



Risk Behavioural Tendencies and Susceptibility to Scam?

Still thinking about firewalls and encryption? Unfortunately, these traditional security measures can only serve as limited defense against socially engineered tactics. The uncomfortable truth is that human risk stands as the weakest link, and risky behaviours are where scammers aim to exploit and weaponise with surgical precision.

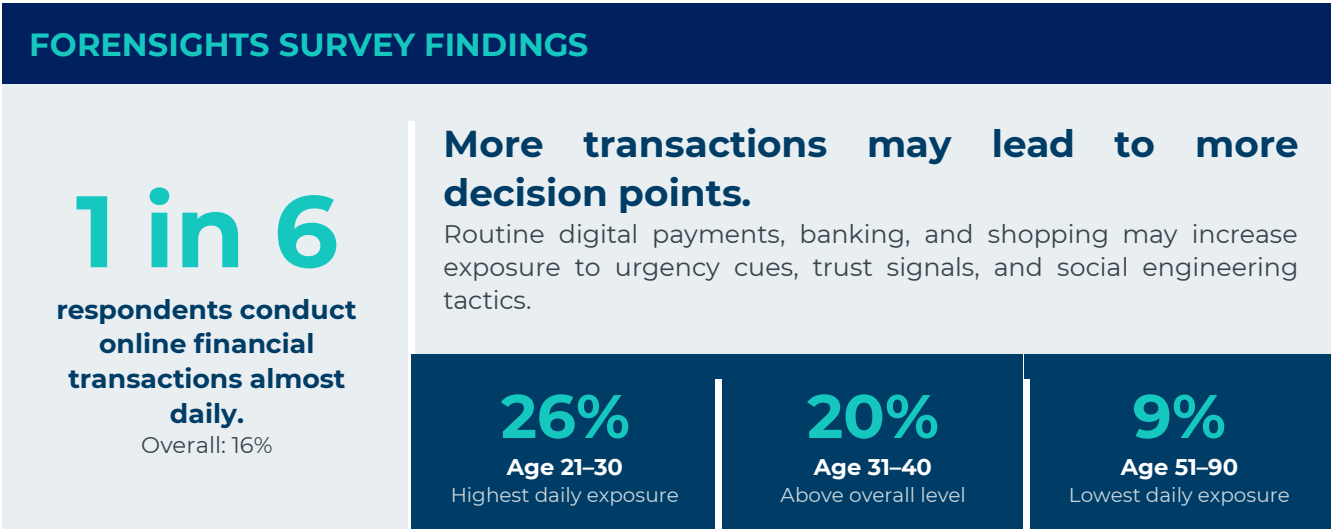


Whistine Chai · Founder & Principal Psychologist
Chen Yongjie · Psychologist

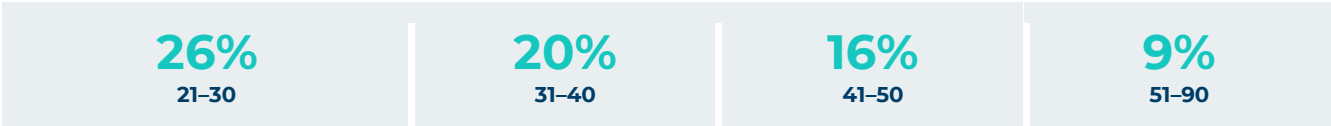
The Scam Landscape



What these signals: scam risk is not only technical; it is behavioural, fast-moving, and often triggered before reflective judgement catches up. In our study, we found that more transactions may lead to more decision points and higher behavioural risk.



Age-gradient snapshot: almost-daily online financial transactions decline from 26% among ages 21–30 to 9% among ages 51–90.



Question: How often do you conduct online financial transactions (e.g., online banking, e-wallet payments, online shopping)?

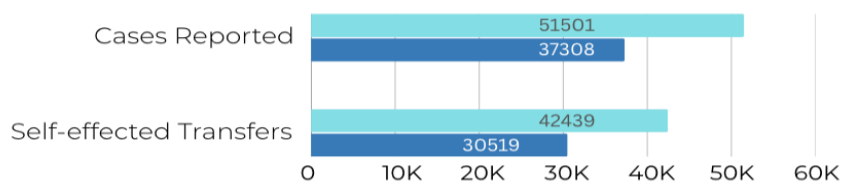
Sources: ForenSights Survey Findings (N = 809) (Nationally representative sample of Singapore residents)

Daily exposure plus daily urgency equals daily risk, and the data proves it.

From our study, 16% of respondents reported conducting online financial transactions almost daily. This exposure was most pronounced among younger adults, with 26% of those aged 21–30 reporting almost-daily transactions, followed by 20% among those aged 31–40. In the context of Singapore’s scam landscape, frequent digital transaction habits may create repeated decision points where urgency, trust cues, and social engineering tactics can be exploited.

Most Scam Losses are Self-Effectuated

Scam Landscape in Singapore



Self-Effectuated
Transfers in 2024



Self-Effectuated
Transfers in 2025

Sources: SPF Annual Scam & Cybercrime Brief 2025 (Feb 2026); SPF Annual Scam & Cybercrime Brief 2024 (Feb 2025).

In 2024, a total of 51,501 scam cases were reported, amounting to a loss of \$1.1 billion, hitting an all-time high. With local law enforcement efforts and cybersecurity measures stepping up within organisations, the Singapore Police Force recorded a decrease in scam cases to 37,308 with a reduced loss of \$913 million in 2025.

However, self-effectuated transfers (i.e., scammers who did not gain direct control of the victims' accounts but manipulated them into performing monetary transactions through deception and social engineering) remained unchanged at 82.4% in 2024 against 81.8%.

These numbers warrant our attention to shift our focus towards better understanding the psychological mechanisms driving our risk behavioural tendencies that are associated with increasing our susceptibility to socially engineered tactics and scam victimisation.

When 8 in 10 victims willingly transfer their own money, shouldn't we be asking **why instead of how they were deceived?**

THE PROBLEM

Urgency Bypasses Logic, and Psychology is the Real Vulnerability.

Prevalence of social engineering-driven fraud is alarming, as around half of the victims fell for scams within minutes (Global Anti-Scam Alliance, 2025). Such a phenomenon signifies a clear reflection of how an individual's risk of impulsive decision heightens under pressure. Amongst 64% of victims who fell prey to scams within a day, about 48% of them were victimised within minutes, and 13% reported that they acted too fast to recognise the deceit.

These data highlight that social engineering exploits psychological triggers (and not technical gaps) to drive irrational thoughts and rapid emotional responses.

Parallel to ForenSights' findings, we found risk behavioural tendencies as a significant predictor of scam risk and scam victimisation. Additionally, our study revealed that **5% of the participants reported a financial loss of SGD \$100,000 and above.**

"In the time it takes to read about the prevalence of victims falling for scams due to risk behavioural tendencies, someone just lost money to a scam."

ForenSights · Intelligence Brief Issue 04

FORENSIGHTS FINDINGS

Risk-taking Tendencies and Scam Susceptibility

DeLiema and colleagues (2020) conducted a profiling study on victims of investment fraud and found that individuals with stronger materialist values may tend to discount risk, making them more susceptible to scams. Complementing these quantitative findings, Wen et al. (2022) ran qualitative research to investigate the mental states of victims and scam compliance. They similarly found scam compliance was associated with risk-taking preferences, distorted risk perceptions, and cognitive biases, such as attribution bias. Together, these studies highlight how risky behavioural tendencies and biased decision-making may increase susceptibility to scams.

Similarly, in our study involving 809 participants, risk-taking tendency was a strong and statistically significant predictor of scam susceptibility, as measured through responses to simulated scam scenarios ($B = 0.610$, $SE = 0.106$, $z = 5.776$, $p < .001$). After controlling for demographic and behavioural factors, the odds ratio was 1.84 (95% CI [1.50, 2.26]). This indicates that **each one-unit increase in risk-taking tendency was associated with an approximately 84% increase in the odds of scam**

susceptibility. This finding highlights risk-taking tendencies as important behavioural indicator of scam vulnerability.

WHY IT HAPPENS: THE MECHANISM

Dual Processes: One Reflects, One Reacts.

In our minds, two systems run the show. One's the thinker, as it takes time to check and ensure the validity of the experience before deciding on the next course of action. The second system skips the thinking process and reacts to tone, pressure, or the hottest emotion at the moment.

"Your account will be locked."

"I need you to transfer this now."

"Boss said that this request should be processed immediately."

Such messages trigger the second system, where the brain fires before the first system has a chance to catch up.

Under the psychological lens, this mechanism linking risk behaviour tendencies to scam susceptibility is effectively explained by the dual-process model of cognition, such as the Elaboration Likelihood Model (ELM). Petty and Ciacoppo (1986) posit that human decision-making within the ELM operates via two distinct pathways: the central (reflective) route and the peripheral (reactive) route. The central route involves deliberate, effortful, and logical evaluation of information. In contrast, the peripheral route is fast, automatic, and heavily influenced by emotional cues and mental shortcuts (heuristics). Scammers utilise social engineering tactics to trigger the latter.

For instance, by creating a sense of urgency (*"Your account will be locked"*), they activate a scarcity heuristic, prompting a quick reaction without thoughtful analysis. By impersonating an authority figure like a CEO, they leverage the authority heuristic. Successful phishing emails often utilise consistency and reciprocity principles, which are highly effective in bypassing rational thought.

Individuals with strong risk-taking tendencies may be especially vulnerable to this reactive mode of thinking, as they are more willing to tolerate uncertainty and act on anticipated rewards without fully evaluating the potential risks.

Other Behavioural Risk Factors

RISKY BEHAVIOURAL FACTORS	HOW SCAMMERS EXPLOIT IT ELM perspective	OUTCOME
Impulsivity	Creates urgency, fear, or time pressure, reducing motivation and opportunity for central-route processing. Victims rely on peripheral cues such as urgency and authority.	Faster decisions with minimal verification.
Risk-taking	Frames the scam as a high-reward opportunity, increasing the attractiveness of peripheral reward cues over careful evaluation.	Greater willingness to proceed despite uncertainty.
Overconfidence	Encourages reliance on one's own judgement, reducing systematic scrutiny and perceived need for verification.	Lower suspicion, fewer verification behaviours, and increased susceptibility to sophisticated scams.
Desensitisation to scams	Repeated successful scam evasions may dull the brain's threat response. Scammers mimic familiar processes to trigger risky habits that bypass the central route.	Greater reliance on heuristics and reduced central-route engagement.
Acceptance of risky behavioural norm	Threat actors match normalised expectations, so the central route remains engaged but is hijacked by distorted norms.	Risky group norms rewrite the rules of normal behaviour and increase susceptibility.

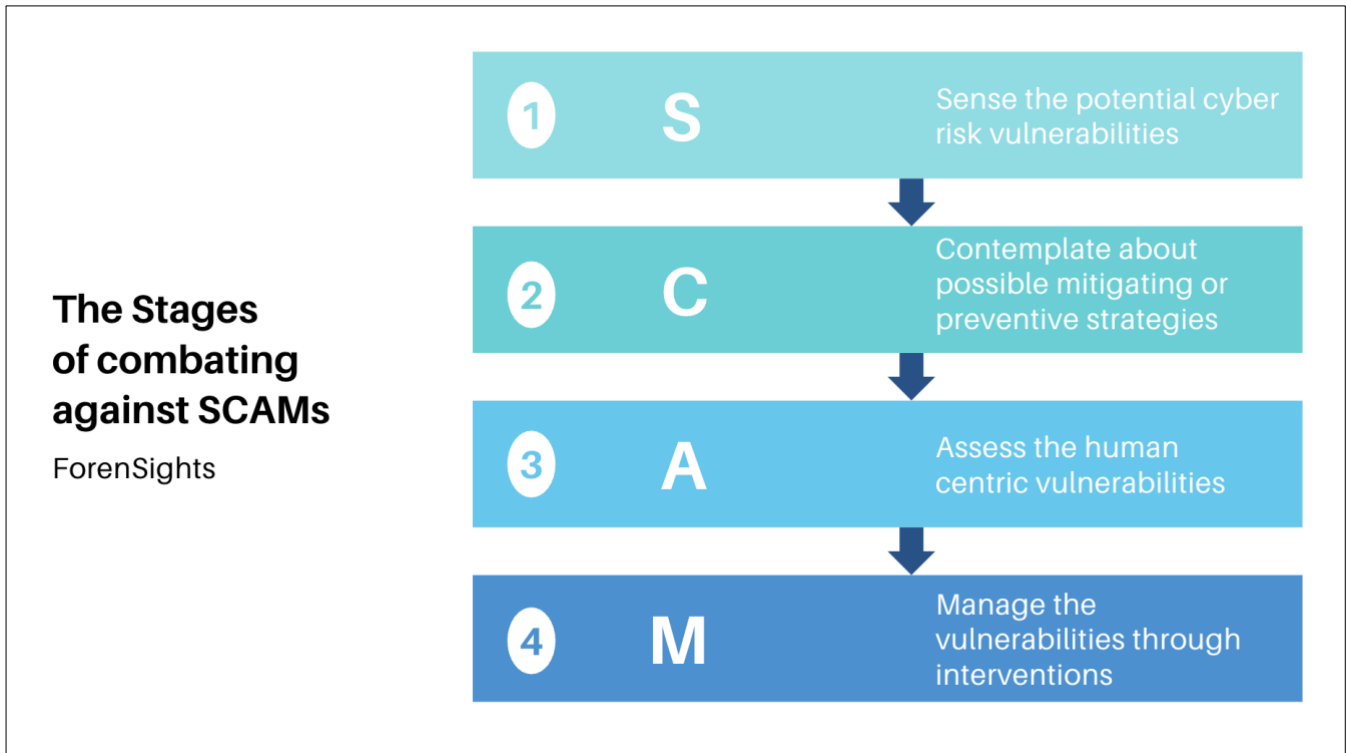
ORGANISATIONAL IMPLICATIONS

From Awareness to Behavioural Risk Management

Put together, organisations cannot address scam and social engineering risk through technical controls and generic training alone. When employees are exposed to urgency, authority cues, attractive rewards etc., their behavioural tendencies could determine whether they pause, verify or proceed.

Effective scam prevention requires organisations to move beyond asking whether employees recognise scams and begin measuring how they make decisions under pressure

and sense of urgency. Organisations should also incorporate behavioural indicators into their broader cyber-risk strategy.



Forensights' Application

Building on insights from behavioural sciences, ForenSights applies psychological principles to understand the human factors that contribute to cyber risk. This approach supports organisations to move beyond purely technical indicators by integrating human centric factors (e.g., bias, habits, perceptions) into cyber risk management.

PILLAR	OBJECTIVE
1. Measure Behavioural Risk	Identify the behavioural factors that increase susceptibility to scams and social engineering
2. Target the Behavioural Precursors of Risk	Design interventions that address the psychological processes preceding risky decisions, rather than relying solely on standardised awareness training.
3. Strengthen Organisational	Treat behavioural risk as a systemic issue, not solely an individual one. Leadership practices, workload, communication norms, and culture can reduce or amplify vulnerability.

PILLAR	OBJECTIVE
Systems and Norms	
4. Monitor Change and Adapt Interventions	Behavioural risk is dynamic across roles, departments, work conditions, and emerging scam tactics. Periodically assess whether interventions change actual behaviour.

To explore this topic further or learn more about our research on behavioural risk intelligence, visit www.forensights.com

ABOUT OUR RESEARCH

FORENSIGHTS — WHERE MIND MEETS DATA

Operationalising Human-centric Data in Strengthening Predictability towards Scam Susceptibility.

Extant literature of empirical studies on the differences between scam evaders (i.e. individuals who avoid falling for scams) and scam victims remains dearth. Through recognising this gap, ForenSights conducted two independent studies that aim to strengthen the empirical basis of how certain individual factors drive personnels to respond to social engineering tactics both in personal contexts and within organisational environments.

Our studies highlighted risky behavioural tendencies increasing the risk of individuals falling prey to scams, further validating the notion of ELM’s peripheral route as the breach for scammers to penetrate.

The key question, therefore, is how these human vulnerabilities can be measured in a structured, reliable, and operationally meaningful way.

If your organisation is exploring evidence-based approaches to understanding and managing human cyber risk, we'd be pleased to discuss how behavioural risk assessment can complement your existing cybersecurity strategy.

This is the fourth in a series of research-informed perspectives from ForenSights. We welcome your thoughts, questions, and perspectives on the findings presented. Please reach out if you would like to discuss further.

Global Anti-Scam Alliance. (2025). *Global State of Scams 2025 Report*. <https://gasa.org/knowledge-base/reports/global-state-of-scams-2025>

Singapore Police Force. (2026a). *Annual scams and cybercrime brief 2025*. <https://www.police.gov.sg/-/media/SPF/Advisories/Scams/Annual-Scam-and-Cybercrime-Brief-2025.pdf>

Singapore Police Force. (2026b). *Crime cases recorded, annual* [Data set]. SingStat Table Builder. <https://tablebuilder.singstat.gov.sg/table/TS/M891481>

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 19, pp. 123–205). Academic Press. [https://doi.org/10.1016/S0065-2601\(08\)60214-2](https://doi.org/10.1016/S0065-2601(08)60214-2)

Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental states: A key point in scam compliance and warning compliance in real life. *International Journal of Environmental Research and Public Health*, 19(14), Article 8294. <https://doi.org/10.3390/ijerph19148294>

ForenSights Pte. Ltd.
<https://forensights.com>

Behavioural Risk · Cyber Psychology · Risk Prediction
Organisational Resilience · Human Factors · Singapore

© 2026 ForenSights Pte. Ltd. All rights reserved.
No part of this publication may be reproduced in any form without the prior written permission of ForenSights Pte. Ltd. For permission or enquiries, please visit forensights.com