



RESEARCH SERIES · HUMAN RISK & SOCIAL ENGINEERING

Your Position in an Organisation Shapes the Scams That Target You

Your job title may be doing more than defining your role. ForenSights research data shows it is also shaping the scam/fraud landscape you face, and whether you even recognise that you have been targeted.

Whistine Chai · Founder & Principal Psychologist

Ethan Phua · Research Associate



BACKGROUND

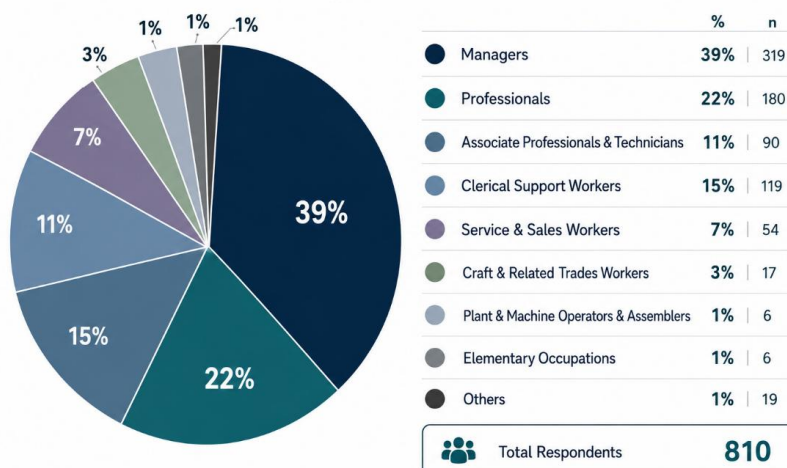
ForenSights recently conducted two studies involving over 1,600 respondents on scam and fraud risk in Singapore. The first study involved 810 working adults across Singapore, representing diverse industries, organisational levels, occupations and sectors. The participants ranged from junior employees to senior leaders across public, private and non-profit organisations. The study was designed to examine patterns associated with behavioural cyber risk, scam susceptibility and organisational exposure. This diversity allows ForenSights to examine how scam and fraud risks may vary across different organisational contexts, job functions and seniority of roles. The current article is based on this study.

Scams no longer target organisations via one-size-fits-all approaches. Our findings suggest that different organisational positions are exposed to different scam types.

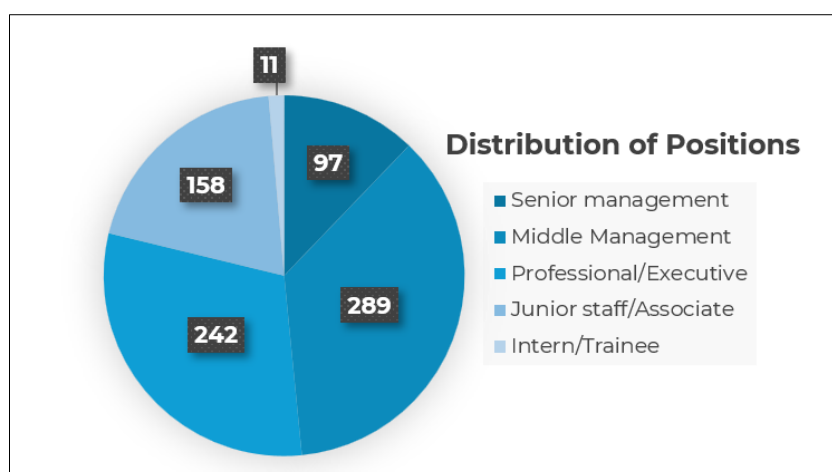
Traditional one-size-fits-all scam/fraud awareness training is therefore also **structurally mis-calibrated** for today's fraud strategies.

ForenSights survey data shows statistically significant associations between organisational position and a variety of scam-related outcomes.

Distribution of Occupations



*Managers include directors, senior managers, chief executives, and business owners, consistent with the occupational classification used in this study.



Notably, significant associations emerged between organisational positions and the following:

- Diverse types of scam/fraud faced.
- Scam/fraud uncertainty
- Scam/fraud behavioural risk patterns.

WHAT WE FOUND

Three findings. One clear signal.

1. Senior positions show vulnerability to specific scam types.

Across various industries and sectors, employees occupying higher organisational positions showed a small but statistically significant positive association with payment redirection fraud ($r = .10, p = .005$) and credential harvesting ($r = .14, p < .001$).

Payment redirection fraud refers to scams in which attackers impersonate legitimate vendors, suppliers, and business partners to deceive employees into transferring funds to fraudulent accounts. **Credential harvesting** refers to attempts to steal authentication information through social engineering techniques such as phishing emails.

While the associations were modest, our findings suggest that higher-ranking employees may face a disproportionately greater risk of exposure to these scam types compared to employees in less senior roles. This points to more specific scam targeting strategies. One possible explanation is that protective heuristics accumulated from years of experience may become insufficient in the face of more modern and sophisticated tactics.

"Experience-built heuristics may create blind spots rather than protection."

Sophisticated scams are designed precisely to work around the mental shortcuts that competence produces."

ForenSights · Intelligence Brief Issue 03

2. Junior positions are less likely to recognise being targeted

In contrast, junior positions within an organisational hierarchy were found to be positively associated with scam uncertainty ($r = .13, p < .001$). Without as much professional working experience, junior employees are more likely to report uncertainty about whether they had been targeted.

This is a distinct vulnerability from that faced by senior employees. It is not about failing for a sophisticated tactic but about lacking the contextual reference points to identify that something suspicious occurred at all.

Not recognising a threat is not the same as ignoring one. For more junior employees, scam uncertainty means the incident may never be reported because it was never identified as one.

3. Junior positions exhibit lower organisational protective factors

Organisation position was negatively associated with reporting culture ($r = .08, p = .032$) and organisational risk perception ($r = .11, p = .002$). This implies that as organisational seniority decreased, reporting culture and organisation risk perception also decreased. Although these associations were small, they suggest that employees in junior positions may possess fewer organisational protective factors against scams and fraud.

Several explanations may account for this pattern. Lower reporting culture among junior employees may reflect organisational environments characterised by stronger hierarchical structures that reward following directions from superiors over employees taking their own initiative.

Different accountability expectations across the hierarchy may also discourage more junior employees from reporting suspicious activities or raising concerns.

At the same time, a lack of experience can dampen the ability to recognise the relevant risks within a specific industry or organisational context.

IMPLICATIONS FOR ORGANISATIONS

The same hierarchy that structures work also structures risk.

01 Scam targeting strategies work differently across organisational positions.

Even where more senior positions have accumulated industry experience, certain scam types are designed to work around the blind spots of well-developed heuristics. **Seniority may not be a reliable proxy for scam resistance.**

02 Recognition of being scammed varies across the hierarchy.

Lack of experience at junior levels reduces the ability to recognise scams in real-world organisational contexts. **Uncertainty itself could become a risk when it prevents reporting.**

03 Authority pressures can suppress protective behavioural patterns.

Despite knowing the indicators of fraud, hierarchical pressures can deter employees from flagging concerns, especially when the threat is ambiguous. **Reporting culture is therefore a behavioural variable that organisations can actively shape.**



KEY TAKEAWAYS

Behavioural risk is structural, not just individual.

Together, these findings suggest that behavioural systems are inherent to cyber and fraud risk, including seemingly unrelated aspects such as organisational hierarchy and an employee's position within it.

One-size-fits-all scam awareness training is therefore not enough. Vulnerability to scams goes beyond awareness. Organisational influences and one's role in the hierarchy create psychological and behavioural nuances that can increase exposure in ways that generic training does not address.

Approaches to scam countermeasures can shift from generating awareness to addressing the specific behavioural dynamics that emerge across various positions in an organisation.

FORENSIGHTS — WHERE MIND MEETS DATA

Identifying and solving behavioural risk at the organisational level.

Technological approaches to cybersecurity often overlook vulnerabilities at the level of the human user. ForenSights research addresses this gap by identifying organisational behavioural risk patterns that existing security frameworks may not capture.

Our ongoing work in understanding the full suite of behavioural vulnerabilities to scams and fraud aims to augment present-day security safeguards, by unravelling and solving what underlies human errors.

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

ForenSights Pte. Ltd.

[Http://forensights.com](http://forensights.com)

Behavioural Risk · Cyber Psychology · Risk Prevention
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. The findings, research methodology, and frameworks referenced herein are protected. For permission or enquiries, visit forensights.com.