

TECH FOR GOOD INSTITUTE

in partnership with

center for inclusive growth

Report — November 2026

Realising Scam Resilience in Southeast Asia-6

Table of Contents

About the Study 04

Authors 05

Acknowledgements 05

Funding Statement 05

About Tech for Good Institute 06

Disclaimer 06

Executive Summary 07

1. Introduction 09

1.1 The Growing Need for Scam Resilience 09

1.2 Report Structure 10

1.3 Terms and Concepts 11

1.4 Methodology 12

1.5 Scope and Limitations 15

2. The State of Scam Resilience in Southeast Asia 16

2.1 Protect: The Exposure Risk 17

2.2 Identify and Detect: The Confidence Trap 20

2.3 Respond & Recover: The Action Gap 25

2.4 Adapt: The Trust Build 29

3. Policy Recommendations 33

3.1 Protect Universally 34
3.2 Verify Routinely 35
3.3 Respond Collectively 36
3.4 Trust Confidently 37
3.5 Translating Recommendations into Initiatives 38
Appendix A. Spot-the-Scam Scorecard 46
Appendix B. Country Highlights 48
B.1 Indonesia 49
B.2 Malaysia 50
B.3 Philippines 51
B.4 Singapore 52
B.5 Thailand 53
B.6 Vietnam 54
Appendix C. Supplementary Exhibits 55
C.1 Protect: The Exposure Risk 56
C.2 Identify and Detect: The Confidence Trap 58
C.3 Respond and Recover: The Action Gap 59
Endnotes and References 60

About the Study

In 2025, the Tech for Good Institute (TFGI) extensively studied scams and fraud in Southeast Asia:

- *Strengthening Scam Readiness in Singapore*, done in partnership with Bamboo Builders with the support of Google.org
- *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of-Society Approach*, done in partnership with Bamboo Builders with the support of Google.org; and
- *Building Resilience Against Digitally-Enabled Scams in ASEAN,* a policy paper created in collaboration with the ASEAN Think Tank Summit (ATTS).

The series of reports surfaced the growing speed, scale and sophistication of the region's digitally-enabled scams and fraud landscape.

This report intentionally builds on these findings to examine the state of scam resilience in the region in 2026, focusing on six countries: Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam. The approach to data collection is primarily quantitative, utilising a survey distributed through online panels in the countries of focus, with a target sample of 1,000 respondents aged 18 to 70 per country. The total study sample is 6,000 respondents in Southeast Asia.

The report is structured as follows:

- Chapter 1 outlines the problem statement, situating the severity of the challenge presented by the evolving scam landscape to the region's digital economy aspirations. This provides readers with the context on why and how the study was conducted.
- Chapter 2 presents the report findings through the lens of the scam intervention pillars (Protect, Identify and Detect, Respond and Recover, and Adapt). It discusses the factors that drive scam exposure, the relationship between confidence level and actual skills in scam detection, the region's level of scam response readiness, and the impact of scams on trust and digital participation. Readers will be able to find here the key insights surfaced from the survey.
- Chapter 3 provides an overview of policy implications based on the report findings and an initial set of recommendations to address them. It selectively illustrates how recommendations can be translated into specific interventions, and further, how different stakeholder groups can collaborate on each intervention. This gives readers a view of how they might utilise the insights from the report to tailor solutions for their unique context.

This report is intended to be a resource and an invitation to dialogue. It provides evidence to guide future policies, initiatives and partnerships in ensuring a safe and secure digital landscape. The Tech for Good Institute remains open to feedback, insights and opportunities to collaborate. To share your thoughts, please contact info@techforgoodinstitute.org.

Authors

Keith Detros is a Programme Manager at the Tech for Good Institute, where he handles policy studies on digital economy, tech policy, and cyber resilience. He leverages nearly 15 years of experience in government affairs and evidence-based policy research.

Vicah Villanueva is a Programme Associate for the Tech for Good Institute, where she leads research and engages stakeholders on inclusive, empowered and sustainable digital society development in Southeast Asia.

* For citation purposes, this report should be attributed to the Tech for Good Institute.

Suggested Citation

Tech for Good Institute (TFGI). 2026. Realising Scam Resilience in Southeast Asia-6.

Acknowledgements

The Tech for Good Institute (TFGI) would like to thank Blackbox Research for their support in this study.

We would also like to extend our gratitude to the TFGI Programmes team for their support in the review process. Special thanks to Jamie Ko, Fairoz Ahmad, Basilio Claudio, and Nurin A'liyah Binte Mohammed Iskandar.

TFGI is also grateful to the Mastercard Center for Inclusive Growth and Grab for supporting TFGI's mission of leveraging the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia. Funders do not determine research findings nor the insights and recommendations of research.

Funding Statement

This study was supported by Mastercard Center for Inclusive Growth (CFIG) and Grab for TFGI's mission of leveraging the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia. Funders do not determine research findings nor the insights and recommendations of research.

About Tech for Good Institute

The Tech for Good Institute (TFGI) is a non-profit policy research institute working to advance the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia (SEA).

With a population twice the size of the US and having strong demographics, SEA's digital economy is evolving rapidly. At the same time, the region's trajectory is unique, shaped by its diverse cultural, social, political and economic contexts. TFGI serves as a platform for research, conversations and collaborations focused on SEA, while staying connected to the rest of the world. Our work is centred on issues at the intersection of technology, society and the economy, and is intrinsically linked to the region's development. We seek to understand and inform policy with rigour, balance and perspective by using research, effective outreach and evidence-based recommendations.

TFGI works in partnership with the Mastercard Center for Inclusive Growth and Grab, to advance the vision of a thriving and innovative SEA for all. We welcome opportunities for partnership and support, financial or in-kind, from organisations and individuals committed to fostering responsible innovation and digital progress for sustainable growth in the region.

More information about the Institute can be accessed at www.techforgoodinstitute.org

Disclaimer

The information in this paper is provided on an “as is” basis. This paper is not to be considered as a recommendation for investments in any industry. This document is produced by the Tech for Good Institute and has been prepared solely for information purposes over a limited time period to provide a perspective on the region. The Institute and any of its affiliates, or any third party involved make no representation or warranty, either expressed or implied, as to the accuracy or completeness of the information in the paper, and no responsibility or liability whatsoever is accepted by any person of the Institute, its affiliates and its respective officers, employees or agents.

Copyright © 2026 by the Tech for Good Institute. All rights reserved.

Permission is granted for reproduction of this file or its contents, with attribution to the Tech for Good Institute.

For citation purposes, this report should be attributed to the Tech for Good Institute.

Executive Summary

Scams are increasingly prevalent in Southeast Asia. Data from this survey, which covers Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam, notes that six in ten respondents (60%) have encountered a scam in the past year. In addition, 38% of Southeast Asians have lost money, other valuables, or personal information due to scams. In the region, the most common are prize scams, job scams, and phishing. However, respondents find impersonation of authorities and fake bank notifications as the most concerning forms of scams.

Southeast Asia's journey toward achieving scam resilience presents both gaps and opportunities. From examining user experiences throughout the scam lifecycle, several interconnected themes emerge. Each stage offers a window, from exposure to recovery, into how Southeast Asians behave at that point in an attempt, and identifies the areas where resilience breaks down.

- **The Exposure Risk.** Scam exposure across Southeast Asia is widespread and defies conventional assumptions regarding vulnerability. Rather than being confined to a specific demographic, exposure is more broadly distributed than originally believed. For instance, 65% of respondents aged 18 to 34 and 62% of employed respondents report encountering a suspected scam. These are significantly higher rates than those observed among older (44%) or unemployed groups (49%). The nature of digital participation appears to play a role in the degree of exposure and likelihood of victimisation.
- **The Confidence Trap.** A persistent gap exists between how confident people feel in detecting scams and their demonstrated skills. Only 42% of respondents express confidence in their ability to detect a scam, yet actual detection performance is considerably stronger, with consumers correctly identifying scams 71% of the time on average. This disconnect gives rise to four personas that characterise the region's diverse approaches to scam detection: Resilient Realists (55%), who balance high confidence with high skills; Overconfident Vulnerable (29%), whose skills are not as high as their confidence; Cautious Capable (10%), who are more skilled than they are confident; and the Underprepared (6%), who exhibit both low confidence and skills. Additionally, Southeast Asia's strong overall scam recognition belies susceptibility to certain kinds of scams. Detection accuracy, for example, falls to as low as 60% for sophisticated tactics such as authority impersonation. Notably, neither experience nor confidence are reliable predictors for scam detection skills.

- **The Action Gap.** Even when scams are correctly identified, the region's ability to respond and recover remains limited. Majority of Southeast Asia is moderately scam-ready (61%), but only 53% clearly know where to report an incident. There is also a tendency for repeated victimisation due to taking unsafe actions, such as victims contacting the scammer to ask for their money back (13%). In the aftermath, users continue to be affected by the encounter, leading to changed digital behaviour due to concerns about scams. Victim recovery is further constrained by a tension between empathy in principle and blame in practice: while 78% agree that victims should be able to report without embarrassment, 48% still view victims as careless, greedy, or at fault.
- **The Trust Build.** Restoring trust after a scam is central to sustaining digital participation. Only 11% of respondents say they would not significantly limit their use of digital services because of scams. This means that for the majority, reduced participation is a real and present risk if scam harm goes unaddressed. Law enforcement (54%) and government agencies (53%) are the most trusted to help people respond to scams, consistent with users' instinct to contact their bank or the police once a scam has succeeded. Beyond this, strengthening security measures is key to winning back trust, though a small proportion of users say that trust can never be restored once lost.

Achieving scam resilience requires enhancing trust infrastructure throughout the scam lifecycle. Protecting users universally demands an inclusive, culturally aware scam strategy. Lifelong, scenario-based scam training pathways enable users to verify digital interactions routinely and critically. Closing the action gap requires a unified, well-rehearsed response playbook paired with transparent, blame-free victim support mechanisms. Ultimately, sustaining trust is facilitated by developing adaptive capacity to evolve alongside the scam landscape. This relies on a whole-of-society approach, where authorities, businesses, civil society, local communities, and end-users actively work together for resilience against scams in the region.