a safe verification route	Scenario accuracy
Attitudes	Perceived immunity, uncalibrated trust or urgency acceptance	Acknowledge susceptibility and tolerate delay	Threat appraisal and trust calibration
Practices	Failure to act despite correct beliefs	Pause, verify, protect and report	Behavior frequency or simulation

Domain	Primary gap	Behavioral response	Example indicator
Environment	High exposure and weak guardianship	Add friction, timely warnings and accessible support	Exposure and safeguard use

Table 1. Translating the conceptual framework into prevention and measurement targets.

Institutions should complement individual capability with structural guardianship. Transaction cooling-off periods, confirmation through known channels, detection of unusual transfers and immediate response services reduce reliance on memory during high-pressure decisions. Messages should specify one feasible action rather than merely intensify fear. Where subgroup differences are found, prevention should be adapted to exposure channels and resource needs rather than based on assumptions that one demographic category is inherently gullible.

7.0 Limitations and directions for future research

This framework is conceptual and does not establish the magnitude or causal direction of the proposed relationships. The narrative synthesis is selective rather than exhaustive, and the category “commercial crime” includes scams with different emotional, financial and technological mechanisms. The propositions should therefore be examined both across general commercial crime and within specific scam categories.

A first empirical test could use an adult Malaysian survey that measures objective knowledge, attitudes, self-reported practices, routine exposure and victimisation risk as distinct constructs. Confirmatory factor analysis should test whether KAP and risk remain empirically separable, followed by multivariable modelling of their unique associations. Interaction terms could assess whether overconfidence, urgency or exposure weakens the protective role of knowledge. Measurement invariance should be considered before comparing risk across age, gender, education or language groups.

Cross-sectional self-report designs will remain vulnerable to common-method bias, recall error and socially desirable reporting. Stronger evidence would combine surveys with vignette decisions, phishing simulations, longitudinal follow-up or transaction-level behavioral measures. Intervention studies should test whether scenario practice and just-in-time prompts improve verified behavior rather than only post-session knowledge. Qualitative interviews with victims and investigators can additionally identify how KAP fails under emotion, relationship pressure or novel scam scripts.

8.0 Conclusion

Commercial crime victimisation cannot be explained by technology exposure or public awareness alone. It emerges through an interaction among opportunities, personal appraisal, social influence, environmental safeguards and behavior at a critical decision point. The proposed framework positions knowledge, attitudes and practices as distinct but interacting protective capacities: knowledge enables recognition, attitudes calibrate trust and susceptibility, and practices enact guardianship.

Integrating KAP with Social Cognitive Theory and Routine Activity Theory clarifies why information may fail to become action and why demographic characteristics do not define a universal victim profile. For Malaysia, the framework supports a move from broad awareness toward measurable behavioral capability, timely verification and shared institutional guardianship. Its six propositions provide a coherent foundation for subsequent empirical

testing and for prevention strategies designed around the actual point at which exposure becomes harmful compliance.

Acknowledgements: The author acknowledges the academic support provided by the Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia.

Funding: The author received no specific funding for this conceptual paper.

Data Availability: No new data were generated or analysed in this conceptual paper. All sources used are cited in the manuscript.

Author's Contributions Statement: T.S. conceptualised the paper, synthesised the literature, developed the integrated framework and prepared the manuscript.

Competing Interest: The author declares no competing interests.

Ethics Statement: Ethical approval was not required because this conceptual paper did not involve human participants, personal data or animal subjects.

References

- Adeyinka-Ojo, S., & Miraz, A. P. D. M. (2025). *A Routine Activity Theory Approach in Developing a Framework for Mitigating E- Commerce Fraud and Cybercrime Praxis*. 4, 49–93.
- Azmi, S., Jais, Z., Samsudin, S., Hasini, N., Izhar, N., Idris, N., & Hassan, A. (2025). A Qualitative Approach of KAP Model Against Online Scam in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 15. <https://doi.org/10.6007/IJARBS/v15-i2/24701>
- Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLOS ONE*, 20. <https://doi.org/10.1371/journal.pone.0317232>
- Basir, M., Yahya, M., Mustafa, H., & Soh, W. (2026). Capable Yet Deceived: A Qualitative Exploration of Cognitive and Behavioural Processes in Online Financial SCAM Victimization in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 16. <https://doi.org/10.6007/IJARBS/v16-i5/28337>
- Burton, A., Dar, A., Mathews, L., & Tripathi, K. (2021). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, 159, 111678. <https://doi.org/10.1016/j.exger.2021.111678>
- Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). What really works in preventing fraud against organisations and do decision-makers really need to know? *Security Journal*, 37, 965–983. <https://doi.org/10.1057/s41284-023-00402-4>
- Koning, L., Junger, M., & Veldkamp, B. (2023). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, 30, 443–479. <https://doi.org/10.1177/02697580231215839>
- Mukred, M., Mokhtar, U. A., Moafa, F. A., Gumaei, A., Sadiq, A. S., & Al-Othmani, A. (2024). The roots of digital aggression: Exploring cyber-violence through a systematic literature review. *International Journal of Information Management Data Insights*, 4(2), 100281. <https://doi.org/10.1016/j.jjime.2024.100281>
- Santhidran, S., Periyayya, T., Tan, S. A., Wilson, S., Rajasakran, T., Hassan, N., & Tripathi, K. (2026). Psychological predictors of scam susceptibility among Malaysian older adults: a cross-sectional study. *Asian Journal of Gerontology and Geriatrics*, 21, 22. <https://doi.org/10.12809/ajgg-760>

Williams, E., & Beardmore, A. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72.
<https://doi.org/10.1016/j.chb.2017.03.002>