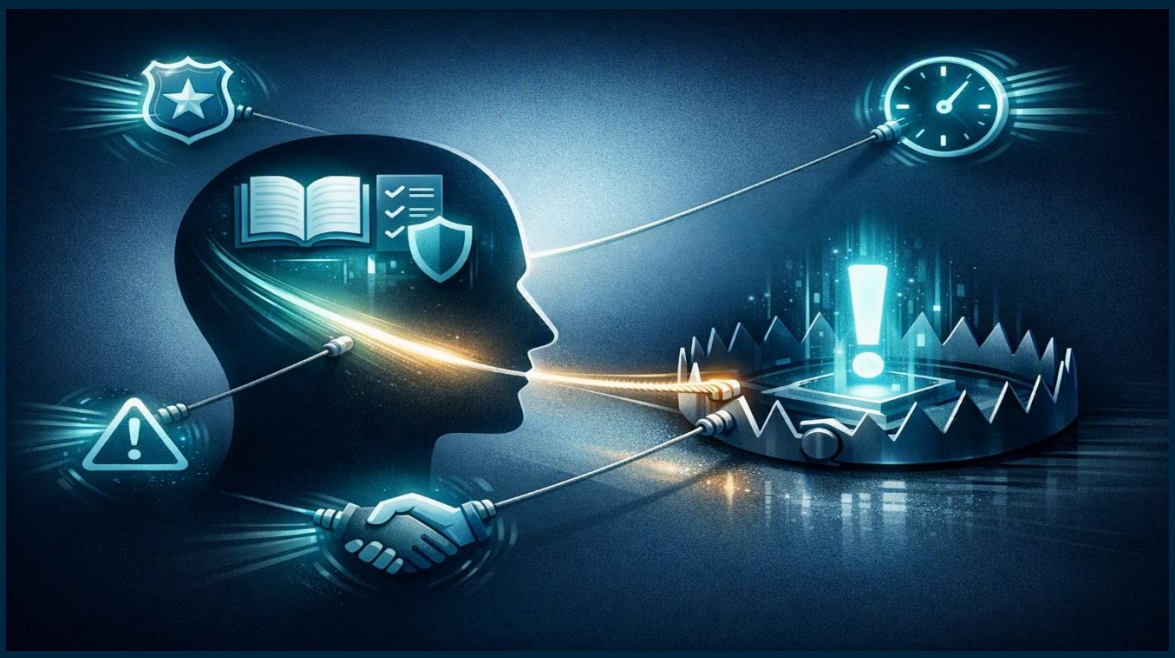
FORENSIGHTS INTELLIGENCE BRIEF
Issue 01 · June 2026

RESEARCH SERIES · HUMAN RISK & SOCIAL ENGINEERING

Why Knowledge Alone Does Not Protect Against Scams

In a landscape where scams have become the dominant form of crime, awareness training continues to be the default response. This brief examines why protection may fail not at the point of knowledge — but at the point of action.



Whistine Chai · Founder & Principal Psychologist
Leow Pei Hann · Research Associate

© 2026 ForenSights Pte. Ltd. All rights reserved.

37,308	81.8%	20,857
Scam cases recorded in Singapore in 2025	**Of 2025 scams were self-effected transfers — no breach required**	**Physical crime cases in the same period — scams consistently outnumbered physical crimes since 2022**

(Singapore Police Force, 2026a; Singapore Police Force, 2026b)

THE PROBLEM

Scams don't breach accounts. They bypass minds.

In 2025, 81.8% of scams reported in Singapore required no technical intrusion (Singapore Police Force, 2026a). No account was compromised. No system was breached. The victim transferred the money personally, guided by a scammer who had, in the preceding moments, displaced their capacity for rational evaluation.

"*Don't send money to strangers*" is near-universal knowledge. However, our knowledge fails at the moment it counts. The reason is not a gap in information. It is a gap between *knowing* a risk and *acting* on that knowledge under pressure.

> ***"Social engineering tactics thrive on deception that disrupt the cognitive pathways underlying rational thinking. "***
> ForenSights · Intelligence Brief Issue 01

Being informed raises confidence, but it does not reliably raise resistance. This distinction carries significant implications for how organisations design and evaluate their human risk programmes.

© 2026 ForenSights Pte. Ltd. All rights reserved.

Scams are now Singapore's dominant crime category.

Singapore Police Force. (2026). *Crime cases recorded, annual* [Data set]. SingStat Table Builder (Table M891481).

In 2025, the Singapore Police Force recorded 37,308 scam cases against 20,857 physical crime cases (Singapore Police Force, 2026b). Scams have outnumbered physical crime every year since 2022, while physical crime has remained broadly stable. This is not a temporary spike. It is a structural shift.

The distinction matters for prevention. Physical crime is done *to* a victim. A scam, on the other hand, is increasingly carried out *by* the victim unknowingly - through their own credentials, their own devices, and their own hands — under conditions engineered to make them feel necessary and urgent.

When the leading crime category is one the victim performs themselves, knowing the risk is clearly not the binding constraint. The question the becomes: what is?

© 2026 ForenSights Pte. Ltd. All rights reserved.

Different pressure levers. One predictable sequence.

When someone falls for a scam, it is less about what they know and more about how they react under the pressure (Lea et al., 2009). It rarely happens all at once. Instead, the pressure builds step by step, leaving victims to act on instinct, with little room left to think.

Authority

A caller presents credible institutional identity — a bank, a government agency, or police. Perceived legitimacy makes the victim more willing to comply, even before any request is made (Fischer et al., 2013).

Urgency

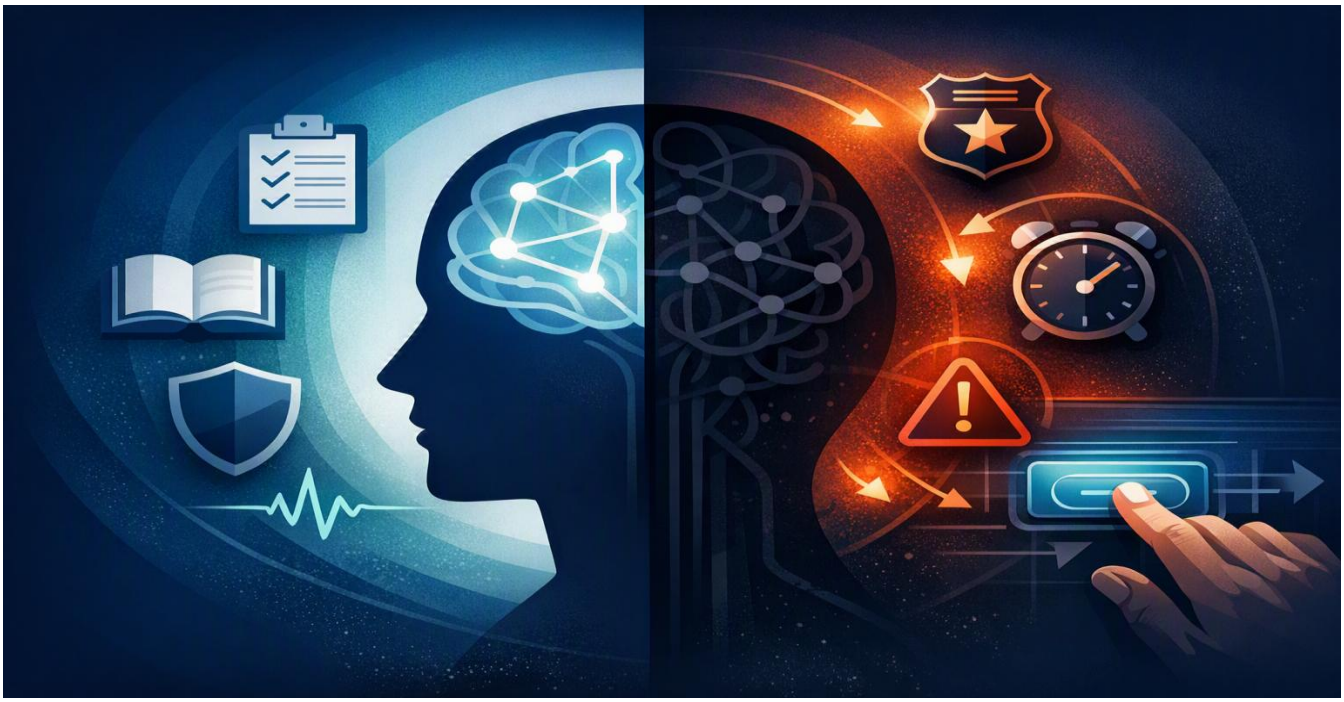
A deadline is introduced: an account about to be frozen, a fine due immediately. Time pressure prevents verification and forces reactive rather than deliberate decision-making (Williams et al., 2017).

Fear

Consequence framing activates threat response — arrest, financial loss, family harm. Under fear, the brain shifts from analytical processing to immediate threat mitigation (Fischer et al., 2013).

Affect Heuristic and Decision-Making Shifts

By the time the victim acts, they rely on raw emotional response rather than deliberate judgement (Skagerlund et al., 2020). What they know about scams rarely enters the decision. Knowledge is bypassed and not overridden.

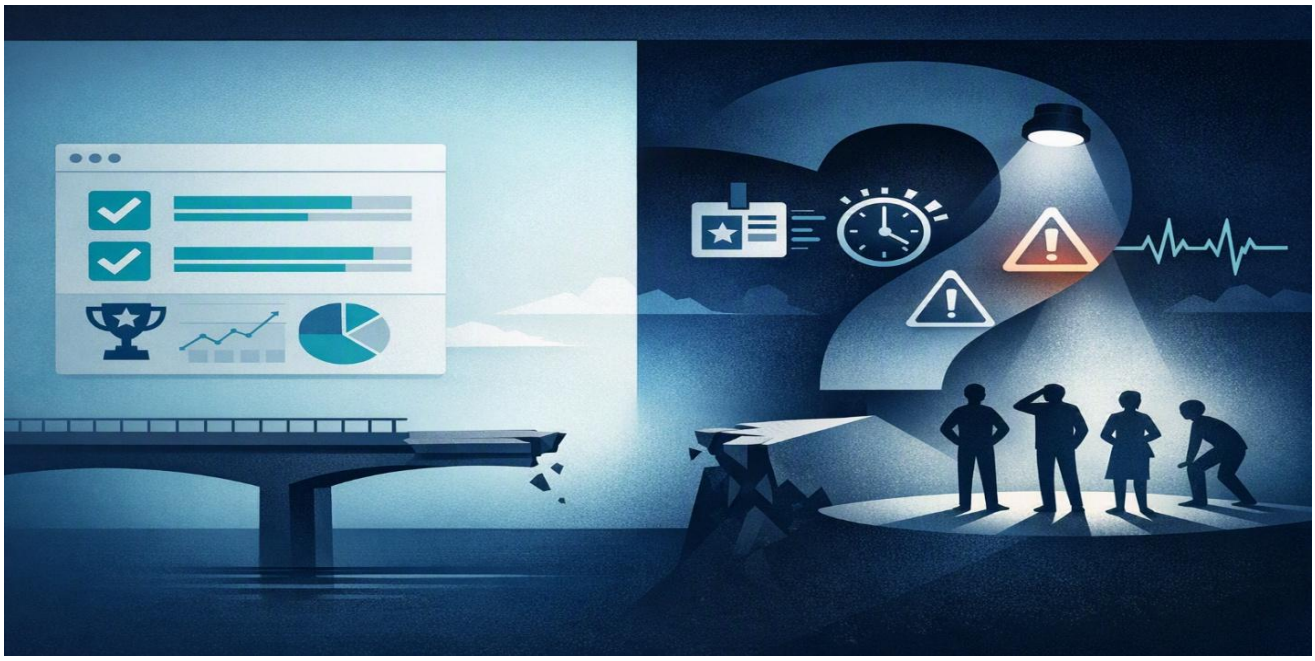


© 2026 ForenSights Pte. Ltd. All rights reserved.

There is a counterintuitive finding reported in the literature: knowing more about a domain may *increase* vulnerability rather than reduce it. When people have above-average knowledge, it is possible that these individuals may tend to get overconfident in their ability to spot a scam. Examples of optimism bias were documented in both phishing (Owen et al., 2024) and investment-fraud contexts (Xiao et al., 2022). In fact, many victims sensed something was wrong, but nevertheless complied, trusting their own judgements over the warning signals (Lea et al., 2009).

ORGANISATIONAL IMPLICATIONS

The question your programme is not answering.



For decision-makers, the most critical question is not "H*ave our people been trained*?" It is: "H*ow do our people behave under pressure they did not expect*?"

Completion rates and quiz scores measure recall in calm conditions. However, they may not measure resistance at the moment of an urgent, authoritative, emotionally charged request.

THE DIAGNOSTIC QUESTION

The capability that actually matters — whether people can hold up under real pressure — is what most programmes assume rather than measure. So, the question for any organisation with a human risk programme is:

Do we actually measure how our people behave under pressure — or is that capability simply assumed?

© 2026 ForenSights Pte. Ltd. All rights reserved.

ABOUT OUR RESEARCH

FORENSIGHTS — WHERE MIND MEETS DATA

Measuring the gap between knowing and doing.

ForenSights works in the gap between knowing and doing. Across two separate studies conducted by ForenSights (each with over 800 participants), we have assessed the individual factors and environmental conditions that shape how people respond to social engineering tactics in a corporate environment.

This is the first in a series of research-informed perspectives from ForenSights. Subsequent issues will present findings on susceptibility patterns, the conditions that amplify and attenuate risk, and what meaningful human risk measurement looks like in practice.

1,600+ participants across two independent studies

This is the first 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.

REFERENCES

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology, 43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Lea, S. E. G., Fischer, P., & Evans, K. M. (2009). *The psychology of scams: Provoking and committing errors of judgement* (OFT1070). Office of Fair Trading.

Owen, M., Flowerday, S. V., & van der Schyff, K. (2024). Optimism bias in susceptibility to phishing attacks: An empirical study. *Information and Computer Security, 32*(5), 656–675. https://doi.org/10.1108/ICS-02-2023-0023

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

Skagerlund, K., Forsblad, M., Slovic, P., & Västfjäll, D. (2020). The affect heuristic and risk perception: Stability across elicitation methods and individual cognitive abilities. *Frontiers in Psychology, 11*, Article 970. https://doi.org/10.3389/fpsyg.2020.00970

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Xiao, X., Li, X., & Zhou, Y. (2022). Financial literacy overconfidence and investment fraud victimization. *Economics Letters, 212*, Article 110308. https://doi.org/10.1016/j.econlet.2022.110308

© 2026 ForenSights Pte. Ltd. All rights reserved.

© 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 permissions or enquiries, please visit forensights.com

© 2026 ForenSights Pte. Ltd. All rights reserved.